Commissaire à
l'information et à la
protection de la
vie privée/Ontario

Exposé au Comité permanent de la citoyenneté et de l'immigration de la Chambre des communes concernant les conséquences pour la vie privée de l'instauration d'une carte nationale d'identité et de la technologie biométrique

Ann Cavoukian, Ph.D.
Commissaire
Le 4 novembre 2003

Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

Cette publication est disponible sur le site Web du Bureau du commissaire.

This publication is also available in English.

Exposé au Comité permanent de la citoyenneté et de l'immigration de la Chambre des communes concernant les conséquences pour la vie privée de l'instauration d'une carte nationale d'identité et de la technologie biométrique

Je vous remercie beaucoup de m'avoir invitée à faire part de mon point de vue sur l'instauration éventuelle d'une carte nationale d'identité et de la technologie biométrique. Une carte nationale d'identité, particulièrement si elle est associée à un ou plusieurs identificateurs biométriques, aurait de profondes répercussions sur la population canadienne. À titre de commissaire à l'information et à la protection de la vie privée de l'Ontario, j'aimerais vous faire part de mon point de vue sur ces questions importantes.

Pour commencer, j'aimerais distinguer clairement les notions de carte nationale d'identité et de technologie biométrique. En effet, il s'agit de deux concepts tout à fait distincts.

À mon avis, l'instauration d'une carte nationale d'identité doit s'appuyer sur des arguments convaincants, car elle comporterait à la fois des avantages et des inconvénients. Ceux-ci et la question de savoir s'il faut ou non assortir une telle carte d'identificateurs biométriques doivent être examinés séparément. La technologie biométrique actuelle permet de confirmer l'identité des personnes et, lorsqu'elle aura été suffisamment améliorée pour permettre de distinguer une personne au sein d'un groupe, elle pourra être employée à une variété de fins, et non seulement pour une carte nationale d'identité. Cependant, quel que soit son mode d'utilisation, la biométrie comporte un ensemble particulier et distinct de difficultés et pourrait avoir un effet néfaste durable sur notre société.

Je me concentrerai aujourd'hui sur les aspects touchant la vie privée dont les institutions gouvernementales devront tenir compte avant de concevoir ou d'implanter des systèmes biométriques, que ce soit pour une carte nationale d'identité ou pour tout autre programme.

M. Robert Marleau, Commissaire à la protection de la vie privée du Canada par intérim, vous a déjà fait un excellent exposé sur les inquiétudes associées à une carte nationale d'identité en matière de vie privée, notamment les avantages minimes que son instauration procurerait en regard de ses importants inconvénients, notamment son coût et le fait qu'elle porterait atteinte à nos valeurs démocratiques. Je n'ai donc pas l'intention de revenir sur les aspects dont le commissaire fédéral a traités en profondeur.

Cependant, j'aimerais insister sur certains des arguments clés de M. Marleau.

On n'a pas encore justifié à la population canadienne le bien-fondé d'un tel programme, en donnant une analyse détaillée de ses coûts. Le Comité a reçu des observations selon lesquelles ces coûts pourraient s'établir entre cinq et sept milliards de dollars. Un programme de cette envergure et de ce coût doit donc être étayé par des avantages clairs et tangibles. D'après les observations que le Comité a reçues, cela n'a pas encore été fait.

En outre, une carte nationale d'identité, qui nécessiterait une énorme base de données et générerait une forte demande d'accès de la part de différents ministères, nous rendrait particulièrement vulnérables sur le plan de la vie privée et de la sécurité. Si Microsoft et le Pentagone peuvent être piratés, il faut en tenir compte dans l'analyse des risques et des avantages. Ainsi, des renseignements personnels de nature délicate pourraient être employés à des fins abusives par des employés malhonnêtes et le crime organisé, et ces données pourraient permettre la surveillance et le profilage malveillants de la population canadienne.

Que le Canada décide ou non d'instaurer une carte nationale d'identité, il fera l'objet de pressions en vue d'inclure des identificateurs biométriques dans les documents de voyage. Ainsi, en 2002, les États-Unis ont adopté la *Enhanced Border Security and Visa Entry Reform Act*. Cette loi oblige les citoyens de pays qui ne sont pas tenus de demander un visa pour se rendre aux États-Unis de présenter à compter du 26 octobre 2004 un passeport lisible à la machine doté d'identificateurs biométriques. Il semble probable que le Canada sera soustrait, du moins temporairement, à cette exigence. Je crois toutefois que la nécessité éventuelle de disposer de documents de voyage comportant des identificateurs biométriques ne justifie en rien l'instauration d'une carte nationale d'identité. Un passeport canadien en règle suffit à remplir cette exigence. L'ajout d'identificateurs biométriques à un passeport serait très peu coûteux par rapport à la conception et à l'instauration d'une carte d'identité.

