COMMISSION CANADIENNE DES DROITS DE LA PERSONNE
CANADIAN HUMAN RIGHTS COMMISSION

La certification de l'identité et la protection des droits de la personne

Rapport préparé par :
Caleb Chepesiuk
Chercheur indépendant

et

Maciej Mark Karpinski
Analyste principal de la recherche,
Division de la recherche et de l'analyse statistique
Commission canadienne des droits de la personne

et

Charles Théroux, Ph. D.
Directeur, Division de la recherche et de l'analyse statistique
Commission canadienne des droits de la personne

Août 2010

HR4-8/2011F-PDF
978-1-100-97243-5

SOMMAIRE

La présente étude examine les diverses méthodes employées pour certifier l'identité d'un individu comme façon d'explorer les implications pouvant découler de la mise en œuvre de ces méthodes sur les droits protégés en vertu de la *Loi canadienne sur les droits de la personne* (LCDP). La LCDP vise à protéger les individus contre la discrimination fondée sur des motifs de distinction illicites (race, origine nationale ou ethnique, couleur, religion, âge, sexe, orientation sexuelle, état matrimonial, situation de famille, déficience physique ou mentale ou état de personne graciée) en matière d'emploi et de prestation de services. Le fait de priver un individu ou de le défavoriser sur la base des motifs prohibés énumérés ci-dessus constitue une infraction à la loi, sauf en cas de motif justifiable.

La présente étude passe en revue les diverses méthodes d'identification. L'impact possible ou réel de chaque méthode d'identification est ensuite étudié en fonction des motifs énumérés dans la LCDP. Pour chaque méthode d'identification, nous étudions la jurisprudence canadienne pertinente portant sur l'impact discriminatoire, y compris les mesures d'adaptation ou les motifs justifiables, lorsqu'il était impossible de prendre des mesures d'adaptation.

L'étude examine les mesures biométriques et non biométriques, y compris le nom, la date de naissance, le visage, la main, les empreintes digitales, l'iris et la signature originale d'une personne.

Les documents d'identité étudiés sont le passeport, la carte de résident permanent du Canada, le programme CANPASS Air et le programme NEXUS.

L'étude a constaté que la plupart des mesures biométriques ont des limites et peuvent avoir des répercussions sur un ou plusieurs des groupes protégés en vertu de la LCDP.

La Cour suprême du Canada a indiqué que les employeurs et fournisseurs de services avaient le devoir d'empêcher l'apparition de nouveaux obstacles. Ils doivent ainsi mettre la mesure en œuvre de la façon la plus inclusive possible. La biométrie doit par conséquent être instaurée de manière à inclure le plus grand nombre possible d'individus. Là où se posent des limites technologiques, il faut envisager l'adoption d'autres mesures ou de mesures supplémentaires. Le recours à des mesures supplémentaires, par conséquent la création d'un système multimodal, permet un degré de souplesse qui pourra peut-être contrer un certain nombre de conséquences possiblement discriminatoires. Là où des exceptions supplémentaires sont nécessaires, il faut également envisager la mise en place de politiques et de pratiques visant à tenir compte des différences individuelles sans contrainte excessive.

La *Charte canadienne des droits et libertés* et la *Loi canadienne sur les droits de la personne* reconnaissent qu'il peut y avoir des limites à l'exercice des droits d'une personne. Il revient cependant à l'organisme qui a recours à la mesure de prouver que le système utilisé a été conçu de façon à s'harmoniser avec les principes de droits de la personne.

TABLE DES MATIÈRES

1. Introduction

Les attaques terroristes perpétrées contre les États-Unis le 11 septembre 2001 ont eu d'importantes conséquences sur le Canada et les Canadiens. Le gouvernement canadien a, entre autres mesures, mis en œuvre la première politique de sécurité nationale de son histoire : *Protéger une société ouverte*.[1] La politique est conçue pour « répondre aux besoins en matière de sécurité nationale tout en protégeant des valeurs canadiennes fondamentales, à savoir l'ouverture, la diversité et le respect des libertés civiles. » L'un des huit sujets couverts par cette politique porte sur la sécurité à la frontière.

Le long de la « plus longue frontière non défendue au monde », la sécurité frontalière présente de nombreux défis variés, y compris la tâche ardue de mettre en place de nouveaux contrôles. Le Canada comme les États-Unis dépendent, d'un point de vue culturel et économique, d'une frontière ouverte. Environ 300 000 personnes et 35 000 camions traversent la frontière canado-américaine chaque jour, tout comme des échanges commerciaux bidirectionnels de 1,6 milliard de dollars[2].

En plus de sa politique de sécurité nationale, le gouvernement canadien a lancé son *Plan d'action pour la création d'une frontière sûre et intelligente*[3]. Ce plan d'action se concentre sur quatre enjeux : la circulation sécuritaire des personnes, la circulation sécuritaire des biens, la sécurité des infrastructures et la coordination et la mise en commun de l'information.

Les auteurs souhaitent remercier les organismes du gouvernement fédéral qui ont offert une rétroaction précieuse lors de la rédaction d'une version antérieure de ce rapport et leur expriment leur gratitude.

[1] "Securing an Open Society: Canada's National Security Policy." Privy Council Office. Avril 2004.

[2] "A Canada–U.S. Border Vision." Canadian Chamber of Commerce. Décembre 2008. http://www.chamber.ca/cmslib/general/blueprint.pdf.

[3] « Plan d'action pour la création d'une frontière sûre et intelligente », Affaires étrangères et Commerce international Canada, 2001, http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-fr.asp.

Aux fins de la présente recherche, l'enjeu qui suscite une préoccupation particulière en lien avec la sécurité à la frontière a trait à la circulation sécuritaire des personnes. À ce sujet, le *Plan d'action* insiste grandement sur l'identification et la gestion des risques, et catégorise les voyageurs comme étant à risque élevé ou à faible risque[4]. L'objectif est d'établir la catégorie de risque dans laquelle se trouve une personne avant qu'elle n'arrive à un poste frontalier ou à une porte d'embarquement pour faciliter le passage des voyageurs à faible risque et empêcher l'entrée au pays de ceux présentant un risque élevé[5]. Les États-Unis ont aussi lancé la *Western Hemisphere Travel Initiative*, qui exige que tous leurs citoyens présentent un document de voyage et d'identité sécuritaire à leur entrée au pays.

Les documents d'identité sont depuis longtemps une nécessité pour traverser les frontières à peu près partout dans le monde. La pression croissante pour se munir de frontières « intelligentes » a favorisé l'évolution de documents intégrant des technologies de plus en plus perfectionnées qui exigent l'utilisation de nouveaux identifiants afin de certifier la véritable identité d'une personne. La biométrie constitue l'une de ces technologies. La question de la biométrie – science et technologie qui étudie et analyse des données biologiques – fait partie du *Plan d'action*, qui affirme que le Canada et les États-Unis mettront « au point conjointement et le plus rapidement possible des mécanismes d'identification biométrique dans la documentation, comme les cartes de

[4] Voir David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003; Davina Bhandar, "Renormalizing Citizenship and Life in Fortress North America." *Citizenship Studies 8* (3) Sept. 2004. p. 261–278; Matthew B. Sparke, "A Neoliberal Nexus: Economy, security and the biopolitics of citizenship on the border." *Political Geography* 25 (2006): p. 151–180.
[5] « Sûreté et sécurité : Gestion de l'accès au Canada », Agence des services frontaliers du Canada, 31 juillet 2008. http://www.cbsa-asfc.gc.ca/security-securite/safety-surete-fra.html.

résident permanent, les cartes NEXUS[6] et d'autres documents de voyage, afin d'assurer une plus grande sécurité »[7].

Le gouvernement du Canada a l'obligation de délivrer les documents nécessaires aux personnes qui désirent voyager. En même temps, l'État est également tenu de protéger la sécurité territoriale et la sécurité de ses citoyens. Cette protection comprend le contrôle de l'accès au Canada et l'authentification et la vérification des documents d'identité sécuritaires pour faciliter ce contrôle[8]. La *Loi canadienne sur les droits de la personne* (LCDP) régit en partie la manière dont l'État s'y prend pour mettre en place de telles mesures de sécurité.

La LCDP a une valeur quasi constitutionnelle. Elle a pour but de donner effet « au principe suivant : le droit de tous les individus (...) à l'égalité des chances d'épanouissement et à la prise de mesures visant à la satisfaction de leurs besoins, indépendamment des considérations fondées sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial, la situation de famille, la déficience ou l'état de personne graciée »[9]. Il est par exemple contraire à la LCDP de refuser l'accès à des documents de voyage ou de défavoriser une personne ou un groupe de personnes en ayant recours à des méthodes précises de certification de

---

[6] Le programme NEXUS est conçu pour accélérer le passage à la frontière tant canadienne qu'américaine des voyageurs préautorisés à faible risque. Consultez le site http://www.cbsa-asfc.gc.ca/prog/nexus/menu-fra.html pour de plus amples renseignements sur ce programme.

[7] « Plan d'action pour la création d'une frontière sûre et intelligente », Affaires étrangères et Commerce international Canada, 2003. http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp.2008 http://www.international.gc.ca/anti-terrorism/actionplan-fr.asp (bonne adresse). http://www.spp.gov/pdf/key_accomplishments_since_august_2007.pdf.

[8] La responsabilité du gouvernement de faciliter la mobilité se trouve en partie limitée par les conditions d'entrée établies par d'autres États. La permission d'entrer dans un pays donné ne peut être accordée que par ce pays. De plus, "the right of a Canadian to leave Canada is a one sided coin. The right to enter the United States does not exist as the other side of the coin. A Canadian may practically not be able to leave Canada if no foreign country will let him enter it." (*N.B. v. Canada (Attorney General)*. 27 A.R. 135, 40 C.P.C. (4th) 244. p. 55.)

[9] *Loi canadienne sur les droits de la personne*, L.R. 1985, ch. H-6., art. 2 2.

l'identité fondées sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial, la situation de famille, la déficience physique ou mentale ou l'état de personne graciée, sauf en cas de motif justifiable.

La présente recherche explore le lien entre les droits des personnes protégées par la LCDP et certaines des méthodes les plus utilisées dans les processus de certification de l'identité. L'objectif est de définir s'il existe des limitations généralisables pouvant rendre des méthodes de certification de l'identité possiblement discriminatoires du point de vue des droits de la personne. Le document commence par un aperçu général de certaines méthodes non biométriques et biométriques. L'étude n'a pas la prétention d'être complète ni exhaustive. La méthode est ensuite analysée sous l'angle de la jurisprudence pertinente comme façon de comprendre le lien entre la méthode et les droits des personnes touchées par la méthode. Les résultats pointent vers certains principes clés dont on doit tenir compte au moment de mettre au point des méthodes de certification de l'identité.

L'étude se base sur des recherches antérieures faites sur la question de la sécurité nationale[10], et se concentre sur les conséquences de la technologie sur les droits de la personne dans un contexte de sécurité en évolution. Les préoccupations en matière de vie privée et l'« utilisation détournée »[11] sont du ressort de la *Loi sur la protection des renseignements personnels* et ne seront pas étudiées dans le présent document.

[10] Wesley K. Wark, « Les préoccupations relatives à la sécurité nationale et aux droits de la personne au Canada : étude de huit questions cruciales dans le contexte de l'après-11 septembre », rapport destiné à la Commission canadienne des droits de la personne, 2007.
[11] L'utilisation détournée se produit lorsque des renseignements recueillis à une certaine fin commencent à être utilisés à d'autres fins.

