



## **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**

## Avant-propos

La *Ligue des droits et libertés* est un organisme à but non lucratif, indépendant et non-partisan fondé en 1963. Les objectifs poursuivis par la Ligue sont la défense et la promotion des droits reconnus dans la *Charte internationale des droits de l'homme*, dont elle soutient l'universalité et l'indivisibilité. La *Ligue des droits et libertés* est membre de la *Fédération internationale des ligues des droits de l'homme* (FIDH). Elle est une des plus anciennes organisations de droits des Amériques.

Dans le cadre de sa réflexion sur les enjeux éthiques soulevés par l'utilisation de la biométrie à des fins de sécurité la *Commission de l'éthique de la science et de la technologie du Québec* a invité les organisations de la société civile à lui soumettre leurs observations sur les impacts de la biométrie. C'est avec un vif intérêt que nous répondons à cette invitation en vous soumettant le présent mémoire et nous espérons que la démarche entreprise permettra d'amorcer un débat public sur cette question aux enjeux importants pour notre société.

## Introduction

Depuis les dernières années, et particulièrement depuis les mesures de lutte au terrorisme mises en place par les États, la Ligue des droits et libertés est particulièrement préoccupée par les techniques, programmes et politiques de surveillance des citoyens : caméras de surveillances, constitution de bases de données et de mégafichiers, partage d'information sur les citoyens entre agences de l'État ainsi qu'avec des agences étrangères (incluant les services de police et les agences de renseignements), documents d'identité obligatoires et universels, affaiblissement des mécanismes de protection de la vie privée et de contrôle de ces infrastructures de surveillance. Bien que la biométrie ne soit pas le seul élément soutenant ces phénomènes, nous estimons qu'elle constitue un facteur important, et inquiétant, de l'accroissement de la surveillance des citoyens par l'État.

La capacité d'identifier les individus semble devenue une obsession des gouvernements à la suite des attentats du 11 septembre 2001. Sans en avoir démontré la nécessité et presque toujours sans aucun véritable débat démocratique, les gouvernements de plusieurs pays ont adopté un nouveau paradigme en vertu duquel notre sécurité serait assurée à travers une surveillance généralisée des populations.<sup>1</sup> Dans cette perspective, ces gouvernements ont opté pour un recours massif aux nouvelles technologies : informatique, communications électroniques, caméras de surveillance et biométrie.<sup>2</sup> D'autant plus que le développement extrêmement rapide des technologies ainsi que la baisse constante de leur coût rendent maintenant possible leur utilisation à grande échelle. Il suffit de penser au fait que plus de deux millions de caméras de surveillance sont déployées au Royaume-Uni. Les budgets alloués à la sécurité nationale ont augmenté en flèche<sup>3</sup> et une industrie de la sécurité a rapidement pris corps, qui fait partout la promotion de ces nouveaux outils de surveillance.<sup>4</sup>

Le recours généralisé à ces technologies est en voie de transformer considérablement les rapports entre l'individu et l'État ainsi que l'exercice de la vie démocratique. Il menace plusieurs libertés fondamentales, de même que le

---

<sup>1</sup> Voir *Campagne contre la surveillance globale*, [www.i-cams.org](http://www.i-cams.org)

<sup>2</sup> Secrétariat de l'intégration de l'information de la justice, Sécurité publique et Protection civile Canada, *Combattre le terrorisme à l'aide de la biométrie*, [IJ@l'oeuvre](mailto:IJ@l'oeuvre), vol. 3. no. 1, été 2004.

<sup>3</sup> Le budget pour l'année 2005 du *Department of Homeland Security* des États-Unis est de 40,1 milliards de dollars US. Cette somme représente 57 % des dépenses pour la sécurité du territoire. (<http://www.heritage.org/research/features/issues2004/homesecurity.cfm>)

Depuis 2001, le gouvernement du Canada a dépensé 9 milliards de dollars au chapitre de la sécurité. (Le Devoir, 24 novembre 2005)

<sup>4</sup> Brendan I. Koerner, *The Security Traders*, Mother Jones, septembre/octobre 2002, page 42.

caractère inviolable de la dignité humaine ainsi que la vie privée. Au Canada et au Québec, nous sommes déjà grandement engagés, par des ajouts à la pièce, dans la mise en place d'une infrastructure de connaissance et de reconnaissance de tous les citoyens, laquelle risque de faire sauter toutes les barrières de protection de la vie privée de chacun.

Dans ce mémoire, la Ligue des droits et libertés traite la question de la biométrie en lien avec l'accroissement indéniable des infrastructures de surveillance des citoyens par l'État. Nous examinons d'abord ce qu'on entend par « biométrie », puis les systèmes mis en place aux niveaux international, canadien et québécois, les problèmes que peut poser l'utilisation à grande échelle de la biométrie. Le mémoire se termine par quelques recommandations.

## Les limites des systèmes biométriques

Il importe ici de distinguer deux objectifs fréquemment associés à la biométrie :

- L'**authentification** consiste à s'assurer de la concordance des données biométriques d'une personne avec celles colligées sur un support (passeport, carte d'identité, etc.). C'est ce que fait un douanier lorsqu'il compare un visage à la photo dans le passeport. Ce type d'opération ne permet pas la traçabilité ou le profilage des personnes.
- L'**identification** est la recherche de l'identité d'une personne en comparant les données biométriques de la personne avec celles d'un ensemble de personnes dans une base de données.

