Commissariat à la
protection de la vie privée
du Canada

Office of the
Privacy Commissioner
of Canada

L’identité, la protection de la vie privée et le besoin d’autrui de savoir qui vous êtes : document de travail sur l’identité et les questions qu’elle soulève

Septembre 2007

Table des matières

Auditoire cible 1
Introduction 2
Notions élémentaires 8
Qu'est-ce que l'« identité »? 8
Systèmes d'identité 12
Présentation de preuves pour établir la véracité d'une identité — « Authentification » 14
Authentification d'une autorisation ou d'un droit 15
Moyens d'établir avec certitude une identité, une autorisation ou un droit 16
Limites de l'authentification de l'identité pour accroître la sécurité 20
Protéger la vie privée avec des identificateurs impossibles à corréler 20
Protéger la vie privée avec des « symboles réservés au porteur » 22
Qui s'intéresse à l'identité? 25
Intérêts communs et conflictuels de la gestion de l'identité 29
Repenser la gestion de l'identité pour mieux protéger la vie privée 34
Faire table rase pour mieux étudier les systèmes d'identité 34
Établir les paramètres de protection de la vie privée dans la gestion de l'identité 35
L'avenir de la gestion de l'identité 41
Conclusion 52
Annexe A : Le débat sur la carte d'identité nationale 55
Annexe B : Évaluations des facteurs relatifs à la gestion de l'identité 61
Glossaire 64

Auditoire cible

Ce document de travail s’adresse principalement au lecteur profane. C’est pourquoi, sans sacrifier l’exactitude des informations présentées, on a évité le langage technique.

Introduction

Qu'est-ce que l'« identité » et comment est-elle liée à la protection de la vie privée? Voilà la principale question dont traite le présent document de travail. Notre façon de nous présenter à des personnes, à des entreprises et à des organismes gouvernementaux (autrement dit, notre façon de « gérer » notre identité) a de profondes conséquences sur nos relations avec autrui. L'identité joue un rôle central dans le difficile dilemme entre la protection de la vie privée et les efforts pour créer par ailleurs une « société de surveillance ». Par exemple,

- Ces dernières années, le gouvernement du Canada a envisagé la possibilité de lancer une carte d'identité nationale. Dans un sondage effectué en 2003, 30 p. 100 des répondants canadiens s'étaient dits fortement en accord avec l'obligation pour chaque Canadienne et Canadien de garder sur soi en tous temps une carte d'identité délivrée par le gouvernement, et 23 p. 100 s'étaient dits un peu en accord[1]. Cependant, les Canadiennes et les Canadiens seraient-ils aussi favorables à la création d'une carte d'identité nationale s'ils connaissaient toutes ses conséquences sur la vie privée et ses limites pour ce qui est d'accroître la sécurité et de prévenir le crime? Selon sa conception, une carte d'identité nationale pourrait donner aux ministères et à d'autres organisations de grands pouvoirs de surveillance des personnes sans pour autant accroître sensiblement l'efficacité du gouvernement ou la sécurité publique. Un système de cartes d'identité nationales serait presque certainement fondé sur une base de données sur les participants ou les personnes « inscrites » dans ce système. Cette base de données contiendrait des renseignements personnels sur toute la population. De

[1] En 2003, le Conseil de recherches en sciences humaines du Canada a octroyé des fonds au Surveillance Project, un groupe de recherché multidisciplinaire affilié au département de sociologie de l'Université Queen's pour étudier la mondialisation des données personnelles. Élément clé du projet : un sondage international mené auprès de 9 000 personnes réparties dans huit pays (Brésil, Canada, Chine, France, Hongrie, Mexique, Espagne et États-Unis). Les conclusions sont tirées des résultats du sondage.

> plus, l’utilisation d’un seul numéro de carte d’identité nationale aiderait les organisations à créer des profils individuels complets, peut-être en temps réel — ce qui constitue une abomination dans une démocratie qui prétend respecter la vie privée.

L’identité n’est pas uniquement une question de relation entre les personnes et le gouvernement. De nombreuses entreprises veulent identifier leurs clients afin de personnaliser leurs services, de surveiller le comportement de ces derniers et d’élaborer des stratégies commerciales en fonction de ce comportement. En outre, des commissionnaires en publipostage — des entreprises qui compilent et vendent des renseignements personnels à d’autres entreprises et à des organismes gouvernementaux — veulent des renseignements sur l’identité des gens afin de dégager des « profils » individuels qu’ils peuvent ensuite vendre à des entreprises ou à des gouvernements. Les manières dont les personnes se présentent peuvent soit faciliter soit limiter le profilage.

Une personne obligée de décliner son identité à tout bout de champ ne peut plus participer à des activités sociales sans que chacun de ses gestes et interactions soient surveillés et lui soient associés. Elle perd le droit de vaquer à ses occupations quotidiennes dans l’anonymat — un aspect important de la vie privée. Par contre, des « systèmes d’identité » gérés intelligemment peuvent préserver, voire renforcer, la vie privée et bon nombre d’autres droits importants qui découlent du respect de la vie privée.

L’identité est souvent, par ailleurs, très utile. Par exemple, le programme fédéral Gouvernement en direct vise à améliorer les services gouvernementaux offerts sur Internet et à en accroître la rapidité, la fiabilité, la commodité et l’accessibilité. La prestation de ces services peut nécessiter l’identification des personnes en direct. Le commerce en ligne — comme les services bancaires électroniques et les ventes sur Internet — requiert également des formes d’identification sécurisée. Un autre exemple est celui du remplacement des dossiers médicaux

sur papier par des dossiers électroniques, tenus à différents endroits, qui peuvent être reliés entre eux dans le but d'améliorer les soins des patients; pour cela, il faut trouver des moyens appropriés de faire correspondre chaque dossier médical au patient concerné.

Des moyens d'identification appropriés peuvent aider à empêcher que des personnes se fassent « voler » leur identité par ceux qui voudraient s'en servir pour établir des relations d'affaires — obtenir un prêt, par exemple. Gérée adéquatement, l'identité peut même protéger les personnes dans leurs relations personnelles — par exemple, en empêchant quelqu'un d'utiliser en direct l'identité d'un ex-époux pour chambouler sa vie privée en envoyant des courriels ou d'autres formes de messages prétendument en son nom. Les personnes ont également besoin de documents délivrés par le gouvernement pour confirmer leur identité (un passeport pour faciliter les voyages internationaux, par exemple), être autorisés à faire certaines choses (comme conduire une voiture) ou avoir droit à des avantages sociaux (les soins de santé publics). Finalement, notre identité peut servir à assurer notre sécurité.

Comment pouvons-nous protéger notre vie privée dans un monde où l'identité et l'identification tiennent une place aussi centrale dans nos vies? Cette question ne concerne pas directement l'identité ou le respect de la vie privée. Comment pouvons-nous gérer l'identité afin d'atteindre des objectifs gouvernementaux et commerciaux légitimes, tout en respectant le besoin, et le droit qu'ont les personnes au respect de leur vie privée?

Même si le Canada est un chef de file dans le domaine du traitement de l'identité, ses mesures législatives et ses politiques n'ont pas évolué au même rythme que les technologies et les conséquences de celles-ci sur la vie privée. De plus, le fait que les Canadiennes et les Canadiens comprennent mal les questions liées à l'identité, par exemple les avantages et les inconvénients d'un

système de cartes d'identité nationales, complique ce problème. Seul un petit groupe d'experts connaissent bien ces questions.

En effet, les questions d'identité peuvent être complexes. Un rapport[2] rédigé en 2002 par la National Academy of Sciences des États-Unis souligne bon nombre des questions que soulève l'adoption d'un système d'identité :

- Quelle est la raison d'être du système?
- Quelle proportion de la population recevrait une carte d'identité et serait a priori inscrite dans le système?
- Comment les identités de ces personnes seraient-elles authentifiées (prouvées)?
- Quelle serait l'étendue des données recueillies sur chaque participant?
- Quels seraient les utilisateurs du système (par opposition aux participants, c'est-à-dire les détenteurs d'une carte d'identité)? Quelles entités du gouvernement ou du secteur privé seraient autorisées à utiliser le système? Qui contribuerait à recueillir les données, à les examiner et à les réviser? (Essentiellement, ces questions visent à déterminer qui sont les initiés/spécialistes du système et quels pouvoirs ils ont.)
- Quels types d'utilisations seraient permis? Qui pourrait demander une carte d'identité et dans quelles circonstances?
- La participation au système ou l'identification serait-elle volontaire ou obligatoire?
- Les participants devraient-ils savoir que leur identité est vérifiée ou y consentir (contrairement à une situation, par exemple, où les vérifications d'identité se feraient à l'insu d'une personne à l'aide de moyens techniques comme la reconnaissance du visage)?

[2] Stephen Kent et Lynette Millett, éditeurs., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press), 2002. Lien Internet : http://www.nap.edu/catalog/10346.html (consulté le 1er février 2007).

- Quelles structures juridiques protégeraient l'intégrité du système, ainsi que la confidentialité des données et le droit de se défendre, et détermineraient la responsabilité des administrations publiques et des parties concernées à l'égard d'une mauvaise utilisation ou d'une erreur du système?

Au-delà de ces considérations stratégiques, l'identité soulève un ensemble complexe de questions sur les plans technique, économique et de la sécurité.

Les Canadiennes et les Canadiens doivent avoir la possibilité de comprendre le rôle que joue dans la société l'identité et les problèmes qu'elle peut poser dans la protection de la vie privée. Le présent document de travail vise justement à leur donner cette possibilité et à les éclairer sur la manière dont l'identité façonne leur droit à la vie privée. Tous les aspects de l'identité ne peuvent y être traités. Des livres entiers, dont certains très techniques, ont été écrits sur le sujet. Le présent document vise plutôt à décrire aussi simplement que possible les notions de base en matière d'identité, mais de façon suffisamment détaillée pour que les personnes comprennent les liens entre l'identité et le respect de la vie privée, et puissent contribuer aux débats concernant les politiques publiques sur les questions d'identité.

Le présent document traite des aspects suivants de l'identité :

- La signification du mot « identité » et ses diverses composantes — par exemple, l'« authentification », les « attributs », les « identificateurs », la « gestion de l'identité », les « systèmes d'identité » et les « symboles »;
- Les personnes ou les organisations qui s'intéressent à l'identité et les raisons pour lesquelles elles s'y intéressent? Par exemple, quand est-il approprié d'avoir des moyens d'identifier des personnes et quel rôle devrait jouer l'identification dans les questions de sécurité nationale?
- Les conflits et les intérêts communs concernant la gestion de l'identité;

- Les questions de respect de la vie privée associées à l’identité;
- Les propositions qui visent à repenser l’identité pour répondre aux questions de respect de la vie privée.

Notions élémentaires

Qu'est-ce que l'« identité »?

Qu'entendons-nous par « identité » et « identification »? La manière la plus facile de comprendre l'identité est peut-être de se la représenter, à la lecture du présent document, comme étant « ce que les autres — des personnes ou des organisations — savent de nous ». Par exemple, les membres de notre famille nous connaissent d'une certaine manière (notamment par notre nom à la naissance, nos traits de caractère ou particularités physiques et notre éducation), tout comme nos employeurs et les nombreux fournisseurs de services avec qui nous traitons. Ils ont tous une idée de ce que nous sommes — c'est-à-dire de notre identité. Autrement dit, l'identité peut désigner un ensemble de renseignements qui distinguent une personne des autres *dans un contexte particulier*.

Plus précisément, l'identité est un ensemble d'affirmations (ou d'allégations) sur les « attributs » d'une personne. Ces affirmations ou allégations peuvent comporter n'importe lesquels des éléments d'information suivants :

- Les attributs d'une personne connus d'une autre personne (son nom, son apparence physique, son appartenance à un groupe social);
- Ses attributs connus d'un employeur (son nom complet, son numéro d'employé);
- Ses attributs connus du gouvernement (son nom, son numéro d'assurance sociale (NAS) ou son numéro de carte d'assurance-maladie).

Dans chaque cas, au moins un des attributs est effectivement *unique* dans un contexte donné, parce qu'*aucune* autre personne n'est censée avoir le même. Le nom de famille d'une personne est propre à sa famille (à moins qu'un membre

n'ait reçu celui d'un autre membre). Les numéros des employés et, peut-être, leur nom complet sont propres à l'employeur. Le NAS ou le numéro d'assurance-maladie sont propres à l'administration fédérale.

« **Identificateur**[3] » : Ce terme désigne un attribut unique dans un contexte donné. En principe, une seule personne peut être associée à un identificateur particulier.

