Université de Montréal

Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée

Par
Julie M. Gauthier

Centre de recherche en droit public
Faculté de Droit

Mémoire présenté à la Faculté de Droit
en vue de l'obtention du grade de Maîtrise (L.L.M.)
Droit des technologies de l'information

Avril, 2014

Résumé

La biométrie, appliquée dans un contexte de traitement automatisé des données et de reconnaissance des identités, fait partie de ces technologies nouvelles dont la complexité d'utilisation fait émerger de nouveaux enjeux et où ses effets à long terme sont incalculables. L'envergure des risques suscite des questionnements dont il est essentiel de trouver les réponses. On justifie le recours à cette technologie dans le but d'apporter plus de sécurité, mais, vient-elle vraiment apporter plus de protection dans le contexte actuel? En outre, le régime législatif québécois est-il suffisant pour encadrer tous les risques qu'elle génère?

Les technologies biométriques sont flexibles en ce sens qu'elles permettent de saisir une multitude de caractéristiques biométriques et offrent aux utilisateurs plusieurs modalités de fonctionnement. Par exemple, on peut l'utiliser pour l'identification tout comme pour l'authentification. Bien que la différence entre les deux concepts puisse être difficile à saisir, nous verrons qu'ils auront des répercussions différentes sur nos droits et ne comporteront pas les mêmes risques.

Par ailleurs, le droit fondamental qui sera le plus touché par l'utilisation de la biométrie sera évidemment le droit à la vie privée. Encore non bien compris, le droit à la vie privée est complexe et son application est difficile dans le contexte des nouvelles technologies. La circulation des données biométriques, la surveillance accrue, le détournement d'usage et l'usurpation d'identité figurent au tableau des risques connus de la biométrie. De plus, nous verrons que son utilisation pourra avoir des conséquences sur d'autres droits fondamentaux, selon la manière dont le système est employé.

Les tests de nécessité du projet et de proportionnalité de l'atteinte à nos droits seront les éléments clés pour évaluer la conformité d'un système biométrique. Ensuite, le succès de la technologie dépendra des mesures de sécurité mises en place pour assurer la protection des données biométriques, leur intégrité et leur accès, une fois la légitimité du système établie.

Mots-clés : Biométrie, donnée biométrique, renseignement personnel, sécurité, nouvelles technologies, vie privée.

Abstract

Biometric technology, applied in a context of automated data processing and recognition of identity, is one of those new technologies whose complexity of use increase continuously and where the long-term effects are undefined. The risks are real and questions abound. For example, do biometrics really bring more security in the current context and is the Quebec legislative framework sufficient to regulate all the risks it generates?

Biometric technology is flexible in that it enables to capture several types of biometric traits and provides users with various modalities of use. For example, it can be used for identification and authentication. Although the difference between the two modes can be difficult to understand, they have different impacts on our rights and do not involve the same risks.

Among the human rights affected by the use of biometrics, the most important is the right to privacy. Still not well understood, the right to privacy is complex and difficult to apply in this new technological context. Circulation of biometric data and increased surveillance, function creep and identity theft are some examples of the known risks of biometric technologies. More, use of biometrics may also affect other fundamental rights, depending on how it is used.

Proportionality and necessity tests of the project will be key in the analysis of the legal conformity. Then, the success of the technology will depend on the security measures put in place to secure biometric data once the legitimacy of the system is established.

Keywords : Biometrics, biometric information, personal information, information security, new technologies, privacy.

Table des matières

Liste des sigles et abréviations

C.c.Q.	Code civil du Québec
CAI	Commission d'accès à l'information
CNCDH	Commission nationale consultative des droits de l'homme
CNIL	Commission nationale Informatique et Libertés
CPVPC	Commissariat à la protection de la vie privée du Canada
FOIP	Freedom of Information and Protection of Privacy Act
IPC	Office of the Information and Privacy Commissioner, Ontario
LCCJTI	Loi concernant le cadre juridique des technologies de l'information
LPRP	Loi sur la protection des renseignements personnels
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques,
LPRPSP	Loi sur la protection des renseignements personnels et des documents électroniques
LSAC	Law School Admission Council
OQLF	Office québécois de la langue française
TWIC	Transportation worker identification credential
US VISIT	Visitor and immigrant status indicator technology

Remerciements

J'ai eu la chance de travailler avec les meilleurs, ceux sur qui j'ai pu m'inspirer tout au long de mes études de maîtrise. Je remercie tout d'abord mon directeur de recherche, le professeur Nicolas Vermeys, qui a su me montrer les subtilités du droit de la sécurité de l'information et avec qui j'ai travaillé sur des mandats de recherche pendant presque un an. Je remercie également le professeur Vincent Gautrais pour m'avoir donné la chance de participer à ce beau projet que fut la création du site Lccjti.ca, dédié à la compréhension de la *Loi concernant le cadre juridique des technologies de l'information*. Je me considère également privilégiée d'avoir participé aux activités du Laboratoire de cyberjustice et d'avoir côtoyé toutes ces personnes compétentes et ambitieuses. Je sors grandie de mon passage au C.R.D.P. et très heureuse d'avoir complété cette grande étape, celle de la rédaction de mon mémoire.

Introduction

Utilisée depuis longtemps, la biométrie est un moyen d'identifier les individus en se servant d'une ou de plusieurs caractéristique(s) corporelle(s) ou comportementale(s)[1]. Autrefois, c'est en identifiant les suspects à l'aide de leurs empreintes digitales que l'on se servait principalement de la biométrie. Depuis qu'elle est couplée aux nouvelles technologies, on assiste à un élargissement des domaines dans lesquels elle est appliquée[2]. Par exemple, elle est de plus en plus utilisée pour contrôler les accès sur les lieux de travail et lors des contrôles aux frontières étatiques. Au Canada, les programmes NEXUS et CANPASS proposent de scanner votre iris afin d'accélérer le processus de passage aux frontières canadiennes et américaines. Tous les nouveaux passeports canadiens délivrés par le gouvernement sont d'ailleurs des passeports électroniques munis d'une puce contenant les renseignements personnels et la photo de l'utilisateur, laquelle est vouée à la reconnaissance faciale[3].

Citoyenneté et Immigration Canada entendent d'ailleurs utiliser les caractéristiques biométriques de tous les non-canadiens entrant au pays afin de traiter leurs dossiers[4]. Administré conjointement par l'Agence des services frontaliers et la Gendarmerie Royale du Canada, le programme demande à ce que les requérants d'un visa de visiteur, d'un permis d'études ou d'un permis de travail fournissent les empreintes de leurs dix doigts et leur photographie avant d'arriver au Canada. Notons que le projet est actuellement en cours

---

1 En Chine, l'utilisation des empreintes en guise de signature était fréquente. Voir : Max CHASSÉ, « La Biométrie au Québec : les enjeux », Commission d'accès à l'information du Québec, juillet 2002, p.4 et Guillaume DESGENS-PASANAU et Éric FREYSSINET, « L'identité à l'ère numérique », Éditions Dalloz, 2009, p. 16. Note : La biométrie peut aussi servir à des fins médicales, tel que nous le verrons à la section 1.1 de la présente partie.

2 Christian CABAL, député, « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », Office parlementaire d'évaluation des choix scientifiques et technologiques, France, 2003, p. 62.

3 Voir PASSEPORT CANADA, « Passeport électronique », en ligne : <http://www.ppt.gc.ca/eppt/about.aspx?lang=fra>.

4 CITOYENNETÉ ET IMMIGRATION CANADA, « Document d'information, Le Canada adopte la technologie biométrique », <http://www.cic.gc.ca/francais/ministere/media/documents-info/2009/2009-06-18.asp>.

d'analyse, notamment en ce qui a trait aux conséquences relatives à la vie privée et à la protection des renseignements personnels[5].

Ainsi, les nouvelles techniques automatisées de contrôle des identités suscitent d'importants questionnements. La biométrie s'inscrit dans un contexte où les évènements du 11 septembre 2001 ont occasionné des resserrements au niveau de la sécurité et, ainsi, accéléré la sécurisation des frontières[6]. En effet, la biométrie a été proposée comme une solution, considérée alors comme « l'un des instruments les plus prometteurs de la lutte anti-terroriste contemporaine »[7]. Plusieurs pays de l'Union européenne se sont d'ailleurs dotés de passeports biométriques sous la pression des États-Unis, à la suite de l'adoption de la USA PATRIOT Act[8] en octobre 2001[9]. La biométrie permettrait aujourd'hui ce que

> « les mécanismes traditionnels de contrôle à la frontière rendaient impossible, à savoir une anticipation du risque en amont de la frontière. En raccordant des données biométriques à des banques de données informatiques, l'État se donne ainsi les moyens de déceler des groupes d'individus indésirables avant qu'ils n'atteignent matériellement la frontière »[10].

En plus des hostilités supranationales, l'espionnage et les fraudes figurent parmi les autres causes favorisant un besoin croissant de sécurité et le développement de ces technologies. Tel que le mentionne Christian Cabal, la biométrie serait un instrument efficace de lutte contre la fraude[11] et un outil fort de protection des renseignements personnels[12], en

---

5 *Id*.

6 Voir : Xavier CRETTIEZ et Pierre PIAZZA, « Du papier à la biométrie : identifier les individus », *Presses de la Fondation nationale des sciences politiques*, Paris, 2006, p. 12.

7 Michaël FOESSEL & Antoine GARAPON, « Biométrie : les nouvelles formes de l'identité », *Esprit*, 327, août-septembre 2006.

8 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (« USA PATRIOT Act »)

9 Voir Xavier CRETTIEZ et Pierre PIAZZA, *préc*.. note 6, p. 12.

10 Michaël FOESSEL & Antoine GARAPON, *préc*., note 7, p. 5.

11 Christian CABAL, « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », *préc*., note 2, p. 46-51.

12 *Id*., p.57.

limitant les risques d'usurpation d'identité et l'accès aux données sensibles[13]. En outre, cette « hyper-technologisation serait fortement poussée par certaines entreprises qui ont développé des technologies diverses en matière de défense, d'aérospatial ou de génie génétique, et qui n'ont guère de débouchés à la hauteur des investissements »[14]. Selon certains auteurs, cette montée en puissance de sociétés proposant ce type de savoir-faire, au début des années 2000, ferait suite à « la reconversion de programmes engagés lors de l'initiative de défense stratégique de Ronald Reagan »[15]. À court d'ennemi soviétiques, ces sociétés se seraient rabattues sur une surveillance plus individualisée des personnes passant les frontières, sur la biométrie ainsi que sur l'électronique de prévision[16].

Dans le secteur privé, les employeurs se servent de plus en plus de la biométrie pour contrôler les horaires de travail. L'entreprise Natural Security a d'ailleurs récemment testé en France le paiement biométrique au moyen des empreintes et, après six mois d'expérimentation, a lancé le développement de la technologie[17]. La biométrie est en vogue, et sa cote de popularité ne fait que s'accroître.

Bien sûr, l'automatisation des procédures biométriques et la recrudescence des mesures de contrôle dans les espaces publics et privés fait naître des problématiques susceptibles de bouleverser la société, tant sur les plans juridique, politique et éthique. Le contexte international contraint les états à réfléchir sur les conséquences de l'implantation de ces technologies et de la création d'une identité biométrique, lesquelles restent mal évaluées. En outre, les risques d'atteinte à la vie privée sont inquiétants et les règles de sécurité applicables à la biométrie doivent être mieux définies. Tel que soulevé dans un rapport d'information

---

13 Voir à ce sujet: John D. WOODMARD, « Biometrics should not be automatically construed as privacy's foe. Quite to the contrary, biometrics is privacy's friend », Proceedings of the IEEE, vol.85, n°9, September 1997, p.1487.

14 Xavier CRETTIEZ et Pierre PIAZZA, *préc*., note 6, p. 256.

15 *Id*.

16 *Id*.

17 LE PARISIEN, « Le paiement biométrique bien accepté par ses utilisateurs après 6 mois de test », 15 mai 2013, en ligne : <http://www.leparisien.fr/high-tech/le-paiement-biometrique-bien-accepte-par-ses-utilisateurs-apres-6-mois-de-test-15-05-2013-2805021.php>.

présenté au Sénat français, la plus-value en matière de sécurité n'est pas déterminée et les questions abondent :

> « Du point de vue de la sécurité, les questions essentielles avant de créer un titre d'identité biométrique sont : quel degré de sécurité veut-on atteindre ? Quel type de fraude faut-il éliminer ? Quels autres usages de la biométrie veut-on permettre ou ne pas permettre ? Quelle est la taille de la population concernée ? »[18]

En dépit de l'absence de réponse à tous ces questionnements, beaucoup de citoyens seraient tout de même favorables à l'établissement de procédures biométriques, si ce n'est que pour protéger les citoyens de la « menace terroriste ». Certains défendent même l'idée que, puisqu'ils n'ont « rien à cacher », la protection de leur vie privée est de moindre importance par rapport au besoin actuel de renforcer la sécurité[19].

Avant de porter des observations sur la reconnaissance biométrique, précisons que trois approches pour établir l'identité sont possibles, soit 1) celle basée sur un mot de passe visant à savoir « ce qu'on se souvient », 2) celle qui prouve l'identité au moyen d'une carte d'identité ou d'une clé « que nous possédons » et 3), celle de la reconnaissance biométrique en fonction de « ce que nous sommes intrinsèquement »[20].

Alors que la tâche fondamentale de la gestion de l'identité est d'établir une association entre un individu et son identité personnelle[21], certains auteurs soutiennent que la reconnaissance par les traits biométriques constitue une manière plus sûre et raisonnablement permanente d'établir ce lien[22]. Notons qu'il existe plusieurs types de technologies et de

---

18 Jean-René LECERF, « Rapport d'information au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire », présenté au Sénat, 29 juin 2005, n° 439.

19 Même si, en apparence, cette position semble légitime, la protection de la vie privée demeure primordiale et le lien entre l'atteinte à ce droit fondamental et l'accroissement de la sécurité n'est pas établi. Voir Daniel SOLOVE, « Why Privacy Matters even if you have nothing to hide », May 15th, 2011, en ligne : <http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/>.

20 Art. 40, *Loi concernant le cadre juridique des technologies de l'information* (« LCCJTI »), L.R.Q., c. C-1.1.

21 Anil K. JAIN, Arun A. ROSS and Karthik NANDAKUMAR, « Introduction to Biometrics », Springer, 2011, p. 2.

22 *Id.*

données biométriques, disposant de degrés différents de fiabilité et dont chacun présente ses propres avantages et inconvénients.

Lors de l'adoption de la *Loi concernant le cadre juridique des technologies de l'information*[23] (« LCCJTI ») en 2001, le législateur québécois s'est porté initiateur d'un encadrement consacrant certaines règles régissant l'utilisation de la biométrie à des fins de reconnaissance de l'identité. La LCCJTI ayant notamment pour mission d'assurer la sécurité juridique des communications et le lien entre une personne et un document technologique, c'est dans ce contexte que les quelques dispositions concernant la biométrie ont été adoptées.

Ce mémoire vise donc l'étude du cadre normatif de l'utilisation de la biométrie dans un contexte civil. En raison du peu de doctrine et de jurisprudence disponibles sur ce sujet au Québec, nous comparerons tout au long de ce mémoire les règles du droit québécois avec celles du droit fédéral, canadien et français, afin d'en faciliter la compréhension.

Notons que le gouvernement fédéral ne dispose d'aucun encadrement législatif précis sur l'utilisation de la biométrie dans les sphères publique et privée. Comme nous le verrons dans la première partie, les renseignements biométriques sont en principe des renseignements personnels[24]. Dans ce contexte, la *Loi sur la protection des renseignements personnels*[25] (« LPRP ») ainsi que la *Loi sur la protection des renseignements personnels et des documents électroniques*[26] (« LPRPDE ») trouveront application en matière de protection des données biométriques. Le Commissariat à la protection de la vie privée au Canada a par ailleurs publié en 2011 un document d'orientation destiné à expliquer en quoi consiste la biométrie, les

---

23 LCCJTI, *préc.*, note 20.

24 Nous verrons qu'il pourrait y avoir certaines exceptions à cet égard, notamment en ce qui a trait au résultat mathématiques des caractéristiques biométriques. Voir la section 2.1 du premier chapitre de la présente partie.

25 *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21 (« LPRP »).

26 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (« LPRPDE »).

répercussions qu'exercent ce secteur sur la protection de la vie privée et quelques mesures d'atténuation des risques[27].

Du côté de l'Ontario, des mesures relatives à l'identification biométrique ont été prises par le législateur ontarien en 1997 pour lutter contre la fraude aux prestations sociales[28]. La fraude reposait en grande partie sur des identités multiples déclarées par les bénéficiaires pour obtenir plusieurs fois la même prestation. Un cadre juridique prévoyant des règles techniques et procédurales a ainsi été défini en collaboration avec le Bureau du Commissaire à la vie privée et à l'information de l'Ontario (Office of the Information and Privacy Commissionner, « IPC »). Ainsi, la *Social Assistance Reform Act*[29] offrait des garanties au regard de la biométrie et pouvait servir de modèle aux administrations envisageant d'avoir recours à la biométrie pour lutter contre la fraude.

Aux États-Unis, l'administration américaine a mis en œuvre le programme *«* US VISIT » (*Visitor and immigrant status indicator technology*), en vertu duquel les données biométriques de presque tous les visiteurs sont collectées. La biométrie est aussi utilisée dans le cadre de programmes de gestion de l'identité tels que TWIC *(Transportation worker identification credential)* pour les travailleurs d'activités de transport et le programme *Registered Traveler*[30]. D'autres programmes sont également mis en œuvre et en cours d'analyse par les autorités américaines[31].

---

27 CPVPC, « Des données au bout des doigts, la biométrie et les défis qu'elle pose à la protection de la vie privée », Documents d'orientation du CPVPC, en ligne : https://www.priv.gc.ca/information/pub/gd_bio_201102_f.asp

28 *Social Assistance Reform Act*, Ontario Regulation 226/98, 1997. Voir Ann CAVOUKIAN, « Privacy and Biometrics », Information and Privacy Commissioner of Ontario, 1999.

29 *Id*.

30 « The Transportation Security Administration (TSA) is currently developing the Registered Traveler Program alongside the private sector in order to strengthen aviation security and to enhance customer service. The Registered Traveler Program will be a voluntary market-driven initiative offered by the private sector with TSA oversight. Companies will enroll Registered Traveler participants using biometric (fingerprint and iris) and biographic information » : <http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx>.

31 *Id*.

Pour arriver à faire la lumière sur l'encadrement normatif de l'utilisation de la biométrie au Québec, les dispositions de la *Loi concernant le cadre juridique des technologies de l'information* ont été évaluées, en corrélation avec les dispositions relatives aux renseignements personnels de la *Loi sur la protection des renseignements personnels dans le secteur privé*[32] et de la *Loi sur l'accès aux documents des organismes publics et les renseignements personnels*[33] (« Loi sur l'accès »). Ainsi, nos conclusions font état de notre interprétation du droit applicable tant au secteur privé qu'au secteur public québécois. Mais, vu la quasi-absence de jurisprudence et de doctrine à ce sujet chez nous, nous n'avons pas hésité à regarder le droit étranger pour nous éclairer davantage sur les enjeux et les solutions.

Dans la première partie, nous tenterons de définir la biométrie et présenterons son fonctionnement. Nous analyserons ensuite les risques qui découlent de son utilisation sur certains droits fondamentaux, tels que le droit à la vie privée, le droit à l'intégrité et le droit à la dignité. Dans la seconde partie, nous expliquerons les règles préalables à la collecte et au traitement des renseignements biométriques, en plus des conditions d'accès et des mesures de sécurité propres à assurer leur confidentialité.

L'adéquation des principes légaux aux paramètres scientifiques étant une condition primordiale à une juste compréhension des risques juridiques dans le domaine des technologies biométriques, le langage technique a été simplifié, dans la mesure du possible, de manière à faciliter la compréhension des enjeux inhérents à la biométrie.

---

[32] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1.
[33] *Loi sur l'accès aux documents des organismes publics et les renseignements personnels*, L.R.Q., c. A-2.1.

PREMIÈRE PARTIE – Assurer la sécurité des données biométriques : utilisation de la biométrie et risques inhérents

Avant de porter des observations sur le cadre législatif de la biométrie au Québec, il est opportun d'expliquer en quoi consiste la biométrie, comment elle est utilisée et quels sont les risques découlant de son utilisation, tant du point de vue des droits fondamentaux que de la sécurité des données. Comprendre ce qu'est la biométrie et en expliquer les mécanismes de fonctionnement est crucial afin d'identifier les risques découlant de son utilisation et, ainsi, de mieux déceler les mesures de sécurité appropriées à son utilisation. Nous verrons par la suite que l'utilisation de cette technologie implique des conséquences importantes sur son objet, les données biométriques.

Chapitre I. Définir la biométrie et les données biométriques

Section 1 – La définition et le fonctionnement de la biométrie

1.1 La définition de la biométrie

La biométrie est une notion fondamentalement vaste faisant référence à de nombreux domaines d'application. En effet, on l'utilise en médecine depuis des siècles pour en étudier les dimensions et la croissance des êtres vivants[34]. Elle est également une « application des méthodes statistiques à la biologie »[35]. La biométrie est aussi intimement liée à l'anthropométrie, définie comme une « science qui a pour objet les mensurations du corps humain »[36].

Au sens où nous l'étudions dans le cadre de ce mémoire, la biométrie est une science dont l'objectif vise à reconnaître l'identité d'une personne. Bien que la biométrie artisanale ait

---

34 *Dictionnaire le Larousse*, en ligne, *sub verbo*, « Biométrie ».

35 OQLF, *Grand dictionnaire terminologique*, 2003, « Biométrie ».

36 OQLF, *Grand dictionnaire terminologique,* 2003*,* « Anthropométrie ».

été le plus souvent utilisée dans le passé[37], la biométrie couplée à l'informatique engendre une reconnaissance automatisée des identités et en faciliterait ainsi grandement le traitement[38]. C'est donc dans ce contexte que nous nous pencherons un peu plus loin sur les enjeux de sécurité et de vie privée de la biométrie.

Plusieurs organismes ont proposé diverses définitions de la biométrie. Nous jugeons nécessaire d'en énumérer ici quelques exemples, afin de se pencher en dernier lieu sur celle qui nous apparaît la plus adéquate.

L'Office québécois de la langue française désigne la biométrie comme une « analyse mathématique des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable »[39]. Au fédéral, le Commissariat à la protection de la vie privée du Canada définit la biométrie comme « un éventail de techniques, d'appareils et de systèmes permettant aux machines de reconnaître des personnes ou de confirmer ou d'authentifier leur identité »[40]. Quant au Larousse, il définit cette notion comme une « technique qui permet d'associer à une identité une personne voulant procéder à une action, grâce à la reconnaissance automatique d'une ou plusieurs caractéristiques physiques et comportementales de cette personne préalablement enregistrée »[41].

Par ailleurs, le Rapport de la conférence citoyenne sur la biométrie et la sécurité, rendu par l'Institut du nouveau monde en 2006, a fournit une définition plus détaillée de la biométrie :

---

37 Par exemple, les techniques de saisie des empreintes digitales à l'encre étaient utilisées depuis le 9e siècle par le chinois afin d'authentifier certains documents. De plus, leur utilisation à des fins criminalistiques remonterait au 18e siècle. Voir : Max CHASSÉ, « La biométrie au Québec : les enjeux », Commission d'accès à l'information, 2002.

38 En effet, les systèmes automatisés seraient beaucoup plus rapides et diminueraient les délais de traitement des données. Voir : Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », Étude générale, Division de l'industrie, de l'infrastructure et des ressources, Service d'information et de recherche parlementaire, Bibliothèque du Parlement, publication no 06-30-F, révisé le 16 avril 2010.

39 OQLF, *Grand dictionnaire terminologique,* 2005*,* « Biométrie ».

40 CPVPC, « Des données au bout des doigts, La biométrie et les défis qu'elle pose à la protection de la vie privée », *préc*., note 27.

41 *Dictionnaire le Larousse*, « Biométrie », en ligne.: <http://www.larousse.fr/encyclopedie/medical/biom%C3%A9trie/11569>.

> « La biométrie (qui signifie littéralement « mesure du corps humain » en grec) est une technologie permettant l'analyse mathématique des caractéristiques biologiques, morphologiques ou comportementales d'une personne, destinée à déterminer son identité de manière irréfutable. Les empreintes digitales, l'iris, la rétine, la géométrie de la main et les empreintes vocales, offrent une preuve irréfutable de l'identité d'une personne dans la mesure où ils sont uniques à chacun »[42].

Notons qu'en France, la Commission nationale de l'informatique et des libertés (« CNIL ») désigne la biométrie comme étant « l'ensemble des procédés tendant à identifier un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales »[43]. Elle ajoute par ailleurs que les systèmes biométriques sont :

> « […] des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services 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) »[44].

En dépit de toutes les définitions proposées ci-haut, la définition suggérée par la CNIL nous apparaît être la plus complète, car elle différencie les types de caractéristiques mesurables et spécifie qu'il peut y avoir reconnaissance de l'identité au moyen d'une ou de plusieurs caractéristiques. Comme nous l'expliquerons à la section 2, les données biométriques seront généralement enregistrées dans un système ou sur un support individuel.

Puisque la biométrie se définit essentiellement par son usage, notons qu'il serait tout autant approprié de parler de reconnaissance biométrique lorsque la biométrie a pour but

---

42 INSTITUT DU NOUVEAU MONDE, « Guide de participation, Rapport de la conférence citoyenne sur la biométrie et la sécurité », dans le cadre du projet Jeunes, Sciences et Démocratie, Montréal, 11-12 mars et 22-23 avril 2006.

43 CNIL, « La biométrie », Mai 2005, en ligne : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/LA_BIOMETRIEmai2005.pdf

44 *Id*.

d'identifier ou d'authentifier une personne[45]. Le gouvernement canadien mentionne d'ailleurs cette expression à quelques reprises dans ses documents d'orientation[46].

1.2 Les fonctions de la biométrie : identification et authentification

La biométrie comporte deux fonctions principales, soient l'identification (a) et l'authentification (b)[47]. Alors que la première vise à rechercher l'identité d'un individu en comparant ses données biométriques avec d'autres personnes dans une base de données (comparaison collective), la deuxième consiste à vérifier la concordance entre les données biométriques saisies et celles de la même personne, colligées sur un support ou dans une base de données (comparaison individuelle)[48]. Comme nous le verrons, les deux types de fonction peuvent comporter des incidences juridiques distinctes pour la sécurité et la vie privée. En pratique, toutefois, la différence entre les deux rôles est exiguë, puisqu'elle dépendra seulement du procédé de comparaison a posteriori de l'étape de la collecte.

Notons que l'identification et l'authentification auront généralement lieu dans un but spécifique. En effet, les finalités ou objectifs sur lesquels se fonde la reconnaissance biométrique peuvent être multiples[49] et serviront à évaluer le bien-fondé de la mise en place de ces systèmes, en vertu notamment des principes de nécessité et de proportionnalité[50]. Certains

---

45 La distinction entre l'identification et l'authentification sera explicitée à la section suivante.

46 Voir notamment Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », *préc.*, note 38.

47 Voir *Id.*; Anil K. JAIN, Arun A. ROSS et Karthik NANDAKUMAR, « Introduction to Biometrics », Springer, 201, p.5; Max CHASSÉ, « La Biométrie au Québec : les enjeux », *préc.*, note 21.

48 LIGUE DES DROITS ET LIBERTÉS, « La biométrie: des implications majeures pour nos droits et libertés », Mémoire présenté à la Commission de l'éthique de la science et de la technologie du Québec, 2005, p.4.

49 Par exemple, la biométrie sera utilisée pour l'identification des suspects, la prévention du crime, la prévention et l'usage frauduleux de documents, les prestations d'aide-sociale, contrôle des accès locaux et des sites physiques, le contrôle des accès à l'équipement informatique et aux applications de chiffrement, la surveillance au travail et contrôle des horaires, le renforcement de fiabilité des titres délivrés, la régulation et contrôle des flux migratoires et le paiement électronique, notamment.

50 Nous verrons plus en détails les règles relatives aux tests de proportionnalité et de nécessité dans la deuxième partie du présent mémoire.

systèmes peuvent par ailleurs cumuler les deux fonctions, soit l'identification dans un premier temps et l'authentification dans un deuxième temps.

a) L'identification

La reconnaissance par l'identification consiste à comparer un échantillon biométrique prélevé aux caractéristiques de plusieurs individus conservées dans une banque de données. S'il y a correspondance entre l'échantillon fourni et celui conservé, il y a identification[51]. Ainsi, « pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris...), puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés »[52]. Selon notre compréhension, la centralisation des données de plusieurs individus est donc nécessaire pour qu'il y ait identification. Celle-ci permet de connaître une identité dans un système, alors que l'authentification permet de vérifier cette identité réclamée[53].

Il existe deux types d'identification : l'identification positive et l'identification négative. Elle est positive lorsqu'elle a pour objet de déterminer l'identité d'une personne à partir d'un système sans réclamer une identité particulière. Dans le cas de l'identification négative, le but est de prévenir les fraudes d'identité et ainsi déceler les individus circulant sous une fausse identité, en effectuant un filtrage dans une banque de données à partir d'une liste de personnes recherchées, par exemple. L'identification négative par la biométrie se fait régulièrement et depuis des années dans le domaine de la criminalistique – par exemple, elle est fréquemment utilisée pour rechercher des suspects lors des contrôles aux frontières étatiques[54].

---

51 <http://www.biometrie-online.net/faq>.

52 Christian CABAL, *préc.*, note 2, p. 8.

53 Voir CPVPC, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », Document d'orientation du CPVPC, *préc.*, note 27.

54 Jean-Baptiste THOMAS-SERTILLANGES, « Identification biométrique, protection des données et droits de l'homme », Mémoire en droit de l'internet public, Université Paris I, 2007, p.15.

Comme nous l'exposerons au deuxième chapitre, l'identification biométrique soulève plusieurs inquiétudes, lesquelles ne sont pas nécessairement partagées avec l'authentification. En effet, la constitution de banques ou de bases de données pourrait engendrer un plus grand risque de fausses correspondances et d'usurpation de l'identité que l'authentification[55].

b) L'authentification

À défaut de procéder à une comparaison collective, l'authentification consiste à apporter la preuve de sa propre identité. La personne doit fournir un document d'identité et, par la suite, fournir ses caractéristiques corporelles pour une comparaison à celles enregistrées lors de l'enrôlement[56]. Le système, ou une personne, détermine alors l'acceptabilité de l'échantillon saisi en le comparant avec le gabarit biométrique, stocké sur un support individuel ou dans une banque de données.

Comme nous l'avons dit, une comparaison avec les données d'autres personnes n'est pas nécessaire : seule une comparaison avec son propre échantillon suffit. Par ailleurs, les données biométriques traitées pour l'authentification seront souvent stockées sur un support individuel, tel qu'une carte à puce. Bien qu'elle puisse aussi procéder par le biais d'une banque de données, le stockage centralisé des données biométriques pour l'authentification n'est pas requis.

Par exemple, un système destiné à contrôler les accès au moyen de l'authentification fonctionnera généralement de la manière suivante : 1) les caractéristiques physiques d'un individu sont captées au moyen d'un appareil, et 2) un logiciel interprète la lecture des données et transforme celles-ci en « signature[57] » ou « gabarit biométrique »[58]. Le système, ou

---

55 *Id*. Voir également COMMISSION NATIONALE DE L'INFORMATIQUE ET LIBERTÉS (CNIL), 21e rapport d'activités 2000.

56 Comme nous le verrons à la section suivante, l'enrôlement est la première étape de la reconnaissance biométrique.

57 Une donnée biométrique ou un « identifiant numérique » peut également servir de signature. En effet, il est généralement admis que l'identification biométrique correspond aux fonctions attribuées à la signature électronique. Voir : Marc LACOURSIÈRE, « La compensation interbancaire à l'ère d'Internet »,

une personne, détermine alors l'acceptabilité de l'échantillon saisi en le comparant avec le gabarit biométrique de la personne préalablement sauvegardé lors de l'enrôlement.

Tel que brièvement abordé ci-haut, le procédé pour authentifier une personne à partir d'une banque de données s'apparente beaucoup à l'identification. Effectivement, dans la mesure où l'on peut authentifier une identité à partir d'une banque de données, il nous apparaît requis de devoir « trouver » cette identité dans le système parmi plusieurs autres, pour que celle-ci puisse par la suite être « vérifiée ». Dans ce contexte, la séparation entre les deux concepts se retrouve en quelque sorte brouillée.

Nous croyons qu'il s'agit ici d'un exemple où la reconnaissance biométrique a lieu de manière bifonctionnelle, c'est-à-dire en procédant à l'identification dans un premier temps et à l'authentification dans un deuxième temps. Mentionnons par contre que nous ne voyons aucune ambiguïté dans la distinction entre l'identification avec une banque de données et l'authentification au moyen d'un support portable.

1.3 Le fonctionnement des systèmes biométriques

Nous l'avons vu, les applications biométriques dépendent d'une comparaison entre une nouvelle mesure saisie et une autre préalablement enregistré dans un système[59]. Il y a donc une première capture ou saisie biométrique qui doit être faite et conservée afin de pouvoir identifier ou authentifier l'individu subséquemment. Cette première capture se nomme « phase d'enrôlement » (ou d'inscription)[60]. C'est à cette étape que la donnée biométrique brute est

---

Développements récents en droit bancaire (2003), Service de la formation permanente du Barreau du Québec, 2003, EYB2003DEV547, p.22.

58 CLUSIF, « Techniques de contrôle d'accès par biométrie », Dossier technique présenté à la Commission Techniques de Sécurité Physique, Club de Sécurité des systèmes d'information français (CLUSIF), 2003, p.24.

59 Roger CLARKE'S, « Biometrics and Privacy », Roger Clarke's website, 2001: <http://www.rogerclarke.com/DV/Biometrics.html>.

60 Voir Max CHASSÉ, *préc*., note 37.

collectée, pour ensuite être stockée dans une base de données ou sur un support - sous sa forme brute ou sous forme de gabarit[61].