Les nouvelles technologies, dont la biométrie, ne permettent pas seulement de faire autrement des tâches existantes, comme l'**authentification**, mais aussi d'accomplir pour la première fois sur une grande échelle des tâches d'**identification**. La capacité d'identifier les individus, de les relier à des banques de données et de partager ces données requiert des systèmes d'identification standardisés, et exploitables par des machines. Les systèmes d'identification biométriques répondent à ces exigences. L'évolution des technologies permet d'exploiter à des fins biométriques de plus en plus de caractéristiques physiologiques, biologiques et comportementales d'un individu :

- **Physiologiques** – empreintes digitales, iris, rétine, faciès, forme de la main;
- **biologiques** – ADN, odeur, salive, urine;
- **comportementales** – écriture, démarche.

Certaines de ces techniques, comme la reconnaissance du visage ou de la démarche, peuvent être utilisées à distance et donc à l'insu de la personne. Plusieurs, comme la reconnaissance des empreintes digitales, de la forme de la main, de l'iris et du visage, sont déjà opérationnelles et utilisées, alors que d'autres sont encore au stade du développement.<sup>5</sup>

Même si la caractéristique physique utilisée par un système biométrique donné est réputée être unique à cette personne, cela ne signifie pas que les systèmes biométriques sont sans failles. Un système biométrique analyse la caractéristique physique choisie au moyen d'un capteur et la convertit en une signature électronique (un code). Or, d'une fois à l'autre, pour toutes sortes de raisons qui dépendent de la technique utilisée, le système ne génère pas exactement la même signature pour la même personne. Les utilisateurs du

---

<sup>5</sup> Pour une description des différents systèmes biométriques voir *La biométrie au Québec : Les Enjeux*, Commission d'accès à l'information, juillet 2002, disponible sur le site : [http://www.cai.gouv.qc.ca/06\\_documentation/01\\_pdf/biom\\_enj.pdf](http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf)

système doivent donc prévoir une marge d'erreur dans la comparaison des signatures. Une marge trop étroite engendrera un haut taux de faux rejets, c'est-à-dire de personnes qui sont rejetées par le système qui n'arrive pas à les reconnaître. Par contre, une marge trop large augmentera le taux de fausses acceptations, c'est-à-dire de personnes non autorisées qui sont acceptées.<sup>6</sup> Par exemple, un test du système de reconnaissance de l'iris de la compagnie Iridian, effectué par le Pentagone sur un échantillon de 270 personnes, a réussi à identifier correctement la personne dans 94 % des cas, alors que le fabricant proclamait un taux de 99,5 %.<sup>7</sup> Il s'agissait là d'un petit échantillon. Or, le taux de réussite d'un système d'identification biométrique diminue lorsque la taille de l'échantillon augmente. Le taux d'erreur sur un échantillon plus grand serait considérablement plus élevé. Pour compenser cette lacune un mot de passe ou une carte sont souvent associés aux systèmes biométriques.

Le système d'identification biométrique le plus répandu dans le monde<sup>8</sup>, celui des empreintes digitales, est particulièrement menaçant pour la vie privée; nous laissons nos empreintes partout où nous passons. L'identité biométrique a aussi la propriété d'être «indélébile». Nous ne pouvons pas nous départir de nos caractéristiques physiologiques ou biologiques. Paradoxalement, cette propriété rend le problème de la «perte d'identité» particulièrement aigu. Comment un individu qui n'est plus reconnu par le système prouve-t-il qu'il est celui qu'il prétend être?

Il faut également retenir les risques associés à l'utilisation de données biométriques identifiées par la *Commission d'accès à l'information* : risques de vol permanent d'identité, de sécurité reliée à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage de technologies, etc.<sup>9</sup>

Par ailleurs, la capacité de ces systèmes d'atteindre les objectifs de sécurité invoqués pour justifier leur déploiement n'a pas été démontrée, bien au contraire. Les terroristes qui ont perpétré les attentats du 11 septembre 2001 voyageaient sous leur véritable identité; un passeport biométrique n'aurait rien changé. Pas plus que les milliers de caméras de surveillance n'ont empêché les attentats de Londres.

---

<sup>6</sup> *Idem*, page 20.

<sup>7</sup> Declan McCullagh et Robert Zarate, *Scanning Tech a Blurry Picture*, Wired News, 16 février 2002, <http://www.wired.com/news/politics/0,1283,50470,00.html>

<sup>8</sup> Le système IAFIS (*Integrated Automated Fingerprint Identification System*) du FBI aux États-Unis possède, à lui seul, une banque d'empreintes digitales de plus de 40 millions d'individus. C'est la plus grosse banque de données biométriques au monde.