Il est possible que des attributs uniques à un contexte donné qui servent d'identificateurs ne puissent remplir la même fonction dans un autre contexte, parce qu'ils ne sont pas uniques dans cet autre contexte. Le prénom d'une personne — Harold, par exemple — est un attribut qui peut être un identificateur pour les membres de la famille directe parce qu'il est unique à ce contexte. Dans la rue, « Harold » ne peut plus servir d'identificateur, puisque de nombreuses personnes se nomment ainsi. « Harold » demeure un attribut de cette personne, mais il n'est plus un identificateur dans ce contexte, parce qu'il ne lui est pas propre. Le nom complet d'une personne peut être unique (et constituer ainsi un identificateur) dans une ville ou même au-delà, mais il n'est probablement pas unique dans un pays. C'est pourquoi la société a conçu des identificateurs uniques même dans un contexte social élargi. Au Canada, le NAS est censé être différent pour chaque résidant. Dans les provinces, le numéro d'assurance-maladie de chaque résidant est unique. Un numéro de carte d'assurance-maladie ne peut être associé qu'à une personne.

[3] [Traduction] « Un identificateur est un renseignement qui nomme ou identifie une personne, un processus, une application, un lieu (p. ex., un endroit sur la planète ou l'adresse mémoire d'une unité centrale), un bien matériel (p. ex., un livre, un fichier-texte ou un appareil) ou toute autre entité ou groupe d'entités. Les identificateurs utilisateurs représentent des utilisateurs (p. ex., des personnes ou des groupes de personnes) dans leurs interactions avec des parties utilisatrices. [...] Dans un contexte donné, les identificateurs utilisateurs permettent aux parties utilisatrices de discriminer les personnes avec lesquelles elles interagissent; c'est ce qu'on appelle l'identification. » Voir Stefan Brands, « Secure User Identification Without Privacy Erosion », (2006) 3:1 University of Ottawa Law & Technology Journal = Revue de droit et technologie de l'Université d'Ottawa 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf.

Aujourd'hui, les gens utilisent différents identificateurs selon les contextes, plutôt qu'un seul identificateur dans l'ensemble de leurs activités. Nous choisissons les moments où nous communiquons nos identificateurs. Autrement dit, nous présentons notre NAS au gouvernement, mais nous ne l'utilisons pas avec nos amis. Avec eux, nous utilisons plutôt notre nom. Chez un détaillant, nous pouvons nous servir de notre numéro de carte de fidélité et, chez un transporteur aérien, de notre numéro de grand voyageur.

Identification : Les identificateurs permettent de distinguer entre elles les personnes que nous rencontrons. Ce processus s'appelle l'identification, et c'est ce qui fait qu'une personne (ou bien une entreprise ou une administration) peut trouver l'identificateur d'une personne pour ensuite « examiner » les attributs associés à cette personne. Prenons l'exemple suivant qui ne fait appel à aucun moyen électronique : Lorsque vous rencontrez un ami dans la rue, cet ami reconnaît votre apparence et, par conséquent, vous « identifie ». Il peut ensuite « extraire » de sa mémoire d'autres renseignements sur vous. Autrement dit, il se sert de votre identificateur pour se rappeler d'autres attributs qui vous caractérisent — votre affiliation au même club ou groupe scolaire que le sien, par exemple. Lorsque vous parlez à cette même personne au téléphone, le seul son de votre voix peut servir d'identificateur, en particulier lorsque vous mentionnez aussi votre nom. Lorsque vous correspondez avec un ami, votre adresse électronique peut lui suffire pour vous « identifier ». Lorsque vous donnez votre NAS à une institution gouvernementale, vous vous identifiez auprès de cet organisme et lui permettez d'extraire de ses dossiers d'autres renseignements concernant vos attributs.

Il n'est pas toujours important de connaître l'identité de quelqu'un. Dans bien des cas, les autres n'utilisent un identificateur que pour s'informer d'un attribut qui les intéresse en particulier. Par exemple, le propriétaire d'un bar peut utiliser le permis de conduire pour s'assurer qu'un client a l'âge légal requis pour fréquenter son bar. Le fait qu'une personne ait atteint la majorité est l'attribut qui

le préoccupe. Un policier peut utiliser ce même permis de conduire pour s'assurer qu'une personne a le droit de conduire un véhicule. Le droit de conduire est également un « attribut ». Dans les deux cas, il n'est pas vraiment nécessaire de connaître l'identité de la personne. Le propriétaire du bar ou le policier veulent simplement vérifier qu'une personne a un attribut particulier — l'âge légal ou la majorité, ou le droit de conduire. Les façons de fournir les renseignements sur les attributs sans dévoiler l'identité d'une personne — et en protégeant ainsi la vie privée — sont présentées en détail plus loin.

Stefan Brands présente une liste[4] de nombreuses méthodes d'identification :

- Noms à la naissance, dénominations sociales, surnoms et pseudonymes d'auteurs;
- Adresses électroniques, numéros de téléphone, numéros de case postale et adresses URL (localisateur de ressources uniformes);
- Empreintes digitales, lecture de l'iris ou de la rétine et échantillons d'ADN;
- Identificateurs du compte d'utilisateur avec le fournisseur d'accès Internet (FAI), les banques, les fournisseurs de services publics, etc.;
- Cartes de crédit, cartes de débit, cartes d'appel et jetons de fidélité;
- Insignes d'employés, cartes de membre d'un club sportif et cartes-clés d'hôtel;
- Numéros de sécurité sociale, numéros d'assurance-maladie, passeports et permis de conduire;
- Noms d'utilisateurs en ligne (p. ex. pour la messagerie instantanée et les clavardoirs), témoins et attestations du protocole sécurisé de cryptage (ou protocole SSL);
- Adresses MAC (*media access control* – ou adresses matérielles), adresses de protocole Internet (IP), numéros de série des cartes à puce,

[4] Stefan Brands, « Secure User Identification Without Privacy Erosion » (2006) 3:1 University of Ottawa Law & Technology Journal = Revue de droit et technologie de l'Université d'Ottawa 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf.

identificateurs du standard Bluetooth, numéros d'identité internationale d'équipement mobile (système GSM), étiquettes d'identification par radiofréquence et autres adresses d'utilisateurs de dispositifs en réseau.

Tous ces identificateurs uniques peuvent être utilisés dans des contextes particuliers pour distinguer les personnes entre elles — autrement dit, pour « identifier » chaque personne.

Gestion de l'identité : La « gestion de l'identité » est une notion centrale au sujet traité dans le présent document. Elle désigne essentiellement « tout ce qui concerne la gestion des identités du début à la fin de leur cycle de vie ». Cependant, la gestion de l'identité n'implique pas nécessairement l'identification d'une personne. Elle peut simplement consister à communiquer des données sur des attributs (comme une carte attestant que son détenteur a l'âge légal requis pour fréquenter un bar), sans donner d'information sur d'autres identificateurs. Dans la mesure où des identificateurs doivent être inclus, ceux-ci peuvent être des identificateurs « locaux », qui réduisent la possibilité de relier entre eux des renseignements sur une personne identifiée et de retracer les activités de cette personne.

Systèmes d'identité

Les attaques du 11 septembre 2001 aux États-Unis, et les autres survenues plus tard en Espagne et au Royaume-Uni, ont suscité de nombreuses discussions sur l'amélioration de la sécurité. Pendant ces discussions, qui portaient en partie sur les moyens de mieux repérer les personnes qui constituent une menace pour la sécurité, certains gouvernements ont laissé entendre qu'une carte d'identité nationale était un élément essentiel pour améliorer la sécurité. (Ailleurs dans le présent document, en particulier à l'annexe A, nous traitons des faiblesses de l'argumentation en faveur d'une carte d'identité nationale pour améliorer la sécurité nationale.) Cependant, cette carte n'est qu'une composante d'un

« système » d'identité complexe qui doit être élaboré à partir d'elle. Voici une citation de la National Academy of Sciences aux États-Unis :

> [Traduction]
> Le terme « système »… implique la mise en relation complexe et interdépendante de nombreuses composantes sociales, juridiques et techniques. Le succès ou l'échec d'un système dépend non seulement des composantes individuelles, mais aussi des façons dont celles-ci fonctionnent — ou ne fonctionnent pas — ensemble. Même si chaque composante individuelle, prise isolément, fonctionnait parfaitement, le système dans son ensemble pourrait ne pas atteindre ses objectifs. Le contrôle de ces interdépendances et l'atténuation des vulnérabilités en matière de sécurité et de leurs conséquences imprévues détermineraient l'efficacité d'un système.
>
> De plus, un système d'identité national ne comprendrait pas simplement une base de données, des réseaux de communications, des lecteurs de cartes et des centaines de millions de cartes d'identité. Il nécessiterait aussi l'élaboration de politiques et de procédures, et la prise en compte de questions liées à la sécurité, au respect de la vie privée et à la variabilité dimensionnelle, en plus des facteurs humains et des aspects relatifs à la maniabilité (des exigences d'utilisation trop coûteuses ou la mise en place de trop d'obstacles, qui inciteraient la partie ayant besoin des renseignements à contourner le système). On devrait peut-être prévoir quels participants seraient inscrits au système, quels utilisateurs (des personnes, des organisations, des administrations) auraient accès aux données et quelles utilisations seraient autorisées, et élaborer des politiques et des procédures juridiques et opérationnelles pour encadrer son fonctionnement. En outre, on devrait déterminer les méthodes pour inscrire les participants, manipuler (saisir, stocker, mettre à jour, chercher et retourner) les renseignements sur leur identité, délivrer les attestations (au besoin) et vérifier, entre autres, les demandes de consultation des bases de données[5].

Il importe de se rappeler la complexité des systèmes d'identification sociaux. Ce ne sont certainement pas des « solutions rapides » aux problèmes de sécurité.

[5] Stephen Kent et Lynette Millett, éditeurs., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002, p. 13-14. Lien Internet : http://www.nap.edu/catalog/10346.html (consulté le 1er février 2007).

Présentation de preuves pour établir la véracité d'une identité — « Authentification »

Lorsque des personnes s'identifient, elles indiquent qui elles sont. Cependant, cette identification ne *prouve* pas qu'elles sont bien qui elles disent être. Autrement dit, le simple fait de présenter un identificateur ne signifie pas que cet identificateur appartient à celui qui l'a présenté. N'importe qui peut entrer dans une banque pour contracter une hypothèque en disant être M. Tremblay, mais cela ne prouve pas qu'il l'*est* vraiment. La présentation de preuves pour établir la véracité d'une identité s'appelle l'« authentification ». Pour « authentifier » une identité (« Je suis M. Tremblay ») ou l'établir avec certitude, on peut se fier à des éléments d'information variés. C'est ce qu'on appelle des « authentificateurs ». Par exemple, le certificat de naissance d'une personne peut servir à authentifier son identité, tout comme son passeport ou sa fiche dentaire[6].

Autrefois, il n'était généralement pas nécessaire d'authentifier l'identité des personnes de manière très poussée. Tous les membres de la collectivité se connaissaient. Ils pouvaient identifier les autres par des attributs comme la voix, les traits physiologiques et des indices biométriques comme la couleur des cheveux ou des yeux. Néanmoins, à mesure que les populations se sont accrues et que les sociétés se sont complexifiées, il a fallu trouver d'autres moyens d'établir son identité auprès de parfaits étrangers, d'entreprises et d'administrations qui ne pouvaient pas s'appuyer sur des caractéristiques comme la voix ou les traits physiologiques pour reconnaître les gens. Au fil du

[6] [Traduction] « Dans le contexte d'une communication ou d'une transaction, on entend généralement par authentification la confirmation de l'identité affirmée. Cela se fait en deux étapes. Dans un premier temps, l'utilisateur présente un identificateur utilisateur (p. ex., « Jean Tremblay » ou « numéro d'employé 13579 ») qui représente l'utilisateur selon le contexte. La deuxième étape, l'authentification de l'identité, prévoit la confirmation que l'utilisateur de l'identificateur est la personne autorisée à l'utiliser, c'est-à-dire que c'est à cette personne qu'il a été attribué. Voir : *Encyclopedia of Privacy* [deux volumes], William G. Staples (éd.), ISBN: 0-313-33477-3, Greenwood Press.

temps, ces moyens ont évolué, y compris les mécanismes symboliques (comme le certificat de naissance ou le passeport) et le contrôle des références (lorsqu'une organisation souhaitant établir l'identité d'une nouvelle personne demande à une personne de confiance connue de confirmer cette identité).