2. Méthodologie

La présente étude commence par une brève analyse documentaire d'un échantillon d'identifiants non biométriques utilisés au Canada, aux États-Unis et en Grande-Bretagne : nom, lieu de naissance, date de naissance, genre ou sexe, âge, nom des parents, situation du casier judiciaire, citoyenneté et codes d'identification. Cependant, l'étude porte principalement sur les méthodes biométriques : reconnaissance du visage, géométrie de la main, empreintes digitales, lectures de l'iris, signatures originales, analyses audiovisuelles et génétiques. Après une brève présentation de chaque méthode biométrique, le document traitera de certaines de ses limites. L'impact discriminatoire possible ou réel de chaque méthode d'identification est ensuite étudié en fonction des motifs prohibés énumérés dans la LCDP. L'information utilisée provient en grande partie des publications de l'industrie, d'articles soumis à l'examen des pairs et de certaines sources gouvernementales.

L'examen des exigences nécessaires à l'obtention d'un passeport, d'une carte de résident permanent du Canada, d'une carte CANPASS Air et d'une carte NEXUS illustre la façon de recourir à ces méthodes. L'information contenue dans cette section provient de publications gouvernementales.

Pour chaque méthode d'identification présentée, nous étudions la jurisprudence concernant les impacts discriminatoires, y compris les mesures d'adaptation ou les motifs justifiables pour motiver un traitement différentiel. L'analyse juridique dans cette section se limite à la jurisprudence canadienne.

Une version préliminaire du présent rapport a été distribuée à des fins de consultation aux organismes gouvernementaux suivants : ministère des Affaires étrangères et du Commerce international (MAECI), Passeport Canada, Citoyenneté et Immigration Canada (CIC), Sécurité publique Canada, Agence des services frontaliers du Canada (ASFC), Transports Canada, Administration canadienne de la sûreté du transport aérien (ACSTA), Gendarmerie royale du Canada (GRC), Commission des plaintes du public contre la GRC, Comité externe d'examen de la GRC, Service canadien du renseignement de sécurité (SCRS), Bureau de l'inspecteur général (SCRS), Comité de surveillance des activités de renseignement de sécurité (CSARS), ministère de la Défense nationale (MDN), Centre de la sécurité des télécommunications Canada (CSTC), Bureau du commissaire du Centre de la sécurité des télécommunications, Bureau du vérificateur général du Canada et Commissariat à la protection de la vie privée du Canada.

3. Méthodes de certification de l'identité

La certification de l'identité nécessite habituellement une « déclaration d'identité » et un « jeton d'identification » dont on se sert pour vérifier la déclaration. Un « jeton » fait référence à tout objet physique pouvant servir à vérifier une déclaration d'identité, par exemple un permis de conduire, une clé ou une carte magnétique. Certifier l'identité d'une personne ou demander à une personne de certifier son identité est un geste que les gens posent de façon quotidienne, depuis la reconnaissance d'un visage dans une foule jusqu'à l'utilisation d'une carte de guichet automatique. Un exemple type est celui d'un conducteur intercepté par un agent de police. L'agent de police peut demander à la personne son nom et, afin de vérifier l'identité de la personne, il lui

demandera de produire un document (par exemple un permis de conduire). L'agent examine le document d'identité produit en le comparant l'information avec ce que la personne lui a répondu. Si le document comporte une photographie, l'agent la compare avec le visage de la personne. De même, si le conducteur veut s'assurer de la déclaration d'identité de la personne en uniforme devant lui, il peut lui demander de lui montrer son insigne. Si l'un ou l'autre a encore des doutes, l'information peut être vérifiée à l'aide d'une base de données ou au quartier général de la police. Cet exemple met en scène des éléments clés de certification de l'identité : information, documents et examen.

Les déclarations d'identité peuvent être explicites ou implicites. Une personne qui donne son nom lorsqu'on lui demande « Qui êtes-vous? » ou le fait d'introduire une carte de débit dans un guichet automatique des exemples explicites de déclaration d'identité. Parmi des exemples implicites, mentionnons le fait de conduire une voiture (qui implique que vous possédez un permis de conduire) ou l'achat d'alcool dans un magasin ou un bar (qui implique que vous avez l'âge légal pour acheter de l'alcool). Selon Downes, une déclaration d'identité peut être appuyée par des assertions ou des jetons. Une assertion consiste habituellement en une déclaration telle que « Je suis Pierre Untel », tandis qu'un jeton consiste en un objet physique tel qu'un permis de conduire. Downes définit l'« identification » comme étant « l'acte de déclarer une identité, où une identité constitue un ensemble d'un ou de plusieurs signes qui signifient une entité distincte »[12].

La certification de l'identité n'est pas seulement une question de déclarer son identité. Elle porte aussi sur la déclaration d'une identité afin d'avoir accès à une

[12] Stephen Downes, "Authentication and Identification." International Journal of Instructional Technology and Distance Learning. Oct. 2005, p. 2.

ressource particulière[13]. L'idée de l'accès dans le processus de certification de l'identité est importante, puisqu'elle aide à préciser le contexte dans lequel la pièce d'identité est souvent présentée. Au sens large, la ressource pourrait être la capacité légale de conduire une voiture, d'avoir accès à l'argent d'un compte bancaire ou d'avoir la permission de pénétrer à l'intérieur d'une installation, d'un espace ou d'un pays en particulier.

Après la déclaration d'identité vient l'étape de l'authentification ou de la vérification de l'identité. On peut percevoir l'authentification comme étant [TRADUCTION] l'« acte de vérifier l'identité, où la vérification consiste à établir, à la satisfaction du vérificateur, que le signe représente l'entité »[14]. Trois catégories courantes d'authentification se basent sur « ce que l'un sait », « ce que l'un possède » et « qui l'on est ». « Ce que l'un sait » est habituellement un mot de passe ou la réponse à une question personnelle. « Ce que l'un possède » consiste en des documents ou objets physiques, par exemple une clé, un permis de conduire, un passeport ou une puce de données. « Qui l'on est » fait référence aux caractéristiques biométriques, qui peuvent être vérifiées manuellement en comparant la photographie sur un document d'identité à la personne qui présente le document, ou de façon électronique avec des systèmes qui comparent l'image numérisée d'une caractéristique à celles contenues dans une banque de données centralisée.

L'authentification de l'identité est principalement une question de confiance. Landahl argumente que l'authentification de l'identité nécessite de se poser la question suivante : [TRADUCTION] « Dans quelle mesure sommes-nous sûrs qu'une personne

[13] Doug Gale, "What's in a Name?" *T.H.E. Journal, 33* (11), Juin 2006, p. 22–24.
[14] Stephen Downes, "Authentication and Identification." International Journal of Instructional Technology and Distance Learning. Oct. 2005, p. 2–3.

est celle qu'elle prétend être[15]? » Cette certitude dépendra des procédures utilisées pour créer le document d'identité. Plus les gens sont persuadés qu'un jeton ne peut être contrefait, plus ils auront confiance en la vérification de la déclaration d'identité. On ne saurait trop insister sur l'importance de la place qu'occupe la confiance dans le processus de certification de l'identité; elle est cruciale.

L'information utilisée pour la certification de l'identité peut aussi être classée « non biométrique » ou « biométrique ». Les deux catégories fonctionnent de façon interdépendante dans les processus de certification de l'identité.

3.1 Identifiants non biométriques

Les identifiants non biométriques sont des caractéristiques qui ne sont pas universelles, distinctes, permanentes ou perceptibles[16]. L'exemple le plus commun est le nom d'une personne. À la question « Qui êtes-vous? », la plupart des gens répondront en mentionnant leur nom. Le nom constitue l'élément d'information principal qui se trouve sur la plupart des cartes d'identité. Parmi les autres identifiants non biométriques, mentionnons le lieu de naissance, la date de naissance, le genre ou le sexe, l'âge, le nom des parents, la situation du casier judiciaire, la citoyenneté ou les codes ou numéros d'identification. Un grand nombre des renseignements visibles sur les cartes d'identité sont des identifiants non biométriques.

À l'heure actuelle, il se fait très peu de certification de l'identité à l'aide d'un identifiant non biométrique unique. Puisqu'il est possible de reproduire un nom et que

[15] Mark Landahl, "Identity Crisis: Defining the problem and framing a solution for terrorism incident response." *Homeland Security Affairs, 3* (3) Sept 2007, p. 2–3.
[16] Il n'existe aucune définition standard de ce qu'est un renseignement non biométrique dans la documentation. La plupart du temps, on emploie l'expression « renseignement non biométrique » par opposition à « renseignement biométrique ». La définition mentionnée dans le présent document constitue une adaptation des définitions standard de ce qu'est un renseignement biométrique.

plusieurs personnes peuvent porter le même nom, on exige habituellement d'autres renseignements afin d'établir une identité unique. Le fait de glisser une carte de débit dans un guichet automatique (déclaration d'identité) et de saisir le numéro d'identification personnel (NIP), qui vérifie que le détenteur de la carte est bien le propriétaire de la carte et a le droit d'accéder aux ressources, explique bien l'exigence moderne d'une « authentification à deux facteurs »[17].

L'authentification à deux facteurs peut aussi inclure l'utilisation d'identifiants biométriques. Le niveau de confiance est plus élevé lorsqu'une caractéristique physique d'une personne est associée à une déclaration d'identité. Par exemple, une personne aura plus de difficulté à reproduire ou à forger les empreintes digitales ou le visage d'une autre personne que sa date de naissance ou son code postal.

3.2 Identifiants biométriques

Les caractéristiques biométriques sont des caractéristiques physiologiques ou comportementales dont on peut se servir pour authentifier une identité. Toute caractéristique peut constituer un renseignement biométrique utile, pourvu qu'elle soit (relativement)[18] universelle, (relativement) permanente, distincte et perceptible[19]. Les trois fonctions de la biométrie sont :

1. Vérification et authentification d'une identité;
2. Identification et confirmation (« cette personne se trouve-t-elle dans la base de données? »;

[17] Doug Gale, "What's in a Name?" *T.H.E. Journal, 33* (11), Juin 2006, p. 22–24.
[18] Anil K. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003, p. 26.
[19] Anil K. Jain et al., "An Introduction to Biometric Recognition." *IEEE Transaction on Circuits and Systems for Video Technology, 14* (1) Janv. 2004, p. 1–2.

3. Dépistage (« cette personne est-elle recherchée »[20]?

Les utilisations courantes et possibles de la biométrie sont variées, tel que le montre le tableau ci-dessous.

Tableau 1. Exemples de secteurs où l'on utilise des systèmes biométriques.

Haut niveau d'utilisation par le gouvernement	**Faible niveau d'utilisation par le gouvernement**	**Utilisation par le secteur privé**
Application de la loi Gestion des établissements de détention Organismes militaires et de sécurité nationale	Contrôle frontalier et vérifications en matière d'immigration Programmes d'admissibilité Émission de permis Carte d'identité nationale et inscription des électeurs	Services bancaires et financiers Contrôle d'accès — gestion du personnel Gestion du système d'information

Source : John D. Woodward Jr. « Biometrics: Identifying Law and Policy Concerns. » dans Anil K. Jain et al. eds. *Biometrics: Personal Identification in a Networked Society*. New York: Springer, 2006.

L'utilisateur doit adhérer au système biométrique en soumettant un échantillon de ses caractéristiques (empreintes digitales, photographie, etc.). Ces images sont ensuite converties en format numérique et saisies dans une base de données. Pour l'authentification de l'identité, les systèmes biométriques fonctionnent en mode un à un ou un à plusieurs.

Le mode un à un signifie que l'on associe une déclaration d'identité à un modèle. La plupart des applications commerciales de certification de l'identité dactyloscopique fonctionnent de cette manière. Les utilisateurs entrent d'abord leur échantillon dans le dispositif (par exemple un ordinateur portatif, une clé USB ou un téléphone cellulaire). Pour accéder au dispositif, les utilisateurs numérisent leurs empreintes digitales. On compare ensuite les empreintes digitales au modèle du système.

[20] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transaction on Information Forensics and Security, 1* (2) Juin 2006, p. 130.

Le mode un à plusieurs signifie que l'on compare la déclaration d'identité à une base de données plus grande. Par exemple, lorsque l'on procède à une lecture de visages dans une foule et qu'on les compare à des gens qui se trouvent sur une liste de surveillance ou une banque de données centralisée.