<sup>9</sup> *La biométrie au Québec : Les principes d'application pour un choix éclairé*, Commission d'accès à l'information, juillet 2002, page 4: [http://cai.gouv.qc.ca/06\\_documentation/01\\_pdf/biom\\_appl.pdf](http://cai.gouv.qc.ca/06_documentation/01_pdf/biom_appl.pdf)

# L'identification par la biométrie et les fichiers de renseignements personnels

## ... aux niveaux canadien et international

Les systèmes biométriques à plus grande échelle sont ceux déployés au niveau international sur la base de décisions prises par des instances sur lesquelles les citoyens n'ont aucune prise. Ainsi, *l'Organisation de l'aviation civile internationale (OACI)* a décidé au printemps 2004 d'adopter le passeport biométrique avec puce d'identification radio-fréquence (RFID)<sup>10</sup> comme nouvelle norme de passeport. La nouvelle génération de passeports canadiens se conformera à cette norme. En juin 2003, *l'Organisation internationale du travail (OIT)* a adopté une convention faisant de la pièce d'identité des gens de mer « la première solution biométrique globale au monde ».<sup>11</sup>

Au Canada, le programme CANPASS-Air, dont le premier centre d'inscription a ouvert à l'aéroport de Vancouver en mars 2003, permet à des grands voyageurs de franchir plus rapidement les postes de douane au moyen d'une carte d'identité biométrique faisant appel à la reconnaissance de l'iris. Au cours des six prochains mois, *Citoyenneté et Immigration Canada (CIC)* procédera à un essai en conditions réelles des technologies biométriques de la reconnaissance du visage et des empreintes digitales auprès de 15 000 demandeurs de visa de résidents permanents, de permis temporaires et réfugiés.

Mais l'intérêt ultime des programmes d'identification repose sur des visées plus ambitieuses. À l'instar des États Unis le gouvernement canadien prévoit la mise en place d'un programme *Secure flight* selon lequel tous les voyageurs aériens seront profilés à partir de l'analyse informatique de banques de données et se verront attribuer, à partir de critères secrets, un niveau de risque « vert » (vérifications courantes), « jaune » (risque intermédiaire – interrogatoire et vérifications plus poussées) ou « rouge » (haut risque – interdiction de prendre l'avion et arrestation pour enquête).

Rappelons que le gouvernement canadien a établi en octobre 2002 un mégafichier sur les voyageurs à l'international qui contient des renseignements sur les passagers : nom, vol, siège choisi, destination, mode de paiement et carte de crédit utilisée, bagages et compagnons de voyage. Ces données seront conservées pendant six ans et pourront être comparées à d'autres bases de

---

<sup>10</sup> RFID - *Radio Frequency Identification Device*: une « puce » électronique minuscule et bon marché qui peut être implantée dans n'importe quel produit ou document, ou même sous la peau d'une personne. Elle a pour caractéristique de s'identifier et de transmettre l'information qu'elle contient lorsqu'elle se trouve à proximité d'un lecteur conçu pour l'interroger.

<sup>11</sup> Secrétariat de l'intégration de l'information de la justice, Sécurité publique et Protection civile Canada, *Combattre le terrorisme à l'aide de la biométrie*, [IJ@l'oeuvre](mailto:IJ@l'oeuvre), vol. 3. no. 1, été 2004.

données, entre autres aux fichiers de police. En mai 2004, le gouvernement adoptait le projet de loi C-7<sup>12</sup> sur la sécurité publique qui amende la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)* et qui autorise les organisations à agir à titre d'agents de l'autorité en recueillant des renseignements personnels sans consentement dans le seul but de communiquer ces renseignements au gouvernement et à des organismes du maintien de l'ordre. Les modifications apportées par le projet de loi C-7 à la *Loi sur l'aéronautique* obligent les transporteurs aériens et les exploitants de systèmes de réservation de services aériens à transmettre des renseignements relatifs aux passagers à des représentants du gouvernement, dont la GRC et le SCRS, ainsi qu'à des représentants de gouvernements étrangers.

L'*Accord sur la frontière intelligente*, signé par le Canada et les États Unis le 12 décembre 2001, prévoit un nouveau système électronique d'échange d'information sur les casiers judiciaires comprenant, entre autres, les empreintes digitales. Cet accord comporte également des ententes de partage d'information en fonction de quoi :

- L'information échangée sur les individus peut être très étendue;
- Les bases de données peuvent faire l'objet d'échanges d'information systématiques;
- L'information reçue n'est protégée que par les lois du pays qui la reçoit;
- L'information peut être transmise à un tiers.

Le 9 septembre 2002, dans le cadre de cette entente qui comporte un plan d'action en 30 points<sup>13</sup>, Jean Chrétien et George Bush se sont entendus sur l'identification biométrique qui en constitue le premier point : « *Le Canada et les États-Unis se sont entendus pour fixer des normes communes et pour adopter une technologie compatible et interopérable afin de lire ces données. En ce qui a trait à l'intérêt d'avoir des cartes pouvant être utilisées pour divers modes de voyage, nous nous sommes mis d'accord sur des cartes qui peuvent emmagasiner des données biométriques multiples.* »<sup>14</sup> (nous soulignons)

Les échanges d'informations et de renseignements sur les citoyens entre les agences des États ont connu une augmentation substantielle depuis les événements du 11 septembre 2001<sup>15</sup>. Les agences de renseignements et

---

<sup>12</sup> *Loi modifiant certaines lois fédérales et édictant des mesures de mise en oeuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, L.C. 2004, c.15 (Projet de loi C-7)

<sup>13</sup> Ministère des Affaires étrangères et du Commerce international, *Plan d'action pour une frontière intelligente*, Rapport d'étape, 6 décembre 2002, <http://www.dfait-maeci.gc.ca> .