Authentification d'une autorisation ou d'un droit

Dans bien des cas, l'authentification dont une organisation ou un organisme a besoin est la preuve d'une autorisation ou d'un droit individuel plutôt que l'identité de la personne concernée. Une organisation ou un organisme peut vouloir s'assurer, par exemple, qu'une personne est autorisée à entrer dans un bâtiment ou qu'elle a droit à certains avantages. L'identité de cette personne ne l'intéresse pas vraiment.

En fait, dans la plupart des transactions effectuées dans une société, les renseignements que les organisations veulent avoir ne sont pas ceux qui prouvent l'identité d'une personne, mais d'autres. Par exemple :

- Un marchand veut vérifier si le client a le droit d'utiliser la carte de crédit qu'il lui présente;
- Un chauffeur d'autobus veut savoir si le billet (ou le « symbole ») utilisé pour monter à bord est valide. Le chauffeur ne cherche pas à savoir quoi que ce soit du passager en question, sauf s'il utilise un billet à prix réduit pour étudiants. Dans ce cas, il veut une preuve du statut de l'étudiant pour confirmer son droit d'utiliser un tel billet. Même dans ce cas, le chauffeur d'autobus n'a pas besoin de connaître l'identité du passager, mais simplement de vérifier son statut d'étudiant;
- Les autorités gouvernementales responsables des transports pourraient délivrer un permis de conduire indiquant que son détenteur a le droit de conduire une voiture, et donner aux policiers le moyen (peut-être par des données biométriques) de s'assurer que la carte appartient bien au

conducteur en question. Cela s'appelle l'« authentification d'attributs[7] ». Les agents de police pourraient vérifier que la personne est bien autorisée à conduire, sans connaître son nom, son âge ou son adresse. Dans ce cas, l'identification du conducteur par son nom ne présente aucun intérêt (et a toujours été sans intérêt pour établir l'autorisation de conduire). L'information sur l'identité du conducteur pourrait être accessible aux policiers si l'intérêt public le justifiait, comme dans une enquête criminelle. Cependant, la communication de renseignements sur l'identité au-delà du droit de conduire un véhicule devrait faire l'objet d'un débat public et non se produire simplement par défaut, comme maintenant, en raison des structures actuelles des permis de conduire.

Lorsqu'une entreprise ou un organisme gouvernemental n'a pas vraiment besoin de connaître l'identité d'une personne, mais cherche simplement à savoir si elle est autorisée à faire quelque chose (utiliser une carte de crédit) ou si elle a le droit de recevoir quelque chose (un avantage social), cette personne peut protéger ses renseignements personnels en limitant l'information qu'elle accepte de transmettre pour prouver son identité. Elle peut ainsi diminuer la capacité d'autrui de surveiller ses activités et d'établir son profil.

Moyens d'établir avec certitude une identité, une autorisation ou un droit

Une personne peut authentifier son identité ou ses attributs (comme une autorisation ou un droit) en fournissant n'importe lequel des éléments d'information suivants ou une combinaison de ceux-ci :

[7] L'authentification d'attributs consiste à établir avec un niveau de certitude établi qu'un attribut appartient à une personne spécifique : Stephen T. Kent et Lynette I. Millett, *éditeurs*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).

- Une chose qu'elle est, par exemple son ADN, la forme de son iris ou ses traits faciaux;
- Une chose qu'elle a, par exemple un billet d'autobus (un « symbole »), un permis de conduire, une carte de crédit ou un passeport;
- Une chose qu'elle sait, par exemple, un mot de passe ou un numéro d'identification personnel (NIP).

En combinant certains de ces éléments d'information, il est possible de réduire le risque qu'une personne donne une fausse identité ou présente une fausse autorisation. Dans une installation nucléaire, par exemple, l'utilisation d'une carte d'accès à un bâtiment (chose que la personne a) pourrait être exigée, en plus de la lecture de l'iris par une machine (chose qu'elle est). Cette lecture serait ensuite comparée à l'image de l'iris enregistrée sur la carte d'accès ou dans une base de données distincte. La combinaison de deux authentifications « monofactorielles » donne une authentification multifactorielle. Dans cet exemple, l'un des deux facteurs est la carte d'accès au bâtiment et l'autre, les caractéristiques de l'iris.

Si l'installation nucléaire n'exigeait qu'une authentification monofactorielle[8] faible, comme un code d'accès, il serait possible d'entrer facilement dans le bâtiment en volant le code d'accès de quelqu'un d'autre. Néanmoins, une authentification monofactorielle solide peut être beaucoup plus fiable qu'une authentification multifactorielle faible. Dans d'autres situations, comme la vérification de l'âge d'une personne qui entre dans un bar, le dommage que pourrait entraîner une authentification faible serait moins grave.

[8] [Traduction] « L'authentification monofactorielle garantit que la personne possède quelque chose qui est associée à l'identificateur utilisateur et qui n'est pas facilement accessible. Cela peut être une chose que l'utilisateur sait (p. ex., un mot de passe ou une clé cryptographique), un chose qu'il a (p. ex., une carte à puce) ou une chose qu'il est (p. ex., un identificateur biométrique de l'utilisateur). [...] Afin de renforcer le processus d'authentification de l'identité, plusieurs méthodes d'authentification monfactorielle peuvent être combinées pour donner une authentification multifactorielle. » Voir : *Encyclopedia of Privacy* [deux volumes], William G. Staples (éd.), ISBN: 0-313-33477-3, Greenwood Press.

En règle générale, les authentificateurs n'offrent pas tous le même degré de certitude concernant l'identité d'une personne ou l'autorisation qu'elle a de faire quelque chose. Un passeport est généralement (selon la fiabilité du délivreur) une meilleure preuve d'identité que la carte de membre d'un club sportif. En effet, la personne qui demande un passeport doit fournir plusieurs authentificateurs, dont la combinaison constitue une preuve d'identité solide. Pour aider à prouver son identité, elle doit présenter les éléments d'information suivants :

- Un document officiel qui atteste sa naissance au Canada ou sa citoyenneté canadienne (par exemple un certificat de naissance d'une province canadienne ou un certificat de citoyenneté);
- Au moins un autre document, comme un permis de conduire, une carte d'assurance-maladie, une autre carte d'identification provinciale, un certificat de statut d'Indien ou une carte d'identité pour les prestataires de la sécurité de vieillesse;
- Deux photos identiques, l'une signée par un répondant attestant que la photo est bien celle du demandeur;
- La déclaration d'un répondant qui a connu le demandeur au moins deux ans et qui certifie l'exactitude de l'information fournie par ce dernier.

Un criminel très futé peut quand même réussir à obtenir un passeport de manière frauduleuse en dépit des preuves rigoureuses exigées. La preuve de citoyenneté canadienne (le certificat de naissance, par exemple) et l'autre pièce d'identification, comme le permis de conduire, peuvent être des faux (comme c'est trop souvent le cas). Pour se fier à une procédure d'identification, il faut être certain de l'intégrité des documents appelés documents « sources » ou « justificatifs », utilisés comme authentificateurs. Essentiellement, l'étude d'une demande de passeport est fondée sur une preuve d'identité potentiellement imparfaite, puisqu'il est possible d'obtenir frauduleusement un permis de

conduire et un certificat de naissance. Néanmoins, l'exigence de plusieurs de ces documents potentiellement imparfaits (en plus de la certification du répondant) rend plus difficile l'obtention frauduleuse d'un passeport, car le fraudeur doit se procurer une multitude de faux authentificateurs : les documents et l'attestation, pas seulement un ou deux.

En revanche, la demande d'adhésion à un club sportif n'exige la présentation que de très faibles authentificateurs — peut-être un nom et une adresse. (Certains font valoir que l'indication d'un nom ne constitue pas un authentificateur, mais simplement l'affirmation d'une identité.)

Si elle avait le choix, une entreprise qui doit vérifier l'identité ou les attributs de ses clients serait mieux avisée de se fier à leur passeport plutôt qu'à une simple carte de membre. Cependant, ces personnes se rebelleraient probablement contre l'intrusion dans leur vie privée qu'entraînerait la présentation du passeport, car celui-ci permettrait à l'entreprise d'obtenir des renseignements potentiellement délicats, comme le pays de naissance ou la nationalité. Le numéro de passeport fournit aussi un identificateur qui peut aider à relier d'autres renseignements personnels, et constituer ainsi une menace à la vie privée.

En se fiant à un nombre insuffisant de preuves pour établir avec certitude une identité, une autorisation ou un droit, une organisation ou une personne se rend plus vulnérable à une fraude ou à d'autres dommages. Logiquement, le degré de certitude requis devrait varier en fonction de l'importance accordée à l'objectif visé. Par exemple, l'exploitant d'une installation nucléaire voudra savoir avec une très grande certitude que la personne qui entre dans son bâtiment est un des employés autorisés, tandis qu'une société de transport en commun ne s'expose qu'à une perte mineure lorsqu'elle se fie à une allégation concernant le droit à une réduction pour étudiants.

Limites de l'authentification de l'identité pour accroître la sécurité

On fait parfois grand cas de la nécessité de porter sur soi des pièces d'identité pour accroître la sécurité nationale ou contrôler le crime. C'est l'un des arguments utilisés par de nombreux pays pour appuyer la création d'une carte d'identité nationale. *Cependant, une preuve d'identité dit peu sur la fiabilité d'une personne.* En donnant une preuve de son identité, une personne montre simplement qu'elle est bien qui elle dit être, mais rien n'y indique que cette personne est ou non un criminel ou un terroriste.

L'authentification peut faire partie de la procédure destinée à établir la fiabilité d'une personne seulement si elle permet, par exemple, de vérifier si son nom apparaît ou non dans une banque de casiers judiciaires. Néanmoins, cette mesure ne permet pas d'identifier les personnes qui ont commis des crimes sans avoir été pris ou identifiés par la police, ni celles qui ont l'intention d'en commettre. Le fait de demander à un passager d'un transporteur aérien de montrer un passeport ou un permis de conduire n'aide pas à déterminer s'il transporte ou non un dispositif explosif. Pour avoir la certitude qu'un passager n'en transporte pas, il faut le fouiller.

Il existe une solution qui protège la vie privée. La technologie permet de présenter directement des « justificatifs » qui établissent, le cas échéant, le lien avec un casier judiciaire par exemple, sans que les personnes aient à révéler d'autres renseignements.

Protéger la vie privée avec des identificateurs impossibles à corréler

Les processus d'identification peuvent nettement faciliter la compilation exhaustive de dossiers sur une personne. Parfois, on n'est pas libre de décider

ce qu'on présente ou non comme preuve d'identité. Pour obtenir un passeport, on doit divulguer son lieu, son pays et sa date de naissance. Pour obtenir un permis de conduire, un particulier doit divulguer sa date de naissance et son adresse. Pour obtenir un prêt bancaire, on doit présenter des renseignements comme son nom, son numéro d'assurance sociale et, peut-être, le nom de son employeur et son salaire.

En d'autres circonstances, on peut choisir les identificateurs qu'on présente. Par exemple, on peut créer[9] soi-même son nom d'utilisateur personnel pour s'identifier auprès d'un groupe de discussion en ligne.

Bref, au-delà des identificateurs qu'on est parfois obligé de divulguer, on peut être sélectif dans ce qu'on divulgue aux autres. On peut choisir son nom d'utilisateur sur Internet et un autre nom pour s'inscrire à un club de lecture. On peut varier les identificateurs, selon les situations.

En minimisant le nombre d'identificateurs qu'on divulgue et en les variant, on fait en sorte qu'il est plus difficile d'établir des liens entre les renseignements que peuvent détenir différentes organisations sur soi. Par exemple, une banque peut avoir le numéro de compte d'une personne, mais pas son numéro de passeport. Un inspecteur de l'Agence des services frontaliers du Canada (ASFC) peut avoir son numéro de passeport, mais pas son numéro de compte bancaire. Le seul moyen de lier les données de leurs deux dossiers serait d'avoir accès aux deux numéros, celui du passeport et celui du compte, mais il n'y a pas d'« identificateur commun » qui permette de relier les renseignements d'un dossier à ceux de l'autre dossier.

La banque et l'ASFC pourraient essayer d'utiliser le nom de la personne pour faire le lien entre les renseignements qu'ils détiennent, mais l'emploi de ce seul

[9] Certains auteurs qualifient le processus de création d'un identificateur particulier dans un contexte donné d'autoproduction d'un identificateur (self generating).

élément d'information présente un haut risque d'erreurs dans le couplage de données. Coupler les données de deux dossiers séparés sur une personne à partir du nom (« Jean Tremblay ») est risqué, car les deux dossiers pourraient ne pas renvoyer à la même personne. Les informations du dossier combiné perdraient toute fiabilité et deviendraient, de ce fait, inutiles.