3.2.1 Reconnaissance du visage[21]

La géométrie faciale constitue l'une des principales méthodes pour reconnaître une personne. Dans sa plus simple expression, la géométrie faciale consiste à associer visuellement un visage à une photographie. Les méthodes ont évolué pour inclure les photographies numériques, les systèmes automatisés et les technologies de traitement biométrique. Le format de l'image saisie dépend du système. L'image peut être en deux ou trois dimensions, en couleur, en noir et blanc, infrarouge ou une combinaison de ces éléments[22]. Les deux approches les plus utilisées pour la reconnaissance automatique du visage se servent de l'emplacement et de la forme des attributs du visage – par exemple les yeux, les oreilles, les lèvres, et leurs relations spatiales – ou ont recours à une analyse globale du visage[23].

La biométrie du visage constitue une méthode non intrusive et familière de certification de l'identité et son usage est devenu répandu dans les efforts de surveillance. La reconnaissance du visage est utilisée par le vaste réseau de surveillance par télévision en circuit fermé de la Grande-Bretagne, ainsi qu'à l'occasion d'événements sportifs de

[21] L'Annexe A contient un tableau comparatif des propriétés générales des caractéristiques biométriques les plus fréquemment utilisées.
[22] John J. Weng et Daniel L. Swets, "Face Rocognition," In Anil K. Jain et al. eds., *Biometrics: Personal Identification in a Networked Society*, New York: Springer, 2006, p. 43–65.
[23] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." IEEE Transaction on Information Forensics and Security, 1 (2) Juin 2006, p. 126.

grande envergure, dans les aéroports et dans les foules. Dans certains États américains, la reconnaissance du visage est utilisée dans les casinos pour identifier les personnes à risque élevé ou bannies. L'entreprise américaine Mr. Payroll Corp a également commencé à recourir à la reconnaissance faciale pour son système d'encaissement des chèques[24].

Les gouvernements ont également accru leur utilisation de cette technologie. Par exemple, le programme de dispense de visa aux États-Unis exige maintenant un document d'identité sécuritaire contenant des données biométriques du visage[25]. Le Canada a commencé à se tourner vers des systèmes de reconnaissance du visage dans les documents produits par le fédéral et les permis de conduire améliorés délivrés à l'échelle provinciale. Des amendements faits en 2004 au *Décret sur les passeports canadiens*[26] ont permis à Passeport Canada de convertir l'information soumise en format biométrique numérique à intégrer dans le passeport, ainsi que de convertir la photographie d'un demandeur en un modèle biométrique aux fins de vérification de l'identité[27]. Lorsqu'il sera pleinement fonctionnel, le système se servira des renseignements biométriques pour effectuer « 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 »[28]. La Colombie-Britannique, l'Alberta, le Québec et l'Ontario ont commencé à mettre au point des permis de conduire munis de renseignements faciaux

[24] Alex Pentland et Tanzeem Choudhury, "Face Recognition for Smart Environments." *Computer, 33* (2) Fév. 2000, 50–55, p. 52.
[25] VISA Waiver Program, United States Department of State: http://travel.state.gov/visa/temp/without/without_1990.html.
[26] Décret sur les passeports canadiens (TR/81-86).
[27] *Décret modifiant le Décret sur les passeports canadiens*, C.P. 2004-951, 1er septembre 2004.
[28] Lalita Acharya, « La biométrie et son usage par l'État », Gouvernement du Canada : Service d'information et de recherche parlementaires, septembre 2006, p. 10–11.

biométriques afin de respecter les exigences du Canada et des États-Unis en matière de passage de la frontière[29].

3.2.2 Géométrie de la main

La géométrie de la main nécessite la prise de certaines mesures de la main d'un utilisateur. Ces mesures peuvent inclure la forme de la main, la taille de la paume, ainsi que la longueur et la largeur des doigts. La géométrie de la main n'est pas reconnue pour être distinctive[30]. En raison de cette limitation, elle ne convient que pour les associations de type un à un. Cependant, les systèmes qui se servent de la reconnaissance par géométrie de la main comportent plusieurs avantages, par exemple un coût modéré, un calcul rapide, la petite taille des modèles, la convivialité et le peu d'entretien[31].

La reconnaissance par géométrie de la main se base sur une photographie du dessus, du côté ou du talon de la main. La main est placée sur un détecteur, ce qui active une caméra et saisit l'image. L'image est traitée en prenant les mesures requises de la main, puis en transformant ces mesures en données biométriques.

La géométrie de la main sert actuellement dans divers contextes. Les résidences des universités et d'autres édifices s'en servent pour contrôler l'accès des étudiants. Les Jeux olympiques de 1996 ont également eu recours à la géométrie de la main pour contrôler l'accès au village olympique. Walt Disney World s'en est servi pour identifier

---

[29] Pour obtenir un calendrier des événements menant à la création dans les provinces de cartes d'identité améliorées et pour savoir quelles provinces ont commencé à les mettre en œuvre, consultez le site de l'Agence des services frontaliers du Canada à la page « Documents requis pour entrer aux États-Unis : Calendrier » 6 nov. 2008: http://www.cbsa-asfc.gc.ca/whti-ivho/chron-fra.html.

[30] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) Juin 2006, p. 126.

[31] Rand Sanchez-Reillo et Ana Gonzalex-Marcos, "Access Control System with Hand Geometry Verification and Smart Cards." *IEEE AES Systems Magazine*, Févr. 2000, p. 46.

les détenteurs réels d'abonnements. Ce système sert également en milieu de travail pour horodater la présence des employés et le nombre d'heures travaillées[32].

3.2.3 Prélèvement des empreintes digitales

Les empreintes digitales constituent une forme omniprésente de renseignement biométrique utilisée principalement aux fins d'application de la loi. Cependant, elles sont de plus en plus utilisées pour des applications commerciales qui emploient des systèmes d'identification, par exemple des ordinateurs portatifs, des postes de travail, des téléphones cellulaires et des clés USB.

La force des renseignements biométriques des empreintes digitales réside dans la conviction qu'il n'existe pas deux empreintes digitales identiques. Il est cependant possible de retrouver les mêmes empreintes digitales chez deux individus, même si les chances que cela se produise sont évaluées à environ 1 sur 64 milliards[33]. Le caractère unique des empreintes digitales peut être compromis lorsque le numériseur d'image ne saisit qu'une partie de l'information distinctive plutôt que l'empreinte en entier. Les systèmes biométriques modernes sont passés à des tailles d'empreintes plus petites afin de ménager l'espace de données, ce qui peut avoir des conséquences sur le caractère distinctif de l'empreinte ou sur les taux d'inscription[34]. Malgré tout, les empreintes digitales demeurent une caractéristique biométrique de qualité supérieure en raison de leurs caractéristiques uniques. On considère que les méthodes de certification de

[32] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) Juin 2006. p. 141.
[33] "Individual Biometrics." National Center for State Courts. 2002: http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html.
[34] Anil R. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003, p. 26.

l'identité qui se servent de la technologie biométrique des empreintes digitales sont rigoureuses en comparaison avec d'autres systèmes biométriques[35].

Les gouvernements utilisent largement le prélèvement d'empreintes digitales aux fins d'application de la loi. Par exemple, le programme US-VISIT recueille, conserve et échange de l'information comme les images numérisées des doigts pour faire une recherche sur les nouveaux venus dans les listes de surveillance. Le FBI conserve la plus importante base de données biométrique au monde (le système intégré et automatisé d'identification dactyloscopique), qui contient des données sur les empreintes digitales d'environ 47 millions de sujets[36].

L'application de la loi au Canada a également adopté un système automatisé d'identification dactyloscopique (SAID). Le Projet d'identification en temps réel de la GRC a pour but de moderniser son traitement des empreintes digitales. L'objectif est de s'éloigner des applications papier et manuelles pour passer à des systèmes qui font la promotion d'une « identification rapide des empreintes digitales » et de « la mise à jour immédiate des casiers judiciaires ». Le projet vise à faciliter l'échange de données avec d'autres partenaires à l'échelle nationale et internationale[37].

3.2.4 Reconnaissance de l'iris

L'iris est devenu une caractéristique biométrique de plus en plus utilisée en matière de certification de l'identité. L'iris contient des motifs distincts qui le rendent semblable à des empreintes digitales en ce sens que les motifs diffèrent énormément

[35] Pour des descriptions techniques détaillées, voir Anil K. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003.
[36] Lalita Acharya, « La biométrie et son usage par l'État ». Gouvernement du Canada, Service d'information et de recherche parlementaires, sept. 2006, p. 11–13.
[37] « Programme d'identification en temps réel ». Gendarmerie royale du Canada. http://www.rcmp-grc.gc.ca/rtid-itr/index-fra.htm.

d'une personne à l'autre. De plus, jusqu'à un tiers de l'iris pourrait être endommagé avant que son utilisation ne soit compromise[38].

Les motifs de l'iris sont saisis et transformés en données biométriques, ou « code représentant l'iris »[39]. La reconnaissance de l'iris sert d'identificateur de connexion sur certains ordinateurs ou réseaux dans des milieux hautement sécurisés. L'armée américaine s'en sert également en Irak et en Afghanistan pour filtrer les employés, contrôler l'accès aux sites et pour surveiller les détenus et les personnes soupçonnées d'être des terroristes[40].

3.2.5 Signature originale

La signature constitue une caractéristique biométrique comportementale. Les signatures peuvent varier grandement et sont difficiles à vérifier de façon automatique. Des systèmes de vérification saisissent l'image au cours du processus d'écriture ou après. Les stratégies utilisées pour saisir l'image au cours du processus d'écriture nécessitent l'enregistrement vidéo de l'utilisateur qui écrit avec un stylo sur une feuille de papier, ou le recours à un stylo électronique ou à un senseur conçu pour enregistrer la vélocité, l'accélération, la pression ou l'inclinaison du stylo. L'inspection manuelle demeure cependant plus fréquente[41].

---

[38] John Daugman, "How Iris Recognition Works." *IEEE Transactions on Circuits and Systems for Video Technology, 14* (1) Janv. 2004.
[39] Michael Negin et al., "An Iris Biometric System for Public and Personal Use." *Computer, 33* (2) Févr. 2000, p. 73.
[40] Dawn S. Onley. "Biometrics on the front line." *Government Computer News*. 16 avril 2008. http://www.gnc.com/print/23_23/26930-1.html?page=1.
[41] Voir S. Impedovo et G. Pirlo, "Verification of Handwritten Signature: An Overview." 14th International Conference on Image Analysis and Processing, 2007.

3.2.6 Autres méthodes biométriques[42]

Les systèmes biométriques audiovisuels fonctionnent en associant des images vidéo fixes du visage ou de certaines parties du visage ou des séquences vidéo du visage ou de la région de la bouche à une méthode de saisie de la voix. On a pu établir de fortes corrélations entre le mouvement du visage, la forme du tractus vocal et l'acoustique du langage. Les systèmes biométriques audiovisuels peuvent fonctionner dans des applications à faible sécurité et extrêmement conviviales, par exemple pour accéder à un poste informatique. Les systèmes biométriques basés sur l'audiovisuel fonctionnent bien dans divers scénarios, y compris ceux axés sur la sécurité[43].

L'ADN constitue une caractéristique hautement distinctive. Elle s'est révélée d'une grande utilité dans des applications légistes, par exemple l'identification parentale, mais est considérée comme extrêmement invasive et est souvent associée au processus de justice pénale. Il faudrait apporter des améliorations technologiques afin d'utiliser l'ADN à des fins de certification de l'identité, car une séquence d'ADN ne peut être saisie assez rapidement pour être viable d'un point de vue commercial[44].