<sup>14</sup> Ministère des Affaires étrangères et du Commerce international, *Rapport d'étape Chrétien-Bush concernant le plan d'action sur la frontière intelligente*, 9 septembre 2002, [http://www.dfait-maeci.gc.ca/can-am/main/border/chr%C3%A9tien\\_bush\\_status-fr.asp](http://www.dfait-maeci.gc.ca/can-am/main/border/chr%C3%A9tien_bush_status-fr.asp)

<sup>15</sup> Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, voir les témoignages de Ward Elcock (SCRS), W. John Hooper (SCRS), James Loeppky, 21, 22,

d'application de la loi travaillent en collaboration dans diverses équipes intégrées incluant des agences et services policiers provinciaux.<sup>16</sup> Le nombre d'agents du FBI au Canada aurait augmenté à un niveau sans précédent<sup>17</sup>. Des renseignements fournis par la GRC se retrouvent dans une des plus importantes bases de données des États-Unis, le TECS (*Treasury Enforcement Communication System*)<sup>18</sup>. Cette base de données constitue de fait un mégafichier puisqu'elle intègre au moins 19 autres bases de données elles-mêmes formées de multiples autres qui possèdent, à elles seules, une somme impressionnante d'informations<sup>19</sup>. Le risque de partage de renseignements sur l'identification des individus entre les agences de l'État et les corps policiers ou les agences de renseignements est de plus en plus important.

### ... et au Québec

La sécurité nationale n'est pas le seul motif invoqué pour instaurer des systèmes d'identification biométriques. Depuis la fin des années 1990 le gouvernement du Québec caresse le grand projet d'instaurer un système de gestion des services gouvernementaux qui repose sur les nouvelles technologies de l'information et des communications. L'inforoute, le gouvernement en ligne, la carte santé à puce et le dossier santé partageable font partie de ce projet. L'objectif du gouvernement du Québec est de mettre en place une structure juridique et technique qui puisse servir non seulement au gouvernement, mais aussi à l'entreprise privée. La question de la vérification de l'identité est centrale à ce projet.

---

23 et 30 juin, et 6 juillet 2004. Signalons que le nombre d'agents de la GRC affectés à la sécurité nationale est passé à plus de 2 000 depuis le 11 septembre 2001 (témoignage de Michel Cabana, 29 juin 2005). Lire à ce sujet le « Mémoire relatif à l'enquête sur les faits », déposé par la *Coalition pour la surveillance internationale des libertés civiles* (CSILC) devant la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, septembre 2005, disponible en ligne sur le site de la Ligue des droits et libertés : [http://www.liguedesdroits.ca/documents/surveillance/arar/CSILC-Arar-mem\\_faits\\_sept05.pdf](http://www.liguedesdroits.ca/documents/surveillance/arar/CSILC-Arar-mem_faits_sept05.pdf)

<sup>16</sup> Équipes intégrées de la police des frontières (EIPF), Équipes intégrées d'exécution de la Loi sur l'immigration (EIELI), Équipes intégrées de la sécurité nationale (EISN), Centre d'évaluation intégrée des menaces (CEIM). Voir à ce sujet le « Document de consultation, Examen de la politique » publié par la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, octobre 2004, modifié le 14 décembre 2004, disponible en ligne sur le site de la Commission : [www.ararcommission.ca](http://www.ararcommission.ca)

<sup>17</sup> Moira Welsh, *FBI Boosts Presence in Canada to Help RCMP*, Toronto Star, 3 novembre 2001, p. A6; Stephen W. Yale-Loehr et Matthew X. Vernon, *An Overview of U.S. Immigration Watchlists and Inspection Procedures, Including U.S.-Canadian Information Sharing* (Submission to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, 31 mai 2005).

<sup>18</sup> *An Overview of U.S. Immigration Watchlists... op. cit.*, note 17.

<sup>19</sup> À titre d'exemple, la base de données du FBI, le NCIC, possède de l'information sur 41 millions de criminels et 2,5 millions de terroristes ou de personnes que l'on soupçonne d'être reliées au terrorisme.

En mars 1997, le Secrétariat de l'autoroute de l'information (SAI) publiait un document de référence *L'identification des citoyens et l'inforoute* dans lequel il proposait la carte à microprocesseur comme moyen d'identification des citoyens. Le SAI préconisait une carte ayant une architecture permettant une évolution ultérieure, par exemple l'ajout de nouvelles fonctions et informations.<sup>20</sup> Le SAI évaluait que la RAMQ et le MSSS seraient probablement les premiers organismes gouvernementaux à émettre des cartes à microprocesseur pour les professionnels et les bénéficiaires du régime d'assurance maladie et qu'il serait envisageable de vendre de l'espace mémoire dans la carte à des organisations ayant de larges clientèles, y compris à l'entreprise privée.<sup>21</sup>

Pour paver la voie à ces systèmes le gouvernement en a établi le cadre juridique dans la *Loi concernant le cadre juridique des technologies de l'information* entrée en vigueur le 1<sup>er</sup> novembre 2001. Cette loi, entre autres:

- Établit la reconnaissance juridique des documents technologiques;
- Assure la concertation en vue d'harmoniser les systèmes, les normes et les standards techniques permettant la communication au moyen de documents technologiques ;
- Énonce en outre les principes de la responsabilité des différents prestataires de services (qui peuvent être privés et étrangers) agissant à titre d'intermédiaires sur les réseaux de communication ;
- Reconnaît également la possibilité d'utiliser divers modes, dont la biométrie, d'authentification de l'identité d'une personne qui communique au moyen d'un document technologique ;
- Prévoit des moyens de faire le lien entre une personne et le document par lequel elle exprime sa volonté ;
- Contient des dispositions pour baliser la prestation de services de certification et de répertoire et offre à tout prestataire de services de certification, qu'il soit du Québec ou d'ailleurs, de se faire accréditer, en fonction des mêmes critères d'appréciation, par une personne ou un organisme déterminé par le gouvernement.