Par contre, si la banque et l'ASFC détiennent toutes deux le numéro d'assurance sociale de la personne, cet identificateur commun des deux banques de données rendrait le couplage des renseignements très simple. C'est dans ce contexte que les identificateurs communs menacent grandement la vie privée. (Les lois et les politiques gouvernementales pourraient limiter ce genre de couplage des banques de données, mais nous nous contentons ici de parler des aspects techniques des identificateurs communs.)

Certains lecteurs s'interrogent peut-être sur l'utilité d'archiver séparément les renseignements détenus par les différents ministères et organisations (certaines personnes parlent d'une classification des renseignements personnels dans différents « silos »). Cependant, si les dossiers sont archivés séparément, c'est pour une raison importante : empêcher les gouvernements et le secteur privé de compiler des dossiers exhaustifs sur les personnes. Ce genre de dossiers est le propre des régimes autoritaires et n'existe guère dans les sociétés démocratiques, du moins, jusqu'à maintenant. Les dossiers exhaustifs violent aussi un des éléments clés du droit à la vie privée dans les sociétés démocratiques, c'est-à-dire le droit qu'on a d'exercer un contrôle sur les renseignements rendus accessibles à d'autres.

Protéger la vie privée avec des « symboles réservés au porteur »

On peut protéger encore davantage ses renseignements personnels par un système de « symboles réservés au porteur ». Par exemple, un organisme gouvernemental peut délivrer une carte (un « symbole ») autorisant le détenteur

à recevoir des soins de santé couverts par la province. Les symboles peuvent être conçus de manière à ce que seul le détenteur légitime puisse obtenir les services. Ils peuvent aussi être conçus de manière à ce que les services obtenus grâce à eux ne puissent être liés au dossier du détenteur. Autrement dit, le détenteur du symbole conserverait son anonymat dans le système de soins de santé et il serait impossible de le surveiller et d'établir son profil d'utilisateur. Bien entendu, dans plusieurs cas, il serait sans doute avantageux pour une personne d'être identifiée dans le système de soins de santé, puisque le système pourrait alors être utilisé afin d'extraire d'autres renseignements à son sujet, lesquels seraient potentiellement utiles au moment de la soigner. Toutefois, la personne déciderait de participer ou non à un système qui permettrait de consulter de tels renseignements et de les lier à une personne.

Comme on l'a souligné ci-dessus, le permis de conduire pourrait également être structuré comme un « symbole » qui certifierait le droit de conduire, mais ne permettrait pas à la personne qui examine le symbole d'accéder à d'autres renseignements et donc de suivre les déplacements du conducteur. Des renseignements autres que la simple démonstration du droit de conduire seraient divulgués à la police seulement si cette dernière avait un besoin légitime d'obtenir des renseignements additionnels au sujet du conducteur ou de suivre ses déplacements.

Il peut néanmoins y avoir des raisons légitimes de vouloir lier les particuliers aux services qu'on leur fournit. Les gouvernements et les entreprises pourraient prouver la nécessité pour eux de suivre les interactions des personnes avec eux. Cependant, dans la plupart des situations, les gens honnêtes n'ont pas besoin de divulguer leurs vrais noms de prime abord. Par exemple, dans le cas d'un permis de conduire, on pourrait demander au conducteur de « divulguer » son vrai nom seulement si des soupçons pèsent sur lui. Une autre preuve d'identité pourrait être utilisée à cette fin.

Conclusion

Jusqu’ici cette étude a expliqué certains aspects fondamentaux des systèmes d’identité. On y a démontré que la manière de gérer les identités peut avoir des incidences notables sur la vie privée. Dans la section suivante, on examinera ce qu’il faut faire pour gérer les identités de manière à protéger la vie privée, tout en répondant aux besoins légitimes des gouvernements, des entreprises et des particuliers en matière d’identité, d’autorisation et d’admissibilité.

Qui s’intéresse à l’identité?

Les gouvernements, les entreprises commerciales et les particuliers ont tous un intérêt, parfois opposé, dans les politiques, les technologies et les lois qui sous-tendent l’identité. Nous traitons dans cette section de certains de ces intérêts qui motivent les manières parfois distinctes qu’ont ces groupes d’aborder les questions d’identité.

Les gouvernements

Les gouvernements ont l’obligation d’offrir de nombreux services aux citoyens et de les protéger contre d’éventuels actes nuisibles. Ils fournissent des services de soins de santé et d’autres programmes sociaux, ils protègent les personnes contre la violence ou d’autres activités criminelles, comme la fraude ou le vol.

Aujourd’hui, les préoccupations en matière de sécurité nationale concernent surtout la crainte d’attaques terroristes. Les gouvernements étudient de nouveaux systèmes d’identification pour rehausser la sécurité, comme un système reposant sur une carte d’identité nationale.

De plus, les gouvernements pourraient être forcés de se pencher sur les questions d’identité pour répondre aux exigences d’autres gouvernements. Les Canadiennes et Canadiens qui voyagent à l’étranger sont habituellement tenus de présenter un passeport où sont inscrits leur nom, et leur date et pays de naissance. Le Canada doit accepter ces exigences s’il veut permettre à ses citoyens de voyager à l’étranger. Pour ce faire, le Canada doit élaborer des processus de vérification de l’identité – dans ce cas, la demande de passeport – qui prouve l’identité du détenteur de passeport de manière à satisfaire les gouvernements étrangers.

Les gouvernements ont aussi la responsabilité de fournir des documents qui confirment le droit à des services, comme les soins de santé, ou l'autorisation de faire une certaine activité, comme de conduire.

De toute évidence, les gouvernements doivent participer à plusieurs aspects de la gestion de l'identité. Leurs rôles ne se limitent toutefois pas à l'élaboration de meilleures pratiques pour identifier leurs ressortissants au nom de la sécurité nationale ou pour mieux administrer les programmes gouvernementaux. Le droit de vote est un bon exemple. L'administration publique doit en effet être capable de distinguer les électeurs pour veiller à ce qu'aucun ne vote plus d'une fois, mais elle doit en même temps respecter sa vie privée (en l'occurrence, son anonymat). Les gouvernements doivent aussi respecter et protéger les droits élémentaires de la démocratie, y compris le droit à la vie privée. Ainsi, la volonté d'un gouvernement d'obtenir des assurances plus efficaces de l'identité de la personne avec qui il traite (ou qu'il veut surveiller) entre en conflit avec l'obligation du gouvernement de respecter la vie privée des personnes.

Les entreprises

De nombreuses entreprises souhaitent vérifier l'identité des personnes avec qui elles font affaire pour s'assurer qu'il ne s'agit pas d'imposteurs. Par exemple, une banque ne voudra pas accorder un prêt hypothécaire à une personne qui a « volé » l'identité d'une autre et qui prétend être cette personne. Les entreprises voudront aussi s'assurer que les moyens utilisés par leurs clients pour payer sont légitimes. Autrement dit, elles voudront vérifier si l'utilisateur d'une carte de crédit ou de débit est bien autorisé à l'utiliser. Enfin, bon nombre d'entreprises veulent en savoir davantage sur les consommateurs (leurs préférences, leurs styles de vie et leurs revenus, par exemple) pour mieux cibler leur marketing auprès des consommateurs.

Les personnes

Les personnes sont avant tout soucieuses de protéger leur vie privée et de surveiller les informations à leur sujet auxquelles les autres ont accès. Ce besoin a d'importantes conséquences sur la gestion de l'identité, parce que les personnes voudront des politiques de gestion de l'identité qui protègent leur vie privée et leur anonymat.

Les personnes voudront s'assurer que les systèmes de gestion de l'identité n'exigent pas d'elles qu'elles communiquent des renseignements personnels, de façon déraisonnable ou superflue, qui pourraient ensuite servir à établir leur profil. La plupart d'entre elles souhaitent simplement limiter l'intrusion dans leur vie privée au minimum absolument nécessaire pour permettre le fonctionnement normal de la société et jouer leur rôle dans cette société. Ainsi, dans leurs relations avec les organisations commerciales, de nombreuses personnes refusent d'adhérer à des systèmes d'identité (cartes de crédit ou cartes de fidélité, par exemple) qui permettraient aux organisations commerciales d'établir leur profil et de les cibler dans des campagnes de marketing.

Il peut arriver aussi que les personnes veuillent éviter que des organisations commerciales ou gouvernementales obtiennent des renseignements permettant de les identifier. C'est pourquoi certaines personnes paient leurs achats en argent comptant. Autrement dit, elles veulent être libres de choisir les identificateurs qu'elles fournissent à autrui et avoir accès à l'éventail de possibilités qui leur permet d'exercer cette liberté, comme la possibilité de protéger leur anonymat, dans certains cas.

Les personnes souhaitent aussi éviter l'exclusion sociale qui peut découler de leur refus d'utiliser certaines formes d'identification, comme une carte d'identité nationale ou une carte de crédit. En effet, le refus d'utiliser ce type de cartes peut faire naître des soupçons et peut même entraîner un refus de l'accès à certains services ou un traitement discriminatoire.

Les personnes visent aussi à se protéger contre le vol de leur identité. Le vol d'identité implique qu'une personne usurpe l'identité d'une autre dans un contexte précis pour se faire passer pour cette dernière, ce qui pourrait permettre à des criminels d'avoir accès à certains services. Par exemple, un voleur d'identité peut tenter :

- de faire des achats avec des cartes de crédit d'autrui ou d'obtenir des prêts avec le nom d'autres personnes;
- d'établir des relations avec le gouvernement (par exemple, pour obtenir des avantages sociaux ou se procurer un passeport);
- de commettre des actes dommageables au nom d'une personne – comme dans le cas d'un ex-conjoint vindicatif qui envoie des courriels de bêtises au nom de son ancien partenaire.

Les voleurs d'identité peuvent aussi commettre des crimes et utiliser l'identité d'un innocent s'ils sont arrêtés et condamnés. L'innocent risque alors d'être obligé de prouver qu'il n'est pas l'auteur du crime, ce qui est presque impossible.

Le vol d'identité n'est pas seulement un problème théorique. Pendant les premières semaines de 2007, certaines organisations commerciales ont perdu les renseignements personnels de centaines de milliers de Canadiennes et de Canadiens, les rendant ainsi vulnérables au vol d'identité. Aussi, des fraudeurs (par une ruse qu'on appelle le faux-semblant) peuvent parfois se faire passer pour d'autres et appeler des établissements financiers afin d'obtenir d'eux des renseignements personnels sur une personne qui leur permettent ensuite de voler l'identité de cette personne.

Comme notre société devient de plus en plus informatisée, les risques de vols d'identité par hameçonnage (version en ligne du faux-semblant expliqué précédemment) augmentent.

Afin de réduire les risques de vol d'identité, les personnes doivent pouvoir profiter de mesures de sécurité. Le niveau de sécurité fourni par ces mesures varie. Une carte de crédit offre une certaine sécurité, car la signature du propriétaire légitime se trouve à l'endos de la carte. Lorsqu'une personne signe une facture de crédit, le commis doit comparer les deux signatures. Le numéro d'assurance sociale à lui seul n'est pas un identificateur protégé, car n'importe qui peut l'utiliser. La carte du numéro d'assurance sociale offre un certain niveau d'authenticité, mais il n'y a pas encore de moyen sûr de vérifier que la personne qui a la carte et qui en utilise le numéro est bien le détenteur légitime. Une carte fournie par une source fiable et présentant une photographie du détenteur constitue une meilleure protection.

De même, afin de participer à bon nombre des activités de la société, les particuliers ont besoin des gouvernements qu'ils leur fournissent des documents fiables qui certifient leur identité, comme des passeports et des certificats de naissance. La société a aussi établi que les justificatifs sont importants pour son fonctionnement – par exemple, des documents fiables qui prouvent l'admissibilité (p. ex. aux soins de santé) ou l'autorisation (p. ex. le droit de conduire). Cependant, les personnes souhaitent éviter que les gouvernements, par leurs systèmes d'identité, procèdent à une surveillance inappropriée.

Tout comme les entreprises et les gouvernements qui veulent vérifier l'identité des personnes, celles-ci veulent pouvoir vérifier l'identité des organisations avec lesquels elles traitent. On parle dans ce cas d'« authentification réciproque ». En effet, l'authentification de ses interlocuteurs par la personne peut réduire le risque de faux-semblant et d'hameçonnage.

Intérêts communs et conflictuels de la gestion de l'identité

Parce que les intérêts de ces trois groupes – les personnes, les entreprises et les gouvernements – en matière de gestion de l'identité divergent, des différends les opposent sur les meilleures politiques de gestion de l'identité.

