PRB 06-30F

Library of Parliament Bibliothèque du Parlement

LA BIOMÉTRIE ET SON USAGE PAR L'ÉTAT

Lalita Acharya
Division des sciences et de la technologie

Le 11 septembre 2006

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

Le Service d'information et de recherche parlementaires de la Bibliothèque du Parlement travaille exclusivement pour le Parlement, effectuant des recherches et fournissant des informations aux parlementaires et aux comités du Sénat et de la Chambre des communes. Entre autres services non partisans, il assure la rédaction de rapports, de documents de travail et de bulletins d'actualité. Les analystes peuvent en outre donner des consultations dans leurs domaines de compétence.

THIS DOCUMENT IS ALSO PUBLISHED IN ENGLISH

TABLE DES MATIÈRES

Page

Page

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

LA BIOMÉTRIE ET SON USAGE PAR L'ÉTAT

INTRODUCTION

La biométrie ou, plus précisément, la reconnaissance biométrique – l'exploitation automatisée ou semi-automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité[(1)] – suscite une attention accrue depuis les attaques terroristes du 11 septembre 2001. Les gouvernements de nombreux pays comptent de plus en plus sur la biométrie pour accroître la sécurité dans les aéroports et aux postes frontaliers et pour produire des pièces d'identité encore plus sûres. Des technologies qui font appel à la biométrie sont aussi utilisées ou mises à l'épreuve dans une foule d'applications commerciales.

Le présent document donne un aperçu comparatif des principales technologies biométriques qui sont disponibles ou le seront sous peu et examine les préoccupations soulevées au sujet de la sécurité et de la protection de la vie privée dans le contexte de la biométrie. Il décrit également l'utilisation de la biométrie par les gouvernements de certains pays, notamment le gouvernement fédéral canadien.

BIOMÉTRIE – CARACTÉRISTIQUES ET SYSTÈMES

Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle répond aux critères suivants :

- Universalité : Chaque personne doit présenter cette caractéristique.

---

(1) La définition donnée de la biométrie dans le dictionnaire est la suivante : « Science qui étudie à l'aide des mathématiques les variations biologiques à l'intérieur d'un groupe déterminé » (voir *Le Petit Robert*, *Dictionnaire de la langue française*; Dictionnaires Le Robert, 2002, p. 259). Toutefois, les mentions de la biométrie dans les politiques publiques sont habituellement une variante de la définition donnée ici. Voir, par exemple, Peter Hope-Tindall, *Technologies fondées sur la biométrie*, OCDE, 2004, p. 11 (http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF).

- Caractère distinctif : La caractéristique doit être suffisamment différente chez deux personnes.

- Permanence : La caractéristique doit être suffisamment immuable pendant une période donnée.

- Perceptibilité : La caractéristique peut être mesurée quantitativement.

Il faut prendre en compte plusieurs autres facteurs pour savoir si l'on doit utiliser un système de reconnaissance biométrique des personnes, notamment :

- La performance : Fiabilité et rapidité de reconnaissance du système; les ressources requises pour obtenir la fiabilité et la rapidité de reconnaissance voulues; et les facteurs opérationnels et environnementaux qui influent sur la fiabilité et la rapidité du système.

- L'acceptabilité : Mesure dans laquelle les gens sont disposés à accepter l'utilisation d'une technologie de reconnaissance biométrique à des fins d'identification.

- La facilité de contournement : Facilité avec laquelle le système peut être induit en erreur par des méthodes frauduleuses(2).

Dans un système de reconnaissance biométrique, un appareil saisit et enregistre les caractéristiques en question et un logiciel interprète les données et détermine l'acceptabilité de la personne (selon le système employé, un préposé peut intervenir dans la détermination de l'acceptabilité). Les systèmes de reconnaissance biométrique fonctionnent à trois niveaux : i) un capteur prend une observation de la caractéristique biométrique, ii) le système traduit l'observation en termes mathématiques et produit une signature – ou gabarit – biométrique et iii) l'ordinateur introduit la signature biométrique dans un algorithme et la compare à une ou plusieurs autres signatures biométriques entreposées dans la base de données du système(3).

Un système de reconnaissance biométrique peut fonctionner en mode vérification ou en mode identification. En mode vérification (comparaison individuelle), le système vérifie l'identité de la personne. Il valide son identité en comparant les données biométriques saisies

---

(2) Anil K. Jain, Arun Ross et Salil Prabhakar, « An Introduction to Biometric Recognition », *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, n° 1, janvier 2004 (http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf).

(3) Ravi Das, « An Introduction to Biometrics », *Military Technology*, juillet 2005, p. 20 à 27.

aux gabarits biométriques de la personne entreposés dans la base de données du système (ou sur une carte à puce portée par la personne). La vérification de l'identité est habituellement utilisée pour l'identification catégorique, lorsque l'on veut éviter que plusieurs personnes utilisent la même identité. En mode vérification, l'enrôlement est une étape cruciale de l'établissement d'un système de reconnaissance biométrique efficace. À cette étape, chaque utilisateur fournit un échantillon de la caractéristique biométrique visée (en interagissant avec l'appareil de saisie). Le système prélève de l'information caractéristique de cet échantillon et entrepose les données produites sous la forme d'un gabarit. L'utilisateur interagit avec le système une autre fois pour vérifier que les données correspondent au gabarit. En cas de non-concordance, le processus est répété jusqu'à ce qu'une concordance soit enregistrée et que l'enrôlement soit terminé.

En mode identification (comparaison collective), le système reconnaît une personne en examinant tous les gabarits dans le système à la recherche d'un appariement. Étant donné que de nombreuses comparaisons doivent être effectuées en mode identification, un appariement accidentel ou des appariements multiples sont possibles. L'identification est un élément crucial pour des applications comme les listes de surveillance, pour lesquelles le système détermine si le gabarit biométrique d'une personne se trouve dans sa base de données.

SURVOL ET COMPARAISON DES SYSTÈMES DE RECONNAISSANCE BIOMÉTRIQUE

Il existe une variété de technologies de reconnaissance biométrique, soit sur le marché, soit à l'étape de la recherche et du développement (R-D). Les technologies les plus courantes servent à la reconnaissance des empreintes digitales, du visage, de l'iris et de la main ou des doigts. Les technologies moins fréquemment utilisées s'appuient sur la reconnaissance des images rétiniennes et de la démarche et sur la vérification dynamique de la signature. Nous effectuerons ci-après un survol des quatre systèmes de reconnaissance biométrique les plus couramment utilisés et une comparaison de 15 techniques de reconnaissance biométrique déjà disponibles sur le marché ou en voie de développement[(4)].