Le 19 décembre 2001 le gouvernement du Québec présentait un avant projet de loi intitulé *Loi sur la carte santé du Québec*. Sous couvert d'un projet visant à rendre disponible un résumé des renseignements de santé accessible dans tous les lieux de pratique, le gouvernement proposait une carte permettant de mieux contrôler les coûts des soins de santé, dont l'usage n'aurait pas été limité au secteur de la santé et qui aurait pu servir de carte d'identité citoyenne.<sup>22</sup> Ce

---

<sup>20</sup> Secrétariat de l'autoroute de l'information, *L'identification des citoyens et l'inforoute* – ISBN 2-550-31399-2, page 38.

<sup>21</sup> *Idem*, pages 36 et 37.

<sup>22</sup> Fédération des infirmières et infirmiers du Québec, *La carte santé du Québec : un détournement majeur*, Mémoire déposé à la Commission des affaires sociales du Québec, 8 février 2002.

projet de loi a suscité beaucoup d'opposition et est mort au feuilleton lors du déclenchement des dernières élections provinciales.

Le 25 novembre 2005, l'Assemblée nationale adoptait le projet de loi 83 modifiant la *Loi sur les services de santé et les services sociaux et d'autres dispositions législatives*. La loi prévoit que la *Régie de l'assurance maladie du Québec* (RAMQ) offrira un service permettant de transmettre à un intervenant<sup>23</sup> la liste des établissements où sont conservés des fragments du dossier patient, accompagnée du « numéro d'identification unique de cette personne ». <sup>24</sup> La RAMQ a donc maintenant le mandat de valider l'identité de toutes les personnes qui y sont inscrites, c'est-à-dire d'à peu près tous les Québécois. Par ailleurs, cette loi prévoit que les intervenants devront faire l'objet d'une certification de la part du « prestataire de services de certification ». Les services de certification seront délivrés par un organisme public ou un ordre professionnel. Ceux-ci pourront faire une entente avec un tiers, c'est-à-dire signer des contrats de PPP pour ces services. De plus, la loi n'exclut pas la possibilité que ces services soient centralisés et donc, elle n'exclut pas la création d'un fichier unique des intervenants. Cette possibilité a d'ailleurs été confirmée par le ministre de la Santé et des Services sociaux en Commission parlementaire. C'est donc dire que, si effectivement le service de certification était donné en partenariat public-privé, l'entreprise privée pourrait détenir une banque de données complète des identifiants de l'ensemble des intervenants du réseau de santé et de services sociaux! Avec la création des réseaux locaux de services (RLS), les intervenants proviendront aussi bien du réseau public que du privé. De plus, la liste des identifiants se termine avec une catégorie dite ouverte (tout autre renseignement) pour laquelle il ne peut être exclu d'ajouter des données biométriques, les nouvelles tendances dans les établissements de santé du Québec en faisant foi.

Le 16 décembre 2004, le gouvernement du Québec présentait le projet de loi 86, *Loi modifiant la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*. Ce projet facilite le transfert de renseignements personnels d'un organisme à un autre et affaiblit le contrôle de la *Commission d'accès à l'information* (CAI) et des citoyens sur l'utilisation qui est faite de ces renseignements. Le projet de loi, entre autres :

- Permet à un organisme public de recueillir un renseignement personnel pour un autre organisme public, si les deux organismes relèvent du même ministre;
- Permet de larges exceptions au fait qu'un renseignement personnel ne peut être utilisé qu'aux seules fins pour lesquelles il a été recueilli;

---

<sup>23</sup> Les dizaines de milliers de personnes, médecins, infirmières, etc. qui auront accès aux dossiers

<sup>24</sup> *Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives*, article 245 h.6 (Projet de loi 83).

- Élimine l'obligation de spécifier les différentes informations relatives à la protection des renseignements personnels lorsqu'un organisme public octroie un mandat ou un contrat de service à un autre organisme public. La loi prévoit déjà que ces transferts de renseignements peuvent se faire sans le consentement de la personne concernée;
- Ajoute de nouvelles exceptions à la règle de confidentialité des renseignements personnels en permettant, dans le cadre d'une entente écrite qui devra être soumise à la CAI pour avis, à un organisme public de transmettre, sans le consentement de la personne concernée, un renseignement personnel à un organisme d'un autre gouvernement que celui du Québec;
- Enlève à la CAI son droit d'intervention lorsque des organismes publics se communiquent des fichiers de renseignements personnels à des fins de couplage, de comparaison ou d'appariement.<sup>25</sup>

---

<sup>25</sup> Commission d'accès à l'information, *Mémoire de la Commission d'accès à l'information concernant le projet de loi N° 86*, septembre 2005, page 13.