Intérêts conflictuels

Pour les personnes, la principale source de conflits découle des intrusions à la vie privée que certains systèmes d'identité entraînent et de l'absence de retombées qui justifient ces intrusions. Le conflit concerne deux aspects : le droit à la vie privée qu'il faut céder et dans quelle mesure pour mettre en œuvre un nouveau système d'identité et, la nécessité véritable et inéluctable de céder ce droit pour obtenir les retombées prévues? Dans certains cas, les avantages sont tellement marginaux que même le moins envahissant des systèmes d'identité n'en vaut pas la peine. Les gens peuvent apprécier les avantages des systèmes d'identité, tant sur le plan individuel que pour la société dans son ensemble, mais veulent aussi que ces systèmes soient le moins envahissants possible.

Les personnes craignent surtout que certains systèmes d'identité – cartes d'identité nationales ou numéros d'assurance sociale (NAS), par exemple – entraînent le couplage de données et l'établissement de profils à grande échelle, tant par les gouvernements que par le secteur privé, qui pourront ensuite recueillir des renseignements sur une personne à partir d'autres banques de données, et ce, grâce aux « identificateurs communs » que sont les numéros d'assurance sociale ou les numéros de cartes d'identité.

Avant l'avènement de l'informatique, la recherche et le couplage des renseignements personnels de différents systèmes d'archivage exigeaient beaucoup de travail. Cela permettait d'assurer un niveau assez élevé de protection des personnes dont les renseignements personnels seraient conservés dans des systèmes séparés. C'était le cas même s'il y avait un identificateur commun, comme le numéro d'assurance sociale, utilisé en tant

qu'indice d'archivage dans chacun des systèmes. Cette protection a complètement disparu depuis l'avènement des dossiers numériques qu'on peut maintenant extraire instantanément, par voie électronique, de différentes banques de données si un identificateur commun est utilisé pour classer les données saisies.

Les personnes peuvent aussi être rebutés par la quantité de preuves d'identité – le nombre d'identificateurs et de pièces d'identité et de documents justificatifs – à fournir parfois pour traiter avec le gouvernement ou certaines entreprises.

À l'inverse, les gouvernements et les entreprises exigent habituellement plus de renseignements personnels sur les personnes que ceux dont ils ont vraiment besoin, et ce, même s'il n'y a aucune raison clair ou justifiée de le faire, à moins que leur curiosité ne soit entravée par la loi, les politiques ou les technologies.

Intérêts communs

Les intérêts des personnes et des entreprises en matière de gestion de l'identité ne sont pas toujours conflictuels. Les deux groupes veulent éviter les opérations frauduleuses. Par exemple, afin d'éviter la fraude par carte de crédit, les deux groupes peuvent être favorables à des mesures semblables – un NIP (numéro d'identification personnel) sur une carte de crédit, ou une procédure de vérification de l'identité en ligne, par exemple. Cependant, même s'ils s'entendent sur les besoins de sécurité, ils peuvent ne pas s'entendre sur les moyens de préserver cette sécurité.

Les personnes et les gouvernements peuvent aussi s'accorder sur certains aspects de la gestion de l'identité. En théorie, aucun de ces deux groupes ne souhaite que des personnes inadmissibles aux services sociaux y aient accès. En théorie, les deux groupes veulent éviter les pratiques qui violent les droits de la personne. Ils désirent tous deux que les gouvernements fournissent des

documents fiables et sûrs qui authentifient leur statut au besoin – en tant que citoyens canadiens, conducteurs autorisés ou résidents ayant droit aux soins de santé couverts par l'État.

Les entreprises et les gouvernements s'intéressent tous deux aux possibilités supérieures de surveillance qu'offrent certaines formes de gestion de l'identité – les identificateurs communs, par exemple – car ceux-ci contribuent à corréler et à coupler des renseignements personnels détenus dans différents dossiers. La gestion de l'identité peut aussi aider les entreprises à retracer les fraudeurs.

Chacun des trois groupes – les personnes, les entreprises et les gouvernements – cherchent à prévenir l'hameçonnage. Celui-ci se produit, par exemple, quand une personne envoie à une autre un courriel frauduleux qui semble provenir de la banque de ce dernier. Dans ce courriel, on incite la personne à visiter un site Web dont l'apparence porte à croire qu'il s'agit en effet du site de la banque. Sur ce faux site, on demande à la personne de saisir ses mots de passe et ses numéros de compte. Si la personne tombe dans le panneau et fournit les renseignements demandés, le fraudeur met la main sur les renseignements dont il a besoin pour accéder au compte bancaire de la personne.

En raison des menaces à la sécurité que constitue l'hameçonnage, par exemple, les personnes veulent avoir la certitude qu'ils traitent avec leur vraie banque et non un fraudeur.

Les particuliers qui téléchargent des mises à jour pour leurs programmes antivirus sur leurs ordinateurs veulent être sûres que la source du téléchargement est légitime, pour éviter de télécharger involontairement un logiciel qui pourrait endommager leurs fichiers ou chercher leurs mots de passe et leurs numéros de compte sauvegardés sur leur ordinateur. Les personnes qui reçoivent des messages de la part d'un organisme gouvernemental veulent être

sûres que ceux-ci ne proviennent pas d'un fraudeur. Bref, les personnes ont des droits légitimes d'exiger l'authentification des organisations avec lesquelles elles font affaire avant de fournir leurs renseignements personnels.

Même si les personnes, les entreprises et les gouvernements ont des intérêts communs en matière de gestion de l'identité, ces intérêts ne revêtent pas la même importance pour les uns et les autres. Les gouvernements pourraient être tentés d'imposer des mesures de sécurité plus strictes que ce que leurs citoyens sont prêts à tolérer, comme par la voie de cartes d'identité.

Repenser la gestion de l'identité pour mieux protéger la vie privée

Faire table rase pour mieux étudier les systèmes d'identité

Pour examiner la gestion de l'identité, on peut adopter deux points de vue :

- On peut supposer que les moyens utilisés à l'heure actuelle pour prouver l'identité, l'autorisation ou l'admissibilité sont acceptables du point de vue de la vie privée. Cette position signifie qu'on accepte *a priori* les processus d'identification parce que c'est ainsi que les choses se sont toujours faites. Du coup, on étudierait (peut-être par ce qu'on appellerait une « évaluation des facteurs relatifs au système d'identité ») seulement les propositions qui présenteraient de nouveaux moyens de gérer l'identité, comme un système de carte d'identité nationale ou un système de carte pour traverser la frontière;

- On pourrait aussi recommencer à neuf et étudier toutes les situations où l'identité est en cause, y compris les situations où l'identité ou l'autorisation sont déjà établies d'une certaine manière, comme avec la délivrance de permis de conduire qui affichent le nom, l'adresse et l'âge. On ne tiendrait pas pour acquis le fait que, parce qu'on a utilisé une certaine méthode de gestion de l'identité par le passé, cette méthode est encore appropriée (surtout en raison de la transposition des processus sur support papier à des processus électroniques). Les méthodes appropriées pour prouver l'identité, l'autorisation ou l'admissibilité pourraient s'avérer très différentes de celles utilisées à l'heure actuelle. Si on décidait de repartir à neuf, il faudrait évaluer les conséquences sur la vie privée de toutes les méthodes de gestion de l'identité, tant nouvelles qu'actuelles.

Ce dernier choix exigerait qu'on repense tous les processus de gestion de l'identité utilisés, mais permettrait aussi d'élaborer de nouveaux modèles acceptables, tant du point de vue de la vie privée que des politiques. Il nous permettrait également de repenser les modèles passés de gestion de l'identité et de les évaluer par rapport aux objectifs de protection de la vie privée et d'autres politiques publiques, comme le fait de minimiser la quantité de renseignements personnels qu'il est nécessaire de divulguer pour continuer ses activités normalement et légalement. Ces modèles respectent-ils le mieux possible la vie privée tout en servant les autres intérêts légitimes, comme ceux des gouvernements qui doivent protéger leurs citoyens, ceux des entreprises qui veulent prévenir la fraude et ceux des personnes qui souhaitent éviter d'être victimes de fraude ou de vol liés à l'utilisation non autorisée de leur identité?

Le fait de faire table rase permettrait aussi d'éviter que les organisations gouvernementales et les entreprises poursuivent ou rehaussent leur utilisation des méthodes d'identification existantes (comme le fait d'exiger le numéro d'assurance sociale), qui peuvent parfois entraîner de graves intrusions dans la vie privée.

Établir les paramètres de protection de la vie privée dans la gestion de l'identité

Une démocratie qui dit valoriser l'autonomie et la vie privée doit limiter les situations où une personne doit s'identifier et la quantité de renseignements exigés de cette personne pour qu'elle participe à la vie en société. En outre, les politiques sur l'identité doivent tenir compte des besoins légitimes des gouvernements et du secteur privé d'avoir des renseignements sur les particuliers pour permettre de traiter avec ceux-ci, de leur offrir des services ou d'administrer des programmes pour eux.

Certains lecteurs peuvent s'interroger sur le besoin de repenser les moyens utilisés à l'heure actuelle pour prouver l'identité, l'autorisation ou l'admissibilité. Cependant, notre société possède des outils de plus en plus sophistiqués qui permettent une surveillance exhaustive, caractéristique des sociétés autoritaires. Nous sommes fortunés d'avoir des gouvernements qui, en règle générale, respectent nos droits, mais pas plus les Canadiennes et les Canadiens que les citoyens de n'importe quel pays démocratique ne doivent tenir pour acquis le rejet des méthodes autoritaires par leurs gouvernements. C'est pourquoi nous devons accorder une attention particulière aux types de surveillance accessibles aux gouvernements, y compris la surveillance facilitée par les systèmes d'identité actuels et possibles.

Par ailleurs, les Canadiennes et les Canadiens doivent aussi se pencher sur les incidences de l'identité sur la vie privée dans leurs relations avec le secteur privé. Le fait de limiter les types de surveillance accessibles aux gouvernements limite aussi, du coup, les possibilités de surveillance par l'intermédiaire de la gestion de l'identité par le secteur privé. En effet, les renseignements recueillis par le secteur privé dans le cadre de ses activités de surveillance peuvent facilement et légalement[10] tomber aux mains d'un gouvernement curieux. Ainsi, la collecte de renseignements personnels par le secteur privé peut contribuer à la surveillance exercée par les gouvernements.

Le droit à l'anonymat comme point de départ : Bon nombre de personnes sont probablement d'accord pour dire que le simple fait de marcher dans la rue ne justifie pas de devoir prouver son identité à un policier ou à un autre agent de l'État, sauf pour une raison justifiable. Elles seraient aussi probablement d'avis qu'elles devraient avoir la possibilité d'utiliser de l'argent comptant pour protéger leur anonymat lorsqu'elles achètent des produits d'épicerie ou prennent

[10] Voir, par exemple, le paragraphe 7(1) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*), L.C. 2000, c. 5 qui permet aux organisations de recueillir et de communiquer des renseignements personnels au gouvernement à l'insu des personnes concernées dans certaines circonstances.

l'autobus. On serait sans doute nombreux à affirmer que le droit à l'anonymat devrait être la norme, à moins d'une raison valable d'exiger des personnes qu'elles s'identifient. Le droit à l'anonymat est certainement le plus important de nos droits et on ne devrait pouvoir le bafouer que pour des raisons justifiables. Et même dans ce cas, on ne devrait pas exiger de divulguer ou de partager plus que les renseignements personnels minimaux nécessaires. Une personne peut évidemment décider de partager des renseignements sur son identité avec d'autres, mais il s'agit là d'un choix personnel qui n'a rien à voir avec une exigence du gouvernement ou d'une entreprise ou la conséquence inévitable d'une technologie et d'un système d'identité qui permettent d'obtenir des renseignements sur une personne.

L'anonymat par l'utilisation de « symboles » : Si l'anonymat reste l'état *par défaut* des personnes, l'authentification par le recours de symboles (ou par « symboles réservés au porteur ») est un moyen essentiel de préserver cet anonymat. Le billet d'autobus est un « symbole » d'une faible technicité. Les technologues ont élaboré des « symboles » électroniques plus sophistiqués qui permettent également aux personnes qui les utilisent de protéger leur anonymat.