Cependant, l'ajout de données biométriques aux documents de voyage soulève des questions sur l'efficacité des mesures de protection de la vie privée qui peuvent être intégrées dans un tel système au moment de sa conception. Je consacrerai le reste de mon exposé à cette question. Vous conviendrez sans doute que l'utilisation d'identificateurs biométriques représente une question importante pour la population canadienne. En fait, d'après une étude menée au MIT, la biométrie a été identifiée comme l'une des principales technologies qui changeront le monde. Pour cette raison, j'aimerais discuter des identificateurs biométriques, c'est-à-dire des caractéristiques qui distinguent chaque personne, comme la forme du visage, la configuration de l'iris, les courbes des empreintes digitales ou le timbre de la voix.

J'ai toujours pensé que la biométrie, si elle est conçue et mise en oeuvre en tenant compte des principes de protection de la vie privée, peut être instaurée d'une façon qui protège les renseignements personnels et respecte la vie privée. Pour ce faire, cependant, il existe un certain nombre de difficultés à surmonter.

L'une des difficultés les plus importantes demeure le fait que la technologie biométrique n'est pas parfaitement maîtrisée. L'absence de normes de conception, conjuguée à une industrie naissante, fait en sorte que les systèmes ne sont pas très précis. À l'heure actuelle, la lecture des empreintes digitales ou de l'iris comporte un taux d'erreur de 1 pour 1 000 à 1 pour 10 000[1]. Les systèmes de reconnaissance des visages sont beaucoup moins précis. À des fins de confirmation de l'identité, un système pouvant atteindre un taux de précision de 99,99 p. 100 pourrait être acceptable. Cependant, dans les faits, ce niveau de précision serait très insuffisant s'il fallait vérifier des millions de modèles lors du processus d'identification.

Par exemple, la comparaison des données biométriques d'une personne aux données recueillies sur un million de personnes pourrait produit produire jusqu'à 1 000 faux positifs, selon le niveau de sensibilité. Dans un aéroport d'où partent 100 000 personnes tous les jours, presque tout le monde ferait l'objet d'une fausse identification si l'on recherchait leurs données biométriques dans une base de données de l'importance de la base d'empreintes digitales du FBI, qui compte environ 46 millions d'empreintes. Une telle base de données semble énorme, mais pour l'identification des voyageurs, il faudra recourir à de nombreuses bases de données disparates, par exemple, celle d'Interpol, les listes de surveillance de différents pays, les bases de données de la police, etc. Par conséquent, pour que la biométrie soit efficace à des fins d'identification, la base de données doit compter des milliers, et non des millions, de modèles. En d'autres mots, la biométrie ne peut actuellement permettre de constituer des listes de surveillance à des fins d'identification.

En guise d'exemple, j'aimerais citer Bruce Schneier, expert en sécurité et cryptographe de renom. Je recommande fortement son dernier ouvrage, *Beyond Fear, Thinking Sensibly About Security in an Uncertain World*, aux personnes qui s'intéressent au débat sur la sécurité nationale. Voici ce que M. Schneier y écrit au sujet de l'utilisation de la biométrie pour identifier les menaces possibles à la sécurité ou les terroristes :

> Si le taux d'erreur est de 1 sur 10 000 empreintes digitales, une personne dont les empreintes sont comparées à une base de données contenant un million de fiches fera l'objet d'une identification positive 100 fois. Il en sera de même pour toutes les personnes dont l'identité doit être vérifiée. Pareil système sera inutilisable parce que tout le monde sera faussement pointé du doigt. Je pourrais élaborer un système tout aussi efficace pour beaucoup moins cher. Ainsi, chaque fois qu'une personne passe sous une arche, une lumière rouge s'allume. Ce système de 10 $ serait tout aussi efficace que le système biométrique pour déceler les terroristes.

[1] Des tests menés en situation réelle dans des aéroports ont révélé un taux d'erreur pouvant aller jusqu'à 50 p. 100. Si l'on suppose un taux d'exactitude de 90 p. 100 et, en moyenne, un terroriste par million de personnes innocentes, un seul terroriste pourrait donner lieu à 100 000 fausses alarmes (Bruce Schneier, *Beyond Fear*, p. 190).