## Les dangers du cumul et du partage de renseignements sur les citoyens

Dans son mémoire sur le projet de loi 86, la *Commission d'accès à l'information* a fait ressortir que le cumul d'informations de toute nature sur les individus, qui ne cesse de s'enrichir, met à la disposition de celui qui accède au dossier d'un citoyen l'histoire, même la plus personnelle et intime, de celui-ci:

*«Les technologies de l'information et des communications permettent maintenant de colliger et de conserver un nombre presque illimité d'informations : convergence des technologies et des réseaux, liens de communication ultrarapides, protocoles de communication communs (IP), standardisation des interfaces (duplication, réplication, mémoires) et capacité de traitement favorisent un traitement centralisé de l'information. À ces facteurs s'ajoutent les possibilités d'intégration de plusieurs systèmes en un seul, le regroupement en un seul fichier des données réparties physiquement (fichier éclaté) dans plusieurs entités administratives et en des lieux différents et la création d'immenses silos de données traitées par des progiciels de gestion intégrés.*

*Ce phénomène de centralisation qu'observe la CAI depuis plusieurs années est particulièrement évident à la Régie de l'assurance maladie du Québec et au ministère du Revenu, mais également observable dans plusieurs secteurs d'activités gouvernementaux: éducation, justice, gestion des ressources humaines, financières et matérielles. Bien souvent, cette centralisation résulte simplement d'une volonté d'améliorer la performance administrative. Dans ce contexte, le plan de modernisation de l'État présenté par le gouvernement en mai 2004, et plus particulièrement la création de Services Québec et du Centre de services administratifs, ont pour effet d'ouvrir la voie à une plus grande centralisation des renseignements personnels.»<sup>26</sup>*

La *Commission d'accès à l'information* souligne le danger de cette dérive :

*«L'un des fondements des lois de protection des renseignements personnels, au Québec ou ailleurs, est basé sur la nécessité de maintenir l'étanchéité des fichiers de renseignements personnels détenus par les multiples entités et composantes de l'appareil administratif pour éviter la centralisation de l'information (...)*

---

<sup>26</sup> *Idem*, page 19.

*Pourquoi éviter la centralisation de l'information ? Essentiellement pour atteindre l'objectif suivant : préserver l'individu contre la toute-puissance de l'État. Cet objectif sera atteint si des profils sur les individus ne peuvent être dressés et si le citoyen peut avoir l'assurance que des décisions à son sujet ne pourront être fondées sur des renseignements personnels colligés à son insu ou utilisés à des fins qu'il ignore. Invoquer des mécanismes de sécurité aux fins de la protection des données et des garanties de confidentialité ne peut suffire à justifier la centralisation de l'information.*

*Le législateur doit maintenir et, au besoin, solidifier tous les garde-fous qui assurent aux citoyens qu'un même organisme public ne puisse tout connaître à son sujet en obtenant des informations sur : ses revenus, son état de santé, ses démêlés avec l'administration municipale au sujet de l'évaluation de sa résidence ; les infractions qu'il a commises au Code de la sécurité routière, ses échecs scolaires, les prestations reçues en vertu d'un programme d'aide.»*

La très grande majorité des citoyens considère que les informations sur l'état de santé de chacun sont des données éminemment personnelles. *Et ils ont raison.* Il importe d'en interdire la circulation entre les ministères et entre les agences, ou dans le privé, et de prévenir que leur diffusion permette divers types de profilage et puisse faciliter l'exclusion, ou même le chantage *auprès de personnes ou groupes de citoyens.*

## **L'impact combiné des accords de commerce et du Patriot Act**

La constitution de fichiers centralisés contenant les dossiers de toute la population dans différents domaines, comme la santé, est d'autant plus préoccupante que la gestion de ces fichiers peut être confiée à des entreprises privées dans le cadre de partenariats public-privé qui pourraient se multiplier, si les choses vont comme le désire le gouvernement actuel. En effet, en vertu d'accords internationaux déjà en vigueur, comme *l'Accord général sur le commerce des services (AGCS)* et *l'Accord sur les marchés publics*, ces entreprises peuvent très bien être étrangères, et dans le cas de compagnies des États-Unis, celles-ci sont soumises au Patriot Act qui les oblige à remettre sur demande toutes les données en leur possession au FBI.<sup>27</sup> Une telle situation s'est présentée en Colombie-Britannique, lorsque la compagnie américaine Maximus a obtenu le contrat de gestion des programmes *Medicare* et

---

<sup>27</sup> L'article 215 du Patriot Act permet à une cour spécialement constituée d'émettre secrètement une ordonnance requérant toute personne ou organisation de divulguer «toute chose tangible». Il est interdit à quiconque de rendre publique l'ordonnance de divulgation.

*Pharmacare* de la province.<sup>28</sup> On peut, par exemple, facilement imaginer les conséquences que pourrait avoir pour un voyageur le fait que le douanier américain sache, par le biais d'un accès aux informations du dossier santé du voyageur, que ce dernier a déjà eu un problème de toxicomanie.