(4) On trouvera un résumé technique des principales technologies de reconnaissance biométrique sur le site Web du U.S. National Science and Technology Council's Subcommittee on Biometrics (http://www.biometricscatalog.org/NSTCSubcommittee/BiometricsIntro.aspx).

A. Reconnaissance des empreintes digitales

La comparaison manuelle des empreintes digitales par les services de police pour identifier des personnes est utilisée depuis la fin des années 1800. À la fin des années 1960 et au début des années 1970, le Federal Bureau of Investigation (FBI) américain a commencé à financer des recherches sur des technologies qui ont conduit à la mise au point de systèmes semi-automatisés de reconnaissance des empreintes digitales. Les progrès technologiques ont conduit à l'élaboration et à la mise en marché de systèmes entièrement automatisés et rapides de vérification des empreintes digitales. Les systèmes employés pour les opérations d'identification sur une grande échelle (comparaison collective) exigent l'information des 10 doigts (plutôt que d'un seul), et les examinateurs humains doivent parfois intervenir pour la comparaison finale des empreintes. Le capteur employé pour saisir l'image numérique de la surface d'une empreinte digitale peut utiliser le balayage optique (le plus courant), capacitif, ultrasonique ou thermique.

La reconnaissance par les empreintes digitales est très fiable, difficile à contourner (dans le cas des systèmes évolués) et généralement peu coûteuse. La technologie n'est toutefois pas discrète et la prise d'empreintes digitales évoque le système pénal et la honte qui l'entoure.

B. Reconnaissance faciale

Les premiers algorithmes de reconnaissance faciale utilisaient des modèles géométriques simples. Le premier système semi-automatisé de reconnaissance faciale a été élaboré au cours des années 1960. L'opérateur devait situer les caractéristiques (yeux, oreilles, nez et bouche) sur la photographie pour que le système puisse mesurer les distances et les proportions par rapport à un point de référence commun puis les comparer aux données de référence. Les technologies actuelles de reconnaissance faciale utilisent des représentations mathématiques complexes et des procédés d'appariement évolués.

Le rendement des systèmes de reconnaissance faciale disponibles sur le marché dépend de la manière dont les images faciales sont obtenues. Ces systèmes réussissent mal à reconnaître un visage à partir d'images saisies de deux points de vue très différents sous des éclairages différents. Certains analystes se demandent si le visage, en l'absence de toute information contextuelle, constitue une base suffisante pour reconnaître une personne avec un degré de confiance très élevé en la comparant à un grand nombre d'identités(5).

(5) Voir, par exemple, Jain, Ross et Prabhakar (2004).

C. Reconnaissance de l’iris

L’iris est un muscle à l’intérieur de l’œil qui règle la taille de la pupille et détermine ainsi la quantité de lumière qui y pénètre. Chaque iris présente une texture très détaillée et unique dont la striation, les creux et les sillons permettent de reconnaître une personne. Les systèmes automatisés de reconnaissance de l’iris sont relativement récents – le premier brevet pour l’algorithme a été délivré en 1994 et les premiers produits commerciaux ont été mis en marché en 1995. Ces systèmes illuminent l’iris avec une lumière proche de l’infrarouge (inoffensive pour l’œil) et en prennent une photo au moyen d’une caméra numérique de grande qualité. Les motifs aléatoires de l’iris sont alors encodés en termes mathématiques et les codes ainsi produits sont comparés de manière statistique à un ou à plusieurs gabarits(6).

Étant donné qu’il est difficile de modifier chirurgicalement l’iris et que les iris artificiels (p. ex. lentilles de contact) sont faciles à reconnaître, il est relativement difficile de tromper un système de reconnaissance de l’iris. Ces systèmes sont très fiables(7) (dans la mesure où l’enrôlement est réussi) et rapides, puisqu’ils produisent le résultat en quelques secondes. Un de leurs inconvénients tient à ce qu’ils ne sont pas largement acceptés par le public comme outil de reconnaissance, surtout en raison de craintes (non fondées) que la lumière infrarouge endommage l’œil.

D. Reconnaissance de la main et des doigts

Les systèmes de reconnaissance biométrique de la géométrie de la main sont disponibles sur le marché depuis les années 1980 et sont utilisés dans des centaines d’endroits partout dans le monde. Ces systèmes mesurent et enregistrent la longueur, la largeur, l’épaisseur et la surface de la main d’une personne. Une caméra prend une image de la main du dessus et des miroirs disposés à certains angles permettent la prise d’une image latérale, créant ainsi un gabarit de vérification qui est comparé au gabarit créé lors de l’enrôlement.

Les systèmes de reconnaissance de la géométrie de la main sont très répandus, parce qu’ils sont faciles à utiliser, largement acceptés par le public et relativement peu coûteux. La géométrie de la main n’est toutefois pas unique, de sorte que ces systèmes doivent être limités à la vérification et ne peuvent servir à l’identification.

---

(6) John Daugman, *Iris Recognition for Personal Identification* (http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html).

(7) Essais des algorithmes de reconnaissance de l’iris de Daugman (http://www.cl.cam.ac.uk/~jgd1000/iristests.pdf).

E. Comparaison des systèmes de reconnaissance biométrique

Un certain nombre d'autres techniques de reconnaissance biométrique sont disponibles sur le marché ou en sont à l'étape de la R-D. Le tableau 1 compare 15 identifiants biométriques utilisant sept facteurs (on trouvera la description des facteurs dans la partie précédente du présent document, « Biométrie – Caractéristiques et systèmes »).

Tableau 1

Comparaison de différentes technologies de reconnaissance biométrique (E = Élevé, M = Moyen et F = Faible)

Identifiant biométrique	Universalité	Caractère distinctif	Permanence	Facilité de saisie	Performance	Acceptabilité	Facilité de contournement
ADN	E	E	E	F	E	F	F
Oreille	M	M	E	M	M	E	M
Visage	E	F	M	E	F	E	E
Thermogramme facial	E	E	F	E	M	E	F
Empreintes digitales	M	E	E	M	E	M	M
Démarche	M	F	F	E	F	E	M
Géométrie de la main	M	M	M	E	M	M	M
Veines de la main	M	M	M	M	M	M	F
Iris	E	E	E	M	E	F	F
Dynamique de la frappe	F	F	F	M	F	M	M
Odeur	E	E	E	F	F	M	F
Empreinte palmaire	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E
Voix	M	F	F	M	F	E	E

Source : Anil K. Jain, Arun Ross et Salil Prabhakar, « An Introduction to Biometric Recognition », *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, n° 1, janvier 2004 (http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf).