La phase d'enrôlement est cruciale et devrait être effectuée d'une manière excessivement minutieuse, car tout le bon fonctionnement du système dépendra de la qualité de l'information saisie lors de l'enrôlement. À défaut d'un enrôlement adéquat, les risques d'erreurs se multiplient[62]. En effet, selon les conclusions du gouvernement canadien, l'un des points faibles de la reconnaissance biométrique se situe au niveau de l'enrôlement lors de la délivrance du titre biométrique[63] :

> « [L]a biométrie peut uniquement confirmer que la personne contrôlée est celle qui a été portée au système; si cette personne a utilisé des documents de base (p. exemple un acte de naissance) falsifiés pour s'enrôler, le système ne pourra pas confirmer la véritable identité de la personne »[64].

En conséquent, un enrôlement frauduleux aura des répercussions sur toute la chaîne des étapes subséquentes et permettra à une personne circulant sous une fausse identité de le faire en toute liberté[65]. Une assistance humaine lors de cette première étape sera évidemment souhaitable afin de s'assurer que les mesures de sécurité sont suivies adéquatement.

À la suite de l'enrôlement, la caractéristique biométrique peut être conservée dans une banque de données centrale ou sur un support portable individuel[66]. La plupart des systèmes comportent quatre modules, nommés détecteur, dispositif d'extraction, base de données et système de transmission (ou module de correspondance)[67]. Le système de transmission, servant à transporter les données entre les systèmes de collecte et de comparaison, peut être

---

61 Voir Ann CAVOUKIAN, « Consumer Biometric Applications : A Discussion Paper », Ontario Information and Privacy Commissioner, September 1999.

62 Jean-René LECERF, *préc*., note 18 , p. 71.

63 *Id.*, p. 67.

64 Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », *préc*., note 38, p. 8.

65 Jusqu'à ce que la personne légitime se rende compte qu'elle s'est fait usurper son identité. Nous verrons dans la deuxième partie tous les risques associés à l'enrôlement.

66 *Id*.

67 Anil K. JAIN, Arun ROSS et Salil PRABHAKAR, « An Introduction to Biometric Recognition », *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, nº 1, Janvier 2004, p.4.

local (interne) ou distant (en réseau)[68]. Si la qualité de l'échantillon brut dépend de la qualité du détecteur utilisé pour la collecter[69], il devient impératif de se doter de technologies performantes afin d'éviter les risques d'incident ou de fraude. Le succès de l'opération de reconnaissance biométrique dépendra ainsi largement de la technologie utilisée.

Lors de l'étape suivante, appelée phase de reconnaissance ou de comparaison, la donnée biométrique est collectée de nouveau pour être comparée à la donnée préenregistrée lors de la phase d'enrôlement. Notons que cette opération est répétée à toutes les fois où la reconnaissance de l'identité doit avoir lieu.

Ainsi, une fois les données couplées, on obtient un résultat correspondant à la mesure de la similarité entre le gabarit et la donnée collectée a posteriori. Selon le degré de concordance que l'on veut obtenir, le processus de reconnaissance de l'identité sera approuvé ou échouera. Il est à noter qu'une comparaison négative, soit la mesure de la non-similarité, peut également être le résultat préprogrammé du système dans le cas d'une reconnaissance biométrique par identification négative[70].

Cependant, il est communément admis que la majorité des applications biométriques ne rencontreront pas une correspondance parfaite entre le gabarit stocké et l'échantillon mesuré subséquemment[71]. La façon de comparer les mesures est donc basée sur un écart de tolérance prédéterminé, permettant de constater si celles-ci concordent suffisamment pour être acceptées. Ceci est dû en partie aux variations que peuvent comporter les caractéristiques physiques – une même caractéristique pouvant différer selon la qualité du détecteur, les conditions ambiantes ou les altérations qu'elle peut subir tout au long d'une vie[72]. En cas d'échec à la comparaison, il est possible de recommencer le processus à l'étape de la collecte

---

68 CLUSIF, « Techniques de contrôle d'accès par biométrie », *préc*., note 58=7, p.25.
69 *Id*.
70 Charles A. SHONIREGUN and Stephen CROSIER, « Securing Biometrics Applications », Éditions Springer, University of East London, United Kingdom, 2008, p.17.
71 CLUSIF, *préc*., note 57.
72 Charles A. SHONIREGUN and Stephen CROSIER, *préc*., note 70.

ou alors de comptabiliser le nombre d'échecs de la même personne et de décider d'un blocage de contrôle[73].

D'ordinaire, il est recommandé que les données soient transformées et conservées sous une autre forme que leur forme brute, afin de contrecarrer certains les risques de vol de la donnée et d'usurpation d'identité. Les données peuvent ainsi être transformées en code binaire, encryptées ou converties en algorithme mathématique, tel que le biohachage pour les empreintes digitales[74].

La transformation des données, aussi appelée biométrie révocable, est utilisée pour sécuriser les données biométriques afin de ne pas utiliser directement les données originales et mieux protéger la vie privée des personnes. Cette pratique dépendra cependant de la technologie employée et devra « nécessairement prendre en compte la sécurité des données et les contraintes de variabilité entre les données. La construction de tels schémas est un important challenge pour la protection de la vie privée et la normalisation de ces techniques est envisageable prochainement »[75].

Section 2 - Qualification et types de données biométriques

Dans un contexte où tout système de reconnaissance biométrique implique directement la collecte des caractéristiques, mesures ou données biométriques, nous jugeons qu'il est essentiel de fournir une définition de celles-ci. Comme nous le verrons, les données biométriques sont sujettes à des incertitudes techniques et physionomiques et ne garantissent pas toutes le même niveau de fiabilité. Nous exposerons également les incertitudes juridiques découlant de leur traitement, notamment en ce qui a trait à leur caractère personnel à la lumière de nos lois sur la protection des renseignements personnels.

---

73 CLUSIF, *préc*., note 58 , p.25.

74 *Id.* Concernant le Biohachage, voir E. CHERRIER, P. LACHARME, C. ROSENBERGER, « La biométrie révocable : principes et limites », dans *Atelier de Protection de la Vie Privée (APVP),* Université de Caen, 2012, p.3.

75 *Id*., p.5.

2.1 Les types de données biométriques

À l'heure actuelle, il existe trois types de donnée biométrique, soit les données morphologiques, comportementales et biologiques. La biométrie morphologique (ou physionomique) est celle qui mesure les parties tangibles du corps humain. Elle comprend les empreintes, la lecture de l'iris ou de la rétine, la reconnaissance faciale, la lecture du contour de la main, de l'oreille, etc.

La biométrie dite comportementale est celle qui mesure les caractéristiques intrinsèques au comportement d'une personne, tel que la reconnaissance de la voix, de la démarche, de la signature et de la frappe au clavier. Les mesures comportementales sont aussi appelées biodynamiques[76].

La biométrie biologique a pour but de mesurer les substances du corps humain ou les traces biologiques, comme l'ADN, le sang, la salive, etc. Celle-ci se distingue toutefois nettement des autres types de technologies biométriques et ce, à plusieurs égards. Selon l'OCDE, l'identification par l'ADN ne relève pas de la biométrie au sens strict, car elle requiert un « échantillon matériel et non une image, une photographie ou une numérisation. Les ADN ne sont pas appariés en temps réel et la majeure partie des opérations ne sont pas automatisées »[77].

De plus, les technologies fondées sur la lecture de l'ADN sont beaucoup plus intrusives sur le plan de l'intégrité physique. Celles-ci font d'ailleurs l'objet de dispositions particulières tant en droit criminel qu'en droit civil[78]. Pour ces raisons, la présente étude fera fi des règles relatives aux données concernant l'ADN et consacrera exclusivement aux systèmes biométriques fondés sur des caractéristiques morphologiques ou comportementales.

---

76 CLARKE'S Roger, « Biometrics and Privacy », Roger Clarke's website, 2001: <http://www.rogerclarke.com/DV/Biometrics.html>.

77 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Technologies fondées sur la biométrie », Éditions OCDE, No. 101, 2005, p. 12.

78 Par exemple, voir les articles 487 et suivants du *Code criminel* et l'art. 43, *LCCJTI*.

Les types de mesures biométriques d'une personne ne sont pas limités et se diversifient. Comme le mentionne le député Cabal dans son rapport présenté au Sénat français, « quasiment tout, dans l'anatomie ou le comportement d'un individu, peut être transformé en un code informatique permettant de l'identifier »[79].

Chaque technologie disposant de ses propres spécificités, on tiendra compte de certains facteurs pour déterminer s'il est approprié d'utiliser un système plutôt qu'un autre, tel que la l'acceptabilité, la performance et la facilité de contournement[80]. L'acceptabilité fait précisément référence à l'acceptation générale par les utilisateurs d'une caractéristique particulière utilisée pour l'identification. La performance renvoie à la fiabilité et la rapidité de du système, de même qu'aux facteurs opérationnels et environnementaux qui peuvent affecter celles-ci. La facilité de contournement désigne la facilité de déjouer frauduleusement le système choisi[81].

Par ailleurs, certaines technologies offrent un niveau de fiabilité bas et ne livrent qu'une probabilité que deux images puissent identifier la même personne[82]. Il devra être tenu compte de ces facteurs lors de la détermination du type de technologie à être utilisée.

2.1.1 Les données biométriques morphologiques

a) Les empreintes digitales

La reconnaissance biométrique des empreintes digitales s'effectue depuis presque un siècle dans les domaines pénal et criminel[83]. D'ailleurs, c'est en 1924 que le FBI a débuté la

---

79 Christian CABAL, *préc*., note 2.

80 Anil K. JAIN, Arun ROSS et Salil PRABHAKAR, « An Introduction to Biometric Recognition », *préc*., note 67, p.4

81 *Id.*

82 C'est notamment le cas de la reconnaissance faciale. Voir : ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Technologies fondées sur la biométrie », *préc*., note 77, p. 41.

83 C'est le criminologue Alphonse Bertillon qui inventa l'anthropométrie judiciaire en 1870, autrement appelée « bertillonage », utilisant les empreintes digitales pour l'identification des suspects.

collecte et l'analyse des empreintes pour l'identification[84]. Auparavant manuelle, la façon de traiter les empreintes s'est automatisée depuis le développement des nouvelles technologies. La fiabilité de la reconnaissance des empreintes est considérée comme supérieure, et celle-ci sera augmentée en fonction du nombre de doigts soumis à l'évaluation[85].

Les empreintes digitales sont généralement considérées comme étant assez intrusives sur le plan de la vie privée, notamment car elles sont associées à l'identification criminelle[86]. De plus, les risques de fraude liés aux empreintes sont plus élevés que les autres données, car elles laissent des traces sur tout ce que l'on touche[87]. De ce fait, il est relativement facile de subtiliser une empreinte digitale en récupérant celle-ci sur un objet.

À titre d'exemple d'utilisation, le Village Vacances Valcartier a mis à la disposition de ses clients un système de reconnaissance des empreintes pour le paiement des consommations sur le site. En payant une somme forfaitaire d'avance, ceux-ci n'ont désormais plus besoin de transporter leurs moyens de paiement, mais n'ont qu'à apposer leur index sur le capteur des différents postes de péage[88]. Les empreintes ne sont associées à aucun autre renseignement personnel et sont automatiquement détruites dès lors que le client quitte le site[89], à l'exception des ceux disposant d'un billet de saison.

La reconnaissance de l'empreinte est aussi largement utilisée par les pays de l'Union européenne. Par exemple, la base de données centralisée Eurodac a été mise en ligne afin de comparer les empreintes des demandeurs d'asile, ayant pour but de vérifier si une demande a

---

84 FBI, « Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements – IAFIS », online: <http://www.fbi.gov/foia/privacy-impact-assessments/iafis>

85 OCDE, *préc*., note 77, p. 24.

86 Nous verrons cet élément plus en détails au chapitre 2, section 1. Voir COMMISSARIAT À LA PROTECTION À LA VIE PRIVÉE DU CANADA, « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2008-389, Enquête concernant le Law School Administration Council », 29 mai 2008, par. 54. Voir également : Charles A. SHONIREGUN and Stephen CROSIER, « Securing Biometric Applications », *préc.*, note 70, p. 42

87 Par exemple, la reconnaissance de la rétine et de la main sont des données ne laissant pas de traces. Voir : OCDE, *préc*., note 77.

88 VILLAGE VACANCES VALCARTIER, « Mon argent au bout des doigts », en ligne : <http://www.valcartier.com/parc-aquatique/fr/services/mon-argent-au-bout-du-doigt/>

89 Source : Boris Perron, Analyste en sécurité à la Commission d'accès à l'information du Québec.

déjà été faite dans un autre pays de l'UE[90]. Par ailleurs, et comme nous le verrons plus loin, l'adoption du passeport biométrique en France a suscité beaucoup d'inquiétudes, entre autres en raison des huit empreintes exigées au départ par le gouvernement français[91].

D'autre part, les nouvelles options de sécurité du iphone 5S offrent maintenant le choix au consommateur de pouvoir déverouiller son téléphone à l'aide d'une empreinte digitale. Le capteur biométrique, nommé « Touch ID », serait toutefois facile à déjouer. En effet, un groupe de hackers allemand aurait réussi à pirater le système en seulement deux jours[92].

b) La main

Les données biométriques pouvant être saisies relativement à la main sont les veines, les lignes et la géométrie en 3D. Plusieurs technologies sont aptes à effectuer la capture de ces trois types de données, combinées ou séparées[93].

Il est à noter que le degré d'unicité de la géométrie de la main serait relativement faible, puisque les similarités entre les mains de différents individus ne sont pas rares[94]. C'est pourquoi il est généralement recommandé de l'utiliser pour l'authentification uniquement[95]. Parmi ses autres faiblesses, la reconnaissance de la main requiert un minimum d'hygiène, afin de ne pas nuire à la captation de l'image[96]. Par contre, ce système résisterait à la fraude car il serait impossible de soumettre une paume de main artificielle[97].

---

90 OCDE, *préc*., note 77, p. 25.

91 CNIL, « Passeports biométriques : la CNIL contrôle l'effacement des empreintes digitales surnuméraires enregistrées dans la base du ministère de l'Intérieur », 11 janvier 2013.

92 *Le Huffington Post*, « Le "Touch ID" piraté par des hackers, deux jours seulement après la sortie de l'iPhone 5s », le 23 septembre 2013 [en ligne].

93 CHARLES A. SHONIREGUN and Stephen CROSIER, *préc*., note 70, p. 37.

94 OCDE, *préc*., note 119, p. 26.

95 Lalita ACHARYA et Thomas KASPRZYCKI, *préc*., note 38, p.5. De la même manière, certains auteurs sont d'avis que la reconnaissance de la géométrie de la main ne peut être performante pour l'identification. Voir Charles A. SHONIREGUN and Stephen CROSIER, *préc.*, note 70, p. 39.

96 *Id*., *préc*., note 69, p. 40.

97 Charles A. SHONIREGUN and Stephen CROSIER, *préc.*, note 70, p. 40.

En 2001, le Centre d'éducation physique de l'Université de Montréal (CEPSUM) a mis en place un système de reconnaissance de la morphologie de la main pour l'accès à ses installations sportives. Depuis ce temps, les étudiants peuvent accéder au CEPSUM en soumettant leurs données tridimensionnelles de la main droite. Celles-ci sont saisies et comparées à celles enregistrées dans le dossier lors de l'enrôlement. Le système ne reconnaît que le numéro d'accès de l'usager et « ne peut établir aucun lien avec d'autres informations personnelles telles que son nom, son adresse ou son numéro de téléphone »[98]. Ce moyen d'identification est toutefois optionnel, en raison notamment de l'obligation de consentement de l'utilisateur prévue à la LCCJTI[99]. Nous verrons les dispositions pertinentes de la LCCJTI en détails dans la seconde partie de ce mémoire.

c) L'iris

L'utilisation de l'iris comme moyen d'identification a été initialement proposée par l'ophtalmologiste Frank Burch en 1936 et on a pu en observer l'idée dans les films de James Bond des années 1980[100]. À l'heure actuelle, plusieurs systèmes de reconnaissance de l'iris ont été mis en œuvre dans les aéroports, notamment au Canada[101], au Japon et aux Pays-Bas[102].

L'iris est le muscle coloré à l'intérieur de l'œil, visible à travers la cornée, placé devant le cristallin et percé en son centre de la pupille[103]. Une caméra parcourt l'œil à l'aide d'une lumière infrarouge et capture une image, afin de mesurer plusieurs caractéristiques telles que le relief, les anneaux, les sillons et la texture de l'iris[104]. Étant donné son caractère stable et

---

98 CEPSUM, « Système de reconnaissance de la main : Questions et réponses », Université de Montréal, en ligne : < http://www.cepsum.umontreal.ca/media/wysiwyg/depl_handscanner.pdf>.

99 Art. 44, *Loi concernant le cadre juridique des technologies de l'information.*

100 Seifedine KADRY and Khaled SMAILI, « A Design and Implementation of a Wireless Iris Recognition Attendance Management System », Faculty of Engineering, Lebanese International University, ISSN 1392 – 124X Information Technology and Control, 2007, Vol.36, No.3, p. 323.

101 Les programmes Nexus et CanPass Air ont été déployés dans certains aéroports canadiens afin de réduire le temps d'attente pour l'enregistrement aux douanes.

102 IRIDIAN TECHNOLOGIES, « Solutions : Iris recognition is at work today protecting people around the world through secure identification », en line : <http://www.iridiantech.com/solutions/>

103 *Dictionnaire le Larousse*, en ligne, *sub verbo*, « Iris ».

104 Charles A. SHONIREGUN and Stephen CROSIER, *préc.*, note 70, p. 52.

très unique, la reconnaissance de l'iris est reconnue pour sa fiabilité très élevée[105]. Le système est d'ailleurs à l'épreuve des lunettes, des verres de contacts et des fluctuations de la taille de la pupille[106] et peut observer près de 200 points de comparaison[107]. Sa fiabilité est due en partie à la quasi-impossibilité de le reproduire artificiellement[108]. Toutefois, le succès du système dépendra de la qualité de l'image saisie par la caméra digitale, de la même manière que pour la rétine[109].

Certains auteurs qualifient ce système comme étant peu intrusif, puisque la caméra peut être placée à une distance de douze pieds[110]. Il découle toutefois de sa précision un faible taux d'acceptation et sa technologie serait très coûteuse[111]. A contrario, d'autres perçoivent la lecture de l'iris comme pouvant être intrusive et craignent que la lumière infrarouge puisse endommager l'œil[112]. À cet égard, le *National Science and Technology Council Subcommitee on Biometrics*[113] est plutôt d'avis que la lumière infrarouge ne serait pas assez puissante pour causer des dommages photochimiques à l'œil[114]. Néanmoins, il semblerait qu'un dommage « thermal » puisse être possible pour la cornée et l'humeur aqueuse, découlant des diodes électroluminescentes émises par le rayon infrarouge si la technologie employée n'est pas employée correctement[115].

---

105 *Id*. Voir également : OCDE, *préc*., note 77. Le TNO's Physics and Electronics Laboratory (TNO-FEL) et le Britain's National Physical Laboratory ont également conclu que le système de reconnaissance de l'iris mis en place à l'aéroport Schiphol aux Pays-Bas était très fiable, en ligne : <http://www.airport-technology.com/projects/schiphol/>.

106 Charles A. SHONIREGUN and Stephen CROSIER, *préc*., note 70, p. 52.

107 *Id*., p. 53.

108 *Id*. Notons toutefois qu'il serait possible, à l'aide d'une caméra très performante, de capter à distance l'image de l'iris.

109 NATIONAL SCIENCE AND TECHNOLOGY COUNCIL (NSTC), « Iris Recognition », Subcommittee on Biometrics, United States, Updated August 7th, 2006, p.4.

110 Charles A. SHONIREGUN and Stephen CROSIER, *préc*., note 70, p. 54.

111 *Id*., p. 53.

112 *Id*., p. 54; NSTC, « Iris Recognition », *préc*., note 109, p. 4.

113 Le *Subcommittee on Biometrics and Identity Management* est un sous-comité américain créé par le *National Science & Technology Council (NSTC) Committee on Technology (COT)* en 2003. La mission du sous-comité est de conseiller et d'assister le COT, le NSTC et les autres entités du *Executive Office of the President* sur les politiques et les procédures relativement aux activités biométriques fédérales. Voir : <http://www.biometrics.gov/nstc/>

114 NSTC, *préc*., note 109, p. 4.

115 *Id*. Voir également Nikolaos KOURKOUMELIS and Margaret TZAPHLIDOU, « Eye Safety Related to Near Infrared Radiation Exposure to Biometric Devices », in *The Scientific World Journal*, Department of Medical Physics, Medical School, University of Ioannina, Ioannina, Greece, March 1st, 2011.

d) La rétine

La reconnaissance de la rétine permet d'observer les ramifications vasculaires qui tapissent le fond de l'œil (surface interne antérieure)[116]. Le capteur enregistre la disposition des veines dans l'œil en balayent la rétine à l'aide d'un faisceau lumineux dans le globe oculaire[117]. Les vaisseaux sanguins sont numérisés et cartographiés sous forme de lignes et de points.

Bien que considérée comme intrusive, l'identification rétinienne est estimée par plusieurs comme étant la plus précise de toutes les technologies biométriques[118]. Toutefois, la technologie serait très couteuse, difficile à utiliser et disposerait d'un faible taux d'acceptation[119]. En outre, le réseau veineux de l'œil peut se modifier légèrement en raison d'une forte alcoolémie ou du diabète[120]. Notons par ailleurs que les risques de dommage thermal à l'œil en raison de la lumière infrarouge s'appliquent autant aux technologies de reconnaissance de la rétine que de l'iris[121].

e) Le visage

La reconnaissance du visage au moyen des technologies est probablement la technique la plus utilisée pour reconnaître l'identité d'une personne[122]. Les casinos sont parmi les premiers à avoir eu recours à cette technologie pour détecter les tricheurs ou les personnes interdites au jeu[123]. Le Surveillance Information Network (« SIN ») a d'ailleurs été créé par une communauté de casinos pour repérer certains individus suspicieux et relie à ce jour plus

---

116 OCDE, *préc*., note 77, p.33.
117 *Id.*
118 Charles A. SHONIREGUN and Stephen CROSIER, *préc*., note 70, p. 55-56.
119 *Id*., p. 55
120 *Id.*
121 Nikolaos KOURKOUMELIS and Margaret TZAPHLIDOU, « Eye Safety Related to Near Infrared Radiation Exposure to Biometric Devices », *préc.*, note 115.
122 Charles A. SHONIREGUN and Stephen CROSIER, *préc*., note 70, p. 49.
123 *Id*., p. 77; OCDE, *préc*., note 77, p. 14.

d'une centaine de casinos ayant accès à une base de données centralisée[124]. Au Royaume-Uni, un système automatisé de reconnaissance des criminels combiné à la vidéosurveillance a été déployé dans certaines rues de Londres[125].

Le système fonctionne en comparant une image captée en deux dimensions à une autre déjà enregistrée dans le système[126]. Or, il appert que la fiabilité des systèmes de reconnaissance faciale a été sérieusement mise en doute[127]. En effet, le visage est susceptible de modifications naturelles ou artificielles tout au long d'une vie. Un visage qui vieillit, est atteint par blessure, est maquillé ou ayant subi une opération chirurgicale sera susceptible de fausser les résultats de l'identification.

Il serait ainsi beaucoup plus facile de tromper son identité et les risques d'erreurs seraient plus grands. Tel que le mentionne Michael Thieme de l'*International Biometric Group,* la reconnaissance faciale ne livre qu'une probabilité que deux images correspondent à la même personne[128]. Toutefois, le développement des nouvelles technologies aurait apporté une nette amélioration du taux de réussite des systèmes de reconnaissance faciale ces dernières années[129].

La reconnaissance faciale pose toutefois des craintes importantes pour la protection de la vie privée, car il serait relativement facile de l'utiliser à l'insu des individus. Une image étant aisément captée à distance, la reconnaissance du visage peut se faire dans le secret à n'importe quel moment dans un endroit public[130]. Nous l'avons vu, ces systèmes sont très souvent utilisés dans un contexte de surveillance vidéo d'individus suspects. Le FBI aurait

---

124 *Id*., p.77.
125 *Id.*, p. 14.
126 *Id*.
127 *Id*. p 50, Michael THIEME, « Was It Really Saddam on TV Last Night? », posting to The Biometric Consortium's Discussion, 20 mars 2003.
128 *Id*.
129 Voir FEDERAL TRADE COMMISSION, « Facing Facts: Best practices for Common Uses of Facial Recognition Technologies », United States, October 2012.
130 Voir OCDE, *préc.*, note 77.

d'ailleurs investit plus d'un milliard de dollars dans une base de données nationale comprenant les données du visage, ayant pour but de repérer des criminels dans une foule[131].

2.1.2 Les données biométriques comportementales

a) La voix

La reconnaissance vocale ou de la parole est une technologie biométrique comportementale qui évalue les aspects de la voix d'une personne pour reconnaître son identité[132]. Elle est qualifiée de non intrusive et serait facile à utiliser[133]. Selon Christian Cabal, un des avantages de cette technologie est d'autoriser une reconnaissance à distance. De plus,

> « [c]ette technique a une bonne acceptabilité, mais présente, à l'évidence, un niveau de sécurité inférieur aux autres techniques. Il est relativement facile d'enregistrer et de reproduire une voix. Il est possible de s'affranchir de ce problème en faisant varier la phrase à prononcer, ou en couplant cette technique avec la prononciation d'un mot de passe. […] »[134].

Par ailleurs, « [l]a performance des systèmes de reconnaissance vocale sera susceptible de varier suivant la qualité du signal audio et la différence entre l'appareil d'enregistrement et l'appareil vérificateur, de sorte que la capture s'effectue normalement avec l'appareil censé servir à la vérification ultérieure »[135]. La voix pouvant se modifier et changer au cours du

---

131 Le système se nomme Next Generation Identification (« NGI »), voir : <http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi>; Adrien GENESTE, « Le FBI investit 1 milliard de dollars dans un projet de reconnaissance faciale », *Le Monde Informatique*, 11 septembre 2012.

132 Voir CPVPC, « Une organisation utilise la biométrie à des fins d'authentification », Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2004-281.

133 Charles A. SHONIREGUN and Stephen CROSIER, *préc.*, note 70, p. 57.

134 Christian CABAL, <http://www.assemblee-nationale.fr/12/rap-off/i0938.asp>.

135 OCDE, *préc.*, note 70, p. 35

temps, la fiabilité de sa reconnaissance est estimée moyenne[136]. Aussi, les bruits de fond et les problèmes de transmission peuvent affecter la qualité du résultat[137].

b) La signature

La saisie dynamique de la signature mesure le comportement alors que la saisie statique en analyse le tracé statique[138]. Le temps requis pour signer, l'angle d'inclinaison et la pression exercée sur le stylo font partie des aspects mesurés. Les données peuvent être analysées à l'aide d'une tablette électronique et/ou d'un stylo lecteur. Ce système est facile à utiliser, mais sa fiabilité est qualifiée de moyenne[139]. De même que pour la géométrie de la main, il n'est pas possible de comparer la saisie d'une signature avec un gabarit préalablement stocké dans une base de données[140]. Les systèmes d'authentification sont donc à privilégier pour la saisie dynamique de la signature.

c) Les pulsations cardiaques

La reconnaissance des battements du cœur serait au programme des prochaines technologies biométriques. En effet, c'est une chercheuse de l'Université de Toronto qui a lancé cette technologie, nommée Bionym[141]. Agissant comme un électrocardiogramme, cette technique permettrait une identification en 1,2 seconde et serait facilement intégrable à n'importe quel appareil électronique. Unique à chaque personne, les capteurs auraient la capacité de lire le rythme cardiaque par le bout des doigts. Il semble que la technologie soit proposée à titre de clé chiffrée afin de protéger les autres caractéristiques biométriques enregistrées[142].

---

136 *Id*.
137 Charles A. SHONIREGUN and Stephen CROSIER, *préc.*, note 70, p. 59.
138 BIOMETRICS INSTITUTE, « Types of biometrics », UK, online: http://www.biometricsinstitute.org/pages/types-of-biometrics.html
139 OCDE, *préc*., note 77, p. 35.
140 *Id*., p. 37.
141 <http://www.bionym.com/tech/be/>
142 *Id*.

D'autres technologies existent par ailleurs, telles que celles de la mesure de la frappe au clavier et de la reconnaissance de la démarche d'une personne[143]. En plus de tous ces types de caractéristiques, on constate que d'autres types de technologies biométriques émergent et permettent par exemple de capter l'odeur corporelle et même les émotions[144].

2.2 La qualification juridique de la donnée biométrique

La LCCJTI ne définit pas la *donnée biométrique*, pas plus que nos lois sur la protection des renseignements personnels[145]. Dans son rapport sur les enjeux de la biométrie, la Commission d'accès à l'information du Québec (« CAI ») a toutefois mentionné que « toute mesure ou caractéristique biométrique est un identifiant unique universel » qui est composé d'informations intimes[146]. La CAI précise à cet égard que les mesures ou les caractéristiques biométriques diffèrent passablement des autres identifiants comme les mots de passe, car elles ont « la capacité de livrer des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général »[147].

De son côté, le gouvernement fédéral définit une donnée biométrique comme étant une caractéristique physique ou comportementale permettant d'identifier une personne et qui est enregistrée dans un système biométrique[148]. Suivant cette définition, toutes les caractéristiques physiques d'une personne étant mesurables pour l'identification et pouvant être enregistrées dans un système seraient ainsi des données biométriques. En outre, il a énoncé quatre critères[149] cumulatifs pour qu'une caractéristique puisse être considérée comme biométrique :

---

143 Max CHASSÉ, *préc*., note 37, p. 10.

144 L'odeur, étant particulière à chaque être humain, est captée par un dispositif sur des parties du corps, telles que le dos de la main, le bras ou le cou. Ainsi, un « nez électronique » serait capable d'identifier les individus en mesurant leurs substances chimiques. Voir Laura SPINNEY, « Crooks smelly armpits give the game away », *New Scientist*, Vol. 143, Issue 1943, September 14th, 1994, p.10.

145 Voir la *LPRPSP* et la *Loi sur l'accès*, *préc*., note 24.

146 Max CHASSÉ, « La Biométrie au Québec : les enjeux », *préc*., note 37, p.24.

147 *Id*.

148 Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », *préc*, note 38.

149 Notons que ces critères sont généralement reconnus par plusieurs auteurs. Voir : Anil K. JAIN, Arun ROSS et Salil PRABHAKAR, « An Introduction to Biometric Recognition », *préc.,* note 67.

1. Elle est universelle. En principe, chaque personne doit pouvoir posséder et présenter cette caractéristique.
2. Elle est distinctive. La caractéristique doit être suffisamment différente chez deux personnes pour qu'elle puisse être différenciée.
3. Elle est permanente. la caractéristique doit être suffisamment immuable pendant une période donnée.
4. Elle est perceptible. La caractéristique doit pouvoir être mesurée quantitativement[150].

En Ontario, la *Loi de 1997 sur le programme Ontario au travail* énonce que les données biométriques sont des « renseignements dérivés de caractéristiques uniques d'un particulier, à l'exclusion toutefois d'une image photographique et de l'image d'une signature »[151]. En Alberta, la *Freedom of Information and Protection of Privacy Act* (« FOIP ») définit l'information biométrique comme étant « [TRADUCTION] toute information dérivée des caractéristiques mesurables et uniques d'un individu »[152].

Une distinction doit être faite entre les données biométriques laissant des traces et celles ne laissant pas de traces, car les risques de sécurité et d'atteinte à la vie privée diffèrent. Une donnée laissera des traces lorsqu'il est possible de les retrouver dans la vie quotidienne, comme les empreintes et la reconnaissance faciale[153]. Ces données sont donc plus sensibles car plus facilement piratables[154]. Selon la CNIL : « l'empreinte digitale est presque aussi redoutable que les traces d'ADN, car elle est omniprésente : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence »[155].

---

150 Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », *préc*., note 38.

151 *Ontario Works Act,* (S.O. 1997 c 25 Sch. A) section 76(1), en ligne : <http://www.e-laws.gov.on.ca/html/statutes/french/elaws_statutes_97o25a_f.htm#BK80>. Sans que nous en sachions la raison, il est intéressant de constater que l'Ontario a volontairement exclut de sa définition la reconnaissance faciale et l'image de la signature.

152 Art. 1(b.1) de la FOIP : « *Biometric information* means information derived from an individual's unique measurable characteristics ».

153 CNIL, Rapport d'activité n°21 – 2000.

154 Nous en discuterons plus en détails au point 1.4.

155 CNIL, Rapport d'activité n°21 – 2000.

2.2.1 Une donnée biométrique est-elle un renseignement personnel?

Au Québec, rien n'est précisément indiqué à cet égard dans la loi ou la jurisprudence. C'est donc en interprétant les différentes définitions de renseignement personnel proposées dans nos lois que nous pourrons fournir une réponse à cette question. Dans le secteur public, la *Loi sur l'accès* prévoit que « sont personnels les renseignements qui concernent une personne et qui permettent de l'identifier »[156]. De la même manière, « tout renseignement qui concerne une personne physique et permet de l'identifier »[157] est un renseignement personnel au sens de la LPRPSP. Selon ces définitions, un renseignement doit permettre d'identifier une personne pour qu'il soit qualifié de renseignement personnel au sens des lois applicables, disposant ainsi d'un caractère « identifiable ».

De manière tout à fait similaire à nos lois québécoises, la LPRP fédérale définit un renseignement personnel comme un « renseignement concernant un individu identifiable, quel que soit sa forme et son support »[158]. Selon la LPRPDE, il s'agit de « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail »[159]. Une donnée morphologique ou comportementale, étant en principe propre et unique à chaque individu, permet normalement d'identifier une personne. A priori, une donné biométrique concerne donc une personne physique et permet de l'identifier, ce qui correspond aux définitions prévues dans nos lois[160]. D'ailleurs, c'est pour des raisons d'identification que la reconnaissance biométrique est utilisée.

Selon le Commissariat à la protection de la vie privée du Canada (« CPVPC ») les données biométriques sont effectivement des renseignements personnels en vertu de son

---

156 Art. 54, *Loi sur l'accès,* L.R.Q., chapitre A-2.1.
157 Art. 2, *LPRPSP*, L.R.Q., chapitre P-39.1.
158 Art. 3, *LPRP*, L.R.C. (1985), ch. P-21.
159 Art. 2, *LPRPDE*, L.C. 2000, ch. 5.
160 Voir notamment la *Loi sur l'accès* et la *LPRPSP*.

interprétation de la LPRPDE[161]. De plus, les empreintes digitales ainsi que « tout numéro ou symbole, ou toute autre indication identificatrice » qui est propre à un individu sont des renseignements personnels selon la LPRP[162].