## **La banalisation de la biométrie**

L'identification biométrique est également utilisée dans des cadres plus restreints. Dans les grands aéroports canadiens, l'accès aux zones protégées est contrôlé par un système de reconnaissance de l'iris. À Montréal l'accès aux armoires de narcotiques de l'hôpital Maisonneuve-Rosemont est contrôlé par la biométrie des empreintes digitales. Le Centre d'éducation physique de l'Université de Montréal (CEPSUM) se sert de la reconnaissance de la main pour contrôler l'accès à ses installations. Ces applications, bien qu'elles ne posent pas les mêmes menaces aux libertés que les grands projets mentionnés précédemment, contribuent à banaliser l'utilisation de la biométrie et la nécessité de s'identifier dans des circonstances de plus en plus nombreuses.

---

<sup>28</sup> Fédération des infirmières et infirmiers du Québec, *Une mise en péril du droit à la vie privée*, mémoire déposé à la Commission de la culture dans le cadre de la consultation générale portant sur le projet de loi 86, pages 14 à 17.

## Sur la nécessité de s'identifier dans une société démocratique

La volonté des gouvernements d'imposer des documents d'identité biométriques, obligatoires et universels, ne fait pas de doute. Toutefois, tout projet national ayant ce but explicite est susceptible de rencontrer une solide résistance, comme ce fut le cas pour le projet de carte d'identité canadienne proposé par le ministre Denis Coderre à l'automne 2002. Pour contrer cette résistance et arriver par voie indirecte aux mêmes fins, on constate que nos gouvernements peuvent compter sur d'autres stratégies, soit en n'offrant aucune opposition aux instances internationales qui imposent, par exemple, de nouvelles normes de passeport, soit en modifiant des documents existants conçus à d'autres fins, comme ce pourrait être le cas de la carte d'assurance maladie du Québec.

Comme l'écrivait la *Ligue des droits et libertés* dans son mémoire sur le projet de carte d'identité du gouvernement canadien, l'obligation de détenir une carte d'identité représenterait un changement majeur dans le rapport entre le citoyen et l'État:

*«... Dans les sociétés qui adhèrent à une tradition de liberté anglo-saxonne, comme, entre autres, le Canada, l'Angleterre et les États Unis, le citoyen n'est pas obligé de porter sur lui une pièce d'identité et il n'a pas l'obligation de décliner son identité à un agent de l'État, à moins d'être en état d'arrestation. Nous sommes obligés de produire un permis nous identifiant, seulement lorsque nous nous livrons à une activité spécifique qui requiert un tel permis (conduire, chasser, etc..). L'objet premier de la vérification, de la part de l'agent de l'État, n'est pas de contrôler notre identité, mais de s'assurer que nous avons l'autorisation légale de pratiquer l'activité en question. Par ailleurs, d'autres documents, comme la carte d'assurance-maladie, nous donnent accès à des services particuliers. Encore une fois, ces documents n'ont pas comme fonction première de nous identifier. La carte d'identité est un document de nature complètement différente. **Son unique but est de nous identifier.** Elle introduit l'idée que le citoyen devra, dorénavant, être en mesure de s'identifier en tout temps et elle remet en question le droit à l'anonymat qui est un des principes de notre démocratie. Effectivement, dans des États où la carte d'identité est inscrite dans les mœurs, les citoyens doivent porter leur carte et la présenter sur demande. Cela accrédite l'idée que le citoyen doit rendre des comptes à l'État dans ses activités quotidiennes.*

*Les chartes canadienne (art. 7 et 8) et québécoise (art. 5) protègent le droit à la vie privée. Selon la Cour suprême du Canada<sup>29</sup>, le droit à la liberté de l'article 7 de la Charte canadienne des droits et libertés dépasse la simple notion d'absence de contrainte physique et protège une sphère limitée d'autonomie personnelle dans laquelle les individus peuvent prendre des décisions intrinsèquement privées sans intervention de l'État, c'est-à-dire dans la jouissance de la dignité et de l'indépendance individuelle.*

(...)

*La liberté peut se caractériser par l'absence de coercition ou de contrainte. Si une personne est astreinte par l'État ou par la volonté d'autrui à une conduite qu'elle n'aurait pas choisi d'adopter autrement, alors cette personne n'agit pas de son propre gré et on ne peut pas dire qu'elle est vraiment libre. L'un des objectifs importants de la Charte est de protéger le citoyen, dans des limites raisonnables, contre la coercition et la contrainte. La coercition comprend non seulement la contrainte flagrante [...] mais également les formes indirectes de contrôle qui permettent de déterminer ou de restreindre les possibilités d'action d'autrui.»<sup>30</sup>*

---

<sup>29</sup> *Godbout c. Ville de Longueuil*, [1997] 3 R.C.S. 844.