On ne peut donc affirmer que la biométrie est un moyen d'identification idéal. Il est vrai que les systèmes biométriques sont excellents pour confirmer l'identité d'une personne, c'est-à-dire pour déterminer si des données biométriques précises correspondent à une personne en particulier. Cependant, il est beaucoup plus difficile de déterminer si ces données biométriques correspondent à des données qui se trouvent dans une base de données sur des terroristes ou des criminels. Ce problème s'aggrave lorsque le système interroge non seulement la base de données de terroristes connus, mais également d'autres bases de données plus ou moins étroitement reliées pour déterminer si la personne en question est un terroriste possible ou pourrait menacer la sécurité publique.

Une personne qui est faussement identifiée de cette façon pourrait éprouver de graves problèmes. Identifiée faussement comme une menace à la sécurité, elle subirait à tout le moins un dérangement et de l'embarras, mais parfois également des conséquences plus graves. Des retards importants dans les projets de voyage peuvent occasionner des coûts élevés en termes humains et financiers. La personne pourrait devoir subir un interrogatoire aux conséquences physiques et affectives désagréables. Elle devrait alors tenter de convaincre le personnel de sécurité que le système biométrique a commis une erreur et qu'elle fait l'objet d'une fausse accusation. Il s'agit là d'un risque légitime, notamment dans un contexte de sécurité publique ou nationale, où le maintien du secret est primordial.

Les problèmes que pourrait causer l'identification positive erronée de nombreuses personnes se répercuteraient également sur le personnel de sécurité de l'aéroport. Ainsi, il faudrait prévoir des installations supplémentaires pour le traitement secondaire de ces personnes faussement ciblées. En outre, le nombre élevé de faux positifs pourrait paralyser le personnel de sécurité, qui tenterait de faire correspondre des clichés qui sont souvent de mauvaise qualité.

Il faut également tenir compte des répercussions du manque de fiabilité des processus d'identification sur les déplacements et le commerce internationaux. Les déplacements et le commerce transfrontaliers sont essentiels à l'économie canadienne. La confusion et la congestion causées tous les jours par la fausse identification de milliers de personnes, considérées à tort comme des risques pour la sécurité, menaceraient d'interrompre les déplacements et le commerce entre le Canada et d'autres pays, particulièrement les États-Unis.

La possibilité que des Canadiennes et des Canadiens ordinaires soient faussement identifiés comme étant des menaces à la sécurité illustre l'importance d'intégrer dans tout système biométrique une procédure de recours. En effet, il doit être possible d'établir rapidement et facilement sa véritable identité et de réfuter l'identification biométrique. Une procédure de recours est essentielle pour protéger non seulement le droit à la vie privée, mais également les droits de la personne en général.

Il faut également tenir compte des conséquences graves qui seraient associées au mauvais fonctionnement d'un système biométrique. Nous sommes tous au courant de situations où des systèmes ont connu une défaillance qui a exposé au grand jour des renseignements personnels délicats. Il est possible de changer un numéro d'assurance sociale qui a été utilisé à mauvais escient, mais il beaucoup plus difficile de changer un identificateur biométrique, qui est statique et limité. En effet, on a un nombre fixe de doigts et d'yeux pour s'identifier.

Il est également tout à fait possible de tromper les systèmes biométriques. Récemment, un simple ourson de gélatine a été réchauffé pour recevoir une empreinte digitale, et a été employé par la suite pour tromper une technologie biométrique de balayage des empreintes. Il serait dangereux de tenir pour acquis que tous les systèmes biométriques futurs seront invulnérables à des attaques tout aussi novatrices et, parfois, simples. Par exemple, pour ce qui est du balayage de l'iris, on peut s'attendre à la conception de lentilles cornéennes conçues pour empêcher l'identification positive ou permettre une fausse identification.

On tente souvent, et à tort, de justifier l'adoption de la biométrie en invoquant les vols d'identité. On prétend en effet que l'instauration de cartes d'identité munies d'identificateurs biométriques entraînera une réduction de ces vols. Cependant, j'aimerais vous présenter un autre point de vue sur cette question.

Un identificateur unique, comme un renseignement biométrique, qui est conservé dans une base de données et qui est employé pour relier entre eux des renseignements personnels disparates, pourrait en fait accroître le risque de vols d'identité. Le fait est que l'identificateur biométrique est l'équivalent d'un numéro d'identification personnel que l'on ne peut changer. Lorsqu'il est porté atteinte à l'intégrité d'un identificateur biométrique qui est utilisé pour commettre un vol d'identité, le temps et les efforts nécessaires à la victime innocente pour rétablir son identité iront bien au-delà des 14 mois requis en moyenne pour résoudre un vol d'identité relativement simple résultant du vol d'un numéro d'identification personnel et de renseignements sur une carte de crédit. En outre, un pirate qui vole des renseignements personnels contenus dans un système d'identification, signale qu'il a perdu sa carte d'identité puis se réinscrit au moyen des renseignements qu'il a volés en y associant ses propres identificateurs biométriques obtiendra ainsi une carte tout à fait valable, certifiée par ses attributs biométriques. Pour le voleur, l'acquisition d'une identité comportant un identificateur biométrique est donc beaucoup plus payante.