3.3 Limitations des méthodes biométriques

En se basant sur l'examen précédent, on constate deux limitations importantes à l'utilisation d'identifiants biométriques. Une limitation se produit lorsqu'une méthode

[42] Il existe un nombre infini de caractéristiques biométriques qui font l'objet de recherches et qui sont mises en œuvre dans les nouvelles technologies. En voici certaines ne faisant pas partie de l'étude, mais susceptibles de faire leur apparition dans l'avenir : rétine, démarche, odeur, veine, caractéristique thermale et réflexe.
[43] Petar S. Aleksic et K. Katsaggelos Aggelos, "Audio-Visual Biometrics." Proceedings of the IEEE, 94 (11) Nov. 2006, p. 2026–2028.
[44] Voir Gary Roethenbauch, "Biometrics Explained." International Committee for Information Technology Standards, Sept. 2005.

devient inaccessible. La seconde limitation a trait aux décisions discrétionnaires prises au moyen d'une inspection manuelle.

3.3.1 Accessibilité

Du point de vue des droits de la personne, l'accessibilité fait référence à la notion qu'un utilisateur cible devrait pouvoir se servir de quelque chose – par exemple une empreinte digitale, un système biométrique d'empreintes digitales – sans faire face à des obstacles fondés sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial, la situation de famille, la déficience physique ou mentale ou l'état de personne graciée. Selon l'examen, la méthode de certification de l'identité pourrait ne pas être accessible pour différentes raisons.

Un système biométrique pourrait ne pas être accessible à l'inscription lorsque la technologie ne réussit pas à enregistrer une caractéristique physiologique ou comportementale parce qu'une personne ne dispose pas de l'identifiant biométrique requis. Par conséquent, un demandeur peut se voir refuser un document d'identité en raison de sa déficience (c.-à-d. doigts, mains ou iris manquants) si le document dépend uniquement d'une caractéristique biométrique particulière que la personne ne peut fournir.

Aussi, un système biométrique pourrait ne pas être accessible si l'utilisateur présente une caractéristique qui ne peut être lue par le système. Par exemple, des empreintes digitales peuvent devenir inadéquates, même pour des systèmes perfectionnés. En dépit de l'omniprésence des systèmes d'identification dactyloscopique, un faible pourcentage de la population ne peut y adhérer. Cette situation est causée par l'usure des crêtes ou par l'assèchement de la peau en raison de l'âge, de facteurs

génétiques, de conditions environnementales, de conditions de travail ou de dommages physiques au bout des doigts[45]. Les personnes qui souffrent de tremblements ou d'autres difficultés motrices peuvent aussi éprouver des problèmes à s'inscrire à ces systèmes. L'incapacité d'adhérer à ces systèmes tend à être plus grande chez les sujets de race noire comparativement aux sujets de race blanche et chez les femmes comparativement aux hommes[46].

Même si une personne peut être inscrite avec succès à un système donné, des systèmes biométriques peuvent demeurer inaccessibles dans la mesure où ils génèrent des résultats inexacts[47]. Par exemple, une étude réalisée au R.-U. sur la biométrie a relevé un taux d'exactitude plus élevé chez les sujets asiatiques en comparaison avec les sujets caucasiens lors du recours à des méthodes de reconnaissance du visage. Les taux d'exactitude étaient également meilleurs chez les personnes plus âgées et chez les hommes[48]. Certaines technologies, cependant, sont meilleures que d'autres en vertu du type de caractéristiques échantillonnées. Les taux d'exactitude pour des technologies telles que la reconnaissance de l'iris sont très élevés[49].

3.3.2 Décisions discrétionnaires fondées sur une inspection manuelle

La seconde limitation se produit lorsque l'identité d'une personne fait l'objet d'une inspection manuelle. Comme mentionné précédemment, une inspection manuelle se fait souvent dans le cas de signatures originales. Bien qu'une inspection manuelle

---

[45] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) Juin 2006, p. 126.
[46] UK Passport Service. "UKPS Biometrics enrollment trial report." Mai 2005.
[47] Les taux d'exactitude font référence à la fréquence des faux positifs et des faux négatifs. Un faux négatif se produit lorsqu'un système ne réussit pas à identifier quelqu'un comme étant celui qu'il prétend être. Un faux positif se produit lorsqu'un système identifie une personne comme étant quelqu'un d'autre.
[48] UK Passport Service. "UKPS Biometrics enrollment trial report." Mai 2005.
[49] John Daugman, "How Iris Recognition Works." *IEEE Transactions on Circuits and Systems for Video Technology, 14* (1) Janv. 2004.

pourrait être plus exacte que certaines technologies biométriques, la possibilité existe que l'identité d'une personne puisse être évaluée sur la base de prédispositions individuelles ou de préjugés, ce qui pourrait mener au profilage racial ou à d'autres formes de profilage discriminatoire[50].

3.3.3 Façons d'atténuer les limitations de la biométrie

La vérification et la collecte de données constituent deux techniques que l'on peut utiliser pour évaluer et relever les effets discriminatoires négatifs possibles engendrés par une technologie donnée sur un groupe de personnes et y remédier. Par exemple, la taille de l'image des empreintes digitales utilisée dans un système automatisé d'identification dactyloscopique (SAID) peut avoir des répercussions sur les taux d'inscription – plus la taille de l'image est petite, plus le nombre d'utilisateurs qui seront dans l'incapacité de faire partie du système en raison des propriétés de l'extrémité de leurs doigts sera élevé. C'est ce qui s'est produit avec la carte d'identité nationale en Grande-Bretagne. Le système a éprouvé de la difficulté à inscrire les personnes âgées de plus de 75 ans. On a émis l'hypothèse qu'il serait possible d'obtenir des empreintes de meilleure qualité en augmentant la taille de l'image[51]. Faire l'essai de la technologie sur un échantillon représentatif d'utilisateurs cibles pour vérifier si un groupe particulier de personnes est exclu, puis parfaire la technologie en fonction des résultats peut favoriser une participation et une précision accrues.

---

[50] Position commune de la Commission canadienne des droits de la personne et de la Fondation canadienne des relations sociales sur l'importance de la collecte de données pour contrer le profilage. http://www.chrc-ccdp.ca/research_program_recherche/profiling_profilage/page9-fra.aspx

[51] Ian Drury, "ID cards could be derailed by pensioners as finger prints of over-75s are hard to scan." *The Daily Mail*, Aug. 15, 2008: http://www.dailymail.co.uk/news/article-1045659/ID-cards-derailed-pensioners-finger-prints-75s-hard-scan.html.

La collecte de données n'est pas seulement importante au cours de la phase de vérification d'une technologie donnée. Elle l'est également au cours de sa mise en place, particulièrement si l'on a recours à des inspections ou vérifications manuelles. Le type de données recueillies doit inclure des données fondées sur les droits de la personne[52], le cas échéant. Ces données incluent de l'information sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, la déficience physique ou mentale ou l'état de personne graciée le cas échéant. Lorsqu'un agent prend une décision discrétionnaire au moment de vérifier l'identité d'une personne, l'enregistrement des données fondées sur les droits de la personne et le type de décision rendue peuvent permettre de déceler si un parti pris ou des préjugés entrent en ligne de compte dans le processus de décision.

4. L'utilisation de méthodes non biométriques et biométriques dans les documents d'identité

Les sociétés modernes exigent que les citoyens conservent des documents d'identité pour de nombreuses raisons. La diversité des types et buts de ces documents a encouragé les chercheurs à les classer en deux principales catégories : « documents d'appui » et « documents d'identité secondaires »[53]. Les « documents d'appui » font référence aux documents d'identité qui confirment la naissance, par exemple les actes de naissance, de baptême et d'adoption. Les « documents d'identité secondaires » font référence aux documents requis à des fins particulières de certification de l'identité, par

[52] Pour de plus amples renseignements, veuillez consulter la *Position commune de la Commission canadienne des droits de la personne et de la Fondation canadienne des relations sociales sur l'importance de la collecte de données pour contrer le profilage.*
http://www.chrc-ccdp.ca/research_program_recherche/profiling_profilage/page9-fra.aspx
[53] Voir Alane Kochems et Laura Keith. "Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft." *Heritage Foundation Backgrounder*. No. 1946, 27 juin 2006.

exemple un passeport, un visa, un permis de conduire et une carte de citoyenneté. Les documents d'appui sont nécessaires pour obtenir tout document d'identité secondaire ayant trait à la certification de l'identité.

La façon actuelle de délivrer des documents d'identité secondaires constitue une faiblesse, puisque l'on considère les documents d'appui comme les principaux documents d'identité. Cependant, une personne n'aurait qu'à se procurer des documents d'appui frauduleux pour obtenir de façon frauduleuse des documents d'identité secondaires. Afin de parer cette faiblesse, on a recours aux systèmes biométriques pour renforcer les documents d'identité secondaires en ajoutant une autre couche distinctive au document d'identité[54].

La certification de l'identité dépend du caractère unique de l'information fournie. On se sert des dates de naissance pour distinguer deux personnes portant le même nom. L'introduction des photographies sur les documents d'identité constitue l'un des premiers exemples de l'utilisation d'une caractéristique biométrique visant à solidifier le lien entre le jeton et la déclaration d'identité. L'ajout d'autres caractéristiques biométriques aux documents d'identité augmente la confiance nécessaire pour que les documents secondaires soient considérés comme des jetons valides.

De nombreux documents émis par le gouvernement et qui permettent aux Canadiens ou aux personnes résidant au Canada de voyager exigent divers identifiants non biométriques et biométriques. L'examen qui suit du passeport, de la carte de résident

[54] Anil K. Jain, Arun Ross, et Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) Juin 2006, p. 140.

permanent du Canada, de CANPASS Air et de NEXUS explique la façon dont on se sert des méthodes de certification de l'identité.

4.1 Passeport, carte de résident permanent du Canada, CANPASS Air et NEXUS

« Le passeport est devenu l'indicateur clé de l'identité et une exigence élémentaire pour la pleine participation au marché mondial[55]. » En vertu du *Décret sur les passeports*, Passeport Canada a le pouvoir d'accorder ou de refuser la délivrance d'un passeport. Il peut refuser de délivrer un passeport si la personne a fourni de faux renseignements au cours du processus de demande de passeport, a été accusée d'un crime grave, est actuellement incarcérée, est frappée d'une interdiction de quitter le Canada, est frappée d'une interdiction de posséder un passeport ou a été condamnée pour une infraction en lien avec le passeport au Canada ou à l'étranger. Il peut révoquer le passeport d'une personne si celle-ci s'en sert pour commettre un délit grave au Canada ou à l'étranger, permet à une autre personne d'utiliser son passeport ou a obtenu son passeport au moyen de renseignements faux ou trompeurs[56].

La principale exigence pour obtenir un passeport canadien est d'avoir la citoyenneté canadienne (c.-à-d. un ancien passeport, un acte de naissance ou un certificat de citoyenneté). Les autres exigences incluent des documents pour prouver l'identité du demandeur. Il peut s'agir d'un permis de conduire, d'une carte d'assurance maladie, d'un certificat de statut d'indien ou de tout autre document d'identification ou carte d'employé

[55] « Document d'information : Refus ou révocation de passeports. » Passeport Canada: http://www.ppt.gc.ca/articles/20080213a.aspx?lang=fra.
[56] « Document d'information : Refus ou révocation de passeports. » Passeport Canada: http://www.ppt.gc.ca/articles/20080213a.aspx?lang=fra.

à l'échelle municipale, provinciale ou fédérale, d'un ancien passeport, d'une carte de résident permanent des États-Unis ou d'une carte de sécurité de la vieillesse.

La carte de résident permanent du Canada est un document d'identité qui atteste du statut officiel d'une personne à son arrivée au Canada et qui lui donne accès à certains services et programmes gouvernementaux[57]. On a instauré ces cartes en 2002 dans la foulée du *Plan d'action pour la création d'une frontière sûre et intelligente*. Tous les nouveaux résidents permanents reçoivent immédiatement une carte, et les résidents permanents déjà établis doivent en faire la demande. Pour être admissibles, les demandeurs doivent être résidents permanents du Canada et se trouver physiquement au Canada. Les requérants ne peuvent faire l'objet d'une mesure de renvoi exécutoire ou être accusés d'une infraction en lien avec une utilisation abusive d'une carte de résident permanent.