<sup>30</sup> Ligue des droits et libertés, *Le projet de carte d'identité: un changement majeur dans les rapports entre le citoyen et l'État*, mémoire présenté au Comité permanent de la citoyenneté et de l'immigration du Canada, octobre 2003, page 4. En ligne : [http://www.liguedesdroits.ca/documents/surveillance/identite/memoire\\_cartelD\\_LDL.pdf](http://www.liguedesdroits.ca/documents/surveillance/identite/memoire_cartelD_LDL.pdf)

## Conclusion

La *Ligue des droits et libertés* est fortement préoccupée par le risque élevé de violation de droits fondamentaux (vie privée, liberté) que représentent la biométrie, la constitution de bases de données intégrées et le partage d'informations entre agences de l'État. Comme le rappelait la *Ligue des droits et libertés* dans son mémoire sur le projet de carte d'identité nationale :

*« Dans l'affaire Dymont<sup>31</sup>, le juge La Forest écrit que la notion de vie privée « est au cœur de celle de la liberté dans un État moderne (p.427) et qu'elle se fonde « sur la notion de dignité et d'intégrité de la personne » (p. 429). Dans Aubry c. Vice-Versa<sup>32</sup>, la Cour énonce que dans la mesure où le droit à la vie privée consacré par l'article 5 de la Charte québécoise cherche à protéger une sphère d'autonomie individuelle, ce droit doit inclure la faculté de contrôler l'usage qui est fait de son image puisque le droit à l'image prend appui sur l'idée d'autonomie individuelle, c'est-à-dire sur le contrôle de chacun sur son identité. »<sup>33</sup>*

Les nouvelles technologies offrent des possibilités sans précédent de cumuler des informations sur les individus et de s'en servir à des fins de contrôle. Il importe de plus en plus que le recours à toutes les technologies soit décidé *d'abord* en fonction de la promotion de la dignité des personnes et de la protection de leurs droits et libertés. En particulier, on doit considérer des droits comme le droit à la vie privée et le droit de chacun à la confidentialité, en particulier dans le domaine de sa santé, comme des éléments essentiels de la liberté, de la dignité et également de la vie démocratique. Le respect de ces droits fondamentaux doit avoir préséance sur les motifs de sécurité nationale des États ainsi que sur les préoccupations de gestion des gouvernements et de l'entreprise privée. Cette situation pose un nouveau défi aux sociétés démocratiques, qui ne peuvent s'en remettre à une confiance aveugle dans la bienveillance de l'État pour la protection des libertés individuelles.<sup>34</sup>

Nous demandons donc aux deux paliers de gouvernement d'abandonner tout projet de document d'identité biométrique, de mettre un frein aux pratiques de convergence des fichiers d'informations sur les citoyens et d'encadrer celles-ci de limites et de règles strictes.

---

<sup>31</sup> *R..c. Dymont*, [1998] 2 R.C.S. 417.

<sup>32</sup> *Aubry c. Editons Vice-versa Inc.* [1998] 1 R.C.S. 591.

<sup>33</sup> Ligue des droits et libertés, *Le projet de carte d'identité: un changement majeur dans les rapports entre le citoyen et l'État.*, op. cit., note 30, page 5.

<sup>34</sup> Au Québec, la convergence des pouvoirs confiés à la RAMQ, jumelée à la diminution des pouvoirs de la Commission d'accès à l'information ne laisse pas d'inquiéter sérieusement.

## Recommandations :

Par conséquent, *Ligue des droits et libertés* recommande :

1. Que l'on ne puisse avoir recours à la biométrie comme moyen d'identification des personnes que si l'on démontre qu'aucun autre moyen d'identification, moins intrusif, n'est possible. Dans ce cas, la collecte de données biométriques doit être limitée au strict minimum de caractéristiques ou de mesures liées au besoin requis d'identification ou permettant de relier la personne à l'action qu'elle pose.
2. Que l'on mette fin à tout projet de créer un document d'identité universel, directement ou indirectement, biométrique ou non. Par « document d'identité universel », nous entendons un document qui sert à identifier l'individu auprès d'un agent des forces de l'ordre et dans toutes ses transactions avec l'État ou dans ses transactions personnelles.
3. Que l'on n'utilise les données personnelles recueillies par des organismes, gouvernementaux ou privés, qu'aux seules fins pour lesquelles elles ont été obtenues.
4. Que l'on mette en place des mécanismes spécifiques et simples qui permettent aux citoyens de vérifier régulièrement l'exactitude des informations qui les concernent, dans chacun des grands fichiers gouvernementaux, et d'apporter des corrections au besoin. Ces mécanismes existent déjà relativement à certains fichiers : il importe d'en faire un élément constitutif du fonctionnement de chaque fichier public.
5. Que les données personnelles recueillies par un organisme, gouvernemental ou privé, ne puissent être recueillies ni partagées avec un autre organisme, gouvernemental ou privé, sans le consentement libre, éclairé et explicite de chaque personne concernée et dans chaque cas.
6. Que l'on soumette clairement toute entreprise privée, qu'elle soit québécoise, canadienne ou étrangère, impliquée dans la mise en place ou le traitement de données biométriques et de bases de données sur les individus, aux principes qui ont prévalu lors de la mise en place de notre régime de protection des renseignements personnels.
7. Que le gouvernement du Québec apporte des amendements aux projets de loi 83 et 86 de façon à rétablir les principes fondateurs de notre régime de protection des renseignements personnels.
8. Que l'on renforce les pouvoirs de contrôle et de surveillance de la Commission d'accès à l'information.

9. Que les gouvernements fédéral et provinciaux confient au Commissaire à la vie privée et aux commissions provinciales le mandat conjoint d'examiner la portée actuelle de l'ensemble des politiques, programmes et dispositifs de cueillette et de transfert de renseignements personnels. Qu'à la suite de cet examen, un mécanisme de veille soit mis en place et que des rapports soient produits régulièrement et transmis à des ministres responsables qui auraient l'obligation de les déposer aux assemblées législatives.