Il faut également envisager la possibilité qu'un système biométrique devienne de fait un système national d'identification. À moins que les données biométriques d'une personne ne soient employées pour générer des numéros différents pour chaque service qu'elle utilise, les possibilités de surveillance sont élevées. Le recours aux mêmes identificateurs biométriques par différents programmes gouvernementaux pourrait entraîner les mêmes pratiques qui portent atteinte à la vie privée qu'une carte nationale d'identité.

Une autre difficulté réside dans la prévention de l'usage abusif des renseignements personnels à des fins qui n'étaient pas prévues au moment de leur collecte. Il s'agit là d'une atteinte aux principes les plus fondamentaux de la protection de la vie privée.

Prenons le cas de la ville de Londres. Afin de réduire la congestion sur les routes, la ville a instauré des « frais de congestion » de cinq livres. Pour percevoir ces frais, la ville a installé des centaines de caméras vidéo numériques et un logiciel de reconnaissance des caractères. Il s'agit là d'un objectif tout à fait louable. Cependant, avant que le système ne soit lancé, on a constaté que les images ainsi recueillies pourraient être fournies à la police et aux forces armées qui sont à la recherche de terroristes et de criminels. Il y a eu dans ce cas une absence fondamentale de responsabilisation qui aurait pu être rectifiée à la suite d'un débat public. Imaginez les graves conséquences pour la vie privée qui s'ensuivraient si une base de données biométriques nationale, conçue pour la sécurité des voyageurs, était employée à des fins moins légitimes sans l'accord du public.

L'un des mythes au sujet des systèmes biométriques réside dans la croyance qu'une fois les personnes inscrites, il est possible d'identifier les menaces à la sécurité et d'assurer la sécurité du public. En fait, c'est le contraire qui se produit. Comme il a déjà été démontré, les terroristes et les personnes qui représentent une menace à la sécurité s'inscrivent de façon légitime et obtiennent des documents d'identité authentiques. On crée ainsi un faux sentiment de sécurité. Grâce à l'instauration des identificateurs biométriques, une personne qui représente vraiment une menace à la sécurité pourrait obtenir un nouveau niveau d'accès, que ce soit à un avion ou à un autre élément d'infrastructure essentiel.

Enfin, on ne peut sous-estimer le fait que des bases de données comportant des renseignements liés entre eux au moyen de modèles biométriques représentent des cibles très tentantes. Les bases de données conçues pour lutter contre les terroristes et les criminels seront irrésistibles pour ces personnes. Il ne faut jamais sous-estimer le temps et les ressources qu'un pirate pourrait consacrer à accéder à un tel système.

À mon avis, il faudra se pencher sur ces questions avant que le gouvernement ne mette en oeuvre des identificateurs biométriques. Cependant, ces problèmes ont effectivement des solutions. Notre bureau a tenu compte de ces questions lors de l'élaboration d'une norme sur l'utilisation des identificateurs biométriques en Ontario. En 1994, lorsque la ville de Toronto a envisagé de recourir à la biométrie pour réduire les cas de fraude dans le régime d'aide sociale, mon bureau a collaboré avec la ville et le gouvernement de l'Ontario pour élaborer un ensemble d'exigences qui ont par la suite été enchâssées dans un texte de loi, la *Loi de 1997 sur le programme Ontario au travail*. Si je ne m'abuse, il s'agit là du cadre législatif le plus rigoureux qui ait été adopté en vue de l'implantation d'un système biométrique par un organisme gouvernemental.

Cette loi prévoit les exigences suivantes pour l'utilisation d'un système biométrique aux fins de l'aide sociale :

- Les renseignements biométriques ne peuvent être recueillis et utilisés qu'à des fins limitées et précises établies dans la loi;
- Les renseignements biométriques ne peuvent être recueillis qu'auprès du particulier auquel ils se rapportent;
- Les renseignements biométriques doivent être stockés sous forme codée;
- Les renseignements biométriques originaux doivent être détruits après l'encodage;
- Les renseignements biométriques codés ne peuvent être transmis que sous forme codée;
- Les renseignements biométriques codés ne peuvent servir d'identificateurs uniques;
- Les renseignements biométriques codés ne peuvent être associés à des renseignements sur les programmes;
- Il doit être impossible sur le plan technique de reconstituer les renseignements biométriques à partir de leur forme codée;
- Il doit être impossible de comparer les images biométriques provenant d'une base de données avec des images biométriques provenant d'autres bases de données ou avec des reproductions de ces renseignements qui n'ont pas été obtenues auprès de la personne concernée;
- Les responsables de l'application de la loi ne peuvent accéder à la base de données biométriques à moins d'obtenir une ordonnance d'un tribunal ou un mandat.