CANPASS est un programme géré uniquement au Canada. Le programme CANPASS Air[58] permet aux utilisateurs préautorisés et à faible risque de retourner au Canada plus rapidement en contournant les douanes et les contrôles d'immigration aux postes frontaliers canadiens des aéroports, terrestres et maritimes[59]. Le programme a été lancé en 2003 et s'étend maintenant à la plupart des grands aéroports du pays. Le contrôle de sécurité comprend une vérification du casier judiciaire, du dossier aux douanes et du statut d'immigration du demandeur afin d'établir son niveau de risque. On procède à ces vérifications chaque année.

---

[57] « Carte de résident permanent. » Citoyenneté et Immigration Canada : http://www.cic.gc.ca/francais/information/carte-rp/index.asp

[58] Les programmes CANPASS Autoroutes, CANPASS Aéronefs d'entreprise, CANPASS Aéronefs privés et CANPASS Bateaux privés. CANPASS Air est le plus complexe et progressif de ces programmes et servira par conséquent d'exemple pour la discussion.

[59] CANPASS — Air. Agence des services frontaliers du Canada : http://cbsa-asfc.gc.ca/prog/canpass/canpassair-fra.html.

Instauré en 2004, NEXUS est un programme conjoint canado-américain actuellement en vigueur dans certains aéroports canadiens et américains. L'objectif du programme est de faciliter le traitement rapide des voyageurs à faible risque qui traversent la frontière. Ce processus comprend la collecte et la conservation de données sur les voyageurs avant qu'ils ne traversent la frontière. La carte NEXUS représente la pièce d'identité la plus rigoureuse au Canada pour traverser la frontière. Pour être admissible, il faut :

- Être citoyen ou résident permanent du Canada ou des États-Unis;
- Être admissible au Canada ou aux États-Unis en vertu des lois d'immigration;
- Fournir des renseignements véridiques et exacts;
- Satisfaire à toutes les autres exigences du programme NEXUS (formulaire de demande, vérification de sécurité);
- N'avoir aucune infraction documentée des dispositions législatives en matière de douanes, d'immigration ou d'agriculture.

Une personne n'est pas admissible si elle a été reconnue coupable d'une infraction criminelle grave, dans un pays quelconque, pour laquelle elle n'a pas été graciée[60].

Le passeport, le programme CANPASS Air et le programme NEXUS constituent des systèmes volontaires. Les Canadiens ne sont pas tenus de se procurer l'un de ces documents. Cependant, pour voyager, les Canadiens doivent détenir au moins un de ces documents pour quitter le pays et y revenir. La carte de résident permanent du Canada ne constitue pas un système volontaire. Comme mentionné, tous les nouveaux résidents permanents recevront une carte. Les résidents permanents déjà établis ne sont pas tenus

[60] « Adhérez à NEXUS. » Agence des services frontaliers du Canada, 11 janvier 2008. http://www.cbsa-asfc.gc.ca/prog/nexus/elig-admis-fra.html.

de se procurer la carte, mais celle-ci peut être exigée pour accéder à certains services au Canada et pour voyager à l'étranger.

4.2 Exigences des identifiants non biométriques

Le passeport, la carte de résident permanent du Canada, CANPASS Air et NEXUS exigent tous des formes semblables de renseignements non biométriques. Le Tableau 2 décrit les renseignements nécessaires pour l'obtention de chaque document. Les principaux sont le nom, la date de naissance, le sexe ou genre et l'adresse. Toutes les demandes nécessitent que le requérant fournisse un historique d'emploi et de résidence. Selon le document, l'historique demandé peut varier de deux à cinq ans. Un demandeur a la possibilité de ne pas faire apparaître le lieu de naissance sur le document, mais il doit quand même fournir l'information sur le formulaire de demande.

Tableau 2. Renseignements non biométriques exigés pour être admissible à l'obtention d'un passeport, d'une carte de résident permanent du Canada, d'une carte CANPASS Air et d'une carte NEXUS.

Renseignements non biométriques	Passeport	Carte de résident permanent du Canada	CANPASS Air	NEXUS
Prénom, second prénom, nom	X	X	X	X
Date de naissance	X	X	X	X
État matrimonial	X	X		
Lieu de naissance	X (possibilité de retirer cette information du passeport)			
Sexe ou genre	X	X	X	X
Couleur des yeux	X	X		
Couleur des cheveux	X			
Taille	X	X		

Poids	X			
Numéro de téléphone	X	X		
Déclaration du répondant	X			
Adresse	X	X	X	X
Adresse des deux dernières années	X			
Adresse des cinq dernières années		X	X	X
Historique d'emploi des deux dernières années	X			
Historique d'emploi des cinq dernières années		X	X	X
Historique d'éducation des cinq dernières années		X		
Références	X			
Personne à contacter en cas d'urgence	X			
Nombre d'années de mariage si l'on demande le nom de l'époux	X			
Avez-vous voyagé ou résidé à l'extérieur du Canada au cours des cinq dernières années?		X		
Citoyenneté canadienne	X		X	X

Autre		Date à laquelle vous êtes devenu résident permanent		Êtes-vous membre d'autres programmes de passage de la frontière?

4.3 Exigences pour l'utilisation d'identifiants biométriques

Une photographie du visage est obligatoire pour le passeport, la carte de résident permanent du Canada, la carte CANPASS Air et la carte NEXUS. CANPASS Air et NEXUS exigent également une lecture de l'iris comme principale caractéristique biométrique. La proposition visant à créer la carte de résident permanent du Canada dans le *Plan d'action* incluait le recours à la biométrie; cependant, cette mesure n'avait pas encore été mise en œuvre au moment de rédiger le présent document[61]. Des exigences standard existent pour les photographies : expression neutre, arrière-plan pâle et aucun élément ne venant obstruer le visage. Ces exigences permettent d'utiliser la photo dans des techniques de reconnaissance du visage fondées sur la biométrie.

Tableau 3. Renseignements biométriques exigés pour l'obtention d'un passeport, d'une carte de résident permanent du Canada, et pour adhérer aux programmes CANPASS Air et NEXUS.

Renseignements biométriques	Passeport	Carte de résident permanent du Canada	CANPASS Air	NEXUS
Signature	X	X	X	X
Photographie	X	X	X	X
Empreintes digitales				X
Iris			X	X

[61] Un projet pilote a été entrepris pour évaluer l'efficacité du système, en ce qu'il a trait aux voyageurs non citoyens. Une des caractéristiques du projet est le recours à une photographie et aux empreintes digitales pour certifier l'identité, et jusqu'à présent les résultats sont positifs. À l'heure actuelle, les empreintes digitales ne constituent pas une exigence pour obtenir la carte de résident permanent du Canada et ne sont donc pas mentionnées dans le tableau. « Foire aux questions : Mise à l'essai de la biométrie sur le terrain. » Citoyenneté et Immigration Canada, 12 juin 2008 : http://www.cic.gc.ca/francais/information/faq/biometrie/index.asp.

4.4 Problèmes de droits de la personne portés devant les tribunaux à la suite de l'utilisation d'identifiants non biométriques

Jusqu'à présent, aucun problème de droits de la personne n'a été porté devant les tribunaux à la suite de l'utilisation de systèmes non biométriques d'identification. Le cas le plus pertinent est celui de l'affaire *Veffer c. Canada*[62]. M. Veffer avait inscrit « Jérusalem, Israël » comme lieu de naissance sur sa demande de passeport. Passeport Canada a pour politique d'inscrire « Jérusalem » comme une ville apatride, comme reconnu par les Nations Unies, et l'a inscrit de cette façon sur son passeport. M. Veffer a ensuite intenté une poursuite contre Passeport Canada, arguant que l'on portait atteinte à son droit à l'égalité et à sa liberté de religion en vertu de la *Charte*. La Cour d'appel fédérale a rejeté ses arguments, en concluant qu'il avait la possibilité de ne rien indiquer dans ce champ sur son passeport, en vertu de la politique d'exception de Passeport Canada, ou d'inscrire « Jérusalem ». Par conséquent, Passeport Canada ne contrevenait pas à ses droits de manière déraisonnable en raison des choix qui s'offraient à lui. Passeport Canada informe les demandeurs que certains pays pourraient refuser un passeport si le lieu de naissance n'y est pas mentionné de façon lisible et les invite à tenir compte de ce fait lorsqu'ils présentent une demande pour laisser ce champ vide sur un passeport.

4.5 Problèmes de droits de la personne portés devant les tribunaux à la suite de l'utilisation d'identifiants non biométriques

Les exigences de reconnaissance du visage aux fins d'obtention d'un permis de conduire provincial ont été contestées pour raisons religieuses, particulièrement lorsqu'il

[62] *Veffer c. Canada (Ministre des Affaires étrangères)*, 2007 CAF 247. Autorisation d'appel rejetée par la Cour suprême du Canada, 2007 WL 4926336 (C.S.C.), [2007] A.C.S.C. no 457 457.

s'agit de l'utilisation d'une photographie. Dans l'affaire *Bothwell v. Ontario*[63], M. Bothwell s'est opposé à ce que sa photographie soit prise et entreposée dans une base de données informatisée. Il a présenté la demande d'exemption pour motifs religieux offerte par la province, exemption qui lui a été refusée. M. Bothwell a ensuite poursuivi le gouvernement de l'Ontario pour discrimination fondée sur ses convictions religieuses. Le tribunal a jugé que les objections de M. Bothwell n'étaient pas sincèrement fondées sur des convictions religieuses et s'est prononcé en faveur du gouvernement. Le tribunal ne s'est pas prononcé sur la question de savoir si l'exigence enfreignait sa liberté religieuse.

Dans l'affaire *Hutterian Brethren v. Alberta*[64], les tribunaux ont examiné l'exigence de photographie en regard des convictions religieuses huttérites. Les Huttérites s'opposaient à se faire photographier, en toute circonstance. Ils se prévalaient d'une exemption prévue dans la *TSA*, loi albertaine sur la sécurité routière (*Traffic and Safety Act*[65]), qui permet aux demandeurs d'obtenir un permis de conduire sans photographie en opposant une conviction religieuse sincère. Il existait quelque 450 de ces permis assortis de la « condition G », dont 56 % étaient détenus par des membres de la Hutterian Brethren. En 2003, lorsque la loi a été mise à jour, l'exemption a été éliminée, l'Alberta souhaitant mettre au point un « permis de conduire amélioré » et une base de données incorporant une lecture biométrique du visage. La province offrait alors deux solutions de rechange pour le nouveau permis de conduire régulier, mais dans les deux cas il fallait se faire photographier. La Hutterian Brethren a proposé une autre solution : on ne prendrait

[63] *Bothwell v. Ontario (Minister of Transportation).* [2005] O.J. No. 189.
[64] *Hutterian Brethren of Wilson Colony v. Alberta.* 2007 ABC 160, 49 M.V.R. (5th) 45. Demande d'autorisation d'appel devant la Cour suprême du Canada accordée, 2007 WL 4227549 (S.C.C.)
[65] *Traffic Safety Act*, R.S.A. 2000, c. T-6 (*TSA*)

pas de photographie et les permis de conduire sans photo seraient assortis de la mention « à ne pas utiliser aux fins d'identification ».