LIMITES TECHNIQUES DES SYSTÈMES DE RECONNAISSANCE BIOMÉTRIQUE

A. Fiabilité

La fiabilité d'un système de reconnaissance biométrique est caractérisée par deux statistiques sur l'erreur :

i) le taux de faux rejets, lorsque le système détermine que deux mesures biométriques d'une même personne proviennent de deux personnes;

ii) le taux de fausses acceptations, lorsque le système détermine que les mesures biométriques de deux personnes appartiennent à la même personne.

Ces deux mesures d'erreur sont reliées et il existe un point d'équilibre entre les deux pour chaque système biométrique. Chacune est fonction du seuil de décision du système, une valeur établie par le concepteur ou l'opérateur du système, qui définit le point auquel un appariement est effectué. Les résultats supérieurs au seuil sont des équivalences et les résultats inférieurs au seuil, des non-équivalences. Si le seuil est abaissé pour rendre le système plus tolérant aux variations des données saisies et au bruit, le taux de fausses acceptations augmente. Inversement, si le seuil est haussé pour que le système soit plus sûr, le taux de faux rejets augmente. Le point auquel les deux taux sont égaux est le point d'équivalence des erreurs. Plus cette valeur est faible, plus le système est fiable, car il y a alors un bon équilibre de la sensibilité. Outre ces taux d'erreur, le taux d'échec à la saisie et le taux d'échec à l'enrôlement sont également employés pour établir la fiabilité d'un système biométrique(8).

Il convient d'étudier attentivement les affirmations faites par les fournisseurs au sujet de la fiabilité de leurs produits, car : i) il se peut que le fournisseur ne mentionne qu'une des statistiques décrites ci-dessus, pour soutenir ses prétentions; ii) les taux de fiabilité présentés par les fournisseurs sont habituellement établis au moyen de tests ou de l'utilisation de systèmes de reconnaissance de petite envergure dans des conditions contrôlées; et iii) les impératifs de fiabilité d'un système biométrique dépendent de l'utilisation à laquelle on le destine : vérification ou identification.

(8) *Ibid.*

B. Vulnérabilité

Un système de reconnaissance biométrique peut être « dupé » à dessein ou accidentellement. Les systèmes sont vulnérables à des dommages ou à des attaques, d'une part, au niveau de l'appareil ou de l'équipement connexe à l'interface utilisateur et, d'autre part, au niveau du système. Les appareils peuvent être vulnérables à la duperie (contournement par un imposteur), à la détérioration par l'environnement ou à des attaques matérielles, et à des dommages aux câbles, fils et conduits de communications. Pour ce qui est du système, les algorithmes et les gabarits sont vulnérables aux attaques de pirates informatiques; les données peuvent être effacées, modifiées ou volées au niveau de l'administrateur ou du compte; et les éléments logiciels (p. ex. les pilotes) peuvent être vulnérables à des attaques. L'emploi de systèmes de reconnaissance biométrique multimodaux faisant appel à plusieurs technologies et aux données de plusieurs caractéristiques biométriques est un moyen de repousser les limites de fiabilité et de vulnérabilité évoquées ci-dessus.

Il faut également souligner que, pour ce qui est de la vérification de l'identité, la 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. ex. un acte de naissance) falsifiés pour s'enrôler, le système ne pourra pas confirmer la véritable identité de la personne.

AUTRES PRÉOCCUPATIONS RELATIVES AUX SYSTÈMES DE RECONNAISSANCE BIOMÉTRIQUE

A. Protection de la vie privée

1. Surveillance de masse et préoccupations connexes

De nombreux défenseurs des libertés civiles s'opposent à l'usage de systèmes de reconnaissance biométrique (et à d'autres outils de reconnaissance), parce qu'ils considèrent ces systèmes comme des éléments d'une « société surveillée » dans laquelle le gouvernement et les entreprises privées collectent de plus en plus de renseignements personnels, parfois sans raison. Ils estiment que l'État ne devrait pas suivre les citoyens ou violer leur vie privée à moins d'avoir des éléments de preuve d'actes répréhensibles(9). Ils craignent également que certaines

(9) Voir, par exemple, Jay Stanley et Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union, janvier 2003 (http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf).

techniques de reconnaissance biométrique (p. ex. du visage) donnent lieu à une surveillance sans le consentement des intéressés et même à leur insu.

2. Utilisation détournée

Les systèmes de reconnaissance biométrique soulèvent également la crainte d'une utilisation détournée, c'est-à-dire l'élargissement d'un processus ou d'un système selon lequel les données recueillies à une certaine fin servent ultérieurement à une autre fin non prévue ou non autorisée. Un exemple de fin détournée est celui du numéro de sécurité sociale aux États-Unis. Dans les années 1930, lorsque le gouvernement a introduit ce numéro, il a donné à la population l'assurance qu'il servirait uniquement au suivi des cotisations ou de l'admissibilité d'une personne à la sécurité sociale. Aujourd'hui, il est utilisé largement par les organismes du gouvernement fédéral américain et les entreprises privées pour identifier des personnes et il est souvent volé par des individus impliqués dans des cas d'usurpation d'identité. On a adopté ou proposé des mesures législatives fédérales destinées à limiter l'utilisation du numéro afin d'enrayer ce phénomène(10).

3. Loi désuète en matière de protection de la vie privée

Certains défenseurs de la vie privée notent que l'accroissement de la surveillance par l'État et les entreprises privées au moyen de nouvelles technologies ne s'est pas accompagné de changements législatifs destinés à assurer la protection de la vie privée. Par exemple, au Canada, la *Loi sur la protection des renseignements personnels* impose à quelque 150 ministères et organismes fédéraux des obligations en matière de respect des droits à la vie privée en limitant la collecte, l'utilisation et la communication de renseignements personnels(11). Cette loi, entrée en vigueur en 1983, n'a pas subi de modification majeure depuis son adoption. Selon le Commissaire à la vie privée du Canada, les changements technologiques et autres ont profondément modifié le paysage de la vie privée depuis une vingtaine d'années et la *Loi sur la*

(10) Par exemple, l'*Intelligence Reform and Terrorism Prevention Act of 2004* interdit aux États de faire figurer le numéro de sécurité sociale sur les permis de conduire ou les certificats d'immatriculation des véhicules automobiles.