Bien que cette loi soit reconnue dans le monde entier comme la norme en matière de protection de la vie privée dans le cadre du recours aux renseignements biométriques, nous avons beaucoup appris depuis 1994. J'aimerais suggérer les principes suivants sur lesquels devrait s'appuyer l'instauration de tout système biométrique.

1. **Le gouvernement doit énoncer clairement le problème** qu'il compte résoudre grâce au recours à un système biométrique, en fournissant les justifications nécessaires.

2. **Des consultations élargies** doivent avoir lieu, pour permettre aux nombreux groupes d'intérêts du Canada de faire part de leurs points de vue et de formuler des suggestions sur la collecte et l'utilisation des renseignements biométriques.

3. **Il faut adopter une loi** qui limite l'utilisation des renseignements biométriques à des fins précises. Cette loi doit assujettir la collecte, l'utilisation et la divulgation des renseignements biométriques à des limites claires. Il s'agit là du modèle adopté en Ontario avec la *Loi de 1997 sur le programme Ontario au travail*. Comme dans ce cas, il est essentiel d'adopter une loi pour veiller à ce que les renseignements biométriques soient recueillis uniquement à des fins limitées et précises, et non à d'autres fins, comme j'en ai parlé tantôt.

4. **Il faut assurer une surveillance rigoureuse, efficace et indépendante**, par exemple, par l'entremise du Commissaire à la vie privée du gouvernement fédéral, de tous les procédés associés à la collecte et à l'utilisation des renseignements biométriques. Cet organisme de surveillance doit avoir le pouvoir de faire enquête sur les plaintes et de rendre compte au Parlement et aux comités parlementaires pour résoudre les questions relatives à la vie privée. Son indépendance permettrait la vérification régulière du système et l'adoption de normes de codage appropriées. En outre, l'organisme de surveillance serait chargé d'inclure des procédures de recours dans tous les systèmes biométriques; par exemple, il veillerait à l'élaboration de critères de composition d'une « liste de surveillance » des personnes soupçonnées de terrorisme, et veillerait à ce que les personnes innocentes aient des recours à leur disposition pour voir leur nom rayé d'une telle liste.

5. **Une évaluation complète de l'incidence sur la vie privée et du risque pour la vie privée** doit être effectuée à chaque étape de pareils projets, à partir de leur conception jusqu'à leur instauration. Cette évaluation permettra aux responsables d'identifier les lacunes et d'élaborer des solutions efficaces pour protéger la vie privée.

6. **Il faut également mener une évaluation complète du système pour en déterminer les points forts et les faiblesses sur le plan de la vie privée.** Cette évaluation devrait être fondée sur une norme internationale comme les Critères communs, qui sont généralement utilisés pour mettre à l'épreuve les points forts et les vulnérabilités d'un système. Les Critères communs peuvent également être utilisés pour vérifier le respect de la vie privée. Il serait ainsi possible de vérifier la validité des allégations faites au sujet du système en matière de sécurité ou de vie privée.

Comme je l'ai souligné plus tôt, je crois qu'il est important de bien concevoir et de bien gérer un système biométrique. Avec un bon cadre législatif, des normes de conception visant à protéger la vie privée et des mesures de surveillance, il est possible d'instaurer un système biométrique et d'assurer en même temps la protection de la vie privée. Cependant, pareil système peut devenir de fait un système d'identification s'il est utilisé de façon abusive, et instauré de manière inadéquate, ayant ainsi des effets néfastes sur la société.

Je vous remercie de m'avoir invitée à faire part de mon point de vue sur l'instauration éventuelle d'une carte nationale d'identité et de systèmes biométriques. Merci de votre attention. Votre comité se livre actuellement à un débat public essentiel sur un sujet qui se répercutera sur toute la population canadienne. J'espère que j'ai pu vous aider à vous familiariser avec ces notions complexes. Je continuerai de m'intéresser à cette question de grande portée et d'apporter mon aide au Comité au besoin.

Je répondrai maintenant volontiers à vos questions.