Le juge de première instance et la Cour d'appel ont conclu qu'en supprimant l'exemption utilisée par la Hutterian Brethren depuis trente ans sans offrir quelque solution de rechange que ce soit, la province avait déraisonnablement enfreint la liberté de religion garantie par la *Charte*. Les juges d'appel ont conclu majoritairement que la *TSA* provinciale se préoccupait principalement de la sécurité routière et de l'émission de permis, et ne pouvait par conséquent se prétendre investie d'un mandat ciblé de sécurité nationale ou de contrôle frontalier. Le jugement majoritaire déclarait que : « Dans certaines circonstances, un gouvernement peut chercher à harmoniser ses normes de sécurité avec celles d'une autre région et ce désir peut revêtir une importance suffisante pour justifier d'enfreindre un droit protégé par la *Charte*[66]. » [TRADUCTION] Le juge dissident a critiqué l'interprétation de la *TSA*, la qualifiant de trop étroite. Le jugement dissident affirmait que la *TSA* devait nécessairement incorporer des préoccupations de sécurité nationale et internationale, puisque les permis de conduire servent effectivement de documentation pour permettre à leurs détenteurs de franchir les frontières[67].

L'affaire a été portée devant la Cour suprême du Canada, qui s'est penchée sur la question de savoir si l'exigence obligatoire de photographie enfreignait la liberté de religion et si une telle violation pouvait se justifier en vertu de l'article premier de la *Charte*. Le jugement majoritaire, rendu en faveur de la province, a statué que les efforts de l'Alberta pour faire du permis de conduire un document plus sécuritaire l'emportaient

[66] *Hutterian Brethren of Wilson Colony v. Alberta*. 2007 ABC 160, 49 M.V.R. (5th) 45, au paragr. 31.
[67] Voir en particulier les paragraphes 88–97.

sur la liberté religieuse de la colonie huttérite. Résumant les paragraphes 39, 42 et 45, le tribunal a déclaré que :

> Les règlements sont des mesures prescrites par une règle de droit pour l'application de l'article premier et l'objectif du règlement contesté de préserver l'intégrité du système de délivrance des permis de conduire d'une façon qui réduit au minimum le risque de vol d'identité est manifestement un objectif urgent et réel susceptible de justifier des restrictions aux droits. La photo obligatoire universelle permet au système de garantir que chaque permis correspond à une seule personne et que personne ne détient plus d'un permis. La province avait le droit de prendre un règlement concernant non seulement la question principale de la sécurité routière, mais aussi les problèmes connexes associés au système de délivrance des permis[68].

Une autre affaire mettant en cause un système biométrique fondé sur la géométrie de la main a été portée devant un tribunal ontarien du travail contre la société 407 ETR Concession[69]. Afin de contrôler l'accès des employés à divers édifices, l'employeur avait entrepris l'installation généralisée dans les lieux de travail d'un système biométrique par lecture de la main droite, qui s'ajoutait à un système d'horloge pour contrôler l'assiduité et les heures travaillées. Plusieurs employés appartenant à l'Église pentecôtiste avaient présenté le premier grief mais la plupart d'entre eux avaient abandonné la démarche, l'employeur leur ayant proposé d'utiliser la main gauche plutôt que la main droite. Néanmoins, trois employés s'opposaient encore à la technologie[70]. L'arbitre avait conclu que « le lecteur biométrique exerce de la discrimination à l'endroit des plaignants sur la base de leurs convictions religieuses »[71] et que l'employeur n'avait pas offert à ces trois employés un accommodement en deçà d'une contrainte excessive. Le syndicat et les

[68] *Alberta c. Hutterian Brethren of Wilson Colony*, 2009 SCC 37
[69] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1.
[70] Pentecostal faith permits a large range of individual discretion so the beliefs of one Pentecostal may not entirely reflect the beliefs of another. Thus, the court found that their beliefs were sincere, even though they differed from their co-workers. Because of this, the Board found "creed" to be a much more appropriate ground than "religion." *407 ETR Concession Co. V. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. paragr. 120.
[71] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. paragr. 179.

plaignants proposaient une autre solution, soit un système de carte magnétique et de mot de passe, mais l'employeur a tout simplement mis à pied les employés[72]. En retour, l'arbitre a offert d'autres choix, mais a laissé en fin de compte le syndicat et l'employeur régler leur différend[73].

5. L'effet de la biométrie sur les droits de la personne : deux principes clés

Deux principes clés en matière de droits de la personne émergent de l'étude. Le premier, c'est que les fournisseurs de services[74] ont le devoir d'offrir des mesures d'accommodement aux groupes protégés en vertu de la LCDP, sauf si cela impose une contrainte excessive aux fournisseurs en question. Le second, c'est que les fournisseurs de services peuvent implanter une mesure excluant les membres d'un groupe protégé si cette exclusion se justifie.

5.1 Obligation de prendre des mesures d'adaptation

La Cour suprême du Canada a indiqué que les principes applicables en matière de droits de la personne reconnaissent « que les obstacles ne peuvent pas tous être éliminés »[75], mais que néanmoins, les employeurs aussi bien que les fournisseurs de services ont le devoir d'empêcher la création de nouveaux obstacles. Il faut concevoir les mesures de manière à favoriser le plus possible l'intégration sans exercer contre des personnes une discrimination fondée sur un motif de distinction illicite. On ne devrait recourir à des mesures d'accommodement spéciales que dans les situations imprévues[76].

---

[72] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. paragr. 179.
[73] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. paragr. 181.
[74] L'obligation de prendre des mesures d'adaptation s'applique aux fournisseurs de services et aux employeurs.
[75] *Conseil des Canadiens avec déficiences c. VIA Rail Canada Inc.*, 2007 CSC 15, [2007] 1 R.C.S. 650, paragr. 186.
[76] *Conseil des Canadiens avec déficiences c. VIA Rail Canada Inc.*, 2007 CSC 15, [2007] 1 R.C.S. 650, paragr. 175.

Ainsi, dans la création de documents d'identité fondés sur la biométrie, la technologie devrait être mise au point de façon à permettre la participation du plus grand nombre possible de personnes. Lorsqu'il existe des limites technologiques, il faut envisager d'autres moyens et(ou) des moyens supplémentaires de mesurer les paramètres.

Les systèmes multimodaux sont intrinsèquement paramétrés de façon à tenir compte des personnes chez qui une certaine caractéristique est absente ou qui possèdent une caractéristique non lisible dès l'abord. Pour les applications de sécurité névralgiques, on recommande des systèmes multimodaux qui vérifient par recoupements plus d'une caractéristique[77]. Le gouvernement américain, par exemple, utilise un système multimodal pour les employés fédéraux : « Pour chaque employé fédéral ou entrepreneur inscrit, la carte de vérification de l'identité personnelle enregistre à la fois les empreintes digitales et la biométrie résultant d'un balayage du visage, mais elle utilise principalement la biométrie des empreintes digitales. On a recours à la lecture numérique du visage lorsqu'il est impossible pour un employé fédéral ou un entrepreneur de fournir des empreintes digitales ou en présence d'anomalie[78]. »

Les systèmes multimodaux peuvent aussi servir à accommoder une personne qui soulèverait une objection précise. Dans le cas du grief contre la société *407 ETR Concession*, par exemple, l'arbitre a proposé à l'employeur d'utiliser une approche multimodale en offrant non seulement une biométrie de la géométrie de la main mais aussi un système de carte magnétique et mot de passe.

---

[77] Anil K. Jain et al., *Handbook of Fingerprint Recognition*, New York: Springer, 2003, p. 37.
[78] Babita Gupta, "Biometrics: Enhancing Security in Organizations." IBM Center for the Business of Government, 2008, p. 27.

Une autre façon d'intégrer un accommodement consiste à mettre en place des politiques et(ou) des pratiques permettant un nombre limité d'exceptions. L'exemple suivant, bien qu'il n'ait pas été examiné dans la première moitié du rapport, montre comment une politique peut tenir compte des observances religieuses sans miner l'efficacité de la technologie.

En 2007, trois enfants sikhs se sont vu refuser un passeport à cause de leurs photos. Sur leurs photos, ils portaient tous le couvre-chef prescrit par leur religion. Aucun de ces couvre-chefs ne cachait leur visage, conformément à la politique de Passeport Canada selon laquelle « dans la mesure où l'on peut clairement voir les traits du visage du demandeur et que la demande est présentée par écrit », les couvre-chefs sont permis. L'affaire a retenu l'attention de la presse, après quoi Passeport Canada a délivré les passeports et a présenté des excuses aux enfants et à leurs parents. Selon Passeport Canada, le refus avait été opposé par erreur, et les agents en cause ont reçu la formation voulue pour éviter à l'avenir des erreurs semblables d'interprétation de la politique[79]. Dans cet exemple, on avait déjà mis en place une politique visant à accommoder la pratique religieuse et permettant l'accès à un passeport sans violation des droits de la personne, sans nuire à l'efficacité de la technologie biométrique.

5.2 Motif justifiable

Les tribunaux ont reconnu qu'en certaines occasions, les accommodements peuvent se révéler impossibles. Dans de telles circonstances, l'organisation doit fournir un motif justifiable appuyé par des preuves.

[79] « Passport Canada says Sikh photos rejected by mistake. » CBC News. 17 août 2007 : http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-passportcanada.html

Un exemple frappant est celui de l'affaire des membres d'une colonie huttérite, la Hutterian Brethren, dans laquelle la Cour suprême du Canada a reconnu que des objectifs urgents et réels, s'ils sont démontrés, peuvent limiter l'exercice de certains droits. Même si le tribunal a invoqué dans sa décision une analyse fondée sur l'article premier de la *Charte*, le concept est semblable dans le cas des lois régissant les droits de la personne. On peut invoquer un motif justifiable en vertu de ces lois lorsqu'une organisation est en mesure de démontrer que la mesure en cause a été conçue en fonction d'un objectif précis et légitime, qu'il existe un lien avéré entre la mesure et l'objectif, que la mesure est raisonnablement nécessaire pour atteindre l'objectif, et que la mesure prévoit des solutions de rechange pour les personnes qui auraient besoin d'un accommodement, sans que celui-ci n'impose à l'organisation une contrainte excessive.

6. Conclusion

Le présent rapport visait à examiner les répercussions éventuelles sur les droits de la personne des diverses méthodes de vérification de l'identité au moyen de documents tels que le passeport et NEXUS. Pour assurer la protection des droits de la personne, il faut notamment prévoir les domaines exposés à des risques de traitement différentiel et agir de façon à offrir de la flexibilité, dans la mesure du possible, afin de dégager la solution qui aura l'effet le moins négatif sur les groupes protégés en vertu de la LCDP.

Un examen des méthodes de vérification de l'identité a démontré l'existence de certaines limites susceptibles d'affecter les droits d'une personne en lui imposant un traitement différentiel défavorable. Selon le mode de développement de la technologie, la méthode pourrait être inaccessible à une personne ou à un groupe de personnes. Une façon d'atténuer de telles difficultés consisterait à faire l'essai de la technologie auprès

d'un échantillon représentatif des utilisateurs visés. Il faudrait assurer une surveillance continue. Si la méthode comporte une inspection manuelle, il faudra aussi recueillir des données sur les droits de la personne, afin d'aider à repérer toute partialité systémique.

L'étude a aussi démontré que l'on peut parfois remédier aux problèmes d'accessibilité posés par des systèmes unimodaux au moyen de mesures d'accommodement. Comme on l'a vu dans l'affaire *407 ETR*, on a permis aux employés visés d'utiliser leur main gauche au lieu de leur main droite pour prendre la lecture biométrique de la géométrie de la main. Toutefois, les systèmes unimodaux peuvent aussi créer et aggraver les obstacles existants. Les systèmes d'empreintes digitales, par exemple, peuvent être inaccessibles pour les personnes d'un certain âge, d'une certaine profession ou d'une certaine condition physique. L'âge, les conditions de travail et certaines formes d'invalidité sont trois facteurs qui peuvent réduire la qualité de l'image des empreintes digitales au point de la rendre inutilisable. C'est pourquoi il est recommandé d'utiliser des systèmes multimodaux, particulièrement en contexte de sécurité.

Les systèmes biométriques multimodaux offrent une marge d'accommodement et sont préconisés comme solution aux limites des systèmes unimodaux. On en a vu un exemple avec le système de carte d'employé du gouvernement américain, une forme de système multimodal ayant recours à deux caractéristiques singulières et comparables : lorsqu'il est impossible de lire les empreintes digitales du demandeur, on utilise une imagerie du visage. Non seulement les systèmes multimodaux ont-ils la capacité de contribuer à la protection des droits de la personne, mais ils permettent aussi de créer des systèmes de sécurité plus solides et plus fiables.

Des situations pourront survenir où il faudra accorder une exemption à certains utilisateurs. Il faut donc prévoir, dans la création de toute mesure, des politiques et des pratiques permettant d'accommoder ces personnes, sans que ces accommodements n'imposent à l'organisation une contrainte excessive. La politique de Passeport Canada au sujet des couvre-chefs religieux constitue un exemple. S'il n'existe aucune alternative raisonnable à une mesure biométrique particulière, il revient à l'organisation qui utilise la biométrie de démontrer que des mesures suffisantes ont été prises pour explorer d'autres moyens moins discriminatoires d'arriver aux mêmes résultats sans imposer à l'organisation une contrainte excessive.

La *Charte* et la *Loi canadienne sur les droits de la personne* reconnaissent toutes deux des limites à l'exercice des droits individuels. L'affaire de la Hutterian Brethren illustre une situation où les droits d'un individu ont été limités par des objectifs d'intérêt public urgents et réels. Il incombe à l'organisation qui a recours à une mesure particulière de démontrer que le système a été conçu conformément aux principes des droits de la personne.

ANNEXE A

Tableau 1. Comparaison de diverses technologies biométriques
(E = Élevé, M = Modéré, F = Faible)

Identifiant biométrique	Caractère universel	Caractère distinctif	Permanence	Perceptibilité	Performance	Acceptabilité	Contournement
ADN	E	E	E	F	E	F	F
Oreille	M	M	E	M	M	E	M
Visage	E	F	M	H	F	E	E
Empreintes digitales	M	E	E	M	E	M	M
Géométrie de la main	M	M	M	E	M	M	M
Iris	E	E	E	M	E	F	F
Empreinte de la paume	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E

Source : Anil K. Jain et al. “An Introduction to Biometric Recognition.” IEEE Transaction on Circuits and Systems for Video Technology. 14 (1) janv. 2004.

BIBLIOGRAPHIE

Hansard

Chambre des Communes. *Sous-comité de la Sécurité publique et nationale du Comité permanent de la justice, des droits de la personne, de la sécurité publique et de la protection civile.* 38e législature, 1re Session. (15 juin 2005) (Mary Gusella, présidente, Commission canadienne des droits de la personne).

Rapports

Agence des services frontaliers du Canada. « Vérification du processus de demande d'adhésion au programme NEXUS : rapport de vérification interne ». Avril 2007. http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2007/nexus-fra.html.

Bureau du vérificateur général du Canada. « Rapport de la vérificatrice générale du Canada à la Chambre des communes : octobre 2007 ». http://www.oag-bvg.gc.ca/internet/Francais/parl_oag_200710_f_23823.html.

Lois

Charte canadienne des droits et libertés, partie I de la Loi constitutionnelle de 1982, constituant annexe B de la Loi de 1982 sur le Canada, 1982, ch. 11 (R.-U.).

Code de la route, L.R.O. 1990, CHAPITRE H.8.

Décret modifiant le Décret sur les passeports canadiens, C.P. 2004-951 1 septembre 2004.

Décret sur les passeports canadiens (TR/81-86).

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

Traffic Safety Act, R.S.A. 2000, c. T-6.

Jurisprudence

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

About-Al-Rashta c. *Canada (ministre de la Citoyenneté et de l'Immigration).* [2001] A.C.F. no 644., 2001 FCT 344.

Al-Ghamdi c. Canada (Affaires étrangères et Commerce international Canada. 2007 CF 559, 64 Imm. L.R. (3d) 67.

*Andryanov c. Canada (*Ministre de la Citoyenneté et de l'Immigration*).* [2007] A.C.F. no 272, 2007 CF 186.

Bothwell v. Ontario (Minister of Transportation). [2005] O.J. No. 189.

Canada Safeway Ltd. V. U.F.C.W. Local 401. [2006] L.V.I. 3607-3, 145 L.A.C. (4th) 1.

Conseil des Canadiens avec déficiences c. VIA Rail Canada Inc., 2007 CSC 15, [2007] 1 R.C.S. 650.

Gill v. British Columbia (Ministry of Health). 40 C.H.R.R. D/321, 2001 BCHRT 34.

Hutterian Brethen of Wilson Colony v. Alberta. 2007 ABCA 160, affirming *Hutterian Brethen of Wilson Colony* (2006), 33 M.V.R. (5th) 16, 57 Alta.L.R. (4th) 300, 398 A.R. 5 (Alta. Q.B.).

Kamel c. Canada (Procureur général) (C.F.), 2008 CF 338, [2009] 1 R.C.F. 59.

Kerzner c. Canada (Ministre du Revenu national), 2005 CF 1574, 10 T.T.R. (2d) 589.

N.B. v. Canada (Attorney General). 27 A.R. 135, 40 C.P.C. (4th) 244.

Naqvi v. Canada (Employment and Immigration Comm.) [2005] F.C.J. No. 1704, 2005 FC 1392.

R. v. E. (S.H.). 2007 ONCJ 308.

Saqer c. Canada (Ministre de la Citoyenneté et de l'Immigration). [2005] A.C.F. no 1704, 2005 CF 1392.

Turner v. Telus Communication Inc. 2005 FC 1601, 2006 C.L.L.C. 210-022.

United States v. Henry. [2002] O.J. No. 5738, 66 W.C.B. (2d) 104.

Veffer c. Canada (Ministre des Affaires étrangères). 2007 CAF 247.

Autres sources

"A Canada–U.S. Border Vision." Canadian Chamber of Commerce. Décembre 2008. http://www.chamber.ca/cmslib/general/blueprint.pdf.

"Are Your IDs Secure Enough?" *Digimarc: White Paper*. 2007.

"Armed Forces deploying Biocert Clipbio Pro." *PC Business Products*. Déc 2006, p. 5–7.

"Canada to Begin Issuing High-Tech Passports." *CTV*, 18 juillet, 2004. http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20040718/canada_passport_040718?s_name=&no_ads=.

"CPA exam now requires fingerprints." *Practical Accountant*, 41 (6) Juin 2008, p. 7.

"Ensuring security by managing identity." *Card Technology Today*, Juin 2005, p. 12–13.

"Fast-Track Cards a License to Smuggle, Border Guards Fear." *Globe and Mail*, 1er nov. 2008. http://www.theglobeandmail.com/servlet/story/RTGAM.20081101.wbordercar01/BNStory/energy/.

"Further Strengthening of the Use and Verification of Residence Identity Cards." *Chinese Law and Government*, 34 (3) Mai-Juin 2001, p. 90–93.

"Hand Geometry." Subcommittee on Biometrics, National Science and Technology Council. 7 août 2006.

"Key Accomplishments Since August 2007." Statement from Security and Prosperity Partnership Meeting. New Orleans, U.S., 22 avril 2008.

"No fingerprints from under-12s." *Biometric Technology Today*, 16 (10) Oct. 2008, p. 2-3.

"Passport Canada says Sikh photos rejected by mistake." *CBC News*, 17 août 2007. http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-passportcanada.html.

"Sikh passport photos rejected because of headgear." *CBC News*, 17 août 2007. http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-sikhpassports.html

« Carte de résident permanent ». Citoyenneté et Immigration Canada. http://www.cic.gc.ca/francais/information/carte-rp/index.asp.

« Programme d'identification en temps réel ». GRC. http://www.rcmp-grc.gc.ca/rtid-itr/index-fra.htm.

« Regard historique ». Passeport Canada. http://www.ppt.gc.ca/pptc/hist.aspx?lang=fra.

« Vérification de sécurité ». Agence des services frontaliers du Canada. http://www.cbsa-asfc.gc.ca/security-securite/screen-verific-fra.html

Acharya, Lalita. « La biométrie et son usage par l'état ». Gouvernement du Canada, Service d'information et de recherche parlementaires. Septembre 2006.

Agence des services frontaliers du Canada. « Documents requis pour entrer aux États-Unis – Calendrier ». 6 nov. 2008. http://www.cbsa-asfc.gc.ca/whti-ivho/chron-fra.html

Agence des services frontaliers du Canada. « Sûreté et sécurité – Gestion de l'accès au Canada ». 31 juillet 2008. http://www.cbsa-asfc.gc.ca/security-securite/safety-surete-fra.html#s2_1.

Aleksic, Petar S. et Aggelos K. Katsaggelos. "Audio-Visual Biometrics." *Proceedings of the IEEE*, 94 (11), Nov. 2006.

Allan, Roger. "Biometrics looks to solve identity crisis." *Electronic Design*, 56 (12) 19 juin 2008, p. 31 –35.

Ananthaswamy, Anil. "Cracks case doubt on the 'fussy vault'." *New Scientist*, 22 sept. 2007.

Baldassi, Cindy L., DNA, Discrimination and the Definition of Family Class: M.A.O. v. Canada (Minister of Citizenship and Immigration). *Revue des lois et des politiques sociales = Journal of Law and Social Policy,* 21, 2007, p.5.

Bhandar, Davina. "Renormalizing Citizenship and Life in Fortress North America." Citizenship Studies, 8 (3) Sept. 2004, p. 261–278.

Browne, Simone. "Getting Carded: Border control and the politics of Canada's Permanent Resident card." *Citizenship Studies*, 9 (4) Sept. 2005, p. 423–438.

Bureau de Conseil privé. « Protéger une société ouverte : la politique canadienne de sécurité nationale ». Avril 2004.

Burge, Mark, et William Burger. "Ear Biometrics." In Anil K. Jain et al. eds., *Biometrics: Personal Identification in a Networked Society*. New York: Springer, 2006.

Burns, David R. "Virtual Borders and Surveillance in the Digital Age." International Journal of Media and Cultural Politics, 3 (3) 2007, p. 325–341.

Camp, L. J. "Identity, Authentication, and Identifiers in Digital Government." *International Symposium on Technology and Society*, 26–28 sept. 2003, p. 10–13.

Citoyenneté et Immigration Canada. « Demande de citoyenneté ». http://www.cic.gc.ca/francais/citoyennete/index.asp.

Citoyenneté et Immigration Canada. « Foire aux questions : mise à l'essai de la biométrie sur le terrain ». 12 juin 2008. http://www.cic.gc.ca/francais/information/faq/biometrie/index.asp.

Connolly, Christine. "Image Processing Algorithms Underpinning Iris and Facial Recognition Systems." *Sensor Review*, 26 (1) 2006, p. 22–27.

Covavisaruch, Nongluk, et al. “Personal Verification and Identification Using Hand Geometry.” *ECTI Transactions on Computer and Information Technology*, 1 (2) Nov. 2006.

Daugman, John. “New Methods in Iris Recognition.” *IEEE Transactions on Systems, Man, and Cybernetics*, 37 (5) Oct. 2007, p. 1167–1175.

Deravi, F., et al. “Intelligent Agents for the Management of Complexity in Multi-modal Biometrics.” *Digital Object Identifier*, 2, 2003, p. 293–304.

Dimauro, G, et al. “Recent Advancements in Automatic Signature Verification.” *Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition*, 2004.

Dinerstein, Marti. “America’s Identity Crisis: Document fraud is pervasive and pernicious.” *Centre for Immigration Studies*, Avril 2002. http://www.cis.org/articles/2002/back302.html.

Downes, Stephen. “Authentication and Identification.” *International Journal of Instructional Technology and Distance Learning.* Oct. 2005.

Drury, Ian. “ID cards could be derailed by pensioners as finger prints of over-75s are hard to scan.” *The Daily Mail*, 15 août 2008. http://www.dailymail.co.uk/news/article-1045659/ID-cards-derailed-pensioners-finger prints-75s-hard-scan.html.