(11) Au Canada, les personnes sont également protégées par la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui établit les règles selon lesquelles les entreprises privées peuvent recueillir, utiliser et communiquer des renseignements personnels dans le cadre d'activités commerciales.

protection des renseignements personnels « …est une loi dont l'obsolescence prive le Commissariat à la protection de la vie privée du Canada de pratiquement tout pouvoir de protéger le droit à la vie privée des Canadiennes et des Canadiens, plus particulièrement en ce qui concerne la collecte, l'utilisation et la communication de renseignements personnels par le gouvernement fédéral… »(12).

Le Commissariat ne s'oppose pas à l'utilisation de la reconnaissance biométrique dans les circonstances appropriées. Il estime que, bien employés, les outils de reconnaissance biométrique peuvent en fait accroître la protection de la vie privée d'une personne et son contrôle de sa propre identité. Leur utilisation abusive, cependant, peut donner lieu à des intrusions indésirables dans la vie privée. Le Commissariat examine l'utilisation de la reconnaissance biométrique au cas par cas. Il considère que la preuve doit être faite que toute mesure proposée 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, et on doit démontrer qu'aucune autre mesure moins susceptible de porter atteinte à la vie privée ne peut donner le même résultat(13).

B. Coûts de mise en œuvre et d'exploitation

Les coûts de mise en œuvre et d'exploitation sont un autre aspect préoccupant des systèmes de reconnaissance biométrique. Certains systèmes de reconnaissance biométrique utilisés en entreprise, sur une petite échelle, sont relativement peu chers à installer et à entretenir; cependant, le coût global du cycle de vie d'autres systèmes plus complexes destinés à des exploitations sur une grande échelle peut être prohibitif pour certaines entités (y compris des gouvernements). Il faut inclure dans le coût total de ces systèmes non seulement les immobilisations initiales en matériels et logiciels, mais aussi les coûts de la production de pièces d'identité (dans certains cas), la formation et l'embauche de personnel, l'entretien du matériel et la gestion des bases de données.

---

(12) Commissariat à la protection de la vie privée du Canada, *La commissaire à la protection de la vie privée dépose un rapport et se prononce en faveur d'une réforme urgente de la* Loi sur la protection des renseignements personnels du Canada, communiqué, 5 juin 2006 (http://www.privcom.gc.ca/media/nr-c/2006/nr-c_060605_f.asp).

(13) Communication personnelle avec le Commissariat à la protection de la vie privée du Canada et renseignements tirés d'infocapsules fournies en juillet 2006.

L'USAGE DE LA RECONNAISSANCE BIOMÉTRIQUE PAR LES ÉTATS

Dans le monde, de nombreux États utilisent déjà ou envisagent d'employer des systèmes de reconnaissance biométrique à des fins d'identification et de vérification. Nous donnons ci-dessous un tour d'horizon des principaux systèmes (ou programmes) utilisés ou en cours d'élaboration par certains d'entre eux : États-Unis, Royaume-Uni et États membres de l'Union européenne. Nous abordons également la situation du Canada pour ce qui est de l'utilisation actuelle ou projetée par le fédéral de systèmes de reconnaissance biométrique.

A. États-Unis

Il n'est pas étonnant, vu ses préoccupations accrues en matière de sécurité, de constater que le gouvernement des États-Unis est un chef de file mondial en matière de mise en œuvre de technologies de reconnaissance biométrique pour la vérification et l'identification. Le gouvernement américain utilise ou prévoit utiliser plusieurs systèmes et programmes qui font appel à la biométrie; les principaux sont décrits ci-dessous.

1. Integrated Automated Fingerprint Identification System (IAFIS)

Le FBI (qui relève du département de la Justice des États-Unis) exploite l'IAFIS, un système automatisé de saisie et de reconnaissance des empreintes roulées des 10 doigts. L'IAFIS est entrée en fonction en 1999; comptant les empreintes digitales de plus de 47 millions de sujets, il constitue la plus grande base de données biométriques au monde(14).

2. United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT)

Le programme US-VISIT, mis en place par le département de la Sécurité intérieure (DSI) et inauguré en 2004, collecte, entrepose et partage de l'information, y compris des identifiants biométriques, sur des ressortissants étrangers(15) qui entrent aux États-Unis et les quittent. Le programme US-VISIT utilise le balayage numérique des doigts ainsi que des

(14) Federal Bureau of Investigation (http://www.fbi.gov/hq/cjisd/iafis.htm).

(15) La plupart des citoyens canadiens sont actuellement exemptés du programme US-VISIT (http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0695.xml).

photographies pour comparer des personnes à des listes de surveillance (criminels, terroristes, contrevenants aux lois de l'immigration) et pour vérifier qu'un visiteur est bien la personne à laquelle un visa ou un autre titre de voyage a été délivré. Les visiteurs confirment leur départ en faisant balayer leur visa ou leur passeport et en subissant un balayage électronique des doigts à certains points d'entrée aériens et maritimes. Les données biométriques sont entreposées dans la base de données du système automatisé d'identification biométrique (IDENT), qui contient les renseignements sur les empreintes digitales de l'IAFIS du FBI. Le gouvernement souhaite l'intégration totale de l'IDENT et de l'IAFIS.

Le programme a été critiqué par le Government Accountability Office (GAO) des États-Unis, qui considère que le DSI a mis beaucoup de temps à évaluer et à tester la sécurité élémentaire du système et les mécanismes de protection de la vie privée. Le GAO déplore également que le DSI n'ait pas démontré que le programme donne ou donnera un résultat proportionné aux coûts et aux risques prévus. En particulier, le GAO considère que les analyses de rendement d'investissement réalisées par le DSI pour les processus de sortie ne garantissent pas que ceux-ci seront efficients(16).