Qu'en est-il toutefois de la donnée biométrique collectée sous sa forme brute, mais transformée en gabarit algorithmique ou sous forme cryptographique pour sa conservation? Dans le contexte technologique actuel, cette pratique est généralement encouragée et jugée plus sécuritaire, car elle a pour but de protéger les renseignements personnels et confidentiels. En outre, il peut arriver que des organisations impartissent certaines données chiffrées pour leur stockage dans l'infonuagique.

En l'occurrence, de tels renseignements conservent-il leur caractère personnel suite à leur transformation? Tel que le mentionne Éloïse Gratton dans sa thèse de doctorat, *Understanding Personal Information : managing Privacy Risks*, il n'est pas tout à fait clair si les nouvelles formes de données que génèrent les nouvelles technologies peuvent être reliées à un individu :

> « With new types of data generated through the Internet and related technologies, it may not always be clear if such data actually relate to an identifiable individual and therefore, qualify as personal information »[163].

Elle est également d'avis que, « dans la situation où ce type de renseignement (résultat binaire obtenu après la conversion algorithmique des mensurations de la main d'un individu) se retrouve dans les mains d'un tiers qui n'a aucun autre renseignement pour faire une corrélation entre ce renseignement et un individu identifiable, il serait alors plus difficile d'argumenter qu'il s'agit en fait d'un renseignement personnel au sens des LPRP

---

161 CPVPC, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », *préc.,* note 27.

162 Art. 3 c) et d), *LPRP*, L.R.C. (1985), ch. P-21.

163 Éloïse GRATTON, « Understanding Personal Information : managing Privacy Risk », LexisNexis, 2013, p. 32.

applicables »[164]. Le test suggéré pour savoir si l'information conservée par l'organisation est personnelle ou non renvoie donc à la difficulté voire l'impossibilité pour celle-ci d'identifier l'individu en lien avec les renseignements qu'elle détient sur celui-ci[165].

En principe, si les données chiffrées ne peuvent plus être reliées à l'individu, les règles prévues aux lois sur la protection des renseignements personnels relatives à leur traitement, leur utilisation, leur conservation et leur accès ne s'appliquent plus. Pour déterminer si une donnée biométrique chiffrée conserve son caractère personnel, et cela vaut pour tous les autres renseignements personnels, nous devons évaluer de quelle manière une donnée biométrique transformée conservera son caractère identifiable. À cet effet, la décision *Gordon* c. *Canada* (Santé)[166] a fourni une interprétation de la notion d'« individu identifiable » en précisant qu'il doit y avoir une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris isolément ou en association avec d'autres données disponibles :

> « Les renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources »[167].

Comme l'a déjà mentionné le Commissariat à la protection de la vie privée dans un avis relatif à l'application de la LPRPDE, la « désidentification » des données ne constitue pas une réelle anonymisation de l'information lorsqu'il est possible de relier subséquemment les données à un individu identifiable[168]. Dans le même sens que l'affaire *Gordon*[169], le CPVPC ajoute que « les renseignements visent un individu identifiable lorsqu'il y a une grande

---

164 Éloïse GRATTON, « Chronique - Qu'est-ce qu'un renseignement personnel ? Le défi de qualifier les nouveaux types de renseignements », *préc*., note 164.

165 Éloïse GRATTON, « Understanding Personal Information : Managing Privacy Risks », LexisNexis, 2013, p. 112.

166 *Gordon* c. *Canada* (Santé), 2008 FC 258 (CanLII).

167 *Id*., para.34.

168 CPVPC, « Les notes anonymisées d'une psychologue en vue d'un examen par les pairs sont les renseignements personnels d'une patiente », Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2009-018.

169 *Gordon* c. *Canada* (Santé), 2008 FC 258 (CanLII).

possibilité qu'une personne puisse identifier les renseignements disponibles »[170]. De plus, un renseignement pourra identifier un individu « même s'il se trouve sous une forme non consignée, telle que des conversations orales, des échantillons biologiques ou de la vidéosurveillance en temps réel »[171].

En Europe, la *Directive 95/46/CE du Parlement européen relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* mentionne qu'« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[172].

Le *Groupe de travail Article 29* précise que pour déterminer si une personne est identifiable, « il convient de prendre en compte l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne pour identifier ladite personne »[173]. Plus précisément, cela signifie que « la simple possibilité hypothétique de distinguer une personne n'est pas suffisante pour considérer cette personne comme identifiable »[174].

Un des facteurs essentiels « pour évaluer *l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre* pour identifier les personnes sera, en réalité, la finalité visée par le responsable du traitement dans le cadre du traitement des données »[175]. Lorsque la finalité du traitement des données concerne l'identification de personnes physiques, le

---

170 CPVPC, « Renseignements juridiques associés à la LPRPDE », concernant la définition de renseignement personnel, Bulletin d'interprétation, Dernière modification le 2 octobre 2013, en ligne : <http://www.priv.gc.ca/leg_c/interpretations_02_f.asp >.

171 *Id*. Voir aussi : *Morgan* c. *Alta Flights Inc.*, (2006) CAF 121.

172 Art. 2 a), *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*.

173 GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis 4/2007 sur le concept de données à caractère personnel », Adopté le 20 juin 2007, 01248/07/FR, WP 136, p.21.

174 *Id*., p.16.

175 *Id*., p.17.

responsable du traitement ou toute autre personne concernée disposera sans doute d'un moyen « susceptible d'être raisonnablement mis en œuvre » pour identifier la personne concernée.
De ce fait, les données biométriques chiffrées pourraient nécessairement être reliées à un individu pour les traitements subséquents de reconnaissance à l'aide du système, de codes ou de logiciels, sans quoi elles demeureraient inutilisables.

Dans son document de travail sur la biométrie, le *Groupe de travail Article 29 sur la protection des données* en France indique que, dans la plupart des cas, les caractéristiques biométriques ou leur version numérisée sous forme de modèle sont des données à caractère personnel[176]. Il indique que « des données biométriques peuvent toujours être considérées comme des *informations concernant une personne physique*, puisqu'il s'agit de données qui fournissent, par leur nature même, des informations sur une personne précise. Dans le contexte de l'identification biométrique, « la personne est généralement identifiable, puisque les données biométriques sont utilisées à des fins d'identification ou d'authentification, au moins dans la mesure où la personne concernée est distinguée de toute autre personne »[177]. Ainsi, prétendre que les personnes physiques ne sont pas identifiables alors que la finalité du traitement est précisément de les identifier serait une « contradiction absolue »[178].

Le caractère personnel des données biométriques dépendrait donc de leur finalité du traitement. Néanmoins, même si l'identification des personnes physiques est l'une des finalités du traitement des données chiffrées, leur qualification juridique dépendra du traitement effectué par un responsable :

> « Cela ne signifie pas pour autant que tout autre responsable du traitement des données qui traite le même ensemble de données codées doive être considéré comme traitant des données à caractère personnel, si le système spécifique dans lequel ces autres responsables du traitement opèrent exclut expressément la réidentification et que des mesures techniques ont été prises à cet effet »[179].

---

176 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », Commission européenne, Adopté le 1er août 2003, p.5.
177 *Id*.
178 GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis 4/2007 sur le concept de données à caractère personnel », *préc*., note 173, p.17-18.
179 *Id*., p.22.

Le *Groupe de travail Article 29* distingue ainsi le traitement juridique d'un même renseignement, selon les mesures de sécurité appliquées à celui-ci. La logique repose sur le fait que le responsable détenant les clés de déchiffrement devra traiter les données chiffrées comme des renseignements personnels, tandis que les autres employés n'ayant aucunement accès aux clés ne détiendront pas de moyens susceptibles d'être raisonnablement mis en œuvre pour identifier les personnes. En d'autres termes, une donnée pourrait être qualifiée de personnelle ou pas selon le traitement effectué par chaque individu au sein d'une même organisation. Un examen du contexte et des circonstances de chaque situation devra évidemment avoir lieu pour évaluer si un responsable ou toute autre personne détient un tel moyen pour rendre une donnée biométrique identifiable.

En outre, « si des données biométriques, telles qu'un modèle, sont stockées de telle manière qu'aucun moyen raisonnable ne peut être mis en oeuvre par le responsable du traitement ou une autre personne pour identifier la personne concernée, ces données ne sont pas à qualifier de données à caractère personnel »[180]. Ce serait par exemple le cas des données biométriques chiffrées de manière irréversible sans la configuration de la mesure biométrique en question[181]. Dans cette hypothèse, les données ne seraient déchiffrables qu'au moyen de l'acceptation positive de la reconnaissance subséquente de l'individu.

Avec le développement exponentiel de la puissance et de la complexité des nouvelles technologies, il est tout à fait envisageable qu'une donnée personnelle stockée sous forme de formule algorithmique, de codes ou de gabarit puisse être reconstituée par une personne possédant la technologie appropriée. Par exemple, si un individu possédait un logiciel qui permet de reconstituer ou de déchiffrer les renseignements, il se trouverait à avoir accès à ceux-ci sous leur forme originale et, en conséquent, serait en mesure d'identifier la personne

---

180 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », *préc*., note 176, p. 5.

181 Concernant le chiffrement biométrique, voir Ann CAVOUKIAN and Alex STOIANOV, « Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy », March 2007 et Georges J. TOMKO, « Chiffrement biométrique: Nouveautés en biométrie », Discours présenté lors de la *18ième Conférence Internationale de Protection de la vie privée et des données nominatives*, Commissariat à la protection de la vie privée, 19 septembre 1996.

concernée. Une donnée chiffrée et impossible à lire pour une « personne ordinaire » reste possible à déchiffrer pour un individu qui possède certaines compétences et le matériel informatique adéquat.

À titre d'exemple pratique, le commissaire à la protection de la vie privée et de l'information de l'Alberta a déjà conclu qu'un identifiant numérique stocké à la place d'une donnée biométrique originale demeurait un renseignement personnel[182]. Certes, l'entreprise disposait de la technologie lui permettant de déchiffrer les données. De plus, elles étaient combinées à d'autres renseignements personnels, ce qui rendait l'individu identifiable :

> « In the present case, Empire Ballroom uses the numeric identifier representing the thumbprint to identify and track specific employees. The numeric identifier is associated or linked with each employee's name in its computer. I find that the information is therefore personal information, as defined by PIPA, and falls under the purview of the Commissioner »[183].

Dans une autre affaire, un arbitre québécois avait également conclu en ce sens, à l'effet que le résultat binaire obtenu après la conversion algorithmique des mensurations de la main d'un salarié pouvait être considéré comme un renseignement personnel[184].

En définitive, tant qu'il existera une possibilité raisonnable ou sérieuse de relier un renseignement personnel chiffré à un individu, le renseignement devrait être traité par l'organisation comme un renseignement personnel selon les lois applicables. Nous croyons ainsi que (1), une donnée biométrique chiffrée sera considérée comme un renseignement personnel s'il existe une possibilité raisonnable de les décrypter et ce, tant au sein de l'organisation que par un tiers, et que (2) il est probable que les données biométriques chiffrées, mais conservées avec d'autres renseignements personnels sur un même individu,

---

182 OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER, « Report of an Investigation into the Collection and Use of Personal Information, Empire Ballroom (1208558 Alberta Ltd.) », Investigation Report P2008-IR-005, Alberta, August 27th 2008.

183 *Id*., p. 5

184 *Syndicat des travailleurs de Mométal (C.S.N.)* c. *Mométal Inc*., [2001] R.J.D.T. 1967 (T.A.)

soient jugées comme étant des renseignements personnels selon ce qui découle des deux décisions mentionnées ci-haut[185].

Il est cependant difficile de faire valoir qu'un renseignement chiffré et conservé de manière isolé, sans qu'aucun autre renseignement personnel ne soit associé, soit considéré comme un renseignement identifiable et donc personnel. Le tiers ne disposant ainsi d'aucun moyen de déchiffrer les données qu'il conserve n'aurait normalement pas l'obligation de traiter les renseignements comme des renseignements personnels. Toutefois, ces renseignements demeureront personnels à l'égard de l'organisation détenant le contrôle sur ces renseignements et les clés de chiffrement.

Toute la question reposera donc sur le contexte et l'interprétation d'une *possibilité sérieuse* d'identifier un individu au moyen d'un renseignement personnel chiffré, en tenant compte des *moyens susceptibles d'être raisonnablement mis en oeuvre*. Chaque situation factuelle devra être évaluée en tenant compte des circonstances spécifiques et des lois sur la protection des renseignements personnels applicables au domaine de compétence de l'organisation.

Chapitre II. Les risques

Dans ce chapitre, nous traiterons en deux sections les principaux risques pour les droits fondamentaux. En premier lieu, nous mettrons en exergue les risques pour le droit à la vie privé (section 1). Nous verrons alors que c'est ce droit fondamental qui risque d'être le plus atteint de par l'utilisation des technologies biométriques. Ensuite, nous nous pencherons sur le droit à l'intégrité (2.1), le droit à la dignité de la personne (2.2) et, pour finir, nous aborderons brièvement le risque que l'utilisation de la biométrie peut comporter sur la présomption

---

185 *Id.* et OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER, « Report of an Investigation into the Collection and Use of Personal Information, Empire Ballroom (1208558 Alberta Ltd.) », Investigation Report P2008-IR-005, Alberta, August 27th 2008.

d'innocence, soit les présomptions de fiabilité et le renversement du fardeau de la preuve (2.3). Sans minimiser les conséquences possibles de l'utilisation de la biométrie pour les autres droits individuels[186], nous nous attarderons seulement à ces quatre aspects dans le cadre de la présente étude. Nous ferons, pour chaque sujet, un bref rappel des principes applicables et nous étudierons ensuite, pour chacun, les principaux risques que comporte la biométrie.

Certains précédents ont déjà établi que la notion de vie privée incluait celles de dignité et d'intégrité de l'individu[187]. Bien que ces concepts soient liés, nous examinerons ces principes de manière distincte dans le présent chapitre, puisque chacun comporte ses propres subtilités.

Section 1 – Sur le plan du droit à la vie privée

Les institutions vont généralement se défendre de mettre en place un système biométrique en vertu de la nécessité d'y apporter une plus grande sécurité[188]. Même si l'impératif de sécurité renferme une sensibilité indéniable, il se trouve que l'utilisation de la biométrie suscite elle-même de vives interrogations quant aux risques de violation de la vie privée. En effet, le droit à la vie privée n'étant pas un droit absolu[189], il sera généralement défié par un besoin plus fort de sécurité[190]. Le vol et l'usurpation d'identité, le détournement d'usage des données, la surveillance et la circulation des données biométriques à travers le monde sont au nombre des menaces possibles d'atteinte à la vie privée.

---

186 Par exemple, nous croyons que l'utilisation de la reconnaissance faciale pourrait nuire au droit à l'image.

187 Voir *R.* c. *Dyment*, [1988] 2 RCS 417, p. 429 ; *Canada (Commissaire à l'information)* c. *Canada (Bureau d'enquête sur les accidents de transport et de la sécurité des transports),* 2006 CAF 157, [2007] 1 RCF 203.

188 David SAMSON, « La biométrie, un cas d'espèce de l'entrelacement entre sécurité et liberté? », <http://www.implications-philosophiques.org/dossiers/securite/la-biometrie/>.

189 *The Gazette (Division Southam inc.)* c. *Valiquette*, [1997] R.J.Q. 30 (C.A.), p.36.

190 Voir Stanley A. COHEN, « Privacy, crime and terror : legal rights and security in a time of peril », LexisNexis, Ontario, 2005.

Au Québec, le droit à la vie privée est protégé par la *Charte des droits et libertés de la personne*[191] ainsi que par le *Code civil du Québec*[192]. Alors qu'il est expressément mentionné en droit québécois, il n'en est pas ainsi en droit fédéral. Tel qu'il a été mentionné par la jurisprudence, le droit à la vie privée découle des articles 7 et 8 de la *Charte canadienne des droits et libertés,* en étant intimement lié au droit à la sécurité de sa personne et à la protection contre les fouilles et saisies abusives[193]. Les conceptions fédérale et provinciale, bien que différentes dans leur approche, se recoupent à plusieurs égards et seront interprétées de manière analogue pour nous aider à en dégager les éléments essentiels.

Selon plusieurs auteurs, le droit à la vie privée est assez subjectif et difficile à évaluer[194]. Tel que le mentionne Diane Veilleux, ce droit humain est fondé sur l'idée du secret et conférerait le pouvoir d'interdire aux tiers d'avoir accès à sa vie personnelle et de garder l'anonymat [195]. Le droit à la vie privée inclurait également le droit à l'image[196], le droit à l'intimité, ainsi que le droit à l'autonomie dans l'aménagement de sa vie personnelle et familiale[197].

La Cour suprême, dans l'arrêt *R.* c. *Dyment*[198], a dégagé trois dimensions du droit à la vie privée, soient les dimensions spatiale, territoriale et, celle qui nous intéresse davantage, la dimension informationnelle. En citant le Rapport du groupe d'étude fédéral intitulé « L'ordinateur et la vie privée »[199], le juge Laforest a indiqué dans cet arrêt que le droit à la vie privé en matière d'information « découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il

---

191 Art.5, *Charte québécoise*. Notons que la *Charte québécoise* peut uniquement être invoquée entre deux entités privées.
192 Art. 3, C.c.Q.
193 Voir *R.* c. *Dyment*, [1988] 2 R.C.S. 417, *R.* c. *Tessling*, 2004 CSC 67, *Schreiber* c. *Canada (Procureur général)*, [1998] 1 R.C.S. 841, *R.* c. *Beare*, 1988 CanLII 126 (CSC), *R.* c. *Mills*, [1999] 3 RCS 668.
194 Voir Diane VEILLEUX, « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », *Revue du Barreau*, Tome 60, printemps 2000.
195 *Id*., p.7.
196 *Aubry* c. *Éditions Vice-Versa Inc*., [1998] 1 RCS 591
197 *Godbout c. Longueuil (Ville)*, [1997] 3 R.C.S. 844
198 *R.* c. *Dyment*, [1988] 2 R.C.S. 417.
199 *Rapport du Groupe de travail établi conjointement par le ministère des Communications et le ministère de la Justice*, « L'ordinateur et la vie privée », Ottawa : Information Canada, 1972.

l'entend »[200]. La Cour a ajouté que, dans une société comme la nôtre, la conservation de renseignements à notre sujet revêt une importance fondamentale :

> « Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués »[201].

En outre, les conclusions d'un rapport de la Chambre des communes fédérale énoncent que le droit à la vie privée englobe bien plus que le droit d'être seul ou de contrôler ce que les autres disent à notre propos :

> « Canadians view of privacy is far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others – either we trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity »[202].

Ainsi, le droit à la vie privée englobe également le droit à la confidentialité de ses informations personnelles, le droit de choisir comment nous interagissons avec les autres et le droit de ne pas être surveillé, notamment[203]. Un système de reconnaissance biométrique devrait être sensible à cet égard et faire l'objet d'une évaluation pour déterminer dans quelle mesure il risque de porter atteinte au droit à la vie privée des individus, qu'il soit personnel ou informationnel.

Dans un rapport de conclusions d'enquête portant sur l'admissibilité d'un système de reconnaissance du réseau veineux de la paume de la main, le Commissariat à la protection de la vie privée du Canada a estimé que « toutes les mesures biométriques portent plus ou moins

---

200 *R.* c. *Dyment*, *préc.,* note 198.

201 *Id*., par. 22.

202 House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, « Privacy : Where do we draw the line? », *Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, Ottawa, Public Works and Government Services Canada, 1997, p.6.

203 Voir notamment : *Gazette* c. *Valiquette*, EYB1996-6665 (C.A.).

atteinte à la vie privée puisqu'elles supposent la collecte de caractéristiques physiques d'une personne »[204]. Elle a cependant précisé que ce ne sont pas « tous les usages de la biométrie qui portent gravement atteinte à la vie privée »[205]. Selon ces conclusions, le degré d'atteinte à la vie privée dépendrait donc de la nature des données saisies et de l'usage qui en est fait.

Comme nous l'avons mentionné plus haut, certaines caractéristiques biométriques laissent des traces et comporteraient même une connotation négative. Dans une affaire relative à la collecte des empreintes digitales pour l'authentification à un examen d'admission, le Commissariat s'est exprimé ainsi :

> « Par sa nature, la biométrie porte toujours atteinte à la vie privée, dans une certaine mesure. Le LSAC [Law School Administration Council] allègue que les empreintes du pouce portent autant atteinte à la vie privée que les empreintes vocales, que le Commissariat avait considérées comme ne portant atteinte à la vie privée que dans une faible mesure. Cependant, contrairement à une empreinte vocale, une empreinte du pouce a une connotation négative, compte tenu de son lien avec le processus pénal. À mon avis, en raison de ce lien, l'empreinte du pouce porte plus gravement atteinte à la vie privée que l'empreinte vocale »[206]. [Nos soulignements]

L'objectif du LSAC était d'éviter la fraude lors de la passation d'un examen d'admission. Le commissaire a jugé que ceci ne justifiait pas suffisamment la prise d'empreintes digitales et que celle-ci était donc non proportionnelle à l'avantage obtenu pour le LSAC.

Suivant ces conclusions, nous comprenons que le degré d'atteinte à la vie privée sera susceptible d'augmenter lors de l'utilisation d'empreintes digitales pour la reconnaissance biométrique. Une organisation désirant mettre en place un système traitant les empreintes

---

204 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Une candidate au GMAT s'oppose à l'utilisation de la technologie de reconnaissance du réseau veineux de la paume de sa main (Re) », 2011 CanLII 99346 ; COMMISSARIAT À LA PROTECTION À LA VIE PRIVÉE DU CANADA, « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2008-389, Enquête concernant le *Law School Administration Council*, *préc.*, note 129, par. 54.

205 *Id*.

206 COMMISSARIAT À LA PROTECTION À LA VIE PRIVÉE DU CANADA, « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2008-389, Enquête concernant le Law School Administration Council », *préc.*, note 87, para. 54.

devrait alors démontrer que celui-ci comporte des avantages importants, et que l'utilisation d'autres caractéristiques ne permettra pas d'atteindre le même objectif[207]. Par contre, les empreintes vocales pourraient être jugées comme étant peu intrusives sur le plan de la vie privée, selon ce qui découle de cette décision.

La Cour suprême, dans l'arrêt *Oakes*[208], a fourni un test d'évaluation afin de déterminer si l'atteinte à un droit fondamental se justifie dans une société libre et démocratique. La question est de savoir si l'atteinte à la vie privée, de par la mise en place d'un système biométrique, est justifiée compte tenu du besoin de sécurité. Bien que ces critères aient été rendus en vertu du droit fédéral, ils se transposent de manière analogue en droit québécois[209] :

1. Est-il démontré que la mesure est nécessaire pour répondre à un besoin précis?

   Il s'agit ici du test de nécessité, tel que nous le verrons dans la seconde partie du présent mémoire. Le test de nécessité consiste à démontrer que la mesure choisie est nécessaire eu égard aux finalités de l'organisation.

2. La mesure prise répond-t-elle efficacement à ce besoin?

   L'organisation doit démontrer que la mise en place du système de reconnaissance biométrique sera efficace compte tenu du besoin en cause et du degré de certitude qu'apporte la saisie de la caractéristique biométrique. Le taux de défaillance du système sera un critère important[210].

3. La perte au chapitre de la vie privée est-elle proportionnelle à l'avantage obtenu?

   Le principe de proportionnalité exige des organisations qu'elles évaluent la perte relative à la vie privée et aux droits fondamentaux afin de déterminer précisément quels seront les technologies biométriques adéquates et les mesures à être saisies. Le degré d'intrusion pour la vie privée devra être proportionnel à l'avantage obtenu par la

---

207 À cet effet, voir CPVPC, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », *préc.*, note 27.

208 *R.* c. *Oakes,* [1986] 1 RCS 103.

209 Plusieurs doctrines et décisions ont déjà établi ce principe. Voir notamment *Gosselin* c. *Québec (Procureur général),* 1999 CanLII 13818 (QC CA).

210 CPVPC, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », *préc.*, note 27, p.7.

mise en place du système - plus les effets préjudiciables d'une mesure sont graves, plus l'objectif doit être important[211]. De plus, les mesures choisies « doivent être équitables et non arbitraires, être soigneusement conçues pour atteindre l'objectif en question et avoir un lien rationnel avec cet objectif »[212].

4. Existe-t-il un moyen moins envahissant d'arriver au même but?

   L'organisation sera tenue de démontrer que la mise en place d'un système biométrique est le seul moyen nécessaire pour atteindre son objectif et qu'il n'existe pas d'autres systèmes moins intrusifs pour arriver au but fixé.

Suivant cette analyse, nous pouvons conclure que l'analyse de l'ADN aux frontières pour l'authentification des voyageurs serait clairement disproportionnée et non nécessaire par rapport au besoin de sécurité, si fort soit-il. Le choix de la caractéristique utilisée sera un élément judicieux à prendre en compte dans l'évaluation du degré d'intrusion

1.1 La circulation des données et le risque de surveillance accrue

Au 18e siècle, Jeremy Bentham avait imaginé une architecture carcérale invisible, où un gardien de prison espionnait tous les prisonniers[213]. Sans tomber dans une telle caricature oppressive des autorités publiques, la biométrie génère de nouvelles peurs, comme celle d'une éventuelle société de surveillance dans laquelle tous les citoyens sont surveillés, suivis et contrôlés. Caractérisée par la fluidité, la dématérialisation et la déterritorialisation selon certains auteurs[214], cette nouvelle technologie fait ainsi perdre à la frontière son caractère traditionnel et géographique, comme nous allons le voir dans cette section.

---

211 *R.* c. *Oakes, préc.,* note 208.
212 *Id*., par. 70.
213 Jeremy BENTHAM, « Panopticon », 1787.
214 Voir Ayse CEYHAN, « Enjeux d'identification et de surveillance à l'heure de la biométrie », dans *Cultures et Conflits,* Vol. 64, p. 33-47 et Michaël FOESSEL & Antoine GARAPON, « Biométrie : les nouvelles formes de l'identité », *préc*., note 7.

Au regard de la controverse qui secoue actuellement le National Security Agency (N.S.A.) états-unien, nous pouvons assurément appréhender les conséquences éventuelles d'une telle atteinte à nos droits. Les nouvelles technologies détiennent le potentiel de recréer un monde virtuel de traitement d'information de masse. Comme nous l'avons vu ci-haut, le droit à la vie privée englobe celui de pouvoir circuler librement, de façon anonyme et sans constante surveillance[215]. Aujourd'hui, Big Brother[216] n'est plus un personnage fictif, mais une menace bien réelle pour notre droit à la vie privée :

> « Sophisticated, ubiquitous technologies and techniques such as computerized record keeping contain the inherit potential to create immensely wide-ranging and insidious panoptic techniques, thereby increasing the ability of institutions to control people without directing them, using the subtle pressures of internalized discipline. Foucault's conception of the panoptic machine therefore acknowledged the control potential of computers and electronic networks, in which both the distribution of intelligence and the integration of surveillance mechanisms could be concurrently coordinated and controlled ».[217]

En l'occurrence, il est craint que le recours aux technologies biométriques vienne en premier plan des tactiques de surveillance dans les secteurs public et privé[218]. En effet, l'archivage des accès, des lieux et des enregistrements sont au nombre des moyens permettant de suivre les déplacements et de rapidement retracer les individus, en plus de permettre une estimation des parcours futurs[219]. De plus, les procédures de surveillance augmentées par le *USA Patriot Act*[220] accordent au gouvernement américain de généreux pouvoirs d'accès à nos renseignements personnels conservées et donc, nos données biométriques. Tel que le confirme

---

215 Voir la section 1 du présent chapitre.

216 *Big Brother* est un personnage de fiction du roman « 1984 » de George Orwell. L'expression « Big Brother » est utilisée pour qualifier toutes les institutions ou pratiques portant atteinte aux libertés fondamentales et à la vie privée des populations ou des individus [Wikipédia].

217 King RAWLSON, « People fear the future of technological surveillance », Biometric Update.com, 2012. Le philosophe et historien Michel Foucault avait également étudié et exposé une structure de surveillance disciplinaire dans son ouvrage intitulé « Surveiller et punir », Éditions Gallimard, 1975.

218 Voir Ayse CEYHAN, « Enjeux d'identification et de surveillance à l'heure de la biométrie », dans *Culture et Conflits,* Vol. 64, p. 33-47, France, 2006.

219 *Id*.

220 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* « USA Patriot Act ».

un rapport de l'Université d'Amsterdam, les États-Unis auraient accès aux données contenues dans les systèmes infonuagiques appartenant à des entreprises américaines :

> « The U.S. government has ample possibilities to request data from foreign (in this case Dutch) users of the cloud. The most striking example in this regard is the specific provision (50 USC § 1881a) introduced in 2008 for the acquisition of data of non-U.S. persons outside the United States, given the far-reaching powers it grants to retrieve information on a large scale, including access to complete data sets. U.S. authorities also have powers to request information from cloud providers in the context of criminal investigations. Jurisdiction under U.S. law is a necessary precondition, which is effectuated when cloud providers are based in the United States or if they conduct continuous and systematic business in the United States. It is a misconception that U.S. jurisdiction applies only if the data are physically located on U.S. territory »[221].

La « juridiction extra-territoriale »[222] des États-Unis implique que tous les fournisseurs de services infonuagiques opérant n'importe où dans le monde doivent se conformer à des requêtes sur les données qui tombent sous l'application des lois américaines. Ces lois s'appliquent aux fournisseurs dès lors que ceux-ci ont des activités aux États-Unis. Les données ne doivent donc pas être nécessairement stockées sur des serveurs physiquement présents sur le territoire américain pour que le gouvernement puisse y accéder, ce qui implique que nos données biométriques pourront être accessibles par le gouvernement américain dès lors qu'elles seront stockées dans l'infonuagique d'une entreprise américaine.

Notons que les organisations canadiennes peuvent être sujettes à des ordonnances équivalentes à celles du *USA Patriot Act*, les obligeant à communiquer au gouvernement fédéral des renseignements personnels détenus au Canada[223]. En effet, la *Loi antiterroriste canadienne*[224] renferme certaines dispositions qui « renforcent les pouvoirs d'investigation des

---

221 Joris Van HOBOKEN, Axel ANRBAK and Nico Van EIJK, « Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act », Institute for Information Law, University of Amsterdam, November 27th, 2012.

222 *Id*.

223 CPVPC, « Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA PATRIOT Act* », Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-313.

224 L.C. 2001, c. 41

autorités publiques en vue d'assurer la sécurité nationale et, corrélativement, internationale »[225].

D'ailleurs, la circulation des données et le développement de nouveaux systèmes complexes accroît le risque de traçabilité[226] de nos déplacements. Ce risque porte atteinte à notre droit de pouvoir vivre et circuler librement sans être sous constante surveillance. Ce droit, découlant de notre droit à la vie privée[227], se heurtera alors à cette nécessité d'une sécurité dite collective[228]. Selon l'utilisation qui en sera faite, la biométrie pourrait alors entraîner une perte de contrôle de la circulation de l'information personnelle, entraînant à son tour une perte d'autonomie de la personne.

La problématique s'accentue dans le cas où les caractéristiques biométriques sont captées sans le consentement des personnes et à leur insu. En effet, nous pouvons difficilement imaginer une surveillance efficace pour les autorités si la captation des images nécessitait un consentement. De par la manière dont elle est captée, c'est la reconnaissance faciale qui en constitue le plus grand risque. Soulignons toutefois que la majorité des données biométriques comportementales peuvent aussi être saisies à l'insu des personnes, telles que la démarche, la voix, la signature et l'odeur corporelle :

> « It is possible that persons are being identified or authenticated without being aware of it. There are several characteristics, like voice, keystroke, face, and body scent, that can be used in such a way that persons do not notice they are being identified or authenticated. This potentially leads to an undesirable type of secret surveillance »[229].

---

225 Cynthia CHASSIGNEUX, « Quand la sécurité nationale interpelle la protection des renseignements personnels : l'exemple de la USA PatriotAct », dans Service de la formation continue du Barreau du Québec, *Vie privée et protection des renseignements personnels (2006)*, Cowansville, Yvon Blais, 2006.

226 Au Québec, la notion de traçabilité humaine n'a pas encore été définie. L'OQLF ne fournit pas non plus de définition française de la traçabilité humaine, mais la définition anglaise nous apparaît assez juste : Traceability - « Ability to trace the history, application, or location of that which is under consideration », 2009.

227 Nous l'avons abordé à la section précédente. Voir *Aubry* c. *Éditions Vice-Versa inc*., [1998] 1 RCS 591.

228 Voir Ann CAVOUKIAN, « Consumer Biometric Application », *préc*., note 61.

229 Ronald HES, T.F.M. HOOGHIEMSTRA and John BORKING, « At Face Value, on biometrical identification and privacy, Registratiekamer, September 1999, p. 44.

Ces types de caractéristiques sont non seulement biométrisables, mais peuvent au surplus révéler d'autres informations sensibles, tel que nous le verrons au point suivant. Par contre, soulignons que, selon certains auteurs, les technologies actuelles ne seraient pas suffisamment performantes pour identifier des individus à grande échelle en temps réel[230].

En définitive, mentionnons que le NIST (« National Institute of Standards and Technology ») a, en plus de son travail de normalisation, « constitué des bases de tests de millions de données biométriques en provenance du Département d'État, du Département du Homeland Security, du FBI et de différentes autres organisations »[231]. Ceci aurait permis au gouvernement américain de conduire plus de sept campagnes lourdes d'évaluation comparative d'algorithmes de reconnaissance du visage, d'iris et d'empreintes digitales[232]. La volonté de surveillance des autorités publiques irait même plus loin : celles-ci croient pouvoir prédire l'avenir à partir du « forage de données (*data mining*), de la classification, du croisement, du profilage et de l'extraction »[233].

Ainsi, il semblerait que des logiciels soient en cours de développement, afin de déceler, « à partir de multiples sources de données qu'on retrouve notamment sur Internet (courriels, chats, blogues, réseaux sociaux, interrogations aux moteurs de recherche, pratiques de navigation, etc.) », les individus qui « représentent une menace future »[234]. Cette intention a d'ailleurs été soulignée par Didier Bigo et Mireille Delmas-Marty lors de leur participation au colloque international « Vers une intégration du droit à la vie privée et des technologies de sécurité »[235] en octobre 2011 à Montréal. Le risque de surveillance est d'ailleurs intimement lié au risque de détournement d'usage des données, tel que nous le verrons au point suivant.