Egelman, Serge, et Lorrie Faith Cranor. “The Real ID Act: Fixing identity documents with duct tape.” I/S: A Journal of Law and Policy, 2 (1) 2006, p. 149–183.

Ellison, Carl M. “Establishing Identity Without Certification Authorities.” Presented at *6th USENIX Security Symposium*. San Jose, 22–25 juillet 1996.

Fairhurst, M. C., et E. Kaplani. “Perceptual Analysis of Handwritten Signatures for Biometric Authenfication.” IEE Proc.-Vis. Image Signal Process, 150 (6) Déc. 2003, p. 389–394.

Fairhurst, M. C., et S. Ng. “Management of Access Through Biometric Control: A case study based on automatic signature verification.” *Digital Object Identifier*, 1, 2001, p. 31–39.

Ford, Christopher A. “The Determination of “Race” in Race-Conscious Law.” *California Law Review*, 82 (5) Oct. 1994, p. 1231–1285.

Gale, Doug. “What’s in a Name?” *T.H.E. Journal*, 33 (11), Juin 2006, p. 22–24.

Grijpink, J. H. A. M. “Trend report on biometrics: Some new insights, experiences, and developments.” *Computer Law & Security Report*, 24 (3) Mai 2008, p. 261–264.

Gupta, Babita. “Biometrics: Enhancing Security in Organizations.” IBM Center for the Business of Government. 2008.

Hanmandlu, Madasa, et al. “Off-line Signature Verification and Forgery Detection Using Fuzzy Modeling.” *Pattern Recognition*, 38 (3) Mars 2005, p. 341–356.

Hashiyada, Masaki. “Development of Biometric DNA Ink for Authentication Security.” *Tohoku Journal of Experimental Medicine*, 204, 2004, p. 109–117.

Hewitt, Steve. “The Secret History of the Canadian Passport: It’s the preferred choice of discriminating villains everywhere. The question is: why?” *The Beaver*, 1er avril 2004.

Ho, Julian. “SCC to Address Accomodation of Religious Freedom Once Again.” *The Court.* 16 septembre 2008. http://www.thecourt.ca/2008/09/16/scc-to-address-accommodation-of-religious-freedom-once-again/.

Holder, Daniel. “More Than Just a Card: Intrusion, exclusion and suspect communities: Implications in Northern Ireland of the British National Identity Scheme.” Northern Ireland Human Rights Commission. Briefing paper prepared for *Identity Cards and Suspect Communities* seminar. 15 oct. 2008. http://www.nihrc.org/dms/data/NIHRC/attachments/dd/files/104/More_than_just_a_card_FINAL.pdf.

Impedovo, S., et G. Pirlo. “Verification of Handwritten Signatures: An Overview.” *14th International Conference on Image Analysis and Processing*, 2007.

Jacobson, Louis. “Playing the Identity Card.” *National Journal*, 20 mars 1999.

Jain, Anil K., Arun Ross, et Sharath Pankanti. “Biometrics: A tool for information seeking.” *IEEE Transactions on Information Forensics and Security*, 1 (2) Juin 2006.

Jain, Anil K., et al. “An Introduction to Biometric Recognition.” *IEEE Transaction on Circuits and Systems for Video Technology*, 14 (1) Janv. 2004.

Jain, Anil K., et al. eds. *Biometrics: Personal Identification in a Networked Society.* New York: Springer, 2006.

Jain, Anil K., et al. *Handbook of Fingerprint Recognition.* New York: Springer, 2003.

Jain, Anil K., et Nicolae Duta. “Deformable Matching of Hand Shapes for Verification.” Department of Computer Science and Engineering, Michigan State University, 2007.

Jain, Anil, Lin Hong, et Sharath Pankanti. “Biometric Identification.” *Communications of the ACM*, 43(2) Févr. 2000, p. 90–98

James, Tabitha, et al. “Determining the Intention to Use Biometric Devices: An application and extension of the technology acceptance model.” *Journal of Organizational and End User Computing*, 18 (3) Juil.–Sept. 2006, p. 1–24.

Kanellos, Michael. “E-Passports to put new face on old documents.” *CNET*, 18 août 2004.

Karpinski, Maciej Mark, et Charles Théroux. « Dilemmes quant au fait d'assurer la sécurité nationale tout en protégeant les droits de la personne : point de vue de la Commission canadienne des droits de la personne ». Commission canadienne des droits de la personne, 2008.

Kittler, J., et al. “Combining Evidence in Personal Identity Verification Systems.” *Pattern Recognition Letters, 18*, 1997, p. 845–852.

Kochems, Alane, et Laura Keith. “Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft.” *Heritage Foundation: Backgrounder*, No. 1946, 27 juin 2006.

Kruger, Erin et Marlene Mulder, Bojan Korenic. “Canada After 11 September: Security measures and ‘preferred’ immigrants.” *Mediterranean Quarterly*, 15 (4) Automne 2004, p. 72–87.

Landahl, Mark. “Identity Crisis: Defining the problem and framing a solution for terrorism incident response.” *Homeland Security Affairs*, 3 (3) Sept. 2007.

Levine, Jenny. “Biometrics and security.” *Library Journal*, 15 oct. 2004.

Lodge, Juliet. “Trends in Biometrics.” Briefing Note prepared for The European Parliament’s committee on Civil Liberties, Justice, and Home Affairs. 28 sept. 2006.

Lyon, David. “Biometrics, Identification, and Surveillance.” *Bioethics*, 22 (9), 2008. p. 449–508.

Lyon, David. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London: Routledge, 2003.

McCarthy, Shawn. “No Smiling! We’re Canadian.” *Globe and Mail*, 27 août 2003. http://www.theglobalandmail.com/servlet/story/RTGAM.20030826.wsmile0826/BNStory/National/.

Mcleod, Judi. “Canada Took UN Inspiration for New E-Passport.” *Canadafreepress.com.* 21 juillet 2004. http://www.canadafreepress.com/2004/main072104.htm.

Michael, K., et M. G. Michael. “The Proliferation of Identification Techniques for Citizen throughout the Ages.” *Faculty of Informatics-Papers*, 2006.

Ministère des Affaires étrangères et Commerce international Canada. « Plan d'action pour la création d'une frontière sûre et intelligente ». http://www.international.gc.ca/anti-terrorism/actionplan-fr.asp.

Monk, Bruce. “Designing Identity Documents for Automated Screening.” *2004 IEEE Conference on Technologies for Homeland Security*. Cambridge, MA, 21-22 avril 2004.

Muller, Benjamin J. “(Dis)Qualified Bodies: Securitization, citizenship and ‘Identity Management’.” *Citizenship Studies*, 8 (3) Sept. 2004, p. 279–294.

Negin, Michael, et al. “An Iris Biometric System for Public and Personal use.” *Computer*, 33 (2) Févr. 2000, p. 70–75.

O’Gorman, Lawrence. “Comparing Passwords, Tokens, and Biometrics for User Authentication.” *Proceedings of the IEEE*, 91 (12) Déc. 2003.

Onley, Dawn S. “Biometrics on the front line.” *Government Computer News*, Apr. 16, 2008. http://gcn.com/articles/2004/08/13/biometrics-on-the-front-line.aspx.

Organisation de l’aviation civile internationale. « Facilitation et qualité du service aux aéroports ». Note de travail, 20 septembre 2004. http://www.icao.int/icao/en/assembl/a35/wp/wp180_fr.pdf.

Otjacques, Benoit, et al. “Identity Management and Data Sharing in the European Union.” Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

Pankanti, Sharath, Salil Prabhakar, et Anil K. Jain, “On the Individuality of Fingerprints,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24 (8) Août 2002, p. 1010–1025.

Passeport Canada. « Document d'information – Refus ou révocation de passeports ». http://www.ppt.gc.ca/articles/20080213a.aspx?lang=fra.

Pentland, Alex, et Tanseem Choudhury. “Face Recognition for Smart Environments.” *Computer*, 33 (2) Févr. 2000, p. 50–55.

Roethenbaugh, Gary. “Biometrics Explained.” *International Committee for Information Technology Standards*. Sept. 2005.

Rosenzweig, Paul, Alane Kechems, et Ari Schwartz. “Biometric Technologies: Security, legal, and policy implications.” *Legal Memorandum: The Heritage Foundation, 12*, 21 juin 2004.

Ross, Arun, and Anil Jain. “Information Fusion in Biometrics.” *Pattern Recognition Letters*, 24 (13) Sept. 2003, p. 2115–2125.

Roy, Bjorn. « A Case Against Biometric National Identification Systems (NIDS): "Trading-Off" privacy without getting security ». *Revue des affaires juridiques et sociales—Windsor = Windsor Review of Legal and Social Issues, 19* (45) Mars 2005.

Sanchez-Reillo, Rand, et Ana Gonzalex-Marcos. "Access Control System with Hand Geometry Verification and Smart Cards." *IEEE AES Systems Magazine,* Févr. 2000.

Security and Prosperity Partnership. "Fact Sheet: Security and Prosperity Partnership of North America." 31 mars 2006.

Sinoski, Kelly. "Passport Canada apologizes for refusing passports to Sikhs." *Vancouver Sun*, Aug. 18, 2007 on Nov. 18, 2008.

Soutar, Colin. "Implementation of Biometric Systems: Security and Privacy Considerations." *Information Security Technical Report, 7* (4) 2002, p. 49–55.

Sparke, Matthew B. "A Neoliberal Nexus: Economy, security and the biopolitics of citizenship on the border." *Political Geography, 25*, 2006, p. 151–180.

The White House. "Specifics of Secure and Smart Border Action Plan." 7 janv. 2002. http://www.dhs.gov/xnews/releases/press_release_0036.shtm.

Thomas, Rebekah. "Biometrics, International Migrants, and Human Rights." *European Journal of Migration and Law*, *7*, 2005. p. 377–411.

Toledano, Doroteo T., et al. "Usability Evaluation of Multi-modal Biometric Verification Systems." *Interacting with Computers*, *18* (5) Sept. 2006, p. 1101–1122.

Torpey, John. "The Great War and the Birth of the Modern Passport System," in Jane Caplan and John Torpey, eds., *Documenting Individual Identities: The Developments of State Practices in the Modern World.* Princeton: Princeton University Press, 2001, p. 256–270.

Tuller, Mike, et al. "Biometrics: Strategic Technology Analysis." Technology Foresight Dynamics, Group 4 White Paper, 2006.

UK Passport Service. "UKPS Biometrics enrollment trial report." May 2005. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf

Wang, Jia-Ching, et al. "Robust Speaker Identification and Verification." *Computational Intelligence Magazine, IEEE, 2* (2) Mai 2007, p. 52–59.

Wayman, James L. "Fundamentals of Biometric Authentication Techniques." *International Journal of Image and Graphics, 1* (1) 2001, p. 93–113.

Whitaker, Reg. “Securing the ‘Ontario–Vermont border’: Myths and Realities in Post-9/11 Canadian–American Security Relations,” *International Journal*, *60* (1) Winter 2004–2005, p. 53–70.

Wigan, Marcus. “Owning identity—one or many—do we have a choice?” in The Second Workshop on the Social Implications of National Security. Australian Homeland Security Research Centre, Octobre 2007.

Williams, Brent C., et al. “The Accuracy of the National Death Index When Personal Identifiers Other than Social Security Number are Used.” *American Journal of Public Health*, *82* (8) Août 1992, p. 1145–1147.

Wilson, Dean. “Biometrics, Borders, and the Ideal Suspect,” in S. Pickering and L. Weber, eds., *Borders, Mobility, and Technologies of Control*. Netherlands: Springer, 2006, p. 87–109.

Yoruk, Erdem, Helin Dutagaci, and Bulent Sankur. “Hand Biometrics.” *Image and Vision Computing*, *24* (5) Mai 2006, p. 483–497.