3. Registered Traveler Program (RT)

Le DSI élabore actuellement le programme RT. Il s'agira d'une initiative à participation volontaire et axée sur le marché, consistant en un service que le secteur privé offrira moyennant paiement et sous la supervision du gouvernement. L'objectif du programme est de renforcer la sécurité aérienne et d'améliorer le service à la clientèle. Les entreprises qui enrôleront des participants dans le programme recueilleront les empreintes digitales et les données biométriques de l'iris ainsi que des renseignements personnels de base concernant les adhérents (p. ex. les passagers qui prennent fréquemment l'avion). Les renseignements recueillis seront ensuite analysés par le DSI, qui effectuera un « contrôle du risque » avant le voyage pour les participants au programme. En théorie, ces personnes bénéficieront d'un traitement accéléré à l'aéroport. Des expériences ont été menées par le gouvernement dans cinq aéroports des États-Unis en 2004 et 2005 et l'évaluation qui en a été faite permet de conclure que le programme est

(16) United States Government Accountability Office, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*, février 2006 (http://www.gao.gov/new.items/d06296.pdf).

viable[17]. Un « partenariat pilote » public-privé a été réalisé à l'aéroport d'Orlando (Floride). Le lancement national du programme RT était prévu en juin 2006, mais selon le site Web de la Transport Security Administration (TSA), la mise en œuvre débutera plus tard en 2006[18].

Différents groupes sont opposés au programme RT. La Air Transport Association of America estime que le programme mobilisera inutilement les ressources limitées de la TSA et nuira à la capacité de l'organisme d'élaborer des programmes plus globaux qui profiteraient à tous les voyageurs[19]. L'American Civil Liberties Union croit que l'initiative forcera les Américains à choisir entre un passage plus rapide à la sécurité des aéroports ou la protection de leurs renseignements les plus privés et les plus personnels. En outre, fait valoir l'organisme, le programme pourrait rendre les États-Unis plus vulnérables à des attaques terroristes, puisque des terroristes pourraient s'inscrire au programme en utilisant de fausses identités[20].

B. Royaume-Uni

En 2006, le Parlement britannique a adopté une loi[21] visant à instaurer une carte d'identité nationale à composante biométrique. Selon le gouvernement, la carte présente de nombreux avantages, notamment ceux de réduire les fraudes à l'identité et l'immigration illégale au Royaume-Uni et d'aider à réduire le crime organisé et le terrorisme. Conformément au calendrier établi à la promulgation de la loi, quiconque voudra renouveler son passeport à compter de 2008 recevra sa carte d'identité, et ses renseignements personnels (y compris les données biométriques) seront portés à une base de données – le registre national de l'identité. La partie biométrique du système utilisera probablement la reconnaissance du visage, des empreintes et de l'iris. Par la suite, le gouvernement prévoit de délivrer une simple carte

(17) United States Department of Homeland Security, Transportation Security Administration, déclaration de Kip Hawley, secrétaire adjoint au sous-comité de la sécurité économique, de la protection des infrastructures et de la cybersécurité, Committee on Homeland Security, Chambre des représentants des États-Unis, 3 novembre 2005 (http://www.tsa.gov/assets/pdf/110305TRAV.pdf).

(18) United States Department of Homeland Security, Transportation Security Administration, voyageur inscrit (http://www.tsa.gov/what_we_do/layers/rt/index.shtm, site consulté le 6 septembre 2006).

(19) Air Transport Association, lettre ouverte, juin 2006 (http://www.airlines.org/files/AirportDirectorsLetter.pdf).

(20) Témoignage de Timothy D. Sparapani, conseiller législatif à l'ACLU, au sujet de la sécurité aérienne et de l'inscription des voyageurs devant le Comité sénatorial du commerce, des sciences et des transports, 9 février 2006 (http://www.aclu.org/safefree/general/24113leg20060209.html).

(21) *Identity Cards Act 2006* (http://www.identitycards.gov.uk/downloads/ukpga_20060015_en.pdf).

d'identité aux personnes qui ne désirent pas obtenir de passeport. Avant 2010, on pourra choisir de ne pas recevoir la carte, mais on devra tout de même la payer, et les renseignements seront versés dans la base de données. La carte d'identité deviendra un jour obligatoire.

Le projet de carte d'identité nationale a suscité des inquiétudes au sujet de la fiabilité et de la vulnérabilité des systèmes de reconnaissance biométrique. Selon un rapport(22) rendu public par des chercheurs de la London School of Economics and Political Science (LSE) avant l'adoption de la loi, la technologie sous-jacente n'a pas fait l'objet de tests à l'échelle proposée par le Home Office (ministère de l'Intérieur) du Royaume-Uni et la base de données contenant les informations sur chaque titulaire de carte risque de devenir une cible importante d'attaques contre la sécurité. Un autre rapport publié par un comité de la Chambre des communes souligne un manque de transparence concernant la prise en compte des avis scientifiques et déplore le fait que les choix concernant la technologie de reconnaissance biométrique aient précédé les essais(23).

Bien que le programme de carte d'identité soulève des inquiétudes relativement à la protection des renseignements personnels, ce sont surtout les coûts impliqués qui font l'objet de critiques. Par exemple, dans son rapport, la LSE estime que la mise en œuvre et l'exploitation du système coûteront entre 10,6 et 19,2 milliards de livres sterling (entre 22,3 et 40,4 milliards de dollars canadiens) au cours des dix premières années (aux prix de 2005-2006)(24), des chiffres bien supérieurs à l'estimation de 584 millions de livres par an du gouvernement britannique(25). Le Home Office a réagi au rapport en qualifiant les estimations de la LSE de vagues et basées sur des hypothèses erronées(26) et en présentant un extrait d'une autre étude selon laquelle la

---

(22) LSE Identity Project 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, London School of Economics and Political Science, juin 2005 (http://is2.lse.ac.uk/idcard/identityreport.pdf).

(23) Comité des sciences et de la technologie de la Chambre des communes, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, sixième rapport de session (2005-2006), août 2006 (http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf).

(24) LSE Identity Project 2005.

(25) UK Home Office, *Regulatory Impact Assessment*, mai 2005 (http://www.identitycards.gov.uk/downloads/Identity_cards_bill_regulatory_impact.pdf).