Que cela signifie-t-il en pratique? Cela signifie que les personnes pourraient vaquer à leurs occupations de manière anonyme, sans laisser de traces pouvant mener à des renseignements sur leur identité. Le fait de payer ses achats en argent comptant est une forme de préservation de l'anonymat à faible technicité. Le paiement de biens par carte électronique prépayée est une version à haute technicité qui ne laisse aucune information permettant de lier l'achat à la personne. Dans les deux cas, l'acheteur reste anonyme. À l'inverse, pour les achats par carte de crédit, le marchand a accès au nom du détenteur de la carte et la société de crédit conserve un relevé des achats, ce qui permet de faire un suivi et d'établir le profil de l'acheteur.

De même, l'utilisation du permis de conduire comme preuve d'âge à l'entrée d'un bar peut favoriser le développement d'un réseau de surveillance autour des personnes qui souhaitent simplement prouver qu'elles sont majeures. Ce type de surveillance est tout à fait injustifié pour la majorité des gens qui mènent leurs activités quotidiennes dans la légalité. La solution de rechange favorisant l'anonymat est la délivrance d'une carte (d'un « symbole ») avec la photo du jeune détenteur par une organisation fiable, comme une organisation gouvernementale, qui certifie que le détenteur est majeur. Cette solution peut ne pas plaire aux propriétaires de bar qui souhaitent en savoir le plus possible sur leurs clients pour des raisons de marketing, mais elle protège l'anonymat des clients en leur permettant de décider ce qu'ils divulguent au propriétaire du bar et aux entreprises connexes.

Dans une installation nucléaire, une carte d'accès pourrait, par exemple, contenir des informations biométriques, comme les empreintes digitales. Le détenteur de la carte pourrait alors placer son doigt sur un appareil de lecture qui comparerait l'empreinte avec celle de la carte. Si elles étaient identiques, la personne aurait l'autorisation d'entrer sur les lieux. Aucun renseignement supplémentaire sur la personne n'aurait besoin d'être exigé par l'agent de sécurité (par contre, des renseignements supplémentaires seraient nécessaires au moment de la délivrance de la carte et il faudrait aussi vérifier la fiabilité de la personne avant de lui accorder la carte).

Les obligations d'authentifier doivent être proportionnelles aux circonstances : Dans les situations où il est justifié pour les gouvernements et les entreprises de refuser l'anonymat, les personnes doivent prouver leur identité.

Le critère de proportionnalité est fondamental. Il est nécessaire d'établir des limites sur les types et sur l'étendue des preuves exigées. Le niveau de certitude requis sur l'identité ou les attributs d'une personne devra correspondre au

minimum nécessaire pour atteindre les objectifs légitimes d'identification ou d'autorisation. Un étudiant qui souhaite se procurer un billet d'autobus à tarif réduit ne devrait pas être obligé de fournir son numéro d'assurance sociale, des informations biométriques et un permis de conduire en plus de sa carte d'étudiant. Cependant, le niveau de certitude requis pour l'employé d'une installation nucléaire est nécessairement plus élevé, car les conséquences d'une entrée non autorisée sur les lieux pourraient être graves. Par exemple, avec le nom du candidat à l'emploi, l'employeur peut vérifier s'il a ou non un casier judiciaire. Les renseignements que l'employeur obtient sur les études faites par le candidat lui permettent de s'assurer que celui-ci a les qualifications requises pour travailler dans l'industrie nucléaire.

Il faut tenir compte du fait qu'une méthode d'authentification solide ne révèle pas nécessairement plus de renseignements sur la personne qu'une méthode d'authentification faible. Il est possible de procéder à une authentification solide tout en exigeant très peu de renseignements personnels.

La divulgation sélective des identificateurs : L'anonymat protège la vie privée, mais il n'est pas toujours possible ou souhaitable. Dans les situations où l'anonymat n'est pas approprié, la meilleure solution est de permettre aux personnes d'utiliser différents identificateurs pour différents types d'opérations ou d'interactions. Ces identificateurs doivent être structurés de manière à ne pas permettre de corrélation entre eux. Ces identificateurs impossibles à corréler découragent les tentatives de lien entre les renseignements associés à ces opérations et à ces interactions archivées dans différentes banques de données. C'est ainsi que le monde fonctionne dans une large mesure et depuis longtemps.

Si différentes organisations utilisent des identificateurs distincts, chacune d'entre elles peut difficilement corréler les renseignements qu'elle détient sur une personne. De toute évidence, il lui est quand même possible de corréler des renseignements en fonction d'« attributs » comme le nom et l'adresse, mais

l'utilisation d'identificateurs différents réduit énormément la possibilité de faire le lien entre les renseignements de différentes banques de données. Comme les organisations ne sont pas toutes soucieuses de préserver la vie privée des personnes sur lesquelles elles détiennent des renseignements, il peut être nécessaire d'adopter des mesures qui découragent la collecte d'identificateurs communs qui permettent de corréler les renseignements personnels des différentes banques de données. Il faut aussi se rappeler que de nombreuses organisations sont convaincues de protéger la vie privée, mais qu'elles parlent de « sécurité » contre les intrusions de l'extérieur et pas de l'utilisation illégitime des renseignements personnels, comme par le couplage de données, à l'interne.

L'utilisation d'une solide méthode d'authentification pour prévenir le vol d'identité : Les personnes sont très soucieuses de pouvoir obtenir des documents qui certifient leur identité ou leur droit de faire quelque chose, comme de conduire ou d'acheter des biens, mais qui soient difficiles à utiliser par d'autres de façon illégitime. On pourrait penser que les organisations voudraient elles aussi prévenir l'utilisation illégitime de documents, mais les intérêts des organisations et des personnes ne coïncident pas toujours. Dans certains cas, l'organisation (une banque, par exemple) peut tolérer une méthode d'identification ou d'autorisation déficiente, comme celle utilisée pour retirer de l'argent d'un guichet automatique. L'organisation peut tolérer ces défauts si les pertes qui en résultent sont minimes ou si elle peut les transférer aux clients par des intérêts sur les coûts de crédit ou des frais bancaires plus élevés. Les gouvernements peuvent devoir intervenir pour forcer les organisations à adopter des méthodes d'identification et d'autorisation moins vulnérables au vol d'identité.

L'avenir de la gestion de l'identité

Les rôles du Parlement et de l'administration fédérale

Protéger le droit à la vie privée : Le droit international et la *Charte canadienne des droits et des libertés* obligent le Parlement à protéger le droit à la vie privée et à l'autonomie des personnes. Le Parlement ainsi que les ministères et organismes fédéraux doivent donc éviter de prendre des mesures sur l'identité qui limitent indûment le droit à la vie privée quand d'autres mesures moins envahissantes permettent d'atteindre le même objectif.

Le Parlement devrait examiner les lois actuelles sur la protection des données – soit la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*) – pour s'assurer que ces lois ne présentent pas des lacunes qui permettent au gouvernement ou au secteur privé d'exercer une surveillance indue au moyen des systèmes d'identité actuels ou émergents. Les mesures législatives doivent également être conçues pour éviter la mise en place de systèmes d'identité trop puissants, même si cette puissance n'est pas utilisée présentement pour exercer une surveillance indue, car la simple possibilité de le faire peut représenter une tentation irrésistible pour les gouvernements futurs.

Loi sur la protection des renseignements personnels : la *Loi sur la protection des renseignements personnels* régit la collecte, l'utilisation et la communication de renseignements personnels par les institutions fédérales. Toutefois, le Commissariat à la protection de la vie privée a souvent critiqué l'inefficacité de la *Loi sur la protection des renseignements personnels* à protéger le droit à la protection de la vie privée des Canadiennes et des Canadiens dans leurs interactions avec l'administration fédérale.

Dans le contexte de la gestion de l'identité, la Loi ne comporte aucune disposition sur les identificateurs communs et le partage de renseignements personnels entre des bases de données distinctes (couplage de données). Des identificateurs communs comme le numéro d'assurance sociale ou le numéro de carte d'identité peuvent servir au couplage de données. Pourtant, la Loi n'impose aucune mesure de contrôle significative sur la collecte, l'utilisation ou la communication des identificateurs communs. Elle autorise une institution gouvernementale à recueillir des renseignements personnels s'ils ont un lien direct avec ses programmes et ses activités[11]. On n'y trouve aucune disposition stipulant que la collecte d'information doit être nécessaire ou raisonnable. De plus, la Loi permet aux institutions gouvernementales de communiquer des renseignements personnels à divers autres organismes dans un large éventail de circonstances, même sans le consentement de la personne concernée[12].

Depuis longtemps, les critiques déplorent l'absence de contrôle sur le couplage de données dans la Loi. Dans son rapport annuel au Parlement de 2004-2005 sur la Loi, la commissaire à la protection de la vie privée du Canada observait ce qui suit :

> Bien que l'usage que fait le gouvernement du couplage de données (ou « interconnexion des ordinateurs ») constitue vraisemblablement la plus grande menace à la protection de la vie privée des personnes, la *Loi sur la protection des renseignements personnels* reste silencieuse en ce qui a trait à cette pratique. Les commissaires à la protection de la vie privée (soutenus par les comités parlementaires) ont tous reconnu les dangers inhérents à la collecte excessive ou non justifiée de données. Tous ont fait la recommandation d'apporter des modifications à la *Loi sur la protection des renseignements personnels* afin de s'assurer que les institutions gouvernementales relient les dossiers personnels dans des systèmes discrets uniquement lorsqu'il est possible d'en démontrer la nécessité, et

[11] Article 4.
[12] Paragraphe 8(2).

> sous la surveillance permanente et vigilante de la commissaire à la protection de la vie privée du Canada. Ces recommandations n'ont pas été exécutées.

Dans le même rapport, on notait que le Conseil du Trésor fédéral avait émis des lignes directrices en 1989 décrivant la procédure à suivre par les ministères avant de recourir au couplage de données, y compris la présentation d'une proposition détaillée à faire approuver par la commissaire. Toutefois, le Commissariat a signalé qu'il n'avait reçu que peu d'avis, malgré la fréquence probable de cette pratique.

La *Loi sur la protection des renseignements personnels* s'applique aux institutions fédérales. L'ajout de dispositions sur le couplage de données pourrait aider à limiter la combinaison de renseignements personnels provenant de bases de données distinctes. Ainsi, même si les institutions gouvernementales utilisaient un identificateur commun comme le numéro d'assurance sociale ou un numéro de carte d'identité nationale pour indexer les dossiers des personnes, on pourrait leur interdire (à moins qu'un gouvernement futur ne modifie la Loi) de combiner les données de ces dossiers.

Certains critiques soulignent également la faiblesse des pouvoirs d'application de la *Loi sur la protection des renseignements personnels.* Même si une institution gouvernementale contrevient aux dispositions déjà faibles de la Loi, la commissaire à la protection de la vie privée n'a aucun pouvoir direct pour l'obliger à la respecter. Elle peut enquêter sur la supposée contravention et présenter ses conclusions au public et au Parlement, mais elle n'a alors que le pouvoir d'un ombudsman.

Les éléments fondamentaux de la *Loi sur la protection des renseignements personnels* sont demeurés pratiquement inchangés depuis l'entrée en vigueur de la Loi en 1983. Malgré les nombreuses recommandations pour la modifier, aucun gouvernement, depuis vingt-cinq ans, n'a entrepris de la renforcer pour mieux

protéger le droit à la vie privée des Canadiennes et des Canadiens. Compte tenu de l'intérêt que porte sans doute le gouvernement fédéral aux possibilités de surveillance offertes par certains systèmes d'identité (systèmes de carte d'identité nationale, par exemple), il semble peu probable qu'il soit intéressé à modifier la Loi de manière à limiter l'utilisation de ces systèmes. Les groupes d'intérêt publics et les organismes de protection du droit à la vie privée sont probablement les seuls intervenants capables de faire renforcer la protection des renseignements personnels.

L'omniprésence de la gestion électronique des données exigera peut-être que l'on aille au-delà d'une simple modification des dispositions de la *Loi sur la protection des renseignements personnels* pour prévenir l'utilisation inutile ou injustifiée des systèmes d'identité, tant par des personnes de l'intérieur que de l'extérieur. Cela est particulièrement vrai dans le contexte actuel du passage des systèmes d'identité traditionnels à des systèmes d'identité électroniques qui décuplent les risques d'atteinte à la vie privée.

***Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*)** : La *LPRPDÉ* protège un peu mieux le droit à la vie privée relativement à l'identité. Elle s'applique aux organisations qui exercent des activités commerciales ainsi qu'à celles qui ont d'autres buts (par exemple, l'emploi) et qui sont régies par les provinces. Par conséquent, la *LPRPDÉ* couvre le secteur de la vente au détail, de l'édition, des compagnies d'assurances, des services, de la fabrication et d'autres organisations comme dans le secteur de la santé.