---

230 Ann CAVOUKIAN, « Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentification, Security AND Privacy », *préc*., note 181, p. 7.

231 OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « La Biométrie », Compte rendu de l'opinion publique du 4 mai 2006, Assemblée nationale, France, p. 27.

232 *Id.,* p. 28.

233 Karim BENYKHLEF et Esther MITJANS, « Circulation internationale de l'information et sécurité », Éditions Thémis, Université de Montréal, 2012, p. X.

234 *Id*.

235 Le colloque a été tenu au Centre de recherche en droit public de l'Université de Montréal, les 17 et 18 octobre 2011.

1.2 Le risque de détournement d'usage

Une des plus inquiétantes menaces pour la vie privée provient du caractère bavard des renseignements biométriques. En effet, les données peuvent contenir beaucoup plus de renseignements personnels que l'unique mesure captée. Par exemple, la lecture de l'iris et de la démarche peuvent indiquer une maladie ou un handicap. La reconnaissance faciale et la lecture de la voix peuvent donner des indications plus ou moins précises sur l'état émotionnel d'une personne au moment de la capture. La synergologie[236] peut aussi être appliquée à la lecture de la gestuelle et du visage, en ayant pour but de savoir si une personne ment ou est dans un état d'agitation excessive[237].

Le risque de détournement d'usage prend de l'importance dès lors que les renseignements personnels sont reliés à d'autres données et que des profils numériques sont créés, ceci étant favorisé par l'essor des technologies de l'information interopérables et qui facilitent l'interconnexion des données[238]. Ainsi, l'information circulant sur le web s'anastomose et permet aux technologies intelligentes de faire les liens de plus en plus complexes. Il est donc possible que des tiers, ou toute autre personne intéressée, accèdent aux données et les relient à d'autres renseignements sans le consentement du propriétaire légitime[239].

Bien qu'elle soit difficile à évaluer, il est important de s'interroger sur la valeur économique des données biométriques. En effet, des renseignements aussi sensibles risquent d'être convoités par des entreprises diverses, afin d'en faire des analyses pour en extraire de

---

236 La synergologie consiste en une « discipline qui a pour objet l'analyse de la communication non verbale ». Notes : « La synergologie étudie les micromouvements du visage et du corps pour pouvoir interpréter les émotions sous-jacentes. Elle utilise pour ce faire des critères de mesure scientifiques » : OQLF, « Synergologie », Grand dictionnaire terminologique, 2008.

237 Voir Mireille HILDEBRANDT, Serge GUTWIRTH, « Profiling the European Citizen: A Cross-Disciplinary Perspectives », Springer, 2008, p.92.

238 Voir : George TOMKO, « Biometrics as a Privacy-Enhancing Technology : Friend or Foe of Privacy ? », Chairman Photonics Research Ontario, Privacy Laws & Business 9th Privacy Commissioners Data Protection Authorities Workshop, Spain, September 15th 1998.

239 Voir Ann CAVOUKIAN, « Consumer Biometric Applications », *préc.*, note 61, p.3.

l'information utile à leurs activités[240]. Par exemple, des compagnies d'assurance ou des institutions financières auraient intérêt à en faire des analyses de risques et des recherches. Des grandes industries ou des compagnies de crédit pourraient aussi être tentées d'avoir accès aux données biométriques à des fins stratégiques et commerciales. Qui plus est, l'utilisation non autorisée de renseignements sensibles pourrait occasionner des contrôles discriminatoires pour les individus[241].

Si on en croit ce qui est dit, les autorités publiques auraient déjà commencé à relier les systèmes biométriques aux banques de données[242]. Si les entreprises privées font de même, nous pouvons imaginer l'ampleur du danger que cela occasionnera, tant sur les plans national qu'international. Même s'il est encore trop tôt pour en évaluer les conséquences, le risque que le profilage électronique suscite une volonté de contrôle est bien réel. À cet égard, l'auteur Georges Tomko a écrit :

> « [B]iometrics also have the ability to track individuals and their transactions, and to be used as a universal identifier which can associate or link various sources of personal information to an individual – in either case – without their consent »[243].

En France, la mise en place de la première banque de données biométriques à finalité administrative relative aux nouveaux passeports biométriques, dénommée *Titres Électroniques Sécurisés* (« TES ») a suscité et suscite toujours de vives inquiétudes. En 2011, le Conseil d'État a confirmé la légalité du décret du 30 avril 2008 prévoyant « la biométrisation du passeport français par le recueil de l'image numérisée du visage ainsi que des empreintes digitales et l'enregistrement de ces données à caractère personnel dans un fichier centralisé »[244]. Il est prévu que les images numérisées des empreintes et du visage soient

---

240 Concernant la valeur économique des renseignements personnels, voir Pierre COLLIN et Nicolas COLIN, « Mission d'expertise sur la fiscalité de l'économie numérique », Ministère de l'économie et des finances, République française, Janvier 2013.

241 Nous verrons les risques de discrimination à la section 2.2 de la présente partie.

242 OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « La Biométrie », *préc*., note 230, p. 28.

243 Max CHASSÉ, *préc*., note 37, p. 26.

244 Serge SLAMA, « Passeport biométrique : le Conseil d'État donne son quitus au « fichage biométrique général de la population du bout des doigts (CE, Ass., 26 octobre 2011, Association pour la promotion de

conservées pendant une durée de 15 ans lorsque le passeport est délivré à un majeur et 10 ans pour un mineur. En outre, une interconnexion du fichier central avec le système d'information Schengen et Interpol a été mise en place[245].

Évidemment, la centralisation des données et l'accès aux données brutes amplifient le risque de détournement d'usage. D'autre part, la durée de conservation des données aura un rôle déterminant à jouer en ce qui à ce risque. Pour reprendre les mots de la Commission de l'éthique, de la science et de la technologie, « moins longtemps les données sont conservées, moins les risques de détournement d'usage son grands »[246].

Comme nous le verrons dans la deuxième partie, la LCCJTI encadre explicitement le risque de détournement d'usage des données biométriques, en prévoyant que tout autre renseignement concernant une 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 »[247].

1.3 Risques d'erreurs et de confusion de l'identité

Les technologies biométriques sont complexes et leur fiabilité ne serait pas à toute épreuve. Effectivement, deux mêmes échantillons biométriques peuvent comporter une importante variabilité. Selon ce que rapporte la Commission d'accès à l'information, il serait en effet « impossible d'obtenir une coïncidence absolue (100 % de similitude) entre le fichier signature créé lors de l'enrôlement et le fichier signature créé lors de la vérification »[248].

---

l'image et a., Association IRIS et a.) », Combats pour les droits de l'homme, LeMonde.Fr, 12 novembre 2011.

245 *Id*.

246 COMMISSION DE L'ÉTHIQUE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « Viser un juste équilibre, Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité », Avis adopté à la 34e réunion de la Commission, Gouvernement du Québec, 12 février 2008, p. xxiv.

247 *LCCJTI*, art. 44.

248 CLUSIF, *préc*., note 58, p.20.

En effet, tout système biométrique comporte un taux de faux rejets (« FRR ») et de fausse acceptation (« FAR »), pouvant varier d'une technologie à une autre. Ces taux peuvent ainsi venir fausser le résultat de la comparaison. Lorsque l'utilisateur soumet son échantillon et que celui-ci n'est pas jugé par le système comme étant suffisamment similaire au modèle stocké, il y a ici faux rejet, puisque l'identité de l'utilisateur n'est pas reconnue. À l'inverse, lorsque l'échantillon soumis est associé par erreur au modèle d'un autre individu, il y a fausse acceptation et donc, confusion de l'identité[249].

Les taux d'erreur vont dépendre du taux de variabilité des lectures, qui peut être modifié par des mesures techniques. Plus le niveau de variabilité sera bas, et plus le risque de faux rejet augmentera. A contrario, plus le niveau de variabilité sera grand, et plus le taux de fausse acceptation augmentera[250]. Ann Cavoukian écrit à ce sujet :

> « It is important to bear in mind that the collection of biometric samples and their processing into biometric templates for matching is subject to great variability. Simply put, biometrics are "fuzzy" – no two samples will be perfectly identical. Facial recognition technologies, for example, are notoriously prone to variability due to different lighting conditions, angle, subject movement, and so forth. This is the reason, for example, that we are asked not to smile in our passport photos. Similarly, numerous factors affect the ability to obtain reliable and consistent fingerprint samples. Among the various biometric types, irises seem to be the most accurate and consistent »[251].

Un point d'équilibre entre les taux de faux rejet et de fausse acceptation doit donc être correctement configuré afin d'éviter autant que possible les problèmes et les erreurs. Ainsi, l'acquéreur du système devra au préalable définir le seuil applicable en tenant compte des finalités et du niveau de sécurité. Par exemple, plus importants sont les enjeux de sécurité et plus haut devrait être fixé le seuil d'acceptabilité. De tels systèmes comporteraient toutefois un plus haut taux de faux rejet. À l'inverse, les systèmes mis en place pour des raisons comportant moins de risques pour la vie privée devraient contenir un taux de fausse acceptation plus élevé.

---

249 CLUSIF, *préc*., note 58, p.7.

250 Voir: Ann CAVOUKIAN and Alex STOIANOV, « Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentification, Security AND Privacy », *préc.*, note 181, p. 7.

251 *Id*.

Comme le mentionne Jean-René Lecerf dans son rapport présenté au Sénat français, les risques d'erreur sont statistiquement accrus sur de grandes populations. En effet,

> « […] la probabilité que deux signatures biométriques soient identiques ou soient si proches que le traitement informatique les confonde est plus importante. En théorie, ce risque met à mal le principe d'unicité qui relie un individu à une donnée biométrique. En pratique, ce problème peut être réglé, la probabilité variant selon la technique utilisée. Ainsi, pour dix points de comparaison, la probabilité de trouver les mêmes points disposés de façon identique sur les empreintes digitales de deux personnes différentes serait d'une chance sur un million et, pour quatorze à dix-sept points, d'une chance sur dix-sept milliards »[252].

Plus le nombre de points de comparaison sera augmenté, et moindre est le risque d'une confusion d'identité. Par contre, le risque de faux rejet sera plus élevé. Afin de remédier à ce problème, des entreprises pourraient être tentées de mettre sur pied un système biométrique impliquant une collecte et une comparaison de multiples données biométriques, communément appelé « multimodal ». La probabilité que deux données ou plus soient faussement rejetées ou faussement acceptées s'en trouve ainsi largement diminuée, ainsi que le risque de confusion des identités.

Or, la problématique pour la vie privée réside dans le fait que non pas une seule donnée biométrique est collectée, traitée et conservée, mais plusieurs. Plus le nombre de données collectées et traitées est élevé, et plus le risque de détournement d'usage augmente.

Par ailleurs, les systèmes biométriques comportent un risque d'échec à l'acquisition. L'échec à l'acquisition se produit lorsque le système ne parvient pas à capturer une image d'une qualité suffisante pour que les données puissent être valablement comparées. C'est notamment le cas lorsque que la caractéristique physique requise par le système est altérée ou lorsque le système n'arrive tout simplement pas à obtenir une qualité suffisante de l'image. Ceci peut poser des difficultés tant pour les entreprises que pour les individus concernés. En

---

252 Jean-René LECERF, *préc.*, note 18, p. 71.

principe, des solutions d'accommodement devraient être mises en place dans le cas où la caractéristique ne peut être saisie[253].

1.4 Le risque de vol et d'usurpation d'identité

Selon certains auteurs, et nous sommes également de cet avis, les données biométriques ne sont pas entièrement privées[254], puisqu'il est possible de s'approprier certaines données, telles que celles du visage ou de l'iris, les empreintes digitales, et même l'ADN[255]. Cette particularité des données biométriques rend leur utilisation risquée, car, contrairement à un mot de passe que l'on peut retenir et qui demeure confidentiel, les données biométriques ne sont pas réellement secrètes et peuvent être collectées pour s'accaparer l'identité d'autrui[256].

Il existe une certaine confusion quant à la signification du vol, de la fraude et de l'usurpation d'identité. En effet, la différence entre les trois concepts n'est pas claire. Selon le Code criminel, le vol d'identité est défini comme suit :

> « 402.2 (1) Commet une infraction quiconque, sciemment, obtient ou a en sa possession des renseignements identificateurs sur une autre personne dans des circonstances qui permettent de conclure raisonnablement qu'ils seront utilisés dans l'intention de commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge ».

---

253 L'adoption de solutions alternatives pour accommoder les cas particuliers d'échec à l'acquisition font partie des mesures de sécurité qu'il est recommandé de mettre en place, surtout en ce qui concerne les systèmes à grande échelle. Voir la conclusion finale du présent mémoire.

254 Voir Jean-Philippe WALTER, « Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé », *26e Conférence internationale des Commissaires à la protection des données et à la vie privée*, Le préposé fédéral suppléant de Suisse, Wroclaw, Pologne, 14-16 septembre 2004, p. 11 et Bruce SCHNEIER, « Biometrics : Truths and Fictions », Crypto-Gram Newsletter, August 15th, 1998, online : <www.schneier.com/crypto-gram-9808.html#biometrics>.

255 *Id*.

256 Voir la section 2.2.1 du chapitre 1 de la présente partie.

La fraude à l'identité suit de près le vol d'identité mais constitue une infraction distincte en vertu du *Code criminel* :

> « 403. (1) Commet une infraction quiconque, frauduleusement, se fait passer pour une autre personne, vivante ou morte :
> *a*) soit avec l'intention d'obtenir un avantage pour lui-même ou pour une autre personne;
> *b*) soit avec l'intention d'obtenir un bien ou un intérêt sur un bien;
> *c*) soit avec l'intention de causer un désavantage à la personne pour laquelle il se fait passer, ou à une autre personne;
> *d*) soit avec l'intention d'éviter une arrestation ou une poursuite, ou d'entraver, de détourner ou de contrecarrer le cours de la justice ».

Quant à l'usurpation d'identité, l'Office québécois de la langue française définit cette notion comme une « fraude qui consiste à collecter et à utiliser des renseignements personnels à l'insu et sans l'autorisation de la victime »[257]. Suivant ces définitions, l'usurpation d'identité semble donc englober les deux concepts de vol et de fraude à l'identité. Nous comprenons que toutes ces notions disposent de leurs propres subtilités, mais nous les confondrons aux fins de la présente étude, car l'objectif est ici d'identifier les risques liés à la collecte illégale des données biométriques et ainsi, de l'identité d'autrui.

Il n'est donc pas impossible qu'un individu collecte les informations biométriques d'un autre individu et se fabrique ainsi une « fausse identité », dans le but de se faire passer pour ce dernier. Au stade de l'enrôlement, un usurpateur pourrait alors fournir des données biométriques piratées et s'approprier l'identité d'une personne, si cette dernière n'est pas enregistrée dans le système. Notons que, comme nous l'avons déjà abordé au chapitre premier de la présente partie, il est tout à fait possible de contrefaire des mesures biométriques de manière artisanale, généralement à partir de traces laissées au passage et copiées[258].

---

257 OQLF, *Grand dictionnaire terminologique*, 2009, *sub verbo*, « Usurpation d'identité ».

258 Voir Tsutomu MATSUMOTO, Hiroyuki MATSUMOTO, Koji YAMADA, Satoshi HOSHINO, « Impact of Artificial *Gummy* Fingers on Fingerprint Systems », Yokohama National University, Japan, 2002.

Par contre, il faudra être relativement bien équipé et disposer de technologies permettant de saisir correctement la donnée et de pouvoir l'utiliser subséquemment. Dans le cas de la reconnaissance de l'iris, ce ne sont pas tous les systèmes qui sont dotés d'une précision telle qu'il soit faisable d'en retirer une image assez nette. Néanmoins, les technologies futures pourraient permettre ce type de subterfuge.

Parmi les autres techniques d'usurpation d'identité, il serait possible de « contourner la capture de l'image biométrique, avant sa conversion en gabarit pour comparaison, en introduisant directement dans le système une image préalablement prélevée, ce qu'on appelle communément « replay attack » ou « attaque par rejeu »[259]. Les données conservées sur un serveur accessible en réseau ou par Internet sont sans doute plus sujettes à ce type de fraude.

Une identité peut également être usurpée par un pirate ayant réussi à accéder à une banque de données et à y insérer ses propres caractéristiques biométriques, associées aux renseignements personnels d'une autre personne. Cette fraude se nomme « substitution attack », qui s'accomplie en remplaçant le gabarit déjà conservé par les données du fraudeur[260]. En outre, il est possible « d'accéder au paramétrage du système et de le régler sur un seuil d'acceptabilité très haut, de manière à ce que toute donnée présentée par le système soit reconnue (tampering) »[261]. La « réponse d'un système biométrique étant toujours binaire, soit vraie soit fausse, il est également possible d'intercepter la communication de cette réponse entre l'application et la capture des données et donner à la réponse la valeur qu'on souhaite (overriding Yes/No response) »[262].

Alors qu'un mot de passe est facilement renouvelable, la donnée biométrique deviendra caduque et ne pourra être réutilisée une fois subtilisée. En effet, les données

---

259 Jean-Baptiste THOMAS-SERTILLANGES, *préc*., note 53, p. 22. Umut ULUDAG and Anil K. JAIN, « Attacks on Biometric Systems: A Case Study in Fingerprints », Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA 48824, p.1.

260 Ann CAVOUKIAN and Alex STOIANOV, « Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy », *préc.*, note 181, p. 12.

261 Jean-Baptiste THOMAS-SERTILLANGES, *préc*., note 54, p. 23.

262 *Id.*

biométriques ont la particularité d'être irrévocables et tout se complique si l'utilisateur légitime se fait pirater ses données[263]. Un utilisateur dont l'identité a été usurpée et réutilisant ses données après coup sera confondu avec son usurpateur. Ainsi, le propriétaire légitime ne pourra plus utiliser ses données fraudées et elles devront être retirées de tout système les ayant conservées, afin d'empêcher qu'elles puissent être réutilisées frauduleusement. Ceci qui signifie que les systèmes biométriques devraient nécessairement permettre la saisie de données biométriques alternatives pour pallier à cette éventualité.

D'ailleurs, certains auteurs recommandent que la reconnaissance biométrique ne soit pas utilisée seule, mais accompagnée d'un autre système de sécurité :

> « [...] biometric data are not very secret. People leave (poor-quality) fingerprints everywhere, and iris images may be captured by a hidden camera. Generally speaking, the more a biometric is used, the less secret it will be. It would be imprudent to rely on a biometric alone, especially if that biometric became used on a global scale (for example, in the biometric identity cards proposed in some countries). One might expect Mafia-owned businesses to collect biometric data in large quantities if there was any potential exploit path »[264].

Section 2 – Sur le plan des autres droits fondamentaux

2.1 Le droit à l'intégrité

Le droit à l'intégrité de la personne est un droit fondamental expressément consacré dans la *Charte des droits et libertés de la personne,* qui dispose d'une double protection :

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

---

263 Estelle CHERRIER, Patrick LACHARME et Christophe ROSENBERG, « Biométrie révocable », *préc*., note 74.

264 Feng HAO, Anderson ROSS and John DAUGMAN, « Combining cryptography with biometrics effectively », Computer Laboratory, Technical Report, no 640, Cambridge University, UK, 2005, p. 4.

46. Toute personne qui travaille a droit, conformément à la loi, à des conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique »[265].

Au fédéral, le droit à l'intégrité physique découle, tout comme le droit à la vie privée, de l'article 7 de la *Charte canadienne des droits et libertés*, qui prévoit que « chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale »[266]. La Cour suprême a d'ailleurs déjà conclu que le droit à l'intégrité physique prévu à la Charte québécoise et celui découlant de l'article 7 de la Charte canadienne était le même[267]. Notons par ailleurs que « chacun a droit à la protection contre tous traitements ou peines cruels et inusités »[268].

Dans un contexte de reconnaissance de l'identité, le principe de protection de l'intégrité corporelle a été réitéré par le législateur québécois à l'article 43 de la LCCJTI, à l'effet que « 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 ». La question suivante doit se poser : la reconnaissance de l'identité au moyen d'une collecte de renseignements biométriques porte-elle atteinte à l'intégrité physique d'une personne? La réponse n'est pas certaine pour tous les types de saisie biométrique. Notons également que, même si certaines techniques étaient jugées comme portant atteinte à l'intégrité, leur utilisation n'en serait pas systématiquement interdite. Nous y reviendrons.

Tel que l'a mentionné la Cour suprême dans l'arrêt *Pohoretsky*, la « violation de l'intégrité physique de la personne humaine est une affaire beaucoup plus grave que celle de son bureau ou même de son domicile »[269]. Mais d'abord, quelle est la portée du droit à l'intégrité de la personne?

---

265 Articles 1 et 46, *Charte des droits et libertés de la personne*, L.R.Q., chapitre C-12.
266 Art. 7, *Charte canadienne des droits et libertés*, 1982, ch. 11 (R.U.), Annexe B.
267 *Chaoulli* c. *Québec (Procureur général)*, [2005] 1 RCS 791, par. 28.
268 *Id.*, art. 12,
269 *R.* c. *Pohoretsky*, [1987] 1 R.C.S. 945, p. 949

Plusieurs arrêts se sont prononcés sur la signification du droit à l'intégrité prévue à la *Charte québécoise*. La Cour suprême, dans l'arrêt *Québec (Curateur public)* c. *SNE de l'Hôpital St-Ferdinand*[270], mentionna que la notion d'intégrité prévue à l'article 1 de la *Charte* va bien au-delà de l'atteinte physique. Elle vise également l'intégrité psychologique, morale et sociale de la personne. La Cour indique que :

> « Le sens courant du mot « intégrité » laisse sous-entendre que l'atteinte à ce droit doit laisser des marques, des séquelles qui, sans nécessairement être physiques ou permanentes, dépassent un certain seuil. L'atteinte doit affecter de façon plus que fugace l'équilibre physique, psychologique ou émotif de la victime. D'ailleurs, l'objectif de l'art. 1, tel que formulé, le rapproche plutôt d'une garantie d'inviolabilité de la personne et, par conséquent, d'une protection à l'endroit des conséquences définitives de la violation »[271].

La Cour distingue ici le droit à l'intégrité physique du droit à l'inviolabilité de la personne[272]. Comme l'indiquaient les Commentaires du ministre de la Justice sur le *Code civil du Québec*, « l'atteinte à l'inviolabilité est le fait de tierces personnes, alors que l'atteinte à l'intégrité peut être le fait de la personne elle-même en raison de ses propres déficiences; les exceptions légales à l'inviolabilité se justifient d'ailleurs par le droit à l'intégrité ». La distinction entre les deux étant difficile à saisir – nous ne nous pencherons donc pas davantage sur le principe d'inviolabilité de la personne.

Dans une autre affaire, la Cour s'est prononcée à l'égard de l'article 7 de la *Charte canadienne des droits et libertés* en concluant que le « droit à la sécurité de la personne protège à la fois l'intégrité physique et psychologique de la personne »[273]. Le juge en chef déclara que pour qu'une atteinte à la sécurité de la personne soit établie, ses répercussions doivent être plus importantes qu'une « tension ou une angoisse ordinaire »[274]. La Cour conclut que le « préjudice d'inconfort temporaire » subi par les bénéficiaires du centre hospitalier,

---

270 *Québec* (*Curateur public)* c. *SNE de l'Hôpital St-Ferdinand*, (1996) 3 R.C.S. 211
271 *Id*.
272 Dominic GOUBEAU et Édith DELEURY, « Le droit des personnes physiques », EYB2008DPP7, par. 98-99.
273 *N.B. (Min. de la Santé)* c. *G. (J.)*, (1999) 3 R.C.S. 46, p. 76
274 *Id*., p. 78

qualifié de *détresse psychologique mineure* par le juge de première instance, ne constituait pas une atteinte au droit à l'intégrité de la personne garanti à l'article premier de la *Charte* »[275].

En ce qui a trait aux prélèvements d'ADN, la Cour d'appel du Québec, dans l'affaire *A.P.* c. *L.D.*[276] mentionna que l'obligation qui était imposée au père de fournir un échantillon d'ADN pour établir sa paternité, constituait bel et bien une atteinte à son intégrité corporelle, « puisque qu'elle l'oblige à fournir une partie (si infime soit-elle) de son corps »[277]. Cependant, les échantillons devant être fournis (cheveux ou salive) comportaient « un degré d'invasion beaucoup moindre que le prélèvement sanguin » et le droit fondamental des enfants de connaître ses parents biologiques était maintenant reconnu. La Cour a donc accueilli la demande d'ordonnance afin que le père fournisse un échantillon de cheveu ou de salive pour confirmer son ADN, même si elle a jugé qu'il s'agissait d'une violation de son droit à l'intégrité.

Plusieurs autres pratiques ont d'ailleurs été interdites par les tribunaux en vertu du droit à l'intégrité physique. Par exemple, l'obligation de fournir un échantillon de sang[278], de recevoir un vaccin[279] ou de se soumettre à des tests psychiatriques[280] sont des pratiques ayant été jugées contraires au droit à l'intégrité de la personne.

Dans un contexte spécifique d'utilisation de la biométrie au travail, il a été décidé, dans la décision arbitrale *Syndicat des salariés de Mométal (C.S.N.)* et *Mométal inc.*[281], que le système de poinçon-main mis en place par l'employeur pour reconnaître l'identité de ses employés ne violait pas le droit à l'intégrité physique prévu à la Charte québécoise. En interprétant la jurisprudence, l'arbitre a conclu le fait de saisir les données de la main ne comportait pas d'atteinte physique durable ou permanente :

---

275 *Id*.
276 *A.P.* c. *L.D*, (2001) R.J.Q. 16
277 *Id.,* p. 24
278 *R.* c. *Dyment*, (1988) 2 R.C.S. 417
279 *Charbonneau* c. *Poupart*, (1990) R.J.Q. 1136 (C.S.)
280 *R* c. *Rogers*, (1991) 2 C.R. (4th) 192 (C.A. C.B.)
281 *Syndicat des salariés de Mométal (C.S.N.)* et *Mométal inc*., D.T.E. 2001 T-919.

> « Selon moi, il y a une distinction significative entre être tenu de fournir un cheveu, un échantillon de salive ou de sang et même des empreintes digitales et le fait de devoir placer une main sur une platine pendant une très brève période de temps. Je ne retrouve pas dans cette exigence le "désaisissement" qui se retrouve dans toutes les affaires mentionnées plus haut »[282].

En outre, l'arbitre a souligné que les conséquences pour l'intégrité physique seront différente, sinon plus importantes, pour le prélèvement des empreintes digitales :

> « À la lumière de cette preuve - et en insistant bien pour dire que ma conclusion aurait été différente pour un système enregistrant les empreintes digitales - je suis d'avis que les salariés ne peuvent soutenir que le fait de placer une de leurs mains sur la platine pendant quelques secondes affecte leur équilibre physique, psychologique ou émotif. De toute façon, il me semble que si une telle atteinte subsistait « […] celle-ci ne serait que fugace et ne dépasserait pas le seuil minimal fixé par la Cour suprême du Canada pour constituer une atteinte à l'intégrité »[283].

Dans l'affaire *Canada Safeway Ltd. and U.F.C.W., Local 401*[284] en Ontario, l'arbitre a rejeté un grief relativement à un système de reconnaissance de la main. Le syndicat invoquait que la collecte et la conservation des données biométriques par l'employeur portait atteinte à la vie privée des employés. Quant à l'employeur, il faisait valoir que le système lui apportait un avantage économique et que les données collectées n'étaient utilisées qu'à des fins internes. L'arbitre a conclu que le système de reconnaissance de la main avait un impact minime sur la vie privée des employés et qu'il n'était pas physiquement intrusif :

> « First, the method by which this personal information is collected, through an infrared scanning device upon which the hand is placed, <u>is not physically intrusive, time consuming, painful or harmful</u>. This distinguishes the hand scanning device from much more physically invasive procedures such as those used to collect blood or urine samples »[285]. [Notre soulignement]

---

282 *Id.*, p. 7.

283 *Id*., p. 8. À l'heure actuelle, il s'agit de la seule décision québécoise ayant été rendue au regard de la biométrie et de l'atteinte à l'intégrité de la personne.

284 *Canada Safeway Ltd.* and *U.F.C.W., Local 401* (2005), 145 L.A.C. (4th) 1

285 *Id*.

L'arbitre a insisté sur le fait que le système n'était ni douloureux, ni nuisible. Il a finalement recommandé à l'employeur de mettre en place une politique de destruction des données une fois la cessation d'embauche des employés. Mentionnons qu'une telle destruction est une obligation légale au Québec en vertu de la LCCJTI[286].

Bien qu'il s'agisse de décisions arbitrales, les deux décisions ci-haut mentionnées nous donnent de bonnes indications sur la manière dont l'évaluation d'un système biométrique pourrait être faite par nos tribunaux. Ainsi, tout dépendant du type de caractéristique saisie, le degré d'atteinte à l'intégrité physique et psychologique sera évalué en fonction des séquelles, des marques, du niveau de nuisance et l'inconfort subi, notamment. À l'exception de la mesure sanguine de l'ADN, la saisie des données biométriques se fait normalement à la surface de la peau ou à distance, comme pour la reconnaissance faciale ou la lecture de l'iris. Elle ne semble donc pas laisser de séquelle ou de dommage permanent pour l'intégrité physique ou psychologique.

Toutefois, il possible qu'un inconfort temporaire et même permanent soit subi par les personnes utilisant un système biométrique. Par exemple, il a été mentionné à quelques reprises[287] que la prise des empreintes digitales renfermait une connotation négative, celles-ci étant assimilées au système de justice pénal. Pour cette raison, l'inconfort subi serait assurément jugé comme étant plus élevé que les autres caractéristiques.

De plus, dans la mesure où la lecture d'une donnée du corps à l'aide de rayons infrarouges avait des conséquences temporaires ou permanentes sur celui-ci, il y aurait de fortes chances qu'elle soit jugée intrusive et contraire au principe d'intégrité de la personne. Nous pensons notamment à la lecture de l'iris et de la rétine, effectuée à l'aide d'un rayon traversant la cornée. En effet, et comme nous l'avons vu au chapitre 1 du présente mémoire, il

---

286 Art. 44, *LCCJTI*.

287 CPVPC, « Une candidate au GMAT s'oppose à l'utilisation de la technologie de reconnaissance du réseau veineux de la paume de sa main (Re) », 2011 CanLII 99346 (CVPC) ; *Syndicat des salariés de Mométal (C.S.N.)* et *Mométal inc*., D.T.E. 2001 T-919.

existe une possibilité qu'un rayon infrarouge mal employé cause des dommages à l'iris ou à la rétine[288].

Par ailleurs, la mesure de la fréquence cardiaque, de la température corporelle et de l'activité cérébrale ont été dénoncées par la *Commission des questions juridiques et des droits de l'homme* du Conseil de l'Europe comme « faisant partie de la vie privée et de l'intégrité physique la plus intime d'une personne »[289]. Sans nécessairement laisser de séquelle ou de marque, nous croyons que la saisie de ces mesures dépasse néanmoins un certain seuil, puisqu'elle pénètre la surface du corps de manière à en retirer l'information qui s'y trouve. Tel que l'a mentionné la Cour suprême du Canada dans l'arrêt *Tessling*, le droit à l'intégrité du corps protège notre droit à ce que celui-ci ne soit pas exploré pour en divulguer des éléments que nous souhaitons dissimuler :

> « Privacy of the person perhaps has the strongest claim to constitution shelter because it protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal »[290].

Pour ces raisons, nous croyons que le degré d'atteinte à l'intégrité de la personne par la saisie d'une partie du corps à des fins de reconnaissance biométrique dépendra essentiellement de la caractéristique saisie et de la technologie utilisée. Précisons néanmoins qu'il est fort probable qu'un système biométrique n'étant ni douloureux, ne laissant aucune marque ou de séquelle temporaire ou permanente et n'affectant aucunement l'équilibre psychologique ou émotif d'une personne soit jugé comme ne portant pas atteinte à l'intégrité.

L'identité numérique et le droit à l'intégrité

La CAI est d'avis qu'une « mesure biométrique est plus qu'un identifiant numérique » car elle livre « des informations personnelles intimes sur la composition de notre corps et sur

---

288 Voir la section 2.2.1 c) du chapitre 1 de la présente partie.

289 ASSEMBLÉE PARLEMENTAIRE, « La nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme », Conseil de l'Europe, Avis no 12528, 23 février 2011.

290 *R*. v. *Tessling*, [2004] 3 SCR 432, par. 21.

notre comportement en général ». Elle s'est d'ailleurs inquiétée de l'utilisation d'un « identifiant intime, unique et universel » qui rend très faciles le croisement des données provenant de multiples sources et le « traçage » des individus[291]. Tel que l'a mentionné le Commissariat à la protection de la vie privée, les données peuvent dresser un profil très détaillé d'une personne, une fois mises en relation :

> « Une donnée prise isolément ne révèle généralement pas grand-chose. Mais une fois regroupées, recoupées et analysées, les données peuvent brosser un portrait extrêmement détaillé d'une personne. Une fois regroupées, ces données peuvent représenter votre identité »[292].

Avec le traitement numérique de la transcription des mesures corporelles, une nouvelle facette du droit à l'intégrité voit le jour. Tel qu'il l'est souligné dans un article de l'Université de Rotterdam aux Pays-Bas, la question du prolongement du corps numérique et de l'intégrité est intimement liée au droit à la vie privée informationnelle, à partir du moment où le corps est utilisé à titre d'information :

> « How can we ensure the integrity of bodies once these bodies assume an extended existence as *information*? This problem becomes all the more poignant because of the possibilities and particularities of digital data processing. The digital rendering of bodies allows forms of processing, of scrolling through, of datamining peoples' informational body in a way that resembles a bodily search. Beyond mere data privacy issues, integrity of the person, of the body itself is at stake here. Legal and ethical measures and protections should therefore perhaps be modelled analogous to bodily searches, and physical integrity issues ».[293]

En effet, toutes les données du corps associées ensemble peuvent servir de base à une reconstitution numérique du corps physique. De ce fait, la mise en relation de données corporelles donne au corps une existence virtuelle, « ce dernier devenant explorable à

---

291 Max CHASSÉ, « La Biométrie au Québec : les enjeux », *préc.*, note 37.

292 Chantal BERNIER, « Un cadre autour des nuages : Défis contemporains en matière de protection des renseignements personnels », Commentaires à l'occasion du colloque québécois sur la sécurité de l'information, Commissariat à la protection de la vie privée du Canada, La Malbaie, Québec, 18 octobre 2010.