(26) UK Home Office, *Home Office Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint*, juillet 2005 (http://www.identitycards.gov.uk/downloads/Response_LSE_Alternative_Blueprint.pdf).

méthodologie utilisée par le gouvernement pour évaluer les coûts est robuste[27]. Le gouvernement a par la suite précisé que son estimation ne concernait que les coûts d'exploitation annuelle du système pour le ministère responsable (le Home Office). Il n'a pas encore produit d'estimation définitive du coût total du programme, jugeant une telle information délicate du point de vue commercial; toutefois, la loi exige qu'il fournisse au Parlement tous les six mois une estimation des dépenses publiques que le programme occasionnera vraisemblablement.

Des reportages récents et des déclarations du Home Office portent à croire que le programme de la carte d'identité, du moins dans sa forme actuelle, serait en difficulté. Selon ces informations, le calendrier de mise en place de la carte fait l'objet d'une révision dans le cadre d'un examen de toutes les activités du Home Office[28]. Le premier ministre Blair a toutefois soutenu que l'initiative serait réalisée, car elle constitue un élément clé du manifeste du Parti travailliste en vue des prochaines élections générales au Royaume-Uni[29].

C. États membres de l'Union européenne

Vraisemblablement en réponse aux normes (à caractère non obligatoire) établies par l'Organisation de l'aviation civile internationale (OACI), un organisme de l'Organisation des Nations Unies, et aux exigences imposées par le gouvernement des États-Unis dans le cadre du programme US-VISIT, les États membres de l'Union européenne (UE) ont commencé à inclure des identificateurs biométriques dans les passeports. Le programme US-VISIT prévoit qu'à compter du 26 octobre 2006, les 27 pays qui participent au programme d'exemption de visa des États-Unis[30] devront délivrer des passeports électroniques lisibles à la machine. Ces passeports devront contenir un microcircuit intégré pour le stockage des informations biographiques figurant sur la page de renseignements, une photographie numérisée et d'autres données

---

(27) KPMG, *Home Office ID Cards Programme Cost Methodology and Cost Review Outline Business Case Review*, extrait publié, novembre 2005 (http://www.identitycards.gov.uk/downloads/2005-11-7_KPMG_Review_of_ID_Cards_Methodology.pdf).

(28) Voir, par exemple, Richard Ford, « ID cards under threat in review of Home Office », *Times Online*, 12 juillet 2006 (http://www.timesonline.co.uk/article/0,,2-2266071,00.html).

(29) Conférence de presse mensuelle du premier ministre Tony Blair, août 2006 (http://www.pm.gov.uk/output/Page9960.asp).

(30) Pour une description du programme et la liste des pays participants, voir le site du département d'État américain (http://travel.state.gov/visa/temp/without/without_1990.html#2).

biométriques[31]. Pour ce qui est de l'information biométrique interopérable à l'échelon international pour la vérification de l'identité assistée par une machine, l'OACI appuie l'utilisation d'images faciales normalisées mémorisées sous forme numérique. Comme norme pour les dispositifs à mémoire, l'organisme a choisi les puces à circuit intégré sans contact de grande capacité (fonctionnant aux fréquences radio) pour le stockage des données d'identification dans des documents de voyage lisibles à la machine[32].

En 2004, la Commission européenne a promulgué un règlement (exécutoire pour tous les États membres, à l'exception du Royaume-Uni et de l'Irlande[33]) établissant les normes de sécurité minimales applicables aux passeports et aux autres documents de voyage[34]. Selon ce règlement, les passeports et les documents de voyage doivent comprendre un support de données qui contient une image faciale et les documents doivent aussi inclure deux empreintes digitales dans un format interopérable (dans l'ensemble de l'UE). Tous les États membres avaient jusqu'au 28 août 2006 pour se conformer à l'exigence relative à l'image faciale et ils ont jusqu'au 28 juin 2009 pour se conformer à l'exigence concernant les empreintes digitales.

Des critiques du système de passeports biométriques envisagé par l'UE notent que l'inclusion d'une photographie numérisée dans les passeports satisfait aux exigences établies par l'OACI, mais que l'UE est allée plus loin en exigeant l'inclusion d'empreintes digitales. Ils font également remarquer que, puisque seulement deux empreintes digitales seront prises, le taux d'erreur pour une base de données regroupant l'ensemble de l'UE sera relativement élevé si cette information doit être utilisée pour l'identification (plutôt qu'uniquement pour la vérification)[35].

---

(31) Programme d'exemption de visa des États-Unis, Échéanciers 2005-2006 (http://cbp.gov/linkhandler/cgov/travel/id_visa/vwp/vwp_timeline.ctt/vwp_timeline.pdf).

(32) Doc 9303 Spécifications pour les documents de voyage lisibles à la machine (*Specifications for Machine Readable Travel Documents*) (http://www.icao.int/mrtd/publications/doc.cfm).

(33) Le Royaume-Uni et l'Irlande n'ont pas signé la *Convention de Schengen*.

(34) Règlement (CE) N^{o} 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 (http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf).

(35) Voir, par exemple, l'éditorial de *Statewatch* (http://www.statewatch.org/news/2006/jul/04eu-bio-passports.htm).

D. Canada

Le gouvernement du Canada, seul ou en collaboration avec le gouvernement fédéral des États-Unis, utilise des technologies de reconnaissance biométrique dans le cadre de plusieurs programmes. Il est probable que l'utilisation de ces technologies augmentera, notamment compte tenu des changements apportés aux normes internationales applicables aux passeports et des changements proposés aux exigences relatives aux passeports pour les personnes qui se rendent aux États-Unis. On trouvera ci-dessous une description des principaux programmes, ministères ou organismes fédéraux qui utilisent ou prévoient utiliser des technologies de reconnaissance biométrique.

1. Gendarmerie royale du Canada (GRC)

La GRC a entrepris dernièrement de mettre à niveau son système d'identification dactyloscopique pour en améliorer la vitesse et la fiabilité. Le nouveau Système automatisé d'identification dactyloscopique appuiera le traitement fiable des empreintes digitales de qualité, sans aucune ou presque aucune intervention manuelle. Le transfert de quatre millions de fiches dactyloscopiques de l'ancien au nouveau Système devait être terminé à l'été 2006. Un nouveau serveur permettra l'échange électronique des demandes d'identification dactyloscopique. Les nouveaux systèmes devraient être mis en service avant la fin de 2006[(36)].