L'article 3 de la Loi définit ainsi le but de ses dispositions relatives à la protection des renseignements :

> La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de

> renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[13].

Contrairement à la *Loi sur la protection des renseignements personnels*, la *LPRPDÉ* reconnaît explicitement la nécessité d'établir un équilibre entre le droit à la vie privée et celle de permettre aux organisations de recueillir des renseignements personnels. Toutefois, elle exige que les organisations recueillent, utilisent et communiquent les renseignements personnels à des fins raisonnables. Les principes énoncés en annexe de la Loi stipulent également que les organisations ne doivent pas recueillir de renseignements de façon arbitraire et qu'elles sont tenues de recueillir des renseignements personnels de façon honnête et licite[14].

En outre, les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige[15]. Cela limite l'utilisation ou la communication de renseignements personnels pour le couplage de données. À moins qu'une organisation n'obtienne le consentement explicite de la personne concernée, ses renseignements personnels ne peuvent être utilisés ou communiqués pour le couplage de données.

Toutefois, ces limites imposées à la collecte, à l'utilisation et à la communication des données ne sont pas aussi strictes qu'on pourrait le croire de prime abord. L'article 7 de la *LPRPDÉ* décrit une série de situations où les organisations peuvent recueillir, utiliser et communiquer des renseignements personnels sans le consentement de la personne concernée. Par exemple, une organisation peut

[13] Article 3.
[14] Principe 4.4.
[15] Principe 4.5.

recueillir des renseignements personnels à l'insu ou sans le consentement de la personne en vue d'une communication :

- exigée par la loi;
- à une institution gouvernementale ou à une subdivision d'une telle institution qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas, qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;
- à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et lorsque l'organisation, selon le cas, a des motifs raisonnables de croire que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales[16].

En résumé, l'article 7 permet aux organisations d'agir au nom de l'État en recueillant, sans consentement, des renseignements à la seule fin de les communiquer au gouvernement et aux organismes chargés de l'application des lois. Ainsi, une organisation assujettie à la *LPRPDÉ* peut recueillir, utiliser et communiquer des renseignements personnels tirés d'un document d'identité qu'elle n'est pas autorisée à recueillir, à utiliser ou à communiquer à ses propres fins pourvu qu'elle agisse au nom du gouvernement pour les raisons mentionnées plus haut.

Comme la *Loi sur la protection des renseignements personnels*, la *LPRPDÉ* ne donne au Commissariat aucun pouvoir direct pour faire appliquer la loi. La commissaire est un ombudsman. Toutefois, en vertu de la *LPRPDÉ*, elle peut déposer une plainte à la Cour fédérale qui, elle, a le pouvoir de faire appliquer la loi.

[16] Alinéa 7(1)*e*).

Un moyen de forcer les organisations à respecter la *LPRPDÉ* pourrait être de leur défendre, sous peine de sanction, de recueillir, d'utiliser ou de communiquer des renseignements personnels « non pertinents » qui figurent dans les documents d'identité – par exemple, un tenancier de bar qui noterait l'information inscrite sur un permis de conduire qui aurait servi à prouver l'âge d'un client. Ainsi, les organisations n'auraient pas le droit de recueillir des renseignements personnels dans les documents émis par le gouvernement afin de dresser le profil des personnes, et des sanctions seraient imposées à celles qui le feraient. La *Loi de 2004 sur la protection des renseignements personnels sur la santé*[17] de l'Ontario illustre cette approche. Elle défend à quiconque n'est pas dépositaire de renseignements sur la santé de recueillir ou d'utiliser des données sur l'état de santé d'une personne sauf dans les exceptions prévues dans la Loi. Contrevenir à cette disposition peut entraîner une amende maximale de 250 000 $[18].

Les lois sur la protection des données semblent offrir une plus grande protection contre l'utilisation malveillante des systèmes d'identité par le secteur privé que par l'administration fédérale. Toutefois, la *Charte des droits* pourrait limiter l'activité de l'administration fédérale, mais on ne pourrait l'appliquer au secteur privé.

Revoir les systèmes d'identité actuels : Le Parlement devrait également examiner la conception des systèmes d'identité actuels (par des évaluations des facteurs relatifs à la gestion de l'identité semblables aux évaluations des facteurs relatifs à la vie privée) pour établir leurs buts et voir s'ils sont justifiables. Même s'ils le sont, le Parlement devrait limiter les intrusions associées aux systèmes d'identité à ce qui est *nécessaire* pour atteindre les buts visés. En outre, les intrusions doivent être raisonnables et proportionnelles. Dans certains cas, cela

[17] L.O. 2004, chapitre 3, article 34.
[18] *Ibid.*, article 72.

peut mener le gouvernement à promouvoir ou à accepter des mesures qui permettent aux personnes de conserver l'anonymat dans certaines situations si elles le désirent.

Établir le respect de l'anonymat comme norme : Le Parlement devrait adopter des lois où le respect de l'anonymat est tenu pour acquis. Si une institution gouvernementale pouvait montrer que l'anonymat n'est pas approprié, elle devrait quand même, par des mesures juridiques ou techniques, limiter les couplages de données inappropriés et les exigences d'authentification qui portent inutilement atteinte à la vie privée. Dans de nombreuses situations où il suffit de prouver son droit à l'admissibilité ou une autorisation, les systèmes d'identité doivent être faits en conséquence et le gouvernement doit défendre ce principe. L'adoption de lois est peut-être la seule approche efficace, en particulier si elle force les organisations à tenir compte des conséquences de leurs mesures touchant l'identité sur la protection de la vie privée[19].

Défendre le droit à la vie privée dans les relations internationales : À l'échelon international, le gouvernement fédéral devrait mettre en question les exigences d'identification de gouvernements étrangers et d'organismes internationaux trop envahissantes selon les normes canadiennes de protection de la vie privée. Le gouvernement fédéral a un pouvoir d'influence limité sur les exigences d'identification imposées par d'autres gouvernements et organisations internationales, mais il ne doit pas renoncer à défendre ses valeurs relatives à la protection de la vie privée à l'échelon international.

[19] Commissariat à l'information et à la protection de la vie privée de l'Ontario et Registratierkamer des Pays-Bas, *Privacy-Enhancing Technologies: The Path to Anonymity* (volume I), août 1995 : [Traduction] « Lorsqu'on tente d'établir la nécessité d'obtenir des données identifiables dans le cadre d'une transaction, il importe de se demander la quantité de renseignements personnels (données) dont on a réellement besoin pour assurer le bon fonctionnement du système d'information utilisé pour la transaction? Il faut se poser la question dès le départ, c'est-à-dire avant la conception et l'élaboration de tout nouveau système. »

Introduire un « principe technique » : La protection de la vie privée dans la gestion de l'identité exige plus que des mesures techniques comme l'utilisation de symboles attestant que quelqu'un a reçu une autorisation (par exemple, celle de conduire une voiture) ou quelque chose (par exemple des soins de santé publics). Elle exige aussi des principes juridiques et stratégiques à l'appui de ces mesures techniques. Pour ce faire, on peut adopter un principe stipulant que les systèmes d'identité doivent fournir le moins d'information possible pour arriver aux fins justifiables. L'industrie doit porter le fardeau de la preuve de sa conformité au principe au moyen d'« évaluation des facteurs relatifs à la gestion de l'identité ».

Cela étant dit, de telles évaluations présentent des problèmes d'ordre pratique à l'heure actuelle. Il n'existe aucun processus d'assurance de la qualité pour les systèmes d'identité, comme il y en a pour d'autres domaines (ISO 9000, par exemple). Par conséquent, une organisation n'a aucun moyen de déterminer si un système d'identité particulier que lui propose un fournisseur améliore ou favorise véritablement la protection de la vie privée.

Entre-temps, un test de raisonnabilité en quatre critères pourrait être un bon moyen pour les organisations de faire face à la situation :

- A-t-on démontré que la mesure concernant l'identité était nécessaire pour combler un besoin particulier?
- La mesure comblera-t-elle ce besoin de manière efficace?
- L'intrusion dans la vie privée est-elle proportionnelle au bénéfice obtenu?
- Y a-t-il une manière d'obtenir le même résultat en faisant moins atteinte à la vie privée?

Partout dans le monde, les principes de gestion équitable de l'information qui sous-tendent les lois sur la protection des données ont été conçus à l'ère des banques de données sur papier. Des éléments importants de ces principes sont dépassés à cause des progrès technologiques survenus depuis leur adoption en

1980[20]. En particulier, les principes doivent être mis à jour en fonction d'un principe « technique » reconnaissant le pouvoir d'intrusion de la technologie et soulignant la nécessité de bien justifier la mise en corrélation des identificateurs contenus dans des bases de données distinctes. Essentiellement, cela serait une simple généralisation des mesures juridiques adoptées par de nombreux pays relativement aux numéros de sécurité sociale.

Promouvoir les solutions technologiques : Tout comme la technologie a créé la capacité d'exercer une surveillance de plus en plus étroite, elle peut limiter cette surveillance. Comme l'observe Stefan Brands,

> L'identification et la vie privée ne constituent pas des intérêts opposés à peser afin de trouver un juste équilibre : les progrès technologiques mêmes qui menacent d'annihiler la vie privée peuvent être exploités afin de préserver la confidentialité à l'ère de la numérisation[21].

Ce point de vue a aussi été exprimé dans une étude menée en 2005 au Royaume-Uni :

> [Traduction]
> Les technologies comme les justificatifs numériques, le filtrage par liste noire protégeant la vie privée, les preuves à communication minimale, les preuves sans communication d'information, le partage secret et la récupération de renseignements personnels peuvent servir à élaborer une carte d'identité nationale qui répondrait aux besoins de sécurité gouvernementaux et aux besoins légitimes de protection de la vie privée et de la sécurité des particuliers et des fournisseurs de services. Cette

[20] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (1980).

[21] Stefan Brands, « Secure User Identification Without Privacy Erosion » (2006) 3:1, University of Ottawa Law & Technology Journal = Revue de droit et technologie de l'Université d'Ottawa 205-223, http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Brands.205-223.pdf

> carte d'identité réduirait le vol d'identité et les attaques de l'intérieur. […] Ces solutions sont bien connues du secteur privé, mais sont rarement utilisées quand les gouvernements étudient l'élaboration de systèmes d'identité nationaux[22].

La discussion relative aux nombreux moyens technologiques permettant de protéger l'identité dépasse les limites du présent document. Il suffit de dire que la difficulté est de convaincre le gouvernement de soutenir les systèmes d'identité qui intègrent ces moyens technologiques de protection de la vie privée.

Sensibiliser le public : Les personnes doivent comprendre le rôle de la gestion de l'identité dans la protection de leur vie privée. L'éducation est essentielle et doit viser non seulement les experts techniques, mais aussi le grand public. Comme on l'a déjà souligné, c'est un des objectifs principaux du présent document – aider les lecteurs à comprendre certains des principes de base des systèmes d'identité afin qu'ils puissent participer au débat qui permettra de définir les politiques et les lois sur l'identité. Il importe tout particulièrement de mieux comprendre l'impact des systèmes d'identité sur la protection de la vie privée au moment où les préoccupations en matière de sécurité mènent à l'adoption de méthodes d'identification de plus en plus envahissantes et rendent suspecte la défense du droit à l'anonymat.

Les gouvernements qui veulent adopter des systèmes d'identité pour lutter contre le crime et protéger la sécurité nationale ne doivent pas en sous-estimer les conséquences sur le respect du droit à la vie privée. Toutefois, en raison du caractère probable de cette attitude, le public doit disposer d'autres sources d'information qui l'aideront à mieux comprendre les conséquences des diverses mesures concernant l'identité sur la protection de la vie privée.

[22] Department of Information Systems of the LSE (éditeur), « The Identity Project: an assessment of the UK Identity Cards Bill and its implications », Londres, version 1.09, 27 juin 2005.

Conclusion

La gestion de l'identité doit fournir des mécanismes pour établir l'identité, les autorisations et l'admissibilité en fonction des principes généraux qui suivent :

- En règle générale, la protection optimale du droit à la vie privée des personnes doit tenir compte des besoins légitimes des organisations gouvernementales et du secteur privé en matière d'identification, d'autorisation ou d'admissibilité;
- Les systèmes doivent être axés sur la protection de l'anonymat;
- La vérification de l'identité doit répondre uniquement à des besoins légitimes des administrations publiques ou des entreprises et seulement si d'autres mesures moins envahissantes ne permettent pas d'atteindre le but visé. Ce principe doit avoir force légale et être appuyé par des mesures de « fardeau de la preuve » et des « évaluations des facteurs relatifs à la gestion de l'identité »;
- Il faut permettre aux gouvernements de gérer leurs responsabilités de façon efficace, y compris les responsabilités suivantes :
    - la sécurité des citoyens (protection contre le crime et la fraude);
    - l'administration des programmes d'avantages sociaux;
    - la production de documents attestant de l'identité des personnes.