293 Irma VAN DER PLEOG, « Genetics, biometrics and the informatization of the body », *iBMG*, Erasmus University MC, Rotterdam and Zuyd University, Heerlen, Ann Ist Super Sanità 2007, vol. 43, No. 1: 44-50, The Netherlands, p. 48.

distance, transférable, dissocié de l'espace et du temps du corps physique »[294]. Ceci est particulièrement vrai dans le cas d'un traitement par le biais d'une base de données, laquelle constitue la porte d'entrée de tout processus visant à créer un profil, à analyser et à reconstituer l'information. Les données du corps ainsi stockées peuvent générer des nouvelles pratiques de traitement de l'information jusque-là insoupçonnées.

Le corps se trouve alors réduit à des paramètres informatiques et son « *rendu digital* sous la forme de fichiers d'ordinateurs, de codes, de modèles enregistrés, d'images dynamiques et de paquets d'informations permet des formes de traitement, d'explorations, d'analyse de l'intimité qui ressemblent à une véritable recherche corporelle »[295]. Un corps physique acquérant une existence virtuelle devient ainsi susceptible d'être atteint dans son intégrité, « le principe d'inviolabilité du corps par référence à la surface de la peau ne suffit pas à protéger ce corps, redéfinit par les usages qui en sont faits »[296]. Ainsi, « la protection de l'intégrité de ce corps informatisé relèvera uniquement d'une protection technique, de politique d'accès et des matrices d'habilitation, en dehors de tout contrôle par le principal intéressé »[297].

La question de la crainte d'une société de surveillance tire entre autres sa source dans l'aspect informationnel du corps physique. Certes, l'exacte nature des frontières du corps humain est difficile à évaluer[298]. Or, bien que la détermination de l'atteinte à l'intégrité doive avoir lieu au cas par cas, il est urgent d'anticiper les conséquences futures de ce paradigme. Nous sommes d'avis que le droit à l'inviolabilité de la personne et à l'intégrité physique doivent être réévalués en fonction du contexte actuel de contrôle des identités.

---

294 Thomas BERTILLANGES, *préc.*, note 43, p.50.
295 *Id*., p.50.
296 *Id*.
297 *Id*.
298 Certains auteurs sont d'avis que les frontières du corps humain sont essentiellement « une question de culture et de conventions », voir Jean-Baptiste THOMAS-SERTILLANGES, « Identification biométrique, protection des données et droits de l'homme », *préc*., note 54, p. 50.

2.2 Le droit à la dignité humaine

Dans son préambule, la *Charte québécoise* déclare que « tous les êtres humains sont égaux en valeur et en dignité et que le respect de la dignité de l'être humain constitue le fondement de la justice, de la liberté et de la paix »[299]. De plus, son article 4 prévoit que « [t]oute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation ».

En revanche, il n'est nullement fait référence au droit à la dignité humaine dans la *Charte canadienne*. Néanmoins, il a été mentionné à maintes reprises par la Cour suprême du Canada que la dignité inhérente à la personne humaine constitue le pilier de la *Charte canadienne des droits et libertés* et qu'il constitue une valeur essentielle à une société libre et démocratique[300]. De plus, la juge Wilson, dans la décision *Morgentaler c. La Reine*[301] a reconnu que « la *Charte* et le droit à la liberté individuelle qu'elle garantit sont inextricablement liés à la notion de dignité humaine » et que « la notion de dignité humaine trouve son expression dans presque tous les droits et libertés garantis par la *Charte* ». Cependant, la Cour suprême a imposé une certaine limite en disant que :

> « Bien que le respect de la dignité inhérente des gens soit nettement une valeur essentielle de notre société libre et démocratique, qui doit guider les tribunaux dans l'interprétation de la *Charte*, cela ne signifie pas pour autant que l'on fait de la dignité un droit constitutionnel distinct […]. Il vaut mieux considérer la notion de *dignité* comme une valeur sous-jacente »[302].

Mais d'abord, en quoi consiste le principe de dignité de la personne? Bien qu'il puisse exister plusieurs conceptions de la dignité humaine, la juge Wilson, dans l'arrêt

---

299 *Charte des droits et libertés de la personne*, Préambule.

300 *R.* c. *Oakes*, [1986] 1 R.C.S. 103,136. Voir également: L. HUPPÉ, « La dignité humaine comme fondement des droits et libertés garantis par la Charte », (1988) 48 *R. du B.* 724-728; COMMISSION DE RÉFORME DU DROIT DU CANADA, « Dignité humaine et patrimoine génétique », document d'étude (sous la dir. de B.M. Knoppers), 1991, p. 35; Daniel PROULX, « Le concept de dignité et son usage en contexte de discrimination: deux Chartes, deux modèles », *Revue du Barreau*, numéro spécial, 2003, p. 485.

301 *Morgentaler c. La Reine*, [1988] 1 R.C.S. 30.

302 *Blencoe* c. *Colombie-Britannique*, [2002] 2 R.C.S. 307, par. 76-80 (j. Bastarache).

Morgentaler[303], a interprété ce principe en rappelant le principe fondamental du respect de soi par les autres :

> « La *Charte* est fondée sur une conception particulière de la place de l'individu dans la société. Un individu ne constitue pas une entité totalement coupée de la société dans laquelle il vit. Cependant l'individu n'est pas non plus un simple rouage impersonnel d'une machine subordonnant ses valeurs, ses buts et ses aspirations à celles de la collectivité. L'individu est un peu les deux. La *Charte* exprime cette réalité en laissant un vaste champ d'activités et de décisions au contrôle légitime du gouvernement, tout en fixant des bornes à l'étendue appropriée de ce contrôle. Ainsi, les droits garantis par la *Charte* érigent autour de chaque individu, pour parler métaphoriquement, une barrière invisible que l'État ne sera pas autorisé à franchir. Le rôle des tribunaux consiste à délimiter, petit à petit, les dimensions de cette barrière »[304]. [Notre soulignement]

Selon l'auteur Daniel Proulx, c'est le principe kantien de dignité humaine qui semble être retenu par les tribunaux comme interprétation de la dignité de la personne[305], signifiant que « [l]'humanité est par elle-même une dignité: l'homme ne peut être traité par l'homme (soit par un autre, soit par lui-même), comme un simple moyen, mais il doit toujours être traité comme étant aussi une fin; c'est précisément en cela que constitue sa dignité (sa personnalité), et c'est par là qu'il s'élève au-dessus de tous les êtres du monde qui ne sont pas des hommes »[306]. En outre, le juge Iacobucci, dans la décision *Law* c. *Canada*[307]*,* a déjà conclu que la dignité humaine était intimement liée à l'estime de soi : « [l]a dignité humaine signifie qu'une personne ou un groupe ressent du respect et de l'estime de soi. Elle relève de l'intégrité physique et psychologique et de la prise en main personnelle »[308].

Comme l'a indiqué la Cour suprême, dans l'arrêt *Québec* (*Curateur public)* c. *SNE de l'Hôpital St-Ferdinand*[309]*,* la dignité humaine « vise les atteintes aux attributs fondamentaux

---

303 *Morgentaler c. La Reine*, [1988] 1 R.C.S. 30, par.224.
304 *Id*., par.224.
305 Daniel PROULX, « Le concept de dignité et son usage en contexte de discrimination: deux Chartes, deux modèles », *préc.,* note 295*,* p.498.
306 Emmanuel KANT, « Fondements de la métaphysique des moeurs », 1785, trad. par V. Delbos, Paris, Vrin, 1980, p. 113.
307 *Law* c. *Canada (Ministère de l'Emploi et de l'Immigration)*, [1999] 1 R.C.S. 497.
308 *Id*., par. 53.
309 *Curateur* c. *SNE de l'Hôpital St-Ferdinand,* [1996] 3 R.C.S. 211.

de l'être humain qui contreviennent au respect auquel toute personne a droit du seul fait qu'elle est un être humain et au respect qu'elle se doit à elle-même »[310]. De plus, la Cour a précisé que le droit à la dignité de la personne, contrairement à celui d'intégrité, n'exige pas l'existence de conséquences définitives pour conclure qu'il y a eu violation :

> « […] l'inconfort souffert par les bénéficiaires, bien que provisoire, constitue une atteinte à la sauvegarde de leur dignité en dépit du fait que ces patients pouvaient ne pas avoir de sentiment de pudeur. Le droit à la sauvegarde de la dignité de la personne garanti à l'art. 4 de la *Charte* vise les atteintes aux attributs fondamentaux de l'être humain qui contreviennent au respect auquel toute personne a droit »[311].

Ainsi, une atteinte « même temporaire à une dimension fondamentale de l'être humain violerait l'art. 4 de la *Charte* »[312]. Dans cette affaire, les bénéficiaires de l'hôpital avaient été privés de certains soins en raison d'une grève illégale, et cette privation avait été jugée comme étant une violation à la dignité humaine.

D'ailleurs, la dignité de la personne fait partie des enjeux soulevés par le Conseil de l'Europe dans son *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques*[313]. Le Rapport fait valoir que la résistance à soumettre son corps à l'identification biométrique « peut dépendre de facteurs socioculturels, religieux ou propres à chaque individu. L'attitude à l'égard de l'utilisation du corps humain par la biométrie pourrait également évoluer avec le temps »[314].

Bien que le concept de dignité humaine soit complexe et abstrait, nous croyons que l'utilisation d'un système biométrique, dépendamment du type de données biométriques saisi, pourrait porter atteinte au droit à la dignité humaine, dépendamment de la manière dont les

---

310 *Id*., par. 105.
311 *Id*., résumé, par. 2
312 *Id*., par.106
313 CONSEIL DE L'EUROPE, « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques », préparé par le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 2005, p. 7.
314 Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, 2005, p. 7

données sont collectées et traitées par la suite. Nous pensons notamment à l'embarras[315] et à l'inconfort que comporterait l'obligation pour les citoyens de se soumettre à la mesure de leur corps pour s'identifier. Comme il l'a été mentionné lors de la *26e Conférence internationale des Commissaires à la protection des données et à la vie privée*[316] :

> « La dignité humaine sera atteinte dès lors qu'un être humain est réduit à un objet et à un moyen qui débouche sur un dénigrement de son identité personnelle. Tel peut être le cas lorsque des données biométriques sont prélevées sous contrainte, lorsqu'il y a des risques de connecter des données provenant de différentes sources, lorsque l'individu n'a aucun contrôle sur ce qui se passe avec les données le concernant ou lorsque des données supplémentaires sont prélevées au moment du traitement des données biométriques. Par exemple, un système d'accès basé sur le scan de la rétine qui mesurerait en même temps si l'employé a consommé de l'alcool ou des drogues et qui le cas échéant bloquerait l'accès aux installations »[317]. [Notre soulignement]

Dans son Rapport relatif à la nouvelle carte d'identité nationale en France[318], la Commission nationale consultative des droits de l'homme[319] souligne que :

> « […] non seulement la collecte de ces éléments représentatifs touche la dignité humaine en ce qu'elle réduit chacun à l'extraction de son patrimoine biologique, mais de surcroît, le caractère unique du lien rattachant la donnée biométrique à son porteur et l'intangibilité supposée de ce lien conduisent à bien peser la gravité de l'enjeu »[320].

Qui plus est, la saisie de certaines données biométriques comporte un risque de traitement discriminatoire. Nous l'avons vu, les données biométriques peuvent renfermer beaucoup plus de renseignements que la donnée en elle-même. De ce fait, le caractère «

---

315 Voir Roger CLARKE, « Human Identification in Information Systems: Management Challenges and Public Policy Issues », Published in *Information Technology & People* 7,4 (December 1994) 6-37.

316 Jean-Philippe WALTER, « Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé », *26e Conférence internationale des Commissaires à la protection des données et à la vie privée*, Le préposé fédéral suppléant de Suisse, Wroclaw, Pologne, 14-16 septembre 2004, p. 4.

317 *Id*.

318 *Problèmes posés par l'inclusion d'éléments biométriques dans la carte nationale d'identité : contribution de la CNCDH au débat*, Avis adopté par l'assemblée plénière du 1er juin 2006 : <http://www.ines.sgdg.org/spip.php?article62>.

319 La Commission nationale consultative des droits de l'homme (« CNCDH ») est une institution nationale de promotion et de protection des droits de l'Homme en France.

320 CNCDH, *préc*., note 318.

parlant » de la donnée biométrique engendre un risque que des individus soient discriminés sur la base d'informations découlant de leurs données, car certaines données permettront de connaître l'origine raciale, l'état de santé et le handicap, notamment. Toute discrimination fondée sur la nationalité, le sexe, le statut civil, l'état de santé, le handicap, l'orientation sexuelle, l'âge, les opinions politiques et la religion sont interdites en vertu des chartes[321] et contraires au principe de dignité humaine.

D'autre part, ceux et celles dont les données sont illisibles, comportent des défauts ou offrent une faible qualité d'image pourraient se retrouver exclus de l'utilisation de certains systèmes biométriques[322]. Selon la Commission canadienne des droits de la personne, la création de documents d'identité fondés sur la biométrie « devrait être mise au point de façon à permettre la participation du plus grand nombre de personnes. Lorsqu'il existe des limites technologiques, il faut envisager d'autres moyens et (ou) des moyens supplémentaires de mesurer les paramètres »[323]. Il faut ainsi éviter de créer une sous catégorie d'individus non identifiables.

Notons que l'âge, les conditions de travail et d'autres formes d'invalidité sont des facteurs qui peuvent « réduire la qualité de l'image des empreintes digitales au point de la rendre inutilisable »[324]. Même si les systèmes uni-modaux peuvent offrir des alternatives, comme un autre doigt pour l'utilisation des empreintes digitales, il est généralement recommandé d'utiliser des systèmes où une mesure est saisie par défaut, mais dont il est possible de saisir un autre type de caractéristique pour les traitements spéciaux[325]. Parmi ses autres avantages, l'usage de deux modalités permettrait de réduire le taux d'échec à l'acquisition et rendrait plus difficile la falsification[326].

---

321 Articles 10, 12, 19, 20, 20.1, *Charte québécoise;* Art. 15, *Charte canadienne.*

322 Nous avons abordé cette question à la section 2.2 du chapitre 2 de la première partie.

323 Caleb CHEPESIUK, Mark KARPINSKI et Charles THÉROUX, « La certification de l'identité et la protection des droits de la personne », Commission canadienne des droits de la personne, août 2010, p. 35.

324 *Id.*, p. 38.

325 *Id.*, Voir aussi OCDE, *préc.*, note 76 et OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « La Biométrie », *préc.*, note 231.

326 *Id.*, p. 23.

Pour contrer ce risque, tout système mis en place devrait comporter des mesures d'adaptation pour les personnes dont il est impossible de capter la donnée. Par exemple, le gouvernement américain a déjà mis en place un système recueillant à la fois les empreintes digitales et les données du visage, au cas où un employé ne pourrait se faire identifier par ses empreintes[327]. Les systèmes multimodaux peuvent ainsi constituer une mesure d'adaptation, étant normalement paramétrés « de façon à tenir compte des personnes chez qui une certaine caractéristique est absente ou qui possèdent une caractéristique non lisible dès l'abord »[328].

Cependant, l'utilisation d'un système multimodal de reconnaissance biométrique peut également hausser le risque de détournement d'usage des données, si plus d'une caractéristique est saisie et conservée. De la sorte, l'utilisation de ces systèmes aura pour effet d'augmenter à la fois le risque de violation d'un droit particulier tout en étant plus favorable au respect d'un autre droit fondamental. Au lieu de tourner en rond, il y aura lieu de bien peser le pour et le contre lors du choix du système, de manière appropriée aux besoins de l'organisme et en prenant soin d'évaluer l'ampleur de tous les risques associés au système convoité.

Une obligation d'adaptation pourrait également servir d'accommodement pour les personnes soulevant une objection à la saisie d'une mesure[329]. La Commission canadienne des droits de la personne juge que les fournisseurs de services et les employeurs ont l'obligation de mettre en place des mesures d'accommodement aux personnes protégées en vertu de la *Loi canadienne sur les droits de la personne*[330], sauf si cela leur impose une contrainte excessive[331].

---

327 *Id*., Voir aussi: Babita GUPTA, « Biometrics: Enhancing Security in Organizations », IBM Center for the Business of Government, 2008, p. 27.

328 *Id.*

329 Caleb CHEPESIUK, Mark KARPINSKI et Charles THÉROUX, « La certification de l'identité et la protection des droits de la personne », *préc*., note 323.

330 *Loi canadienne sur les droits de la personne*, L.R.C. (1985), ch. H-6.

331 *Id*., p. 34.

Par exemple, dans l'affaire arbitrale *407 ETR*[332], des employés s'étaient opposés à la lecture de la géométrie de leur main droite en raison de leurs convictions religieuses. L'employeur leur avait alors permis d'utiliser leur main gauche au lieu de leur main droite pour saisir leurs données. Cette mesure d'accommodement uni-modale n'a toutefois pas été considérée suffisante de l'avis de l'arbitre, qui a jugé que le lecteur biométrique exerçait « de la discrimination à l'endroit des plaignants sur la base de leurs convictions religieuses »[333]. L'arbitre a aussi conclu que l'employeur ne subissait pas de contrainte excessive à cet égard.

Nous souhaitons ici attirer l'attention sur le fait que l'atteinte à la dignité humaine est un concept général et complexe qui devra être évalué au cas par cas en tenant compte de nombreux facteurs. Nous sommes cependant d'avis qu'en raison du caractère intrusif de certains systèmes et de tous les risques que renferme son utilisation pour les droits fondamentaux, le fait de se soumettre à un dispositif biométrique contre volonté porte atteinte à la dignité humaine. De plus, nous croyons que la perte éventuelle d'autonomie de la personne, la perte de contrôle sur la circulation de nos renseignements biométriques et le risque de création de profils numériques sont des enjeux trop importants pour ne pas être pris en considération par nos tribunaux.

2.4 Les présomptions de fiabilité et le renversement du fardeau de la preuve

Lors de la Journée mondiale des Droits de l'Homme qui a eu lieu le 10 décembre 2013, plusieurs auteurs, dont 5 lauréats du Prix Nobel, ont lancé un appel pour la défense des libertés fondamentales au regard de la surveillance organisée par les entreprises et les gouvernements[334]. Une de leurs conclusions était à l'effet que « la surveillance des masses

---

332 *407 ETR Concession Co.* v. *CAW-Canada Local 414.* [2007] L.V.I. 3701-1.

333 *Id*.

334 LE NOUVEL OBSERVATEUR, « Pétition | Les écrivains contre la surveillance de masse », 10 décembre 2013, en ligne. Les 5 Prix Nobel signataires sont: Orhan Pamuk, J.M. Coetzee, Elfriede Jelinek, Günter Grass et Tomas Tranströmer.

traite chaque citoyen comme un suspect potentiel. Elle remet en question un de nos triomphes historiques : celui de la présomption d'innocence »[335]. Ils n'ont pas tort.

La présomption d'innocence est un principe fondamental adopté par la plupart des pays démocratiques. Selon la Charte québécoise, « tout accusé est présumé innocent jusqu'à ce que la preuve de sa culpabilité ait été établie suivant la loi »[336]. La Charte canadienne va évidemment dans le même sens[337]. Sans nous pencher en profondeur sur le principe de la présomption d'innocence, nous donnerons un aperçu du risque que pose l'utilisation de la biométrie pour cette liberté fondamentale.

Selon certains auteurs, il est possible que, à terme, une présomption de fiabilité des systèmes biométriques se développe[338]. Les autorités pourraient ainsi vouer une confiance aveugle aux technologies biométriques et, ainsi, rejeter le fardeau de la preuve sur l'usager. La commissaire à la vie privée en Ontario s'exprime ainsi :

> « Use of biometric identification is interpreted by some as a questioning of their reputation and trustworthiness. They perceive a requirement to give a biometric as a reversal of the presumption of innocence – as shifting the burden of proof »[339].

Tel que nous l'avons vu à la section précédente, une personne victime d'une erreur du système, d'un piratage de ses données ou d'une usurpation d'identité pourrait devoir apporter la preuve qu'elle est bien la personne qu'elle prétend être. Bien que la présomption d'innocence soit prévue à nos Chartes, aucune disposition précise n'a été adoptée par le législateur québécois pour remédier à cette problématique. En raison du peu d'écrit à ce sujet en droit québécois et canadien, nous souhaitons mettre en lumière les observations du *Groupe de travail Article 29 sur la protection des données* en Europe :

---

335 *Id*.
336 Art. 33, *Charte québécoise.*
337 Art. 11d), *Charte canadienne* : « Tout inculpé a le droit (…) d'être présumé innocent tant qu'il n'est pas déclaré coupable, conformément à la loi, par un tribunal indépendant et impartial à l'issue d'un procès public et équitable ».
338 Voir Max CHASSÉ, *préc*., note 37, p. 28.
339 Ann CAVOUKIAN, « Consumer biometric application », *préc*., note 61, p. 30.

> « A priori, l'utilisation de données biométriques […] pourrait donner l'illusion que l'identification ou l'authentification/vérification de la personne concernée est toujours correcte. Il peut être difficile, voire impossible pour la personne concernée d'apporter la preuve du contraire. Ainsi, un système pourrait identifier erronément une personne comme quelqu'un qui ne doit pas être autorisé à monter à bord d'un avion ou à entrer dans un pays donné, et cette personne n'aura guère la possibilité de résoudre le problème lorsqu'une telle preuve "incontestable" lui sera opposée »[340].

Ainsi, l'Europe a adopté des dispositions avant-gardistes afin d'atténuer ce risque, lesquelles prévoient que « toute décision produisant des effets juridiques à l'égard d'une personne ne doit être prise qu'après vérification du résultat du traitement automatisé »[341], selon la directive 95/46/CE :

> « 1. Les États membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.
>
> 2. Les États membres prévoient, sous réserve des autres dispositions de la présente directive, qu'une personne peut être soumise à une décision telle que celle visée au paragraphe 1 si une telle décision:
>
> a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime
>
> ou
>
> b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée »[342].

Le même principe est explicitement repris en France, selon la *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* :

---

340 GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », *préc.*, note 176, p. 10.

341 *Id*.

342 Art. 15, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.

> « Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.
>
> Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée »[343].

À moins que des règles similaires ne soient adoptées au Québec, un usager pourrait être obligé d'« assumer le poids des erreurs éventuelles commises par un système biométrique »[344] ou d'une usurpation d'identité. Ainsi, des mesures devraient être prises à cet égard lors de chaque étape de reconnaissance de l'identité, pour protéger les personnes contre le renversement du fardeau de la preuve.

****

L'acceptabilité sociale de la technologie biométrique est cruciale pour assurer le succès de son implantation. Les organisations souhaitant s'en prévaloir, qu'elles soient publiques ou privées, devront bien définir le projet convenu et les risques qui en découle. Nous l'avons vu, le vol d'identité, les risques d'erreurs, le détournement de finalités et la circulation des données biométriques sont au nombre des enjeux liés à la vie privée et à la sécurité des renseignements biométriques. Bien que la liste des problèmes de sécurité puisse être longue, il ne faut pas négliger l'importance d'une bonne gestion des systèmes, puisque chaque incident de sécurité engendre un risque de violation des droits fondamentaux.

---

343 Article 10, *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

344 INSTITUT DU NOUVEAU MONDE, « Rapport de la conférence citoyenne sur la biométrie et la sécurité », *préc.*, note 42, p. 20.

SECONDE PARTIE – Cadre juridique de l'utilisation de la biométrie : le cycle de vie des données biométriques et leur protection

Dans cette partie, nous évoquerons les diverses dispositions faisant partie du paysage législatif québécois en matière de sécurité des données biométriques. Au chapitre un, nous décrirons les règles spécifiques à la collecte des données biométriques relatives aux tests de nécessité et de proportionnalité, ainsi qu'au consentement et aux mesures de sécurité appropriées. Au deuxième chapitre, nous décrirons les conditions applicables à chaque étape de traitement des données biométriques, soit celles relatives à leur utilisation, leur conservation, leur transmission et leur communication, à leur l'accès et à leur destruction. En outre, nous mentionnerons, pour chacune des étapes énumérées, les mesures de sécurité que nous croyons appropriées pour protéger adéquatement les données biométriques, selon les conclusions que nous avons obtenues de nos recherches.

Chapitre I. Conditions relatives à la collecte

La collecte des données biométriques implique deux évènements. Le premier a trait à la première collecte, soit celle ayant lieu lors de l'enrôlement et du premier enregistrement, et le deuxième concerne toutes les collectes subséquentes de l'individu servant à procéder à la reconnaissance de son identité. En pratique, le contexte dans lequel la première collecte aura lieu sera crucial : il déterminera les conditions dans lesquelles les caractéristiques seront saisies subséquemment. Nous verrons, dans un premier temps, les conditions préalables à l'enrôlement et, ensuite, les règles relatives aux mesures de sécurité applicables lors des collectes subséquentes.

Section 1 - Conditions préalables à la collecte

Avant qu'une organisation procède à la mise sur pied d'un système biométrique, certaines conditions sont exigibles afin que celle-ci soit jugée légitime. En premier lieu, l'organisation devra passer les tests de nécessité et de proportionnalité[345]. Selon le système choisi, les conséquences relatives aux droits fondamentaux varieront et une telle évaluation devra être faite en examinant les besoins de l'entreprise, l'atteinte à la vie privée et les conditions dans lesquelles les données seront collectées et traitées. En second lieu, la collecte sera aussi assujettie au consentement de l'individu[346]. Précisons que ces conditions sont cumulatives, et que, en principe, les tests de nécessité et de proportionnalité ne pourront être contournés au moyen du consentement[347].

1.1 Les tests de nécessité et de proportionnalité

Tel qu'introduit dans la première partie[348], les principes de nécessité et de proportionnalité sont des principes jurisprudentiels découlant des critères imposés par la Cour suprême du Canada dans l'arrêt *Oakes*[349], en matière de violation d'un droit garanti par la *Charte canadienne*. Le critère de nécessité pour la collecte des renseignements personnels a d'ailleurs été explicitement prévu par le législateur québécois dans la LPRPSP. En effet, « 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 »[350] et « ne doit recueillir que les renseignements nécessaires à l'objet du dossier »[351]. Le principe est également repris à l'article 64 de la *Loi sur l'accès*[352] et dans le *Code civil du Québec*, lequel prévoit :

---

345 *R.* c. *Oakes*, *préc*., note 208. Voir la section 1 du chapitre 2 de la première partie.
346 Art. 44, *LCCJTI*.
347 Pierre TRUDEL, « Introduction à la *Loi concernant le cadre juridique des technologies de l'information* », Cowansville, Yvon Blais, 2012, p. 176.
348 Voir chapitre 2, section 1.1
349 *R.* c. *Oakes*. Voir première partie, chapitre 2, section 1.
350 Art. 4, *LPRPSP*.
351 Art. 5, *LPRPSP*.
352 Art 64, *Loi sur l'accès* : « Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel 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.

> « 37. Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation ».

Autrement dit, une organisation qui souhaite recueillir des renseignements biométriques devra démontrer que la collecte est nécessaire et pertinente à son objectif[353]. Notons que, à l'exception de la décision arbitrale *Syndicat des salariés de Mométal (C.S.N.)* et *Mométal inc.*[354], qui évoque le principe en matière de droit à l'intégrité, aucune autre décision québécoise n'a été rendue à ce jour relativement à l'application des tests de nécessité et de proportionnalité dans un contexte de collecte de données biométriques.

Pour les besoins de l'analyse, nous avons donc évalué quelques cas canadiens et français dont nous pouvons nous inspirer, puisque les principes découlant de ces tests sont similaires. En effet, la LPRPDE fédérale indique que « [l]'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances »[355]. En France, la *Loi Informatique et Libertés* prévoit que les données personnelles « sont collectées pour des finalités déterminées, explicites et légitimes » et « elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs »[356].

> Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.
> La collecte visée au deuxième alinéa s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission ».

353 Voir CAI, « La collecte de renseignements personnels », en ligne : <http://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/>.

354 *Syndicat des salariés de Mométal (C.S.N.)* et *Métalinc*., D.T.E. 2001 T-919.

355 Art. 5(3) *LPRPDE*.

356 Art. 6, *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Le principe de nécessité requiert ainsi, d'une part, que la collecte de la donnée soit indispensable à l'objectif poursuivi et, d'autre part, qu'il n'existe pas d'autres alternatives moins intrusives pour la vie privée pouvant satisfaire au même objectif[357]. Le « caractère indispensable des renseignements recueillis » est un principe d'application adopté par la CAI[358] en matière de biométrie et prévoit une série de questions ayant pour but de déterminer si un organisme se conforme à la législation en vigueur[359]. À cet effet, la CAI mentionne :

> « Tout organisme public qui désire utiliser la biométrie doit s'assurer que les données biométriques personnelles et autres renseignements personnels recueillis sont nécessaires à ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. Dans le secteur privé, les renseignements recueillis doivent être nécessaires à l'objet du dossier constitué. La nécessité signifie que les renseignements recueillis sont indispensables »[360]. [Notre soulignement]

La Commissaire à la protection de la vie privée de l'Ontario, Ann Cavoukian[361], a publié plusieurs avis relativement à l'application du test de nécessité dans un contexte d'utilisation de la biométrie. Entre autres, elle a émis l'opinion que la commodité que comporte l'utilisation de la biométrie ne devrait pas être considérée comme une raison suffisante à l'implantation d'un tel système[362]. Les organisations devraient être en mesure de fournir une explication claire de l'objectif poursuivi, des avantages du système, des inconvénients qu'apportent les solutions alternatives et les raisons pour lesquelles il a été décidé que les besoins du système l'emportaient sur les atteintes potentielles à la vie privée[363]. De plus, elle ajoute qu'il doit être tenu compte du contexte dans lequel oeuvre l'organisation pour en évaluer la nécessité. Par exemple, il sera selon elle plus probable qu'un système destiné à contrôler l'accès à une centrale nucléaire soit jugé plus approprié dans les circonstances qu'un centre sportif. À cet effet, elle précise :

---

357 Voir Première partie 1, chapitre 2, section 1.1 du présent mémoire.

358 COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec: les principes d'application, pour un choix éclairé », 2002, p.2.

359 *Id.*

360 *Id*.

361 Ann CAVOUKIAN, Ph.D. est Commissaire à l'information et à la protection de la vie privée de l'Ontario (Information and Privacy Commissioner of Ontario).

362 Ann CAVOUKIAN, « Fingerprint Biometrics: Address Privacy Before Deployment », November 2008. Information and Privacy Commissioner of Ontario. p.11.

363 *Id.*

> « This is not to say that deployment at a health club is necessarily inappropriate; rather, it should be understood that such a use will require significant justification. Questions that should be addressed might include: What is the *problem* being solved by such a system? Have other alternatives been considered? Would alternatives be more or less privacy invasive? [...] Do other, similar institutions face similar problems? If so, what solutions have been deployed? Are biometrics common in this situation?...and so forth »[364].

Afin d'en illustrer l'application, il a été soutenu par une entreprise, dans la décision arbitrale *407 ETR Concession Company Limited and National automobile, Aerospace, Transportatio*n and *General Workers Union of Canada, Caw-Canada and it's Local 414*[365], qu'elle avait mis en place un système de reconnaissance de la main afin d'augmenter la sécurité de ses employés et de ses équipements. Or, la preuve a démontré que l'entreprise avait un intérêt équivalent sinon supérieur à contrôler les horaires de travail et à établir une meilleure gestion des ressources humaines. L'arbitre a indiqué que, même si l'entreprise pouvait subir à l'occasion des menaces de dommages sérieux, augmenter le niveau de sécurité n'était pas requis, celle-ci n'étant pas une centrale nucléaire ou une manufacture d'armements. Ainsi, la mise en place du système biométrique n'a pas été justifiée au regard des objectifs, et un système de sécurité fonctionnant par le biais de mots de passe et de cartes d'accès a été jugé efficace et propre à assurer une sécurité adéquate selon la vocation de l'entreprise et les finalités suggérées par celle-ci.

En plus de devoir démontrer que le système est nécessaire selon ses besoins de sécurité, un organisme collectant les données biométriques d'une personne ne devra recueillir que le « minimum de caractéristiques permettant de la relier à l'action qu'elle pose »[366], selon ce qui est prévu à la LCCJTI :

> « 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

---

364 *Id.*

365 *407 ETR Concession Company Limited and National automobile, Aerospace, Transportatio*n and *General Workers Union of Canada, Caw-Canada and it's Local 414,* 2007 Canlii 1857 (ON LA).

366 Art. 44, al.1, *LCCJTI.*

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 ».

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.

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 ». [Notre soulignement]

Le caractère minimal de la prise de mesures devra être évalué en fonction de la nature de l'action accomplie par l'individu. Le terme *action* semble ici renvoyer à la finalité de la prise de mesures biométriques, soit l'identification ou l'authentification, bien qu'il puisse être interprété plus largement. Cet article vient donc limiter les abus qu'il pourrait y avoir au niveau de la prise de mesures qui ne seraient pas légitimes compte tenu de du véritable objectif. La collecte de données multimodale, que nous avons évoquée dans la première partie[367] semble également être encadrée par le législateur selon cette disposition. De ce fait, une entreprise ne pourra, même si la collecte de données biométriques lui est indispensable, prélever plus de données que cela lui soit strictement nécessaire.

D'autre part, il y aura donc lieu de déterminer si le système choisi est proportionné par rapport au réel besoin de sécurité. La mise sur pied du système nécessitera que celui-ci passe aussi ce test, en démontrant que la perte subie par rapport à la vie privée est proportionnelle à l'avantage obtenu par le système. L'objectif doit donc être assez important pour qu'il puisse porter atteinte au droit à la vie privée. Toutes ces questions serviront à faire la lumière sur les réels objectifs de l'organisation souhaitant se prévaloir d'un système biométrique.

---

[367] Voir la section 1.1.3 du chapitre 2 de la première partie.

Dans le résumé de conclusions d'enquête n° 2004-281 du CPVPC[368], le commissaire à la protection de la vie privée devait évaluer l'équilibre entre les besoins d'un employeur et l'atteinte à la vie privée d'employés. L'employeur avait donné trois raisons pour justifier la mise en place d'un système de reconnaissance vocale, soient la protection, la rentabilité et l'efficacité. Il alléguait que le système renforçait la sécurité, compte tenu du nombre de données sur les clients qu'il devait gérer, et qu'il était « extrêmement important d'empêcher les personnes non autorisées d'avoir accès à l'information »[369].

L'employeur avait déterminé que ce système offrait le niveau le plus élevé de protection en ce qui concerne les données sur les clients entrées au moyen des applications de gestion. Il a en outre précisé que les empreintes vocales des employés étaient sauvegardées dans une base de données protégée se trouvant dans un endroit « rigoureusement contrôlé », et que l'accès à celle-ci est était limité à un nombre restreint de personnes autorisées à entendre ou à supprimer un enregistrement d'empreinte vocale.

De plus, ces personnes ne pouvaient nullement modifier, interpréter ou remplacer l'enregistrement, « et l'empreinte vocale ne peut faire l'objet d'une rétroconception pour synthétiser une voix »[370]. Selon l'employeur, il était donc impossible que la voix soit utilisée d'une manière frauduleuse et il n'y avait « aucune autre utilisation possible de l'empreinte vocale d'une personne sans qu'elle le sache et qu'elle y consente »[371]. À cet égard, la Commissaire adjointe a convenu que :

> « [l]e système était plus efficace et plus rentable que la gestion des mots de passe et les méthodes fondées sur le papier, et qu'il était logique de la part d'une entreprise de vouloir réaliser des économies et d'améliorer son efficacité afin d'affronter la concurrence et de rester en affaires. Cependant, l'argument le plus convaincant était que le mot de passe vocal permettait d'assurer la protection des données. L'entreprise a évalué le risque associé à la gestion d'un grand nombre de données sur les clients et a conclu que le système offrait la plus grande protection contre un accès non autorisé.

---

368 CPVPC, « Une organisation utilise la biométrie à des fins d'authentification », Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2004-281, en ligne : <http://www.priv.gc.ca/cf-dc/2004/cf-dc_040903_f.asp>.

369 *Id*.

370 *Id*.

371 *Id*.

> Une telle approche visait à protéger les renseignements personnels des clients et à répondre aux attentes de ceux-ci à cet égard »[372]. [Notre soulignement]

Néanmoins, elle a reconnu que l'entreprise collectait des données biométriques comportementales et physiques faisant l'unicité de la voix d'une personne et que l'empreinte vocale était une atteinte à la protection des renseignements personnels. Or, la Commissaire adjointe n'a pas conclu que l'empreinte vocale, dans le contexte des plaintes[373] en question, dévoilait beaucoup de renseignements sur la personne. L'entreprise a ainsi démontré, à la satisfaction du Commissariat, que, « sur le plan technique, elle ne pouvait utiliser l'empreinte vocale qu'à des fins d'authentification compte tenu de la configuration actuelle. Elle ne pouvait pas s'en servir pour la surveillance ou d'autres fins répréhensibles »[374]. De l'avis du CPVPC, l'empreinte vocale ne semblait donc pas violer indûment la vie privée, et un juste équilibre entre le droit à la vie privée des employés et les besoins de l'employeur avait été atteint.

Dans le cadre de l'adoption du nouveau passeport biométrique en France, la CNIL avait jugé nécessaire la collecte des données biométriques eu égard aux finalités prévues, si celles-ci étaient toutefois conservées sur un support portable :

> « À cet égard, la Commission tient à rappeler qu'elle considère comme légitime le recours, pour s'assurer de l'identité d'une personne, à des dispositifs de reconnaissance biométrique dès lors que les données biométriques sont conservées sur un support dont la personne a l'usage exclusif »[375].

La CNIL a toutefois estimé que la conservation de huit empreintes digitales et des images numérisées du visage dans une base de données centrale portait atteinte aux libertés individuelles et semblait disproportionnée, eu égard à l'objectif du gouvernement français. Les finalités alléguées par le ministère de l'Intérieur étaient de faciliter les procédures

---

372 *Id.*

373 *Id.*, Les plaintes des employés concernaient la crainte «que l'empreinte vocale ne soit utilisée pour les surveiller lorsqu'ils sont au téléphone ou pour identifier un employé en comparant sa voix à celles des empreintes vocales sauvegardées (authentification un à plusieurs).

374 *Id.*

375 CNIL, « Délibération n°2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques », en ligne : <http://www.cnil.fr/documentation/deliberations/deliberation/delib/130/>.

d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports ainsi que de prévenir, de détecter et de réprimer leur falsification et leur contrefaçon :

> « […] la Commission considère que, si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle. […] la Commission estime que ledit dispositif ne paraît pas constituer, en l'état, un outil décisif de lutte contre la fraude documentaire de nature à lever les préventions exprimées jusqu'alors par la Commission à l'endroit de la constitution de bases centralisées de données biométriques. Par conséquent, même si le ministère de l'intérieur, de l'outre-mer et des collectivités territoriales s'engage à préciser aux termes du projet de décret qu'il ne sera pas possible de procéder à une recherche en identification à partir de l'image numérisée des empreintes digitales et que le système envisagé ne comportera pas de dispositif de reconnaissance faciale à partir de l'image numérisée de la photographie, la conservation dans une base centrale des images numérisées du visage et des empreintes digitales semble disproportionnée. »[376].

Suite à ceci, le Conseil d'état a annulé la collecte et la conservation de huit empreintes digitales, pour n'en conserver que deux dans la base centrale du ministère de l'Intérieur[377] et dans le passeport biométrique.

À titre d'illustration supplémentaire de l'application du test de proportionnalité, la CNIL a récemment annulé l'octroi d'une « autorisation unique suite à déclaration préalable » d'un dispositif biométrique de reconnaissance de la main pour le contrôle des horaires au travail. En effet, « un consensus s'est clairement exprimé pour considérer comme

---

376 CNIL, « Délibération n°2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques », en ligne : <http://www.cnil.fr/documentation/deliberations/deliberation/delib/130/>. La CNIL était également d'avis que la conservation centralisée des données biométriques outrepassait les exigences fixées par le *Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.*

377 CNIL, « Passeports biométriques : la CNIL contrôle l'effacement des empreintes digitales surnuméraires enregistrées dans la base du ministère de l'Intérieur », 11 janvier 2013, en ligne.

disproportionnée l'utilisation de la biométrie aux fins de contrôle des horaires »[378]. Les procédures allégées mises en place par la CNIL[379] pour accélérer et faciliter l'implantation de certains systèmes biométriques ne s'appliquent donc plus aux systèmes destinés à contrôler les horaires de travail et ceux-ci nécessiteront désormais une autorisation spécifique de la CNIL, selon la procédure ordinaire.

En raison des conséquences sur les droits et des coûts des systèmes pouvant être élevés, nous sommes d'avis que les organisations devraient, a priori de l'implantation du système, faire une évaluation des tests de nécessité et de proportionnalité. D'autre part, les tests de nécessité et de proportionnalité à eux seuls ne seront pas suffisants pour que la collecte de données biométriques soit admissible au Québec - le consentement de l'individu à la collecte de ses données étant également exigible. En effet, et tel que mentionné précédemment, les deux exigences sont cumulatives. La CAI a d'ailleurs précisé que « l'obtention d'un consentement à la collecte est subordonnée à cette exigence de nécessité »[380].

1.2 Le consentement

Au Québec, le consentement de la personne est exigible pour que la saisie de ses mesures ou caractéristiques biométriques soit jugée légitime. Le principe, lequel est énoncé à l'article 44 al. 1, LCCJTI, est à l'effet que « nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques »[381]. De plus, le consentement doit être spécifique à l'action posée et limité à la durée nécessaire à la finalité pour laquelle il est requis[382].

---

378 CNIL, « L'Autorisation unique n° AU-007 ne porte plus sur les contrôles d'horaires des salariés », 23 octobre 2012, en ligne.

379 Nous avons abordé cette question dans la première partie, voir chapitre 2, section 1.1.

380 *Id.* ; CAI, « Le caractère indispensable des renseignements recueillis », en ligne : <http://www.cai.gouv.qc.ca/biometrie/le-caractere-indispensable-des-renseignements-recueillis/>

381 Art. 44, *LCCJTI*.

382 CAI, *préc*., note 358.

Afin que le consentement soit jugé valide, un individu devrait savoir exactement en quoi consiste le procédé utilisé, comment et à quelle fin ses données seront utilisées ainsi que la portée de ses droits[383]. À notre connaissance, le Québec est la seule province canadienne où une telle exigence a été expressément prévue. Le fédéral ne dispose pas non plus d'une telle obligation dans son corpus législatif, puisqu'aucune disposition spécifique à la biométrie n'a été adoptée jusqu'à présent.

Toute personne dispose ainsi d'un droit de refus de se faire saisir ses caractéristiques biométriques pour la reconnaissance de son identité dans les domaines de compétences du Québec. À cet effet, la CAI a publié un modèle de formulaire[384] tenant lieu de consentement exprès. Elle recommande que plusieurs éléments soient préalablement divulgués à la personne, tels que le type de technique utilisée, la nature des mesures saisies, l'ensemble des risques associés à cette pratique, les mesures de sécurité prises pour assurer la conservation des données, la durée de la conservation, le moment de leur destruction et l'explication des droits d'accès et de rectification[385].

De plus, les conditions dans lesquelles seront conservés les renseignements, les possibilités d'utilisation, les règles de couplage de données et de communication devraient être clairement expliquées aux personnes concernées avant l'obtention du consentement[386]. Toutes ces conditions rendront l'étape de l'enrôlement cruciale, car un enrôlement défectueux pourrait avoir de lourdes conséquences sur les étapes subséquentes et sur le droit à la vie privée[387].

---

383 *Id*.

384 Voir *l'Exemple de formulaire de consentement sur la cueillette, l'usage et la conservation de caractéristiques ou de mesures biométriques*, Commission d'accès à l'information, en ligne: <http://www.cai.gouv.qc.ca/documents/CAI_FO_consentement_bio.pdf>.

385 *Id*.

386 CAI, « Avis présenté à la Commission des affaires sociales concernant l'Avant-projet de Loi sur la carte santé », 2002, p. 19 ; CAI, « La biométrie au Québec: les principes d'application, pour un choix éclairé », 2002, p.2.

387 Voir les sections 1 et 2 du chapitre 1 de la première partie du présent mémoire.

Selon Andrew Patrick[388], il existe toutefois un risque que le consentement à la collecte des données biométriques soit obtenu de manière contraignante. À titre d'illustration, une organisation fournissant un service beaucoup plus avantageux aux détenteurs de titres biométriques qu'aux individus qui n'y ont pas consenti contraindrait ces derniers à y consentir. Andrew Patrick donne l'exemple du pont Whirlpool situé aux chutes Niagara en Ontario, lequel serait strictement réservé aux détenteurs d'un laisser-passer Nexus[389]. Pour des citoyens canadiens voulant traverser la frontière, cela les forçait en quelque sorte à s'inscrire au programme Nexus afin de pouvoir utiliser ce pont. L'exemple illustre bien la problématique que pourrait causer une situation visant à favoriser indirectement les utilisateurs d'un système biométrique : le consentement se trouverait à être obtenu d'une manière contraignante et donc, non-libre.

Par ailleurs, et tel qu'exposé dans la première partie[390], l'utilisation de la biométrie favorise le risque que les données biométriques soient captées à l'insu des individus. Prenons l'exemple d'une vidéosurveillance utilisant la reconnaissance faciale afin de rechercher une personne, ou la reconnaissance vocale pour l'identifier sans qu'elle le sache. De telles pratiques seraient néanmoins contraires à l'article 44, qui expose le principe que la saisie des mesures ou caractéristiques doit permettre à l'individu de savoir que celles-ci sont prises. En effet,

> « 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 »[391].

En toute déférence, la rédaction de cette portion de l'article 44 nous laisse perplexe. Toutefois, c'est en la lisant *a contrario* que nous comprenons mieux l'intention du législateur,

---

388 Andrew PATRICK, « Acceptance of Biometrics, Things That Matter That We Are Ignoring », *Presentation to the International Workshop on Usability and Biometrics*, Information Security Group, Institute of Information Technology, National Research Council Canada, Washington, D.C., June 23-24, 2008.

389 *Id.*

390 Voir la section 1 du chapitre 2 de la première partie.

391 Art. 44, *LCCJTI*.

s'articulant comme suit : « l'identité de la personne ne peut être établie que parmi les caractéristiques saisies lorsqu'elle en a connaissance ».

Il est important de souligner que les conditions prévues à l'article 44 LCCJTI ne seront pas applicables si la saisie des données biométriques est effectuée dans un but autre que la reconnaissance de l'identité. Dans la décision *C.R.* c. *Loto Québec*[392], la CAI a conclu qu'on ne pouvait appliquer l'article 44 dans le cadre d'une demande d'accès à l'information visant à consulter un enregistrement vocal. En l'espèce, l'avocat de l'organisme prétendait que la divulgation d'un enregistrement vocal permettait d'obtenir un échantillon biométrique et, qu'en conséquent, son consentement était nécessaire. La voix d'un employé n'a toutefois pas été jugée comme étant une donnée servant à l'identification ou à l'authentification biométrique. Concernant la LCCJTI, la CAI précise :

> « [110] Ces dispositions visent donc un objectif précis, qui n'est pas lié à la détermination de l'accessibilité des documents en litige. Elles n'établissent pas le caractère personnel ou non, au sens de l'application de la Loi sur l'accès, de la voix d'une personne contenue dans un enregistrement audio d'une conversation téléphonique. L'organisme n'a fourni aucune preuve visant à établir que la voix contenue dans les documents en litige constitue un « procédé permettant de saisir des caractéristiques ou des mesures biométriques » aux fins d'établir l'identité d'une personne ni que c'est là l'objectif poursuivi par le demandeur. Le présent litige ne porte pas davantage sur la création d'une banque de données biométriques. Ces dispositions ne s'appliquent donc pas en l'espèce ».

Ainsi, l'article 44 de la LCCJTI s'applique uniquement aux données biométriques étant saisies dans le but de reconnaître l'identité d'une personne. Par contre, les données biométriques étant en principe des données personnelles, un consentement demeure tout de même requis pour la collecte de celles-ci en vertu de la *LPRPSP*[393] et de la *Loi sur l'accès*[394], et ce, même si les données sont collectées pour une autre finalité que l'identification ou la vérification.

---

392 *C.R.* c. *Loto Québec*, 2012 QCCAI 300.
393 Art. 6, *LPRPSP*, c. P-39.1.
394 Art. 53*, Loi sur l'accès*, c. A-2.1.

Section 2 – Les mesures de sécurité requises lors de la collecte

Autant dans les sphères publiques que privées, l'organisation qui recueille des renseignements personnels doit prévoir des mesures de sécurité appropriées, selon la LPRPSP et la *Loi sur l'accès*. Le principe est à l'effet que les entreprises et les organismes publics doivent prendre les mesures de sécurité « propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[395].

Tel que nous l'avons vu dans la première partie, la première étape du fonctionnement de la technologie biométrique est l'enrôlement[396]. Selon Bruce Schneier, le système fonctionne bien lorsqu'il est possible de vérifier que la lecture biométrique est effectuée sur la bonne personne au moment de la vérification et que la donnée biométrique est la même que celle au dossier[397].

Pour ce faire, le système doit être apte à assurer que les données ne puissent être subtilisées ou faussées lors de l'enrôlement. Par exemple, un fraudeur ou un suspect recherché par la police pourrait être tenté d'y insérer une fausse empreinte ou d'utiliser une image autre que la sienne pour s'enrôler dans le système. Notons toutefois que, pour qu'une telle fraude puisse réussir, la donnée subtilisée doit être suffisamment claire et lisible pour être subtilisée et la reproduction de la donnée devrait être quasiment parfaite. En plus, il faudrait que le système biométrique en question ne comporte pas de mesure de sécurité liée à la détection du vivant[398].

Sur ce dernier point, la meilleure façon de contrer le risque de copie artisanale de la donnée biométrique est d'ailleurs que le système soit muni d'un dispositif visant à détecter si

---

395 Art. 10, *LPRPSP* ; Art. 63.1, *Loi sur l'accès*.
396 Voir la section 1.3 du chapitre 1 de la première partie du présent mémoire.
397 Bruce SCHNEIER, « Biometrics: Truths and Fictions », in *Crypto-Gram Newsletter*, 1998 : <http://www.schneier.com/crypto-gram-9808.html#biometrics>
398 Voir la section 2.2 du chapitre un de la première partie.

l'échantillon soumis est vivant. Ainsi, un capteur de température devrait être inclut à tout système biométrique d'identification, ce qui réduirait le risque de fraude à l'enrôlement. Notons que le succès d'une telle fraude comporte un avantage considérable : l'individu pourra circuler sous une fausse identité et le faire librement, jusqu'à ce que le propriétaire légitime s'enrôle. En effet, c'est lors de l'enrôlement du véritable titulaire des données que la fraude aura le plus de chances d'être décelée[399]. Précisons que ceci concerne principalement les données laissant des traces, comme les empreintes, la reconnaissance du visage, de la démarche, de la signature et de la voix.

Des politiques de sécurité devraient également être adoptées par l'organisation pour déterminer les niveaux et les matrices d'habilitations, sécuriser les clés de chiffrement et contrôler les accès logiques et physiques aux serveurs[400]. Par ailleurs, selon les recommandations de l'OCDE, une supervision humaine du système est essentielle lors de l'enrôlement, comme lors du traitement des données, afin de pallier aux diverses fonctionnalités, aux erreurs du système et aux attaques potentielles. De surcroît, certains experts sont d'avis que la sécurité ne devrait jamais reposer sur la biométrie seule, mais prévoir plusieurs autres niveaux de contrôle, tels qu'« un examen visuel (premier niveau), une utilisation d'appareils pour tester les sécurités cachées ou lire la puce (deuxième niveau), et une consultation du fichier de gestion (troisième niveau) »[401].

Dans son rapport intitulé « Biometric Encryption », Ann Cavoukian recommande fortement la cryptographie appliquée à la biométrie comme mesure de protection, en expliquant comment fonctionne la technologie :

> « Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification. The digital key (password, PIN, etc.) is randomly generated on enrolment, so that the user (or anybody else) does not even know it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a

399 Voir Jean-René LECERF, *préc*., note 18.
400 Voir OCDE, *préc*., note 77.
401 C'est notamment l'avis de l'expert Pierre Garcia. Voir Jean-René LECERF, *préc.*, note 18, p. 70.

> biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called "private template." In essence, the key *is encrypted* with the biometric. The BE template provides an excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrolment, both the key and the biometric are discarded »[402].

Les fonctions de chiffrement ou de cryptographie devront être d'une complexité telle qu'il soit presque impossible pour une personne non autorisée d'en déchiffrer les données. Soulignons cependant que nous avons relevé une étude mettant en doute la fiabilité de certaines techniques de chiffrement jumelées avec les technologies biométriques[403]. Effectivement, une « une attaque de force brute » demeure possible dans le cas de données chiffrées.

Lors du projet d'émission des visas biométriques en France, la CNIL a considéré que les mesures de sécurité mises en place étaient suffisantes « dès lors que des précautions particulières étaient adoptées lors de l'enrôlement des données biométriques, et que des mesures de sécurité spécifiques étaient prises pour garantir la confidentialité des données, tout particulièrement contre les risques de captation irrégulière, notamment grâce à des méthodes sûres de chiffrement et de signature électronique »[404]. Dans une autre affaire, la CNIL a autorisé la société Bloomberg L.P à mettre en oeuvre un dispositif biométrique basé sur l'empreinte digitale ayant pour but de contrôler l'accès logique à un service d'informations financières. Elle a conclu que les mesures de sécurité étaient adéquates, en raison du fait que le gabarit était enregistré sur un support portable et n'était pas interopérable avec les systèmes basés sur les minuties[405] :

> « La Commission considère que dans la mesure où d'une part, le dispositif "B-UNIT" repose sur l'enregistrement du gabarit de l'empreinte digitale dans un support individuel

---

402 Ann CAVOUKIAN, « Biometric Encryption », *préc*., note 181, p.16.

403 Voir Feng HAO, Anderson ROSS and John DAUGMAN, « Combining cryptography with biometrics effectively », *préc*., note 263, p. 4.

404 CNIL, *Délibération n°2004-075 du 5 octobre 2004.*

405 Une minutie est « un point qui se situe sur le changement de continuité des lignes papillaires » de l'empreinte. Voir BIOMÉTRIE ONLINE, en ligne : <http://www.biometrie-online.net/technologies/empreintes-digitales>

> exclusivement détenu par la personne concernée, et d'autre part, que le gabarit enregistré est généré à partir d'une analyse des caractéristiques générales du tracé des crêtes du doigt des utilisateurs et n'est pas interopérable avec les systèmes basés sur les minuties, le dispositif soumis par la société Bloomberg L.P. ne comporte pas de risques particuliers pour la protection des libertés et des droits fondamentaux de la personne »[406].

Considérant la nature des données biométriques et les enjeux que leur utilisation comporte, nous concluons qu'une des mesures de sécurité propres à assurer la confidentialité des données biométriques lors de la collecte serait au minimum le chiffrement des données[407].

Chapitre II. Conditions relatives au traitement

Suite à un enrôlement sécuritaire, des conditions spécifiques devront être respectées et mises en œuvre pour le traitement des données biométriques lors de leur utilisation, de leur conservation, de leur communication, de leur accès et de leur destruction.

Section 1 – L'utilisation et la conservation

1.1 L'utilisation

Les conditions relatives à l'utilisation des données biométriques dépendront premièrement des finalités déclarées par l'organisation. Le principe de respect des finalités exige que toute utilisation de renseignements soit pertinente à l'objet de la collecte et soit déclarée à la personne concernée au moment de celle-ci[408]. À cet égard, la *Loi sur l'accès* mentionne qu'un organisme public ne pourra utiliser un renseignement personnel qu'aux fins pour lesquelles ce renseignement a été collecté[409]. De son côté, la LPRPSP interdit à toute entreprise d'utiliser les renseignements personnels à des fins non pertinentes à l'objet du

---

406 CNIL, *Délibération n°2005-206 du 22 septembre 2005.*

407 Le chiffrement des données biométriques est d'ailleurs une condition expresse prévue à la *Loi de 1997 sur le programme Ontario au travail*, *préc*., note, art. 75 (6).

408 Art. 65 (2), *Loi sur l'accès*; art. 8 (2), *LPRPSP.*

409 Art. 65 (1), *Loi sur l'accès.*

dossier[410]. Nous l'avons vu, l'utilisation des données à des fins secondaires constituent un des risques majeurs de l'utilisation de la biométrie[411]. La LCCJTI impose une balise supplémentaire, à l'effet que « [t]out 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 »[412]. De plus, « un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande »[413]. Toutefois, cela supposerait qu'un individu notifie d'avance à un organisme qu'il désire connaître l'information qui pourrait être découverte ou qu'il en fasse la demande « s'il a connaissance qu'elle a été recueillie »[414]. Le système biométrique utilisé devrait donc ne servir qu'à la finalité préétablie et ne devrait pas pouvoir mesurer d'autres caractéristiques sous-jacentes à celles qui sont collectées[415].

1.1.1 Les mesures de sécurité requises lors de l'utilisation

À l'instar de la collecte, les organisations sont dans l'obligation de prendre des mesures de sécurité appropriées lors de l'utilisation des renseignements biométriques. Nous l'avons vu, ces mesures doivent notamment être liées à la finalité de traitement des données. Le principe est identique dans la LPRPSP et dans la *Loi sur l'accès*[416].

En outre, la loi prévoit que les renseignements personnels, qu'ils soient détenus par une entité privée ou un organisme public, ne pourront être utilisés que par les personnes autorisées

---

410 Art. 10, *LPRPSP*.
411 Voir première partie, chapitre 2, section 1.1.2.
412 Art. 44 al. 2, LCCJTI.
413 *Id*.
414 Pierre TRUDEL, *préc.*, note 346, p. 178. Précisons qu'en France, la *Loi n°78-17 du 6 janvier 1978* dispose du même principe, selon lequel les données traitées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs »[414]. De plus, l'usage des données doit être déterminé et légitime et le détournement de finalités est passible de sanctions pénales. Voir CONSEIL NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNSR), « Les 7 principes clés de la protection des données personnelles », *Correspondant Informatique et Libertés*, 18 janvier 2012, en ligne : <http://www.cil.cnrs.fr/CIL/spip.php?article1390>. La LPRPSP prévoit également des sanctions pénales, voir les articles 91-93.
415 Art. 44, *LCCJTI.*
416 Art. 10, *LPRPSP* ; Art. 63.1, *Loi sur l'accès*.

à cet effet et dont l'utilisation est nécessaire dans le cadre de leurs fonctions. La LPRPSP mentionne :

> « 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 ou à toute partie à un contrat de service ou d'entreprise 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 ou de son contrat. »[417] [Notre soulignement]

Le principe équivalent est prévu à l'article 62 de la *Loi sur l'accès* relativement au secteur public, prévoyant que « [u]n renseignement personnel 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 »[418].

Par ailleurs, l'une des mesures possibles pouvant limiter une utilisation détournée de l'information consiste à interdire que soient stockés certains renseignements avec les données biométriques. Dans sa *Loi de 1997 sur le programme Ontario au travail*, le législateur ontarien a spécifiquement prévu cette mesure, à l'effet que seuls certains renseignements personnels peuvent être conservés avec les renseignements biométriques, soient le nom, l'adresse, la date de naissance et le sexe de l'individu. Ainsi, toute autre information (par exemple, un historique de paiements) doitt être stockée séparément de la donnée biométrique[419].

Ceci vient non seulement limiter le risque de détournement de finalités, mais aussi celui d'une discrimination et de l'atteinte à la dignité de la personne[420]. Ainsi, moins il y aura de renseignements accompagnant la donnée biométrique, et plus le risque d'une utilisation détournée semble diminuer. Notons que, comme nous le verrons dans la section relative à la conservation, l'anonymisation pourrait aussi être une alternative permettant d'éviter les

---

417 Art. 20, *LPRPSP*.
418 Art. 62, *Loi sur l'accès*.
419 Art. 75*, Loi de 1997 sur le programme Ontario au travail,* L.O. 1997, CHAPITRE 25.
420 Nous avons explicité ces risques dans la première partie, chapitre II, section 2.2.

dérives en matière d'utilisation secondaire des données. Toutefois, cette solution renferme des incidences pour les droits d'accès et de rectification des données, tel que nous le verrons au point 2.4.

Afin de préserver l'intégrité des données, la LPRPSP prévoit que « [t]oute 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 »[421]. Cette disposition oblige le responsable à vérifier, lors de chaque utilisation, que les données conservées sont bel et bien conformes. Précisons que les règles régissant l'utilisation des renseignements sont liées à celles entourant leur conservation, comme nous le verrons à la section suivante.

1.2 La conservation

Pour qu'elles puissent être utilisées, les données biométriques, ou le résultat mathématique de celles-ci, doivent nécessairement être conservées sur un support. Les principes de sécurité requis pour leur conservation pourront différer selon le support sur lequel elles sont conservées, que celui-ci soit individuel ou collectif[422]. Nous examinerons les règles applicables pour chacun des moyens de conservation dans la présente section.

Le principe général veut que la conservation des données biométriques, ainsi que le support, soit protégée par des mesures de sécurité appropriées afin de préserver leur intégrité et de protéger leur confidentialité[423]. À cet égard, la CAI est d'avis que : « l'intégrité des renseignements entreposés est cruciale lorsqu'il s'agit de mesures biométriques, puisque la fonction d'identification d'un individu ne peut être approximative sans risquer de générer de la

---

421 Art. 11, *LPRPSP*. [Notre soulignement]

422 Par support « collectif », nous voulons signifier une banque de données ou tout autre support local qui conserve les données de plus d'une personne.

423 Art.53, *Loi sur l'accès aux documents des organismes publics et les renseignements personnels*, Art. 10, *Loi sur la protection des renseignements personnels dans le secteur privé*, Art. 25, *Loi concernant le cadre juridique des technologies de l'information.* Voir également : Nicolas W. VERMEYS, « Responsabilité civile et sécurité informationnelle », Cowansville, Yvon Blais, 2010, p.102.

discrimination[424] ». Cette intégrité assurera l'exactitude des renseignements au moment où une entreprise doit prendre une décision[425]. Soulignons que l'intégrité est « le concept phare, du moins en matière de preuve »[426], de ce qui a été promulgué par la LCCJTI :

> « [l]'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue »[427].

Les conséquences d'une mauvaise sécurité lors de la conservation des données biométriques sont énormes. En effet, un piratage des données biométriques pourrait avoir de lourdes conséquences sur l'individu, car il résulte d'une donnée biométrique piratée une caducité d'utilisation de celle-ci. En effet, et tel que nous l'avons vu dans la première partie, celui dont la caractéristique biométrique a été piratée devra vraisemblablement changer de type de mesure pour l'identifier[428]. Par ailleurs, il y a de fortes chances que la victime doive apporter la preuve qu'elle est bien celle qu'elle prétend être dans un tel contexte, ce qui reviendrait à lui imposer le fardeau de prouver son identité et, possiblement, son innoncence[429].

a) La conservation dans une banque de données

Tel que déjà évoqué, les données biométriques pourront être conservées dans une banque pour leur traitement. Cette situation a été explicitement prévue dans la *LCCJTI*, laquelle confère à la CAI un certain pouvoir de contrôle sur les banques de caractéristiques biométriques :

---

424 Max CHASSÉ, « La Biométrie au Québec : les enjeux », *préc.*, note 37, p.36.

425 Art. 11, *LPRPSP*.

426 Vincent GAUTRAIS, « Intégrité », Lccjti.ca, Mis à jour le 25 février 2013, en ligne : <http://lccjti.ca/definition/integrite/>

427 Art. 6, *LCCJTI*.

428 Voir la section 1.1 du chapitre 2 de la première partie.

429 Nous avons traité le risque du renversement du fardeau de la preuve dans la première partie, à la section 1.1.5

> « 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.
>
> 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.
>
> 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 ».

Selon cette disposition, la CAI pourra rendre toute ordonnance appropriée si elle juge que certaines règles ne sont pas respectées. À ce jour[430], la CAI n'a rendu aucune ordonnance en vertu de l'article 45 *LCCJTI*[431].

Afin de déterminer les obligations imputables à la création d'une banque de caractéristiques, nous devons nous questionner sur la signification d'une *banque de données* et déterminer si cette notion inclut celle de *base de données*. La Loi ne mentionne pas précisément ce que constitue une banque de caractéristiques ou de mesures biométriques au sens de l'article 45[432]. L'OQLF définit toutefois une banque (de données) comme étant un « ensemble d'informations organisées autour d'un même sujet, directement exploitables et proposées en consultation aux utilisateurs »[433]. En outre, une banque de données regrouperait souvent plusieurs bases de données[434], lesquelles sont définies comme un « ensemble structuré

---

430 Août 2013. Source : Boris Perron, analyste en sécurité de l'information de la Commission d'accès à l'information du Québec.

431 *Id*. En pratique, de telles ordonnances seront généralement rendues à la suite d'une plainte formulée à la CAI.

432 La Loi précise toutefois à son article 3 qu'«est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite». Nous y voyons ici un indice de ce que peut constituer une banque de données selon la Loi.

433 OQLF, *Grand dictionnaire terminologique*, « Banque de données », en ligne: <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8355655>

434 *Id.*

d'éléments d'information, généralement agencés sous forme de tables, dans lesquelles les données sont organisées selon certains critères en vue de permettre leur exploitation »[435].

Les définitions que nous fournit le Larousse sont équivalentes, une banque de données étant une « collection ordonnée d'informations apparentées et traitées par ordinateur, mémorisées, et qui peuvent être interrogées à distance en ligne »[436]. Une banque contient « une *base de données* et un *logiciel* assurant la création de nouvelles données, la mise à jour des informations déjà existantes et la possibilité d'interrogation »[437]. Ainsi, une base de données serait davantage apparentée à un système muni d'un logiciel permettant l'exploitation des données à l'intérieur d'une banque de données, celle-ci regroupant plusieurs bases de données et permettant la mise en relation des données[438].

À priori, la distinction entre les deux notions est exigüe. Cependant, la « base de données » étant généralement plus spécifique que la « banque de données », nous nous sommes questionné sur l'éventualité où une organisation mettait en place une base de données biométriques, à défaut d'une banque de données biométriques. Si on interprète strictement les règles de l'article 45, la CAI ne disposerait pas de pouvoirs relativement à la constitution d'une base de données biométriques. Néanmoins, la mise en place d'un système ou d'un autre comporterait les mêmes conséquences, soit la centralisation, l'exploitation et la mise en relation des données. Nous croyons pour cette raison qu'il faut interpréter la notion de « banque de données » de manière large en y incluant celle de bases de données.

En France, tout dispositif de reconnaissance biométrique doit être autorisée par la CNIL[439], selon la *Loi no78-17 du 6 janvier 1978*, qui dispose que « [l]es traitements

---

435 Notes de l'Office québécois de la langue française : « Une base de données doit être conçue pour permettre une modification aisée de son contenu. Elle peut être composée d'un seul fichier, lui-même contenant plusieurs tables (comme dans le logiciel Access de Microsoft) ».

436 *Dictionnaire le Larousse*, en ligne, « Banque de données » : <http://www.larousse.fr/encyclopedie/divers/banque_de_donn%C3%A9es/187329>

437 De plus, le Larousse mentionne que « la concentration d'information que constituent les banques de données représente une valeur économique et stratégique importante », en ligne : <http://www.larousse.fr/encyclopedie/divers/banque_de_donn%C3%A9es/187329>

438 *Id.*

439 Art. 25, *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes » sont « mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés »[440] . De plus, « les traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes » doivent être autorisés par « décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'Informatique et des libertés »[441].

Avant de fournir une autorisation, la CNIL doit vérifier si les techniques de saisie des données biométriques sont « adaptées et proportionnées à la finalité assignée au dispositif »[442]. La CNIL considère par ailleurs que la constitution d'une base de données est justifiée uniquement s'il existe un impératif fort de sécurité, et qu'il faut tenir compte des éléments suivants : la finalité du dispositif, la proportionnalité, la sécurité et l'information des personnes concernées[443].

En ce qui a trait à la durée de conservation des renseignements, celle-ci devra être adaptée à la finalité de la collecte et à la pertinence de leur conservation. À titre d'illustration, le CPVPC a jugé raisonnable que des photos soient conservées durant cinq ans lors de l'enquête du *Law School Admission Council*[444](ci-après le « LSAC »). Dans cette affaire, les photos des candidats à un examen d'admission ainsi que leurs empreintes digitales étaient collectées par le LSAC dans le but de mitiger les risques de fraude et de confirmer l'authenticité des résultats obtenus dans les facultés de droit canadiennes. Le CPVPC a fortement recommandé que la collecte des empreintes digitales cesse et que, si les photos étaient toujours collectées, de limiter leur conservation à cinq ans[445]. Bien que le fédéral ne dispose pas de règles de destruction des données similaires à l'article 44 de la LCCJTI

---

440 *Id.*
441 Art. 27, *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
442 CNIL, *Délibération no 04-018 du 8 avril 2004*
443 CNIL, *21e Rapport d'activités*, 2000.
444 CPVPC, *Rapport de conclusions d'enquête en vertu de la LPRPDE no 2008-389, Enquête concernant le Law School Admission Council*, 29 mai 2008.
445 *Id*., par. 77.

québécoise, le principe de respect de la finalité pour laquelle la collecte a lieu s'applique en vertu de la LPRPDE[446].

1.2.1 Les mesures de sécurité requises pour la conservation dans une banque de données

Comme nous l'avons vu, la mise en service de banques de données biométriques, locales ou centrales, comporte de sérieuses menaces pour la vie privée[447]. Un système réunissant des renseignements aussi sensibles et intrinsèques à chaque personne pourrait s'avérer extrêmement attirant et « susciter la convoitise des esprits malveillants »[448]. À cet égard, la centralisation des données augmenterait les risques de fuites, de divulgation et de détournement de finalités selon la CAI[449].

Pour cette raison, un débat a lieu sur la nécessité de constituer une banque de données pour stocker les données biométriques. En effet, Roger Clarke croit que la meilleure façon de sécuriser les données biométriques est de carrément interdire la création et l'utilisation de banques de données biométriques[450]. La CAI est aussi d'avis que « [p]lus les données sont centralisées, plus les conséquences d'une fuite de renseignements ou d'un accès injustifiés risquent d'être élevées »[451].

Cependant, certains auteurs sont d'avis qu'une banque centralisée de données biométriques présente beaucoup plus d'atouts pour la sécurité des identités et moins de risques de fraude qu'une banque de données locale ou un système d'authentification sur support portable[452]. Selon Jean-René Lecerf, on s'assurerait ainsi qu'un individu n'ait qu'une seule

---

446 Art. 3 et 5(3), LPRPDE.
447 Voir la section 1.1 du chapitre 2 de la première partie.
448 CAI., « Mémoire concernant l'avant-projet de carte santé au Québec », Mars 2002, p.25.
449 *Id*.
450 Roger CLARKE, « Biometrics and Privacy », *préc*., note 59.
451 CAI, « Mémoire concernant l'avant-projet de carte santé au Québec », *préc*., note 445, p.25.
452 Jean-René LECERF, *préc.*, note 18 p.64-67. Il ajoute toutefois que les fichiers centraux présentent un point faible au moment de la délivrance des titres biométriques (enrôlement) et qu'un risque d'usurpation d'identité est possible, tel que nous l'avons vu dans la première partie.

identité et qu'une identité n'est utilisée que par un seul individu »[453]. Les usurpations et vols d'identité seraient alors, selon lui, théoriquement impossibles[454].

Tel qu'abordé précédemment, des organisations ont mis au point des technologies convertissant l'image de la donnée biométrique brute en formule codée, la donnée n'étant ni conservée ni accessible sous sa forme originale dans le logiciel du système. Parmi ces mesures de sécurité, on retrouve le chiffrement biométrique, les données biométriques annulables et les jetons biométriques[455].

Dans l'affaire *Syndicat des travailleurs de Mométal (C.S.N.)* c. *Mométal*[456], le représentant de l'employeur affirmait qu'il n'avait pas accès au nombre binaire converti, mais que seule l'entreprise lui ayant vendu la technologie pouvait y avoir accès. L'arbitre a conclu que la preuve avait clairement démontré « que le seul élément enregistré s'avère être le résultat binaire et que celui-ci ne peut être d'aucune utilité pour l'employeur ou tout autre tiers y ayant accès, à moins que le salarié place sa main sur la platine et introduise son numéro d'identification dans le terminal ». L'accès au chiffre binaire dépendait donc de la réidentification du salarié, celui-ci se trouvant à détenir en quelque sorte un certain contrôle sur la disponibilité de ses données.

Sans expliquer les modalités des différentes technologies de sécurité, des techniques de cryptographie symétrique[457] ou de cryptographie asymétrique[458] sont des mesures possibles de protection des données. Certains précisent que l'utilisation de la cryptographie à clé publique

---

453 *Id*.

454 *Id*.

455 Lalita ACHARYA et Tomasz KASPRZYCKI, « La biométrie et son usage par l'État », *préc.*, note 38, p. 10.

456 *Syndicat des travailleurs de Mométal (C.S.N.)* c. *Mométal*, *préc*., note, AZ-01141263.

457 Norme [ANSI] X9.8, American National Standard, « Biometric Information Management and Security », 2001, dans *Techniques de contrôle d'accès par biométrie*, Commission Techniques de Sécurité Physique, Club de la sécurité des systèmes d'information français (CLUSIF), Juin 2003. p. 30. La cryptographie symétrique, ou « à clé secrète », est la « cryptographie dans laquelle la même clé est utilisée pour chiffrer et déchiffrer les données», OQLF, Grand dictionnaire terminologique, 2005.

458 La cryptographie asymétrique est la « cryptographie dans laquelle on utilise une paire de clés asymétriques, une clé publique et la clé privée correspondante, pour chiffrer et déchiffrer les données », OQLF, Grand dictionnaire terminologique, 2005. *Id*., Les données signées doivent être accompagnées du certificat correspondant aux clés de signature ou d'un moyen de retrouver ce certificat.

rehausserait la sécurité des transactions biométriques[459]. Soulignons que, sans qu'elle ne précise de technologie particulière, la *Loi de 1997 sur le programme Ontario au travail* oblige à ce que « les renseignements biométriques recueillis aux termes de la présente loi soient codés sans délai après leur collecte, que les renseignements biométriques originaux soient détruits après l'encodage et que les renseignements biométriques codés ne soient stockés ou transmis que sous une forme codée et qu'ils soient détruits de la façon prescrite »[460]. Même si la législation québécoise ne dispose pas de règle aussi précise, la CAI est d'avis que toutes les données biométriques devraient être chiffrées[461].

Du côté fédéral, le Commissariat à la protection de la vie privée du Canada a indiqué qu'une solution plus protectrice de la vie privée consisterait à extraire certains identificateurs biométriques et à n'enregistrer qu'un « modèle ou un résumé mathématique des renseignements »[462], ce qui équivaut au chiffrement des données. Elle est d'avis que, de cette manière, certains renseignements personnels seraient automatiquement éliminés lors de l'extraction des données et que ceci « diminue la probabilité que les données biométriques soient utilisées à des fins secondaires imprévues »[463].

Selon certaines décisions canadiennes, il appert que cette obligation d'y apporter les mesures de protection appropriées dépasse un certain seuil, à l'effet que les mesures prises ne doivent pas seulement être raisonnables, mais leur efficacité doit être proportionnelle au degré de sensibilité des données[464]. Dans la décision arbitrale *Union des routiers, brasseries,*

---

459 Marc LACOURSIÈRE, « La compensation interbancaire à l'ère d'Internet », *préc*. note 57, p.22. Voir également Jane Kaufman WINN, « Couriers Without Luggage: Negotiable Instruments and Digital Signatures », (1998) 49, *S.C.L. Rev.* 739, 763 et 764; A. Michael FROOMKIN, «The Essential Role of Trusted Third Parties in Electronic Commerce», (1996) 75 *Oregon L. Rev.* 49, 51-53.

460 *Loi de 1997 sur le programme Ontario au travail*, L.O. 1997, ch. 25, Annexe A, art. 75 (6)

461 CAI, « La biométrie au Québec : Les principes d'application pour un choix éclairé », *préc*., note 358, p.5.

462 CPVPC : <http://www.priv.gc.ca/information/pub/gd_bio_201102_f.cfm>

463 *Id*. La question de l'anonymisation des données biométriques a déjà été abordée dans la première partie, voir la section 2.1 du chapitre 1.

464 Les auteurs Doré et Charrette sont semblablement du même avis. Voir Raymond DORÉ et François CHARRETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Yvon Blais, 2001.

liqueurs douces et ouvriers de diverses industries, local 1999 et *L'Oréal Canada*[465], l'arbitre a conclu que les technologies de chiffrement « les plus performantes » devraient être mises en œuvre, et ce, en fonction du degré de sensibilité des données en cause :

> « Autrement dit, il ne suffit pas pour les organismes publics, les entreprises et les ordres professionnels assujettis à l'obligation de mettre en place des mesures de sécurité raisonnables pour assurer le caractère confidentiel des renseignements personnels d'avoir des systèmes de sécurité de leurs données informatiques et de leurs dossiers physiques. Ils doivent suivre les développements technologiques pour être à la fine pointe et empêcher les intrusions injustifiées, surtout lorsque les renseignements en cause ont un haut niveau de sensibilité. Les méthodes de chiffrement ou d'encryptage les plus performantes devraient donc être adoptées puisque les fraudeurs sont toujours à l'affût et qu'il sont en mesure de s'introduire dans les systèmes qui sont plus vulnérables, moins sophistiqués et moins avancés d'un point de vue technologique »[466].

À cet égard, la Cour supérieure s'est déjà prononcée sur la nécessité de prendre des mesures de sécurité appropriées dans un contexte de transactions financières :

> « [51] […] ce serait placer la barre trop haute que d'exiger, en l'instance, que BMO ait été munie de cette technologie en 2005. Mais à l'aube d'une économie instable, d'une période de resserrement du crédit et de difficultés financières, ne serait-il pas approprié que le plus haut niveau de sécurité protège les transactions électroniques faites par les clients des institutions financières? »[467]. [Notre soulignement]

Mentionnons toutefois que des experts ont déjà soulevé la fragilité de la cryptographie au-delà de cinq ans[468]. Comme le mentionne le Professeur Vermeys, une mise à jour constante des technologies de sécurité est nécessaire, afin que celles mises en place ne deviennent pas désuètes, et afin d'en protéger les supports et l'intégrité des données[469]. Il souligne cependant qu'il existe un risque que les nouvelles technologies ne soient pas aussi sécuritaires qu'elles ne

---

465 *Union des routiers, brasseries, liqueurs douces et ouvriers de diverses industries, local 1999* et *L'Oréal Canada,* Tribunal d'arbitrage, AZ-50832524, 6 février 2012.

466 *Id*.

467 *Raphael M'Boutchou* c. *Banque de Montréal*, EYB-2008-150981 (C.S.).

468 Jean-René LECERF, « Rapport d'information au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire », no 439, présenté au Sénat, 29 juin 2005.

469 Nicolas W. VERMEYS, « Responsabilité civile et sécurité informationnelle », *préc*., note 423, p. 125.

le prétendent[470]. Des politiques prévoyant l'acquisition, l'application et la mise à jour des mesures de protection devraient ainsi être adoptées[471].

D'autre part, nous l'avons vu, l'anonymisation des données est une autre solution envisageable pour la protection de la vie privée[472]. Elle implique que les données soient conservées sans qu'aucune autre information permettant d'identifier l'individu ne soit stockée dans le système. Selon Ann Cavoukian, la cryptographie peut être utilisée à cette fin et rehausserait la sécurité, en désidentifiant l'information contenue dans une banque de données :

> « Biometric encryption also may be used in a privacy-enhancing capacity to de-identify information contained in a database; that is, to anonymise the information by separating the identity of an individual from their sensitive information »[473].

Ainsi, seule une donnée chiffrée et non-identifiable serait conservée. Selon ce qu'elle avance, l'individu serait donc en contrôle complet de ses renseignements contenus dans la banque de données, puisque l'unique lien possible entre l'identité de la personne et l'information est l'échantillon saisi[474]. Cette mesure semble, a priori, immuniser les données biométriques contre tout accès non autorisé et protège contre une utilisation détournée de celles-ci.

De plus, il a déjà été recommandé par plusieurs experts, à titre de normes de gestion des technologies biométriques, que les données soient traitées dans un système fermé et qu'il soit interdit d'effectuer des croisements entre différentes sources[475]. Selon la CAI, « le cloisonnement de l'information au sein de plusieurs organismes demeurera toujours la meilleure garantie de confidentialité et l'obstacle le plus approprié pour éviter que l'État ne

---

470 *Id*.
471 *Id*.
472 Voir la section 2.1 du chapitre 2 de la première partie.
473 Ann CAVOUKIAN, « Consumer Biometric Application », *préc*., note 60, p.39.
474 « The link between a person's identity and their information is the finger pattern which scrambles a computer pointer linking the two. This now places the individual in complete control of the information in his database », *Id*., p. 39.
475 INSTITUT DU NOUVEAU MONDE, « Rapport de la conférence citoyenne sur la biométrie et la sécurité », *préc*., note 42, p. 17.

puisse dresser des profils sur les individus ou autrement s'immiscer dans leur vie privée »[476]. Si la création d'une base de données est absolument nécessaire, il sera ainsi préférable qu'elle soit locale plutôt que centralisée[477]. De même, la législation devrait obliger les organisations à déclarer tout bris de sécurité dans le traitement des données.

Pour finir, nous partageons l'avis de certains auteurs à l'effet que la CAI devrait disposer d'un pouvoir de surveillance et de contrôle sur les fournisseurs et les employeurs, en approuvant au préalable toute constitution d'une banque de données[478] ainsi que la mise en œuvre de tout dispositif de lecture biométrique. De la sorte, il pourrait être mis en place un système d'octroi de permis, d'accréditation et de vérification de l'utilisation de ces systèmes[479] afin d'en assurer un contrôle plus rigoureux. En dernier lieu, les mesures de sécurité devraient pouvoir garantir qu'une duplication ou une réplication des données ne sera pas possible, et ce, afin d'en préserver l'intégrité et la confidentialité. Notons par ailleurs qu'il ne faut pas négliger l'importance d'assurer une sécurité physique des locaux contenant les banques de données biométriques et tous les systèmes associés.

b) La conservation sur un support individuel

Comme nous l'avons vu, l'utilisation d'un support externe, individuel ou portable, pour le traitement et la conservation des données biométriques ne peut avoir lieu que pour l'authentification de l'identité (ou la vérification), puisque l'identification requiert une recherche et une comparaison avec d'autres identités[480]. Précisons toutefois que deux situations sont possibles. D'une part, les données contenues sur un support individuel peuvent être traitées en corrélation avec une banque de caractéristiques biométriques[481]. Ceci permet de procéder à l'identification dans un premier temps, et à l'authentification dans un deuxième

---

476 Max CHASSÉ, *préc.*, note 37.
477 Voir OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « La biométrie », *préc.*, note 231, p. 67.
478 Voir INSTITUT DU NOUVEAU MONDE, *préc.*, note 42, p.27.
479 *Id.*
480 Voir les sections 1.2b) et 1.3 du chapitre 1 de la première partie.
481 Voir Jean-René LECERF, *préc.,* note 18, p.65.

temps[482]. D'autre part, les données peuvent être conservées sur un support uniquement, sans qu'il puisse exister de lien avec une banque de données[483]. Selon la CAI :

> « Cette approche est intéressante dans la mesure où les traitements et les données résident sur le support portable, sont protégés par un mécanisme de sécurité et qu'il n'existe aucune possibilité pour l'organisation qui offre le procédé de capturer autrement l'information contenue sur la carte, pas même pour des fins de sauvegarde en cas de perte. Cette approche pour être sûre aurait avantage à être complétée par une homologation des produits afin de s'assurer qu'aucune donnée n'est capturée à l'insu des utilisateurs »[484].

Il est à noter que, selon ce qui est prévu par la LCCJTI, la CAI ne dispose de pouvoirs qu'en matière de constitution ou d'existence d'une banque de caractéristiques. La CAI ne disposerait donc d'aucune compétence dans le cadre d'un traitement de données enregistrées sur un support portable à des fins d'authentification, sans qu'aucune banque de données ne soit liée à celui-ci[485].

En France, un cadre spécifique comportant des formalités simplifiées a été défini afin d'accorder une autorisation unique pour tout dispositif biométrique répondant à certaines conditions. En fournissant à la CNIL une déclaration simplifiée, des entreprises françaises peuvent requérir à la biométrie si elles s'engagent à respecter lesdites conditions. Cette procédure s'applique aux dispositifs de reconnaissance suivants :

> « - du contour de la main pour assurer le contrôle d'accès au restaurant scolaire (autorisation n°AU-009)
> - du contour de la main pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail (autorisation n°AU-008) ;
> - de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-007) »[486].

---

482 *Id*.
483 *Id*., p.64; Max CHASSÉ, *préc*, note 37, p. 33.
484 Max CHASSÉ, *préc*., note 37, p. 33.
485 Voir art. 44, *LCCJTI*.
486 CNIL, « Guide collectivités locales », *Les Guides de la CNIL,* Édition Janvier 2008, p.56.

Les conditions d'éligibilité porteront généralement sur les finalités et les modalités de traitement de l'information, tels que la durée de conservation et les droits d'accès. Par exemple, une des conditions qui doit être remplie pour qu'un organisme soit éligible à une autorisation unique est que le traitement des données « ne [puisse] pas donner lieu à des interconnexions avec d'autres traitements automatisés d'informations nominatives »[487]. Ainsi, la CNIL a prescrit certaines normes tendant à favoriser la mise en œuvre de dispositifs biométriques portables. Ce cadre vient également encadrer les principes de proportionnalité et de respect des finalités dans certains contextes prédéfinis[488].

Un des avantages pratiques de la conservation des données sur un support individuel est qu'il permet aux personnes d'exercer un meilleur contrôle sur leurs renseignements personnels, contrairement aux banques de données. En effet, chaque individu détient la garde de ses renseignements et pourra être tenu responsable en cas de perte ou de vol de données contenues sur le support[489].

1.2.2 Les mesures de sécurité requises pour la conservation sur un support individuel

Tel qu'introduit dans la section précédente, la conservation des données biométriques chiffrées sur une carte à puce dont l'utilisateur est responsable serait la façon la plus sécuritaire de protéger celles-ci[490]. Nous l'avons vu, cette solution est intéressante puisque le décodage ne pourrait se faire « que sur la base d'une nouvelle collecte de données biométriques auprès de l'intéressé lui-même, ce qui éviterait la création de bases de données contenant des modèles de données biométriques susceptibles d'être réutilisés à des fins tout à fait différentes »[491]. Ainsi, seule la présence physique de la personne concernée permet à la

---

487 Article 1er, *Norme simplifiée n° 42 : Délibération n° 02-001 du 8 janvier 2002 concernant les traitements automatisés d'informations nominatives mis en oeuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration.*

488 *Id*.

489 CNIL, « Guide collectivités locales », *Les Guides de la CNIL,* Édition Janvier 2008.

490 GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », *préc*., note 176, p.4.

491 *Id*., p.10.

carte à puce de déverrouiller le système[492]. De plus, les données peuvent être déchiffrées de manière complètement anonyme, en ayant comme support une carte à puce muette[493].

En France, la CNIL recommande d'ailleurs que les données biométriques soient uniquement stockées sur un support portable, en l'occurrence une carte à puce. De cette manière, le « risque social » serait moindre « lorsque l'échantillon d'une caractéristique biométrique demeure sur soi »[494], en particulier si celle-ci laisse des traces dans la vie quotidienne. De plus, cela permettrait à l'utilisateur de contrôler l'utilisation de ses données et d'empêcher un détournement de finalités. La conservation sur support portable permettrait par ailleurs de réduire les risques de piratage de banques de données et de vulnérabilités informatiques. L'OCDE partage également cet avis :

> « Le stockage du gabarit biométrique sur une carte à puce au lieu d'une base de données centralisée pourrait résoudre en partie bon nombre de problèmes de protection de la vie privée associés aux systèmes biométriques, à condition que la carte à puce et le système biométrique soient protégés de façon appropriée, par exemple en limitant l'accès au moyen d'un lecteur autorisé et d'un code d'identification personnelle »[495].

De la même manière, un des principes directeurs du Conseil de l'Europe à l'égard des cartes à puce est à l'effet que :

> « [l]es données enregistrées sur une carte devraient être protégées contre tout accès non autorisé ou accidentel, modification et/ou effacement. Les cartes devraient offrir un niveau de sécurité approprié compte tenu de l`état de la technologie, de la nature sensible ou non des données enregistrées, du nombre et du type d`applications prévues et de l'évaluation des risques potentiels. Les modalités selon lesquelles les tiers peuvent avoir accès aux données enregistrées sur la carte doivent être établies au préalable pour chacune des finalités spécifiques pour lesquels la carte est utilisée »[496].

---

492 Voir OCDE, *préc*., note 77, p. 41.
493 CLUSIF, « Techniques de contrôle d'accès par biométrie », *préc*. note 58, p.24.
494 *Id*., p. 30.
495 OCDE, « Technologies fondées sur la biométrie », *préc.*, note 77.
496 Principe no 6, CONSEIL DE L'EUROPE, « Principes directeurs sur la protection des données à caractère personnel à l'égard des cartes à puce (2004) », préparé par le Groupe de projet sur la protection des données (CJ PD), adopté par le CDCJ lors de sa 79e plénière (11-14 mai 2004), p. 4.

De plus, le Conseil souligne que le risque de détournement d'usage des données conservées sur la carte augmente « si elle incorpore des fonctions de paiement. Il est déconseillé de combiner la fonction de paiement intégrée dans la carte avec des applications au moyen desquelles les données sensibles à caractère personnel du titulaire de la carte sont enregistrées dans la carte »[497].

Lorsque la carte est émise, l'utilisateur devrait être dûment informé de la manière d'utiliser sa carte ainsi que des mesures à prendre en cas de fraude ou de divulgation non autorisée[498]. Par exemple, il pourrait s'agir des conséquences pouvant résulter d'une mauvaise utilisation de la carte ou d'une divulgation des données ainsi que les situations où sa responsabilité pourrait être engagée[499]. De plus, l'utilisateur devrait être informé chaque fois que ses données biométriques sont échangées entre une carte à puce et le système, sauf si cela lui a été divulgué au préalable. Ceci est particulièrement important dans le cas des cartes sans contact, c'est-à-dire lorsque la personne concernée n'insère ou ne présente pas elle-même la carte au système[500].

Notons que l'OCDE favorise grandement l'utilisation de l'authentification plutôt que l'identification biométrique. Elle précise qu'en optant pour les systèmes d'authentification, « on maîtrise plus facilement le taux d'erreur et la performance d'une technologie biométrique donnée et, par conséquent, les chances de réussite de l'application »[501]. En outre, l'authentification empêcherait ou rendrait plus difficile l'utilisation détournée des données à des fins autres que pour lesquelles elles ont été collectées[502].

---

497 *Id*., p. 4, note 8.
498 *Id*., p.5
499 *Id*.
500 *Id*. p. 5.
501 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Technologies fondées sur la biométrie », *préc*., note 77, p.41.
502 Jean-René LECERF, *préc*., note 18, p. 66.

Pour conclure cette section, nous devons mentionner que la LCCJTI prévoit des règles spécifiques à la certification[503] de l'identité et envers le titulaire d'un dispositif permettant de l'identifier. Ainsi, le titulaire d'un dispositif lié à un certificat d'identité[504] et contenant ses données biométriques doit en assurer la confidentialité :

> « 57. Lorsque la certification vise le titulaire d'un dispositif, tangible ou logique, permettant de l'identifier, de le localiser ou d'indiquer un de ses attributs et que ce dispositif comporte un élément secret, le titulaire est tenu d'en assurer la confidentialité. Lorsque cet élément doit lui être transmis, la transmission doit être faite de manière que seul le titulaire en soit informé.
>
> Le titulaire doit voir à ce que le dispositif ne soit pas utilisé sans autorisation. Toute utilisation est présumée faite par lui »[505].

Nous n'avons pas d'indication sur la définition « d'élément secret », mais nous sommes d'avis que cet article pourrait s'appliquer aux données biométriques dans la mesure où ces dernières étaient considérées comme des éléments secrets par les tribunaux. De plus, toute utilisation du dispositif sera présumée faite par le titulaire du certificat. Un dispositif perdu ou volé devrait donc être dénoncé rapidement par ce dernier, sans quoi sa responsabilité pourrait être engagée[506].

---

503 Voir Caleb CHEPESIUK, Mark KARPINSKI et Charles THÉROUX, « La certification de l'identité et la protection des droits de la personne », Commission canadienne des droits de la personne, août 2010, p.10.

504 Un certificat « est un écrit par lequel une personne, en sa qualité d'officier public ou à titre personnel, garantit un fait dont elle a connaissance. Dans le contexte de la *Loi*, le certificat est un document technologique qui comporte les justificatifs d'identité d'une entité et qui est signé par l'autorité de certification qui a vérifié ces justifications », voir Pierre TRUDEL, « Introduction à la Loi concernant le cadre juridique des technologies de l'information », Cowansville, Yvon Blais, 2012, p.137. Voir également l'article 47, LCCJTI : « Un certificat peut servir à établir un ou plusieurs faits dont la confirmation de l'identité d'une personne, de l'identification d'une société, d'une association ou de l'État, de l'exactitude d'un identifiant d'un document ou d'un autre objet, de l'existence de certains attributs d'une personne, d'un document ou d'un autre objet ou encore du lien entre eux et un dispositif d'identification ou de localisation tangible ou logique ».

505 Art. 57, *LCCJTI*. Notons que d'autres règles spécifiques à la certification ont été prévues par le législateur dans la *LCCJTI*. Les articles 47 à 62 traitent des conditions applicables aux certificats numériques. Les règles s'appliquent à la biométrie dans la mesure où l'information utilisée pour certifier l'identité d'une personne contient des données biométriques.

506 Art. 57-58, *LCCJTI*.

Section 2 – La communication, la transmission, l'accès et la destruction

2.1 La communication et la transmission

Mentionnons tout de suite que la communication et la transmission sont deux notions distinctes[507]. En effet, selon plusieurs auteurs, « [t]ransmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer d'un point à l'autre. La transmission s'analyse donc comme une opération technique pouvant éventuellement emporter communication »[508], alors que la communication implique la consultation du document en question. Puisque, pour qu'il y ait communication, il doit nécessairement y avoir une transmission[509], nous joindrons les deux concepts sous le même titre, en prenant soin de mentionner les distinctions légales applicables à chacun en matière de biométrie.

Rappelons que, les données biométriques étant en principe des renseignements personnels, elles ne peuvent être communiquées à des tiers qu'au consentement de l'individu concerné, à moins que la loi ne le prévoie autrement[510]. Cette règle ne semble toutefois pas applicable à la transmission des données biométriques, dans la mesure où celles-ci ne sont pas consultées par les tiers, mais uniquement transmises pour être conservées ou retransmises par un intermédiaire. À cet égard, soulignons les propos des auteurs Vincent Gautrais et Pierre Trudel, à l'effet que « [l]a seule circulation des renseignements personnels n'est donc pas systématiquement synonyme de communication, du fait de cette absence de connaissance »[511].

---

507 En effet, « [t]ransmettre n'est pas « communiquer ». Alors que la seconde, nous l'avons vu, réfère à la connaissance de l'information concernée, la transmission semble impliquer bien davantage le caractère « mécanique » de la connexion entre un point «A» à un point «B». D'ailleurs, la notion de transmission est généralement utilisée dans la Loi sur l'accès et autres lois sur la protection des renseignements personnels dans une perspective qui n'est pas celle de la communication. Plus exactement, les vingt cinq occurrences dans la Loi sur l'accès référant au terme de transmission, ou à une de ses variantes, concernent généralement l'envoi de documents d'une personne à une autre ». Voir Vincent GAUTRAIS et Pierre TRUDEL, « Circulation des renseignements personnels et web 2.0 », Éditions Thémis, 2010.

508 *Id*.

509 Voir *Id*., citant *Goldman* c. *R*. [1980] 1 R.C.S. 976, par. 994-995.

510 Art. 13, *LPRPSP*; Art. 59, *Loi sur l'accès*; Art. 37, C.c.Q.

511 Vincent GAUTRAIS et Pierre TRUDEL, « Circulation des renseignements personnels et web 2.0 », *préc*., note 507.

2.1.1 Les mesures de sécurité applicables lors de la communication et de la transmission

À l'instar de toutes les autres étapes du traitement et de la collecte, l'organisation détenant des données biométriques a l'obligation de mettre en place des mesures de protection adéquates lors de la communication ou de la transmission de celles-ci[512]. De plus, la *LCCJTI* prévoit que des mesures de protection particulières des renseignements confidentiels servant à confirmer l'identité d'une personne doivent être prises lors de la transmission de ceux-ci :

> « 40. La personne qui, après vérification, est en mesure de confirmer l'identité d'une personne ou l'identification d'une association, d'une société ou de l'État peut le faire au moyen d'un document, entre autres un certificat, dont l'intégrité est assurée. Ce document peut être transmis sur tout support, mais les renseignements confidentiels qu'il est susceptible de comporter doivent être protégés.
>
> La vérification de l'identité ou de l'identification doit se faire dans le respect de la loi. Elle peut être faite en se référant aux registres prévus au Code civil ou à la Loi sur la publicité légale des entreprises (chapitre P-44.1) et ce, quel que soit le support au moyen duquel elle communique. La vérification de l'identité d'une personne peut aussi être effectuée à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède.
>
> Cette vérification, faite par une personne ou pour elle, peut être effectuée, sur place ou à distance, par constatation directe ou au moyen de documents dont l'intégrité est assurée et qui peuvent être disponibles sur différents supports pour consultation sur place ou à distance. »[513] [Notre soulignement]

Cette règle d'applique à tout document émis à la suite de la vérification de l'identité d'une personne au moyen de données biométriques et servant à attester l'identité d'une personne. Cette règle de protection semble s'appliquer tout autant à la transmission qu'aux autres étapes de traitement des renseignements confidentiels En outre, les organisations devant

---

512 Art. 10, *LPRPSP*; Art. 63.1, *Loi sur l'accès*; Art. 34, *LCCJTI*.

513 Art. 40, *LCCJTI*. Selon certains auteurs, « une identification par l'entremise de la biométrie engendre la création d'une clé privée. La transmission de cette information chiffrée implique la création d'un certificat d'identité et la nécessité de la présence d'un prestataire de services ». Voir Marc LACOURSIÈRE, « La compensation bancaire à l'ère d'Internet », *préc*., note 57.

émettre ces types de document doivent prendre les moyens nécessaires pour préserver l'intégrité de ceux-ci[514].

Par ailleurs, notons que la vérification de l'identité peut avoir lieu à distance, au moyen de documents dont l'intégrité doit aussi être garantie. Ceci semble impliquer à la fois la consultation de documents dans une banque de données que sur un support portable. Dans tous les cas, un système servant à faire la vérification de l'identité à distance, au moyen de données biométriques, doit pouvoir assurer l'intégrité du document et des données lors de la transmission ou de la communication de celles-ci.

Dans le même esprit, l'article 41 de la LCCJTI dispose que :

> « 41. Quiconque fait valoir, pour preuve de son identité ou de celle d'une autre personne, un document technologique qui présente une caractéristique personnelle, une connaissance particulière ou qui indique que la personne devant être identifiée possède un objet qui lui est propre, est tenu de préserver l'intégrité du document qu'il présente.
>
> Un tel document doit en outre être protégé contre l'interception lorsque sa conservation ou sa transmission sur un réseau de communication rend possible l'usurpation de l'identité de la personne visée par ce document. Sa confidentialité doit être protégée, le cas échéant, et sa consultation doit être journalisée. » [Nos soulignements]

Les mesures de protection des données biométriques devront être assez performantes pour empêcher toute interception lors de la transmission de celles-ci - interception qui pourrait rendre possible une usurpation d'identité. L'intégrité du document et sa confidentialité sont notamment visés par cette disposition. Mentionnons que cette règle s'applique si le document est conservé et accessible via un réseau de communication.

Notons que la *Loi sur l'accès* et la LPRPSP prévoient des exceptions au principe de consentement pour la communication de renseignements personnels dans certaines situations[515]. À supposer que les données biométriques étaient assujetties à ces exceptions,

---

514 Nous vous renvoyons au site LCCJTI.ca pour une définition précise de la notion d'intégrité en droit des technologies de l'information : <http://lccjti.ca/definition/integrite/>.

515 Voir, par exemple, les articles 59 et 59.1 de la *Loi sur l'accès* et l'article 18, *LPRPSP*.

l'organisation ainsi autorisée à communiquer des renseignements personnels devrait, certes, prévoir des mécanismes sécuritaires de communication, tout comme l'organisation qui en fait la demande. Toutefois, il n'est pas clair si ces exceptions sont applicables aux données biométriques, le législateur n'ayant rien précisé à cet égard dans la LCCJTI.

2.2 Les droits d'accès et de rectification

Les droits d'accès et de rectification des renseignements personnels prévus à la *Loi sur l'accès*[516], à la LPRPSP[517] et au *Code civil du Québec*[518] sont applicables aux données biométriques[519]. D'ailleurs, le droit de l'accès à l'information est un droit fondamental consacré par la *Charte québécoise*[520]. Les organisations qui conservent ces données doivent donc accorder des droits d'accès aux individus concernés et leur permettre de les faire rectifier ou corriger, si elles sont inexactes, incomplètes ou équivoques, notamment[521]. De plus, la *Loi sur l'accès* prévoit que « [l]e droit d'accès à un document s'exerce par consultation sur place pendant les heures habituelles de travail ou à distance »[522]. Ainsi, « [l]'organisme public donne communication d'un renseignement personnel à la personne qui a le droit de le recevoir en lui permettant de prendre connaissance du renseignement sur place pendant les heures habituelles de travail ou à distance et d'en obtenir une copie »[523].

Des mesures adaptées au contexte biométrique devront être prises pour permettre l'exercice de ces droits[524], que les documents soient consultés sur place ou à distance. À cet effet, l'article 25 de la LCCJTI prévoit que :

---

516 *Loi sur l'accès*, articles 83 et 89.
517 Articles 27-28, *LPRPSP*.
518 Art. 38 et ss., C.c.Q.
519 Notons que le droit de l'accès à l'information est aussi prévu au *Code civil du Québec* et la *Charte québécoise*, aux articles 39 et 44, respectivement.
520 Art. 44, *Charte québécoise* : « Toute personne a droit à l'information, dans la mesure prévue par la loi ».
521 Art. 89*, Loi sur l'accès*.
522 Articles 10 et 84, *Loi sur l'accès*.
523 Art. 84, *Loi sur l'accès*.
524 Art. 29, *LPRPSP* ; Art. 63.1, *Loi sur l'accès* ; art. 25, *LCCJTI.*

> « 25. La personne responsable de l'accès à un document technologique doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non-autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder »[525].

Selon Vincent Gautrais et Pierre Trudel, la LCCJTI apporte « un encadrement passablement strict »[526] aux conditions d'accès des documents technologiques, laquelle impose « l'obligation de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité »[527].

Comme le mentionne le Professeur Vermeys, une évaluation des risques sera nécessaire pour se conformer à l'article 25, car la « seule façon d'identifier les mesures de sécurité propres à assurer la confidentialité d'informations, c'est d'isoler les informations dont il est nécessaire d'assurer la confidentialité et d'identifier les menaces qui les guettent, ce qui permettra de sélectionner lesdites mesures »[528]. De la sorte, chaque organisation voulant mettre en place un système biométrique devrait au préalable en évaluer tous les risques pour que les mesures de sécurité puissent être appropriées et performantes[529].

Signalons que, en pratique, les droits d'accès et de rectification des renseignements biométriques seront difficiles à mettre en œuvre, « dans la mesure où la donnée n'est pas nécessairement conservée sous une forme visuellement reconnaissable »[530]. Nous l'avons vu, ce serait par exemple le cas du chiffrement ou du hachage cryptographique. Pour que la donnée soit lisible, il faudrait qu'un logiciel soit apte à convertir les gabarits en forme intelligible et mis à la disposition de l'utilisateur.

---

525 Art. 25, LCCJTI.
526 Vincent GAUTRAIS et Pierre TRUDEL, « Circulation des renseignements personnels et web 2.0 », *préc*., note 507.
527 Art. 26, *LCCJTI*.
528 Nicolas W. VERMEYS, *préc*., note 423, p. 73.
529 Nous vous renvoyons au deuxième chapitre de la présente partie pour une notion explicitée de mesures de protection adaptées selon le contexte et la sensibilité des données biométriques.
530 Christian CABAL, *préc*., note 2, p. 75.

En dernier lieu, soulignons que les profils d'accès aux banques de données peuvent être particulièrement difficiles à déterminer, en raison du nombre élevé d'utilisateurs et de groupes d'utilisateurs[531].

2.2.1 Les mesures de sécurité applicables lors de l'accès

Les moyens technologiques mis en place pour contrôler les accès aux données peuvent être variés, comme le chiffrement, les mots de passe ou le fait de rendre les données invisibles à l'écran[532]. En effet, ces derniers constituent des « procédés de visibilité réduite ou qui empêchent une personne non autorisée de prendre connaissance du renseignement »[533]. En outre, le système devrait toujours « être configuré de manière à ce qu'il ne soit pas possible d'accéder de façon détournée à un document ou aux renseignements confidentiels »[534].

Pour qu'un individu puisse exercer ses droits d'accès, le système devrait lui permettre de déchiffrer ses données et de les rendre intelligibles. Ceci crée toutefois un risque que les données soient accessibles des personnes qui ne sont pas autorisées, à moins que l'accès aux données ne soit uniquement conditionnel à l'acceptation de l'identité de la personne présentant la demande d'accès. De cette manière, l'accès aux données par des tiers est protégé – celui-ci étant seulement permis lors de l'acceptation par le système de la concordance entre la donnée saisie lors de la demande d'accès et le gabarit conservé[535]. Cette façon de faire donne donc au propriétaire légitime le contrôle de ses droits d'accès. Notons qu'une telle situation a été prévue par le gouvernement ontarien dans sa *Loi de 1997 sur le programme Ontario au travail*, à l'effet que :

---

531 CAI, « Mémoire concernant l'avant-projet de carte santé au Québec », *préc*., note 446, p. 25.
532 Pierre TRUDEL, « Introduction à la Loi concernant le cadre juridique des technologies de l'information », *préc*., note 343, p. 90.
533 Art. 25, *LCCJTI.*
534 Pierre TRUDEL, *préc*., note 532, p. 90.
535 Voir la section 2 du chapitre 1 de la première partie du présent mémoire.

> « [ni] le directeur ni l'administrateur ne doivent mettre en place un système qui permet de reconstituer l'échantillon biométrique original à partir de renseignements biométriques codés ou de le conserver, ou qui en permet la comparaison avec une copie ou une reproduction de renseignements biométriques qui n'ont pas été obtenus directement du particulier »[536].

Pour finir, mentionnons que toute consultation d'un document technologique présentant une caractéristique personnelle et ayant pour but la preuve de l'identité devra être journalisée selon la LCCJTI[537]. De la sorte, chaque consultation effectuée devra être notée et gardée en mémoire, qu'elle ait été faite par une personne ou par un système automatisé. Précisons que l'Office québécois de la langue française définit un journal comme un « relevé chronologique des opérations informatiques, constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée »[538]. Les consultations devraient donc être notées en y inscrivant « dans un journal le déroulement des opérations informatiques ou des traitements effectués dans un système »[539]. La CAI recommande d'ailleurs que les données biométriques ne puissent être accédées que par le biais d'une application contenue dans un système et que tous les accès soient journalisés, même pour le personnel informatique[540].

2.3 La destruction

Une fois que l'objet sur lequel se fondait la reconnaissance de l'identité est réalisé, les données biométriques devraient être détruites. En effet, rappelons que le second alinéa de l'article 44 de la LCCJTI prévoit que « 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 »[541].

---

536 Art. 75 (7), *Loi de 1997 sur le programme Ontario au travail*.
537 Art. 41, *LCCJTI*.
538 OQLF, *Grand dictionnaire terminologique*, 2001, « Journal », en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8364904>.
539 OQLF, Grand dictionnaire terminologique, 2002, « Journaliser », en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8374422>.
540 CAI, « La biométrie au Québec : Les principes d'application pour un choix éclairé », *préc.*, note 354, p.5.
541 Art. 44, *LCCJTI*.

Cette règle s'applique tant aux entités privées qu'aux organismes publics. D'ailleurs, la *Loi sur l'accès* prévoit que « [l]orsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire »[542]. La *LPRPSP* prévoit de même que les données ne doivent être conservées et utilisées que pour les fins pour lesquelles elles ont été recueillies. Autrement dit, elles doivent être détruites suite à la réalisation de l'objectif de leur collecte et de leur traitement[543].

Cette obligation de détruire les données sera appréciée en fonction de la nature de la finalité en cause et de la durée de celle-ci. En pratique, cette question est délicate puisque la reconnaissance de l'identité aura le plus souvent lieu d'une manière ponctuelle et répétée dans le futur. En interprétant l'article 44, il importe de répondre adéquatement à cette question : quand est-ce que l'objet sur lequel se fonde l'identification ou que le motif qui justifie l'identification n'existe plus? Par exemple, si l'objet qui fonde l'authentification biométrique est le contrôle des horaires de travail, les données biométriques et autres informations afférentes devraient être détruites lorsque le salarié n'est plus à l'emploi de l'entreprise.

Pareillement, si l'objectif est de contrôler l'accès au compte d'un utilisateur d'une institution financière, ses données devraient en principe être supprimées dès que celui-ci ferme son compte. Par contre, si l'objectif de la collecte est la certification de l'identité pour l'obtention d'un titre, comme un permis de conduire ou une carte d'assurance maladie, l'objet du traitement des données pour l'identification s'élargi dans le temps et il devient beaucoup plus ardu d'y fixer un terme.

2.3.1 Les mesures de sécurité requises lors de la destruction

L'obligation de destruction des données biométriques prévue à l'article 44 LCCJTI est certes majeure, mais son utilité est relative s'il est possible de retracer les données dans le système à la suite de leur suppression. Comme nous le savons, l'information circulant sur

---

542 *Loi sur l'accès*, *préc*., note, art. 74.

543 Notons toutefois que la *LPRPSP* ne prévoit pas de devoir explicite de destruction de données, mais seulement implicite. Voir art. 12, *LPRPSP*.

Internet est difficilement effaçable et il est relativement facile de retrouver des données supprimées à l'aide de logiciels ou d'applications plus ou moins sophistiquées[544]. De ce fait, comment s'assure-t-on que la destruction des données biométriques est conforme et respecte la législation en vigueur?

Lorsque le moment où les renseignements biométriques doivent être détruits est déterminé, des mécanismes de sécurité devront ainsi être mis en œuvre pour garantir que la destruction des données a lieu de manière définitive et irréversible. Rappelons que l'article 10 de la *LPRPSP* prévoit que « [t]oute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[545].

De la sorte, les protections mises en place lors de la destruction devraient assurer que les données sont supprimées définitivement, en prenant soin notamment de supprimer les copies et de nettoyer tous les systèmes ayant enregistré les données. Certaines entreprises offrent d'ailleurs des services de destruction de données et garantissent que celle-ci a eu lieu de manière conforme en délivrant un certificat de destruction, de manière à ce que celles-ci ne puissent être récupérées ultérieurement[546].

Comme nous en avons déjà parlé relativement à la collecte et au traitement[547], toute organisation devrait instituer un comité interne d'implantation, de suivi et de contrôle de la gestion des données biométriques, et ainsi prévoir un encadrement et un processus strict de la

---

544 Voir WIKIPÉDIA, « Effacement de données », en ligne: <http://fr.wikipedia.org/wiki/Effacement_de_donn%C3%A9es>.
545 Art. 10, *LPRPSP*.
546 Voir <http://fr.ontrackdatarecovery.be/effacement-donnees-securise/>
547 Voir la page XX du présent mémoire.

destruction des données[548]. Un responsable de la destruction de données devrait être déterminé, suivant scrupuleusement un calendrier de conservation déjà établi.

****

Tel que précisé au premier chapitre, les mesures de sécurité qui seront requises pour les systèmes biométriques devront être évaluées en fonction du contexte d'utilisation des systèmes, puisque le législateur ne définit pas précisément la nature de ces mesures de sécurité. Le principe oblige toutefois les entreprises privées et les organismes publics québécois à appliquer des mesures de sécurité « propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[549]. Selon le professeur Vermeys, « définir précisément les mesures de sécurité requises serait offrir aux responsables du traitement une possibilité d'exonération »[550]. Ces derniers pourraient ainsi apporter la preuve qu'ils n'ont pas commis de faute en ayant respecté des prescriptions techniques plus ou moins pertinentes[551].

Dans ce contexte, et compte tenu des risques que comporte l'utilisation des données biométriques, nous croyons que la CAI devrait disposer de pouvoirs d'enquête et de vérification de tout système biométrique, ainsi qu'un pouvoir de vérification que les données sont détruites conformément à l'article 44, LCCJTI. Au niveau fédéral, une recommandation similaire avait déjà été formulée dans le cadre de la *Conférence citoyenne sur la biométrie et la sécurité*[552], à l'effet que les responsabilités du commissaire à la protection de la vie privée du Canada « soient élargies à la surveillance du développement et de l'utilisation des technologies biométriques susceptibles d'être utilisées au Canada »[553]. Qui plus est, il est

---

548 INSTITUT DU NOUVEAU MONDE, « Guide de participation, Rapport de la conférence citoyenne sur la biométrie et la sécurité », *préc*., note 42, p. 28.
549 Art. 10, *LPRPSP*; Art. 63.1, *Loi sur l'accès*.
550 Nicolas VERMEYS, *préc.*, note 423.
551 *Id*.
552 INSTITUT DU NOUVEAU MONDE, « Guide de participation, Rapport de la conférence citoyenne sur la biométrie et la sécurité », *préc*., note 42, p. 26.
553 *Id*.

recommandé que soient normalisées toutes procédures de mises à jour des données et de destruction de celles-ci[554].

[554] *Id*., p. 28.

Conclusion

Comment est-il possible, compte tenu de la rapidité d'évolution des technologies, d'assurer une cohésion et une harmonie entre ces dernières et le droit? Le législateur devrait-il faire preuve de plus de célérité et anticiper davantage les problématiques potentielles dans le développement des nouvelles technologies? Si certains risques sont bien connus, de nouveaux naîtront et c'est pour cette raison que notre système juridique doit être prêt à faire face à ces nouveaux enjeux, qu'ils soient concrets ou encore abstraits.

Parmi les risques ayant été discutés dans ce mémoire, mentionnons ceux que nous jugeons les plus importants à l'heure actuelle. D'abord, le détournement d'usage des données biométriques est un enjeu fondamental, bien que des balises juridiques viennent en principe encadrer ce risque[555]. Un individu « devrait savoir avec suffisamment de certitude quels renseignements le concernant sont détenus, par qui et comment y accéder »[556]. Comme nous l'avons vu, certaines mesures de sécurité adéquates et efficaces pourront venir réduire ce risque, si elles sont respectées et adéquatement mises en œuvre.

En second lieu, les tests de nécessité et de proportionnalité doivent impérativement être pris en compte pour évaluer la pertinence du projet biométrique. Comme nous l'avons mentionné, le Commissariat à la protection de la vie privée considère qu'il doit être prouvé par l'organisme utilisateur de ces systèmes que « toute mesure susceptible de porter atteinte à la vie privée répond à un besoin précis, qu'elle donnera probablement le résultat escompté et que l'intrusion dans la vie privée est proportionnelle à l'avantage attendu en matière de sécurité »[557]. On doit également « démontrer qu'aucune autre mesure moins susceptible de porter atteinte à la vie privée ne peut donner le même résultat »[558]. Ces conditions obligent à

---

555 Tels que les tests de proportionnalité, de nécessité et le principe de respect des finalités. Voir le chapitre 1 de la seconde partie du présent mémoire.

556 GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis no 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS) », adopté le 11 août 2004, p.8.

557 Lalita ACHARYA et Tomasz KASPRZYCKI, *préc.*, note 38, p.8.

558 *Id*.

s'assurer de l'adéquation de la solution d'identification aux besoins réels de l'organisme ou de l'entreprise désirant se prévaloir de cette nouvelle technologie.

D'autre part, il faut savoir que le degré de certitude de l'identification qu'apporte la saisie biométrique pourrait bien s'avérer être un couteau à double tranchant. Une telle fiabilité risque d'apporter une confiance aveugle en la machine biométrique et par conséquent, une plus grande facilité de malversation par les fraudeurs. En effet, avant que le véritable propriétaire des données biométriques subtilisées ne s'aperçoive de l'usurpation de son identité, le fraudeur pourrait ainsi disposer de celles-ci sans que quiconque ne s'interroge sur la validité de l'authentification. C'est pourquoi nous devons insister sur un enrôlement très rigoureux et une assistance humaine présente tout au long des étapes subséquentes.

En ce qui concerne la circulation des données et le risque de surveillance, Karim Benyekhlef note que « les diverses stratégies de cybersécurité mises de l'avant par les pays occidentaux se caractérisent par une méconnaissance des impératifs juridiques et constitutionnels de la vie privée et, encore là, par une incapacité à mesurer clairement l'ampleur des menaces à la cybersécurité »[559]. Qui plus est, « l'évolution technique entourant la circulation de l'information est de lourdes conséquences à l'égard des modules normatifs voués à régir le contrôle de l'information »[560]. La faisabilité juridique de l'implantation des techniques biométriques nécessitera donc un dialogue entre les expertises techniques et juridiques et une intégration de la dimension juridique très en amont afin déterminer précisément les véritables besoins de sécurité.

Comme nous l'avons abordé dans la première partie, il n'est pas garanti que toutes les caractéristiques physiques d'une personne pourront être captée par les systèmes biométriques. Ainsi, des mesures alternatives devraient être prévues pour pallier aux différentes contraintes individuelles. Tel que le mentionne l'OCDE, « les technologies fondées sur la biométrie ne représentent que l'une des composantes d'un système global de sécurité ou d'identification » et

---

559 Karim BENYKHLEF et Esther MITJANS (dir.), « Circulation internationale de l'information et sécurité », *préc*., note 233, p. IX.

560 *Id*., p. 210.

« il faut toujours créer des systèmes de secours et de traitement des exceptions appropriés faisant appel à des technologies complémentaires et supplémentaires, de telle sorte que notre dépendance à l'égard de la biométrie soit correctement dosée par rapport au profil global de menace du système et tienne compte des limites de la technologie » [561]. Il est d'ailleurs important de s'assurer « que les conséquences pour la sécurité de rejets erronés par un système pour des raisons accidentelles (problème de voix, cicatrice sur un doigt, pansement, etc.) ou à cause d'un simple dysfonctionnement du système sont correctement prises en compte »[562].

De plus, nous croyons qu'il serait préférable que les entreprises se tournent vers des technologies biométriques utilisant les données sans traces[563] et que celles-ci soient sauvegardées sur un support portable détenu par l'utilisateur. L'OCDE est aussi d'avis que des systèmes à petite ou moyenne échelle, internes et décentralisés sont à privilégier, ce qui permettrait de perfectionner le système à mesure que la technologie mûrit[564]. De la même manière, il faut envisager de recourir à des systèmes pilotes et des essais afin de mesurer l'efficacité d'un système avant de l'appliquer à grande échelle[565].

Comme nous l'avons vu, l'utilisation de la biométrie porte presque toujours atteinte à la vie privée. Si l'on considère que le principal avantage de l'utilisation de la biométrie pour les personnes physiques réside dans sa facilité d'utilisation, le spectre d'une telle machination nous interpelle forcément. Le défi est donc de concevoir un système qui « améliore réellement les services d'identification sans porter indûment atteinte à la vie privée »[566].

En définitive, l'industrie des technologies biométriques au Québec doit évidemment être mieux encadrée. Bien que certains risques aient été dégagés ici, il n'en demeure pas moins que le droit à la vie privée doit être bien compris et adapté au contexte technologique. Notons

---

561 OCDE, *préc*., note 77, p. 15.
562 *Id*.
563 Guillaume DESGENS-PASANAU et Éric FREYSSINET, « L'identité à l'ère numérique », *préc*., note 1.
564 OCDE, *préc*., note 1, p. 42.
565 *Id.*
566 CPVPC, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », *préc*., note 27.

toutefois que notre province est en avance en matière de législation sur plusieurs autres communautés et qu'un premier pas a tout de même été fait.

Bibliographie

ACHARYA, Lalita et KASPRZYCKI Tomasz, « La biométrie et son usage par l'État », Service d'information et de recherche parlementaire, Bibliothèque du Parlement, Ottawa, Canada, 11 septembre 2006, 26p.

ASPRAY, William and DOTY Philip, « Privacy in America, Interdisciplinary Perspectives », the scarecrow press inc. Chapter 6, Future biometric systems and Privacy, MODI, Shimon, Spafford, Eugene H. Purdue University, 2011.

ASSEMBLÉE PARLEMENTAIRE, « La nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme », Conseil de l'Europe, Avis n° 12528, 23 février 2011.

BELGUECHI R., LEGO T., CHERRIER E., and ROSENBERGER C., « Étude de la robustesse d'un système de biométrie révocable », Conférence sur la sécurité des architectures réseaux et des systèmes d'information (SAR SSI), 2011.

BENYEKHLEF, Karim et TRUDEL Pierre, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », *Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information*, Centre de recherche en droit public de l'Université de Montréal, septembre 1997, 32 p.

BERNIER Chantal, « Un cadre autour des nuages : Défis contemporains en matière de protection des renseignements personnels », Commentaires à l'occasion du colloque québécois sur la sécurité de l'information, Commissariat à la protection de la vie privée du Canada, La Malbaie, Québec, 18 octobre 2010.

CABAL Christian, « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », Office parlementaire d'évaluation des choix scientifiques et technologiques, France, 2003.

CAVOUKIAN Ann and STOIANOV Alex, « Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentification, Security AND Privacy », Information and Privacy Commissioner of Ontario, 2007.

CAVOUKIAN Ann, « Biometrics and Policing: Comments from a Privacy Perspective », Information and Privacy Commissioner of Ontario, 1999.

CAVOUKIAN Ann, « Consumer Biometric Applications: A discussion Paper », September 1999.

CAVOUKIAN Ann, « Fingerprint Biometrics : Address Privacy Before Deployment », Information and Privacy Commissioner of Ontario, 2008.

CAVOUKIAN Ann, « Privacy and Biometrics », Information and Privacy Commissioner of Ontario, 1999.

CEYHAN Ayse, « Enjeux d'identification et de surveillance à l'heure de la biométrie », dans *Culture et Conflits,* Vol. 64, France, 2006, p. 33-47.

CHASSÉ Max, « La Biométrie au Québec : les enjeux », Commission d'accès à l'Information, Québec, 2002.

CHASSIGNEUX Cynthia, « Quand la sécurité nationale interpelle la protection des renseignements personnels : l'exemple de la USA Patriot Act », dans Service de la formation continue du Barreau du Québec, *Vie privée et protection des renseignements personnels* (2006), Cowansville, Yvon Blais, 2006.

CHEPESIUK Caleb, KARPINSKI Mark et THÉROUX Charles, « La certification de l'identité et la protection des droits de la personne », Commission canadienne des droits de la personne, août 2010.

CLARKE Roger, « Biometrics and Privacy », Department of Computer Science, Australian National University, April 2001, en ligne: <http://www.rogerclarke.com/DV/Biometrics.html>.

CLARKE Roger, « Identified, Anonymous and Pseudonymous Transactions : The spectrum of Choice », *Document prepared for the User Identification & Privacy Protection Conference*, Stockholm, June 14-15, 1999.

CLUSIF, « Techniques de contrôle d'accès par biométrie », Dossier technique présenté à la Commission Techniques de Sécurité Physique, Club de Sécurité des systèmes d'information français (CLUSIF), 2003.

COHEN Stanley A., « Privacy, crime and terror : legal rights and security in a time of peril », LexisNexis, Ontario, 2005

COLLIN Pierre et COLIN Nicolas, « Mission d'expertise sur la fiscalité de l'économie numérique », Ministère de l'économie et des finances, République française, janvier 2013.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Une candidate au GMAT s'oppose à l'utilisation de la technologie de reconnaissance du réseau veineux de la paume de sa main (Re) », 2011 CanLII 99346 (CVPC).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Des données au bout des doigts, La biométrie et les défis qu'elle pose à la protection de la vie privée », Novembre 2011.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle », Document de référence, Novembre 2010.

COMMISSION DE L'ÉTHIQUE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques », Gouvernement du Québec, 2004.

COMMISSION DE L'ÉTHIQUE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « Viser un juste équilibre, Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité », Avis adopté à la 34e réunion de la Commission, Gouvernement du Québec, 12 février 2008.

COMMISSION DE LA CULTURE, DE LA SCIENCE ET DE L'ÉDUCATION, Conseil de l'Europe, Assemblée parlementaire, 23 février 2011, Renvoi 3288 du 22 janvier 2007, document 12528.

COMMISSION NATIONALE DE L'INFORMATIQUE ET LIBERTÉS (CNIL), 21e rapport d'activités, France, 2000.

CRETTIEZ Xavier et PIAZZA Pierre, « Du papier à la biométrie : identifier les individus », *Presses de la Fondation nationale des sciences politiques*, Paris 2006.

CROMPTON Malcolm, « Biometrics and Privacy », in *Privacy Law and Policy Reporter*, Australasian Legal Information Institute, 2002.

DESGENS-PASANAU Guillaume et FREYSSINET Éric, « L'identité à l'ère numérique », Éditions Dalloz, 2009.

DUMORTIER, F., « L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice : une affaire de balance ou une question de dignité? », Académie de droit européen, Éditions Springer, 10 février 2009.

CHERRIER E., LACHARME P. and ROSENBERGER C., « La biométrie révocable : principes et limites », Atelier de Protection de la Vie Privée (APVP), 2012.

FROOMKIN Michael, « The Essential Role of Trusted Third Parties in Electronic Commerce », (1996) 75 *Oregon L. Rev.* 49, 51-53

GAUTRAIS Vincent et TRUDEL Pierre, « Circulation des renseignements personnels et web 2.0 », Éditions Thémis, 2010, 231 p.

GRATTON Éloïse, « Understanding Personal Information : Managing Privacy Risks », LexisNexis, 2013, 515p.

GROTHER Patrick, CHANDRAMOULI Ramaswamy, « Biometric Data Specification for Personal Identity Verification », National Institute of Standards and Technology, NIST special publication 800-76-1, U.S. Department of Commerce, January 2007.

GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis 3/2005 sur l'application du règlement (CE) no 2252/2004 du Conseil du 13 décembre 2004

établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, *Journal officiel L 385 du 29 décembre 2004 p. 1-6*, 1710-01/05/FR, WP 112 04/09/12.

GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis 4/2007 sur le concept de données à caractère personnel », Adopté le 20 juin 2007, 01248/07/FR, WP 136.

GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Avis no 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS) », adopté le 11 août 2004.

GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », adopté le 1er août 2003, Avis 5/2003, 12168/02/FR, GT 80.

GUERRIER, Claudine et CORNELIE Laure-Anne, « Les aspects juridiques de la biométrie », 2005.

HAO Feng, ROSS Anderson and DAUGMAN John, « Combining cryptography with biometrics effectively », Computer Laboratory, Technical Report, no 640, Cambridge University, UK, 2005.

HARNOIS, Isabelle, « La protection constitutionnelle et quasi-constitutionnelle du droit au respect de la vie privée et les banques de données informatisées », dans Congrès annuel du Barreau (1996), Montréal, 1997, 667p.

HES Ronald, HOOGHIEMSTRA T.F.M. and BORKING John, « At Face Value, on biometrical identification and privacy, Registratiekamer, September 1999.

HILDEBRANDT Mireille and GUTWIRTH Serge, « Profiling the European Citizen: A Cross-Disciplinary Perspectives », Springer, 2008.

HOBOKEN Joris Van, ANRBAK Axel and EIJK Nico Van, « Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act », Institute for Information Law, University of Amsterdam, November 27th, 2012.

HUPPÉ L., « La dignité humaine comme fondement des droits et libertés garantis par la Charte », (1988) 48 *R. du B.* 724-728

INSTITUT DU NOUVEAU MONDE, « Rapport de la conférence citoyenne sur la biométrie et la sécurité », dans le cadre du projet Jeunes, Sciences et Démocratie, Montréal, 11-12 mars et 22-23 avril 2006.

JAIN Anil K., ROSS Arun A. and NANDAKUMAR Karthik, « Introduction to Biometrics », Springer, 2011, 174 p.

KADRY Seifedine and SMAILI Khaled, « A Design and Implementation of a Wireless Iris Recognition Attendance Management System », Faculty of Engineering, Lebanese International University, ISSN 1392 – 124X Information Technology and Control, 2007, Vol.36, No.3, p. 323.

KANT Emmanuel, « Fondements de la métaphysique des moeurs », 1785, trad. par V. Delbos, Paris, Vrin, 1980.

KOURKOUMELIS Nikolaos and TZAPHLIDOU Margaret, « Eye Safety Related to Near Infrared Radiation Exposure to Biometric Devices », in *The Scientific World Journal*, Department of Medical Physics, Medical School, University of Ioannina, Ioannina, Greece, March 1st, 2011.

LECERF Jean-René, « Rapport d'information au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire », no 439, présenté au Sénat, 29 juin 2005.

LIGUE DES DROITS ET LIBERTÉS, « La biométrie: des implications majeures pour nos droits et libertés », Mémoire présenté à la Commission de l'éthique de la science et de la technologie du Québec, novembre 2005.

MATSUMOTO Tsutomu, MATSUMOTO Hiroyuki, YAMADA Koji and HOSHINO Satoshi, « Impact of Artificial *Gummy* Fingers on Fingerprint Systems », Yokohama National University, Japan**,** 2002.

HILDEBRANDT Mireille et GUTWIRTH Serge, « Profiling the European Citizen : A Cross-Disciplinary Perspectives », Springer, 2008,

NSTC Subcommittee on Biometrics, « Privacy and Biometrics : Building a Conceptual Foundation », September 2006, en ligne : <http://www.biometrics.gov/documents/privacy.pdf>.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Technologies fondées sur la biométrie », Éditions OCDE, No. 101, 2005.

ORR Stephen, « Privacy of Genetic Information in Canada: A Brief Examination of the Legal and Ethical Tools That Should Frame Canada's Regulatory Response », in Canadian Journal of Law and Technology, Volume 3, number 3, 2004.

PATENAUDE P., « L'expertise en preuve pénale, Les sciences et techniques modernes d'enquête, de surveillance et d'identification », Cowansville, Yvon Blais, 2003.

PATRICK Andrew, « Acceptance of Biometrics, Things That Matter That We Are Ignoring », *Presentation to the International Workshop on Usability and Biometrics*, Information Security Group, Institute of Information Technology, National Research Council Canada, Washington, D.C., June 23-24, 2008.

PROULX Daniel, « Le concept de dignité et son usage en contexte de discrimination: deux Chartes, deux modèles », *Revue du Barreau*, numéro spécial, 2003

RILEY, Steve, « It's Me, and Here's My Proof: Why Identity and Authentication Must Remain Distinct », 2006, en ligne : <http://technet.microsoft.com/en-us/library/cc512578.aspx>.

SCHNEIER Bruce, « Biometrics : Truths and Fictions », Crypto-Gram Newsletter, August 15th, 1998, online : <www.schneier.com/crypto-gram-9808.html#biometrics>.

SHERMAN Darcie, « Biometric Technology: The Impact on Privacy », CLPE Research Paper, 1/2005, Vol. 01 No 1, Osgoode Hall Law School, Toronto, 2005.

SHONIREGUN Charles A. and CROSIER Stephen, « Securing Biometrics Applications », Éditions Springer, University of East London, United Kingdom, 2008.

SOLOVE Daniel, « Why Privacy Matters Even if You Have 'Nothing to Hide' », The Chronicle Review, May 15th, 2011.

SOUTAR Colin, « La biométrie au Canada : équilibrer sécurité et vie privée », dans *Dimensions*, Chroniqueur invité, Conseil national de recherches Canada, Archivé, n°9.

SPINNEY Laura, « Crooks smelly armpits give the game away », *New Scientist*, Vol. 143, Issue 1943, September 14th, 1994.

STODDART, Jennifer, « Des technologies de surveillance sous surveillance », discours [en ligne], septembre 2001.

THEOFANOS M., STANTON B. and WOLSON C.A., « Usability & Biometrics: Ensuring Successful Biometrics Systems », Juin 2008, en ligne: <Http://zing.ncsl.nist.gov/biousa/docs/usability_and_biometrics_final2.pdf>.

THOMAS-SERTILLANGES Jean-Baptiste, « Identification biométrique, protection des données et droits de l'homme », Mémoire, Droit de l'internet public, Université Paris I, 2007.

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

TRUDEL Pierre, « Introduction à la Loi concernant le cadre juridique des technologies de l'information », Cowansville, Yvon Blais, 2012, 303p.

TRUDEL Pierre, POULIN Daniel, F. ABRAN et al., « La loi en ligne : La Loi concernant le cadre juridique des technologies de l'information », 2001, 159p.

ULUDAG Umut and K. JAIN Anil, « Attacks on Biometric Systems : A Case Study in Fingerprints », Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA 48824.

VAN DEN HOVEN Jeroen, « Information Technology, Privacy, and the Protection of Personal Data », in Jeroen Van Den Hoven and John Weckert, Information Technology and Moral Philosophy (New York: Cambridge University Press, 2008) 301 à 311.

VEN DER PLOEG Irma, « Genetics, biometrics and the informatization of the body », *iBMG*, Erasmus University MC, Rotterdam and Zuyd University, Heerlen, Ann Ist Super Sanità 2007, vol. 43, No. 1: 44-50, The Netherlands.

VERMEYS Nicolas W., « Responsabilité civile et sécurité informationnelle », Cowansville, Yvon Blais, 2010.

WALTER Jean-Philippe, « Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé », *26e Conférence internationale des Commissaires à la protection des données et à la vie privée*, Le préposé fédéral suppléant de Suisse, Wroclaw, Pologne, 14-16 septembre 2004.

WINN Jane Kaufman, « Couriers Without Luggage: Negotiable Instruments and Digital Signatures », (1998) 49, *S.C.L. Rev.* 739, 763 et 764.

WOODMARD John D., « Biometrics should not be automatically construed as privacy's foe. Quite to the contrary, biometrics is privacy's friend », Proceedings of the IEEE, vol.85, n°9, September 1997.

ZUREIK Elia, HARLING STALKER Lynda, SMITH Emily, LYON David and CHAN Yolande, « Surveillance, Privacy and the Globalization of Personal Information », *International comparisons,* McGill-Queen's University Press, Montreal & Kinsgton, 2010.

Table des jugements

Cour suprême du Canada

Cour d'appel fédérale

Cour d'appel du Québec

Cour d'appel de la Colombie Britannique

Cour fédérale

Cour supérieure

A.P. c. *L.D*, (2001) R.J.Q. 16

Charbonneau c. *Poupart*, (1990) R.J.Q. 1136 (C.S.)

Raphael M'Boutchou c. *Banque de Montréal*, EYB-2008-150981 (C.S.)

Commissariat à la protection de la vie privée du Canada

CPVPC, « Une organisation utilise la biométrie à des fins d'authentification », Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2004-281

Commission d'accès à l'information du Québec

C.R. c. *Loto Québec*, 2012 QCCAI 300

Décisions arbitrales

*407 ETR Concession Company Limited and National automobile, Aerospace, Transportatio*n and *General Workers Union of Canada, Caw-Canada and it's Local 414,* 2007 Canlii 1857 (ON LA).

Canada Safeway Ltd. and *U.F.C.W., Local 401* (2005), 145 L.A.C. (4th) 1

Syndicat des salariés de Mométal (C.S.N.) et *Mométal inc*., D.T.E. 2001 T-919

Union des routiers, brasseries, liqueurs douces et ouvriers de diverses industries, local 1999 et *L'Oréal Canada,* Tribunal d'arbitrage, AZ-50832524, 6 février 2012.

Table de la législation