2. CANPASS Air

CANPASS Air est un programme de l'Agence des services frontaliers du Canada (ASFC) qui vise à faciliter l'entrée au Canada, d'une façon efficace et sécuritaire, des voyageurs préautorisés à faible risque. Le programme, qui est actuellement en place dans sept aéroports au pays, utilise la technologie de la reconnaissance de l'iris pour vérifier l'identité du passager. Les citoyens et les résidents permanents du Canada qui désirent participer au programme CANPASS font l'objet d'une vérification de sécurité au moment de l'inscription et du renouvellement annuel. Ils paient des frais annuels (actuellement 50 $) et reçoivent une carte d'identité leur permettant d'utiliser les postes de déclaration libre-service CANPASS Air situés dans les aéroports, où leur iris est photographié et comparé à l'information contenue dans la base de données. Une fois leur identité confirmée, les voyageurs peuvent aller chercher leurs bagages et sortir de l'aire des douanes sans autre contact avec les agents de l'ASFC, à moins d'être sélectionnés au hasard pour une inspection.

---

(36) GRC, Projet d'identification en temps réel (ITR) (http://www.rcmp-grc.gc.ca/rtid/report_issue1_f.htm).

3. NEXUS

NEXUS[37] est un groupe de programmes tarifés réalisés conjointement par les gouvernements fédéraux canadien et américain; il découle du Plan d'action en 30 points de la Déclaration sur la frontière intelligente signée par le Canada et les États-Unis en décembre 2001[38]. Pour le groupe des trois programmes NEXUS – NEXUS Autoroute, NEXUS Maritime et NEXUS Air –, des données biométriques (empreintes digitales) sont recueillies au cours du processus de demande pour la vérification des antécédents. Une fois approuvés par les deux pays en tant que voyageurs à faible risque, les membres NEXUS bénéficient d'un processus d'entrée simplifié dans les deux pays lorsqu'ils traversent la frontière canado-américaine à bord d'un véhicule motorisé, d'une embarcation de plaisance ou d'un aéronef.

Le programme pilote NEXUS Air a été mis en œuvre en novembre 2004 et le service est offert uniquement à l'aéroport international de Vancouver. Il permet aux voyageurs préautorisés à faible risque voyageant entre le Canada et États-Unis de s'acquitter rapidement des formalités des douanes et de l'immigration. Le programme fonctionne de façon similaire à CANPASS Air, c'est-à-dire qu'il utilise la technologie de la reconnaissance de l'iris pour vérifier l'identité du passager. Une fois celle-ci confirmée à l'un des postes de déclaration automatisés situés à l'aéroport, les membres répondent aux questions des douaniers et des agents d'immigration canadiens ou américains (selon leur destination) sur l'écran tactile du poste. Le système délivre ensuite un reçu et ceux qui entrent au Canada sont dirigés soit vers la sortie, soit vers l'aire d'inspection secondaire, alors que ceux qui entrent aux États-Unis sont dirigés soit vers l'aire d'inspection secondaire, soit vers l'aire de contrôle de sécurité.

4. Passeport Canada

Des éléments de sécurité de pointe ont été ajoutés aux passeports canadiens délivrés au Canada depuis 2002 et aussi dans les passeports canadiens délivrés à l'étranger depuis avril 2006. Ces éléments sont une photo imprimée numériquement, des hologrammes, de l'encre spéciale et une zone de lecture automatique au bas de la page des renseignements personnels. Actuellement, le passeport canadien ne contient pas d'identificateur biométrique, mais des éléments biométriques seront probablement inclus dans la toute dernière version, qui est en cours d'élaboration. En septembre 2004, les dispositions modifiant le *Décret sur les*

---

(37) NEXUS (http://www.cbsa-asfc.gc.ca/travel/nexus/menu-f.html).

(38) Déclaration sur la frontière intelligente (http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2002/sep/smart-f.pdf).

passeports canadiens sont entrées en vigueur et deux d'entre elles autorisent Passeport Canada à inclure des données biométriques dans les passeports(39). La première modification autorise Passeport Canada à convertir tout renseignement présenté par un requérant en données bionumériques pour l'inclure dans le passeport. Aux termes de la deuxième modification, l'organisme peut convertir la photographie du requérant en gabarit bionumérique pour vérifier son identité.

Passeport Canada travaille actuellement à la mise au point d'un nouveau passeport électronique canadien. Le document sera conforme aux normes de l'OACI, qui exigent l'inclusion d'une puce électronique sans contact contenant, entre autres, une photo numérisée pour la reconnaissance faciale. Peu d'informations ont été rendues publiques par l'organisme au sujet du projet de passeport électronique. Selon le *Plan directeur et d'entreprise 2005-2008* de Passeport Canada, des spécimens du passeport électronique devaient être mis à l'essai par des diplomates et ministres canadiens dans le cadre d'un projet pilote en juillet 2006 et l'utilisation à l'échelle nationale était prévue pour juillet 2007(40). Toutefois, l'organisme affirme maintenant que le passeport électronique est à l'étape du développement et qu'il est trop tôt pour parler des coûts et du calendrier de sa mise en œuvre(41). À l'heure actuelle, Passeport Canada réalise un projet distinct (sans aucun lien, selon l'organisme, avec le passeport électronique) en vue de l'adoption d'un système de reconnaissance faciale qui sera utilisé dans le cadre du processus de traitement des demandes de passeport. Lorsqu'il sera pleinement fonctionnel, le système effectuera les tâches d'identification et de vérification et pourra comparer les images faciales des demandeurs à celles contenues sur une liste de surveillance dressée à partir d'un éventail de sources. Le système aiderait Passeport Canada pour « la prise et la justification des décisions en matière d'admissibilité et de délivrance des passeports »(42).

L'adoption prévue des technologies de reconnaissance faciale et des passeports biométriques se fait sans débat public ou presque. D'après certains opposants à l'adoption du passeport électronique, le gouvernement fédéral s'engage dans un processus de « recyclage de

---

(39) *Décret modifiant le décret sur les passeports canadiens*, P.C. 2004-951, 1er septembre 2004 (http://www.ppt.gc.ca/publications/pdfs/order_04_113.pdf).

(40) Passeport Canada, *Plan directeur et d'entreprise 2005-2008*, juin 2005 (http://www.ppt.gc.ca/publications/pdfs/bp05-08_ca_f.pdf).

(41) Communication personnelle d'un agent des relations avec les médias à Passeport Canada, 30 août 2006.