Comme l'observait un coauteur [23] d'un rapport[24] sur la surveillance à la Conférence internationale des commissaires à la protection des données et de la vie privée de 2006, nous vivons déjà dans une société de surveillance (ses remarques concernaient le Royaume-Uni, mais elles s'appliquent à l'ensemble

[23] David Murakami Wood, allocution prononcée dans le cadre de la 28e Conférence internationale des commissaires à la protection des données et de la vie privée, Londres, R.-U., 2 novembre 2006.
[24] *Un rapport sur la société de la surveillance,* rapport préparé par le Surveillance Studies Network à l'intention du commissaire à l'information, septembre 2006 : www.privacyconference2006.co.uk/files/report_fr.pdf (consulté le 31 mai 2007).

des pays occidentaux). Selon lui, tous les outils de surveillance que pourrait utiliser une société autoritaire sont déjà en place. Il a rappelé aux délégués à quel point il est facile de glisser vers un contrôle social envahissant quand des technologies de surveillance puissantes sont déjà présentes. Autrement dit, les outils de surveillance d'une société démocratique peuvent très facilement être mis au service d'une société autoritaire. Nous devons toujours garder cela à l'esprit quand nous élaborons des politiques et des systèmes, y compris des politiques et des systèmes d'identité.

Une préoccupation peu abordée sur les divers systèmes d'identité présentement à l'étude tient à la nature unidirectionnelle de la protection de la vie privée. Les gouvernements ne veulent pas paraître insouciants face au terrorisme et au crime. Ils sont tentés d'adopter des mesures, y compris des systèmes d'identité envahissants[25], pour contrer, effectivement ou en apparence, le terrorisme, le crime et l'inefficacité. Cependant, ils tendent à minimiser, nier ou méconnaître les conséquences de ces mesures sur la protection de la vie privée.

Quand un puissant système envahissant est adopté en vue de lutter contre le crime ou le terrorisme, il est peu probable qu'on l'abandonne, même s'il se révèle complètement incapable d'atteindre le but visé. Les droits, y compris celui à la vie privée, ne sont pas faciles à recouvrer une fois perdus. C'est ce qu'on appelle le phénomène de la porte à sens unique[26]. Du point de vue des institutions, le maintien d'outils envahissants comporte de trop nombreux avantages (même s'ils sont au détriment des citoyens) et, politiquement, leur abolition présente trop d'inconvénients. Même les tribunaux qui appliquent la *Charte des droits* peuvent hésiter à remettre en question les actions des gouvernements en temps de crise ou d'incertitude, mais c'est justement là qu'ils doivent faire preuve de vigilance.

[25] Certains auteurs qualifient l'adoption de mesures qui donnent l'illusion d'accroître la sécurité de « mise en scène de la sécurité » (sécurity theatre).
[26] Cependant, le Royaume-Uni a effectivement abandonné son système de cartes d'identité en temps de guerre pour les étrangers en 1952 : Privacy International, Interim Report: Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism (avril 2004), p. 3.

C’est pourquoi, il importe tellement de prendre les mesures appropriées en matière de gestion de l’identité.

Annexe A : Le débat sur la carte d'identité nationale

L'adoption d'une carte d'identité nationale est l'une des questions sur l'identité qui a le plus retenu l'attention du public au cours des dernières années. Elle a fait l'objet de sérieuses discussions aux États-Unis après l'attentat du 11 septembre 2001. Au Canada, l'ancien ministre de la Citoyenneté et de l'Immigration a tenu un forum sur la biométrie à Ottawa en octobre 2003 « pour étudier l'utilisation de la technologie biométrique dans le contexte des mesures destinées à mieux protéger l'intégrité des documents d'identité et de voyage pour les citoyens canadiens et les résidents permanents du Canada ». Le Comité permanent de la citoyenneté et de l'immigration a également émis un rapport provisoire sur une carte nationale d'identité en octobre 2003. Les auteurs concluaient :

> Il est clair qu'il s'agit d'une question stratégique très importante qui pourrait avoir de lourdes répercussions sur la protection de la vie privée, la sécurité et la responsabilité financière. En effet, on nous a fait remarquer que cette question pourrait avoir un impact sur les valeurs fondamentales qui sous-tendent la société canadienne. Dans cet esprit, il sera essentiel d'informer largement la population sur les tenants et aboutissants d'une carte nationale d'identité et d'entendre le point de vue du citoyen sur la pertinence de sa mise en place. Nous espérons que ce document suscitera la réflexion et nous encourageons les Canadiens à continuer de faire part de leurs vues au Comité[27].

La discussion dépassait largement la question d'une carte d'identité nationale et la présenter comme telle serait une simplification excessive. Ce qui est en cause est un *système d'identité* national comprenant des mécanismes servant à

[27] Chambre des communes du Canada, « Une carte nationale d'identité au Canada? Rapport du Comité permanent de la citoyenneté et de l'immigration » (provisoire) (Joe Fontana, député, président), octobre 2003, p. 31-32. http://cmte.parl.gc.ca/Content/HOC/committee/372/cimm/reports/rp1085068/cimmrp06/03-cov2-f.htm .

prouver l'identité des personnes, à saisir des données biométriques, à élaborer une carte à l'épreuve des « manipulations », à créer une base de données répondant à des besoins de sécurité légitimes et accessible à divers organismes, à créer une infrastructure bureaucratique pour gérer le système, à intégrer des mesures de sécurité pour prévenir l'accès illégal à la base de données du système, à chercher des moyens de prévenir le détournement du système par piratage technique ou corruption des personnes qui y ont accès, à concevoir des « lecteurs » pour lire les cartes et à traiter des nombreuses questions non liées à la protection de la vie privée, comme le coût.

Divers commissaires à la protection de la vie privée du Canada ont successivement exprimé leurs préoccupations au sujet de la carte d'identité nationale. Voici certaines de ces préoccupations :

- D'aucuns affirment que la carte d'identité nationale serait un moyen efficace de prévenir le terrorisme, mais ne précisent pas comment;
- Quiconque prétend que le droit à la vie privée doit être réduit au nom de la lutte contre le crime et le terrorisme et pour faciliter les passages transfrontaliers doit porter un fardeau de la preuve extrêmement lourd. Ceux qui défendent l'adoption d'un système de carte d'identité nationale doivent en expliquer les avantages du point de vue :
    - de l'accroissement de la sécurité;
    - de la protection des autres libertés;
    - du respect optimal de la vie privée;
    - de l'efficacité de cette mesure pour atteindre le but visé tout en limitant au minimum les atteintes à la vie privée;
- Un système de carte d'identité nationale pourrait accroître le risque pour la sécurité nationale plutôt que le réduire. L'existence d'un tel système pourrait créer un faux sentiment de sécurité, car la sécurité repose sur bien d'autres facteurs que l'identité. En outre, l'efficacité de la sécurité exige de la « profondeur » – une multiplicité de moyens pour protéger la

sécurité. Dans la mesure où une carte d'identité nationale peut créer l'illusion que cette « profondeur » n'est pas nécessaire, elle peut contribuer à accroître la menace à la sécurité. À l'inverse, rien ne prouve qu'une carte d'identité nationale accroîtrait la sécurité;

- Les criminels et les terroristes concentreraient leurs efforts sur le détournement du système de carte d'identité nationale, car une carte obtenue de manière frauduleuse leur accorderait une identité au-dessus de tous soupçons. Le système pourrait être circonvenu par des moyens techniques (comme dans le cas de la carte d'identité nationale pour les immigrants) ou par la corruption des agents. Le système sera aussi une cible de choix pour les voleurs d'identité en raison des nombreux renseignements personnels contenus dans ses bases de données;
- Le fait de posséder une carte d'identité nationale offre peu d'assurance que le détenteur n'est pas un terroriste ou un criminel. Un grand nombre de ceux qui ont participé aux récentes attaques terroristes aux États-Unis et au Royaume-Uni avaient des documents d'identité en règle et auraient pu obtenir des documents d'identité nationaux en bonne et due forme;
- Certains malfaiteurs ne se soucient simplement pas d'obtenir des papiers d'identité et ils échappent au système, tout comme bien des immigrants illégaux;
- Selon sa structure, un système de carte d'identité nationale pourrait permettrait le couplage de données pour de nombreuses bases de données. Autrement dit, le système de carte d'identité nationale pourrait fournir un identificateur commun qui permettrait de combiner des bases de données distinctes pour créer un profil complet d'une personne. Il n'y a rien d'intrinsèquement répréhensible à établir l'identité d'une personne quand elle effectue un achat par carte de crédit, loue un appartement, monte dans un avion, traverse une frontière, paye ses impôts ou négocie un prêt. Toutefois, rassembler toutes ces transactions au moyen d'un identificateur commun est une toute autre chose. En fait, un système de carte d'identité nationale permettrait à l'État ou à des entreprises privées

de créer des bases de données importantes comprenant des renseignements sur les aspects les plus personnels de la vie privée des citoyens à leur insu et sans leur consentement;

- La création d'une carte d'identité nationale biométrique, utilisée à des fins de plus en plus diverses, ouvrirait également la porte à une surveillance excessive des activités, des transactions et des allées et venues des citoyens;
- Dans son essence, le problème que pose la carte d'identité nationale est qu'elle permettrait d'identifier des personnes qui ont parfaitement le droit de demeurer anonymes, qu'elle révélerait sur elles plus d'information que cela n'est strictement nécessaire pour établir leur identité ou leur autorisation dans une situation particulière, et qu'elle lient entre eux des renseignements pour dresser un profil de leurs préférences et de leurs habitudes. L'utilisation d'une carte d'identité n'entraîne pas toujours ce genre de situation, car ce n'est pas nécessaire. Il est possible de structurer et de concevoir les systèmes d'identité de manière à éviter ce genre d'inconvénient. Il demeure que la carte d'identité peut donner lieu à des intrusions dans la vie privée et même les inciter;
- Une carte d'identité nationale changerait radicalement la société canadienne en minant gravement le droit à l'anonymat, élément clé du droit à la vie privée;
- Il n'est pas réaliste de penser qu'il serait possible de conserver à cette carte un caractère facultatif. Avec le temps, elle deviendrait obligatoire ou ceux qui refuseraient de se la procurer ou de la présenter attireraient sur eux des soupçons pouvant mener à des enquêtes portant atteinte à leur vie privée. Le droit à l'anonymat s'en trouverait limité. Des « dérapages » se produiraient presque certainement. Comme l'a déclaré le commissaire à l'information du Royaume-Uni, Richard Thomas, une carte d'identité nationale pourrait amener à une situation « où un degré de validation extrême de l'identité deviendrait la norme pour recevoir le plus banal des services ». Le refus ou l'incapacité de présenter la carte d'identité

nationale pourrait donner lieu à un service de seconde classe dans le secteur privé, y compris à un refus de service. En fait, la carte d'identité nationale pourrait devenir un passeport intérieur;

- Le détournement de fonction – l'utilisation de renseignements dans un but autre que le but initial – cause également des inquiétudes. Il sera tentant d'utiliser l'infrastructure de la carte d'identité nationale à des fins nouvelles – par exemple en ajoutant des données concernant l'état de santé sur la micropuce de la carte ou en combinant les données de systèmes différents. L'historique du numéro d'assurance sociale (NAS) nous indique qu'une carte d'identité nationale donnerait lieu à des utilisations nouvelles et sans lien direct avec sa fonction première. Un tel scénario aurait des conséquences profondes sur la vie privée, car il évoque la possibilité que de plus en plus de renseignements personnels soient emmagasinés dans la carte et que les transactions du détenteur soient automatiquement enregistrées, consultées, transmises et utilisées pour une infinité de raisons et par un nombre croissant d'organisations. Par exemple, le code à barres des permis de conduire qu'utilisent les agents de police pour accélérer les opérations de contrôle, donne accès à bien d'autres renseignements que la date de naissance quand il est lu par le tenancier d'un bar;
- Selon la structure de la carte, de nombreux autres intervenants pourraient y avoir accès, y compris les entreprises (la *LPRPDÉ* et les lois provinciales correspondantes régiraient les activités de collecte, d'utilisation et de communication des organisations engagées dans des activités commerciales au Canada, mais il subsisterait toujours un risque de collecte illégale dans un but lucratif);
- L