(42) Renseignements tirés d'un avis d'appel d'offres concernant une « solution de reconnaissance faciale » parue sur le MERX le 14 juillet 2006 (http://www.merx.com/French/SUPPLIER_Menu.Asp?WCE=Show&TAB=1&State=7&id=PW-%24EEM-006-14751&hcode=shsxpr2tIBMeERly4npDoQ%3d%3d).

politiques », c'est-à-dire l'adoption de politiques élaborées à l'étranger ou sur la scène internationale (dans ce cas, la délivrance de passeports biométriques conformes aux normes de l'OACI) et qui ne seraient peut-être pas adoptées si elles suivaient le processus d'adoption habituel au Canada(43).

Passeport Canada a présenté une évaluation des facteurs relatifs à la vie privée de l'initiative des passeports électroniques au Commissariat à la protection de la vie privée du Canada. Le Commissariat ne s'oppose pas à l'inclusion des identificateurs biométriques eux-mêmes dans les passeports, mais précise que l'Agence des passeports doit s'assurer de la sécurité de l'information stockée dans la puce insérée dans le passeport électronique. Le Commissariat a dit que le système de passeports électroniques, quel qu'il soit, doit protéger les détenteurs de passeport contre les activités telles que l'« écrémage » et l'« interception illicite ». L'« écrémage » consiste à utiliser un lecteur non autorisé pour recueillir de l'information contenue sur une puce de passeport à l'insu du détenteur, par exemple lorsque le passeport se trouve dans la poche de celui-ci. L'« interception illicite » consiste à intercepter et à lire l'information transmise entre la puce du passeport et le lecteur(44).

5. Autres initiatives

En 2002, le ministre de la Citoyenneté et de l'Immigration alors en poste, Denis Coderre, a demandé la tenue d'un débat public sur l'adoption d'une carte nationale d'identité contenant des identificateurs biométriques. Le débat s'est déroulé, en partie, par le truchement des audiences tenues par le Comité permanent de la Chambre des communes sur la citoyenneté et l'immigration. Dans son rapport provisoire déposé en 2003(45), le Comité détaille plusieurs préoccupations que soulève le système de cartes nationales d'identité et conclut qu'un débat public beaucoup plus vaste est nécessaire pour déterminer s'il y a lieu de mettre en place un tel système. Si l'on devait conclure que la carte nationale d'identité est nécessaire, le Comité a fait

---

(43) Voir, par exemple, Andrew Clement et Krista Boa, *Developing Canada's Biometric Passport: Where are Citizens in this Picture?* (http://ts6.cgpublisher.com/proposals/55/index_html, site consulté le 11 septembre 2006).

(44) Communication personnelle du Commissariat à la protection de la vie privée du Canada. Information tirée d'infocapsules datées de juillet 2006.

(45) Comité permanent de la Chambre des communes sur la citoyenneté et l'immigration, *Une carte nationale d'identité au Canada?*, octobre 2003 (http://www.parl.gc.ca/infocomdoc/documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-f.pdf).

remarquer que d'autres questions devraient également être prises en compte, par exemple le coût financier d'un système de cartes d'identité, la nature de la technologie de reconnaissance biométrique à utiliser, la protection des renseignements personnels et d'autres questions relatives à la protection de la vie privée. Le Comité n'a pas déposé de rapport final sur le système de cartes nationales d'identité. La question a disparu de l'ordre du jour du gouvernement fédéral après les élections générales de juin 2004.

CONCLUSION

Étant donné l'omniprésence des préoccupations en matière de sécurité dans le monde d'aujourd'hui, il est peu probable que les systèmes de reconnaissance biométrique disparaîtront. Ils deviendront probablement monnaie courante aux frontières, dans les aéroports et dans les autres établissements où la sécurité est un enjeu. L'Organisation de l'aviation civile internationale a établi des normes pour les documents de voyage lisibles à la machine, y compris l'inclusion d'identificateurs biométriques; ainsi, le passeport électronique biométrique deviendra probablement un jour le seul document acceptable pour les voyages internationaux.

Les systèmes de reconnaissance biométrique sont des dispositifs de sécurité intrusifs. Certaines personnes s'opposent donc carrément à leur utilisation, alors que d'autres sont d'avis qu'ils peuvent être nécessaires dans certains cas, mais seulement si des mesures de sécurité et des mesures juridiques appropriées sont en place pour protéger les renseignements personnels de nature délicate recueillis. Les préoccupations particulières que soulève l'utilisation de ces systèmes comprennent, entre autres, les limites sur le plan technique (fiabilité et vulnérabilité), la surveillance accrue – et dans certains cas inutile – des activités quotidiennes des citoyens, le vol ou la manipulation des données biométriques et d'autres renseignements personnels conservés dans des banques de données centralisées, le détournement de l'utilisation (c.-à-d. que les données biométriques recueillies à une fin précise sont utilisées par la suite à d'autres fins non prévues ou non autorisées) et le coût élevé de la mise en place et de l'exploitation de bon nombre de ces systèmes.

Le gouvernement du Canada, comme d'autres gouvernements ailleurs dans le monde, utilise ou met à l'essai la biométrie dans un certain nombre de situations. Déjà, la vérification biométrique volontaire de l'identité des passagers au moyen de la reconnaissance de

l’iris est effectuée dans plusieurs aéroports au Canada, et un programme conjoint canado-américain similaire en est à l’étape pilote. Passeport Canada travaille à mettre au point un passeport électronique (contenant des données biométriques) et un système de reconnaissance faciale qui lui sera utile pour l’examen des demandes de passeport. Le Commissariat à la protection de la vie privée du Canada ne s’oppose pas à l’utilisation de la biométrie lorsque les circonstances le justifient, mais rappelle la nécessité de revoir de toute urgence la *Loi sur la protection des renseignements personnels* pour qu’elle reflète les changements technologiques récents, y compris l’utilisation de la biométrie.

Les systèmes de reconnaissance biométrique peuvent être des outils importants pour améliorer la sécurité dans certaines situations. Cependant, avant de prendre une décision quant à la mise en place de ces systèmes, les États devraient effectuer des analyses détaillées pour s’assurer que le recours à ces systèmes est vraiment nécessaire et qu’il n’existe aucun autre moyen moins intrusif d’obtenir le même résultat. De plus, les technologies de reconnaissance biométrique employées devraient être à la fois efficaces et utilisées de manière à réduire au minimum toute ingérence dans la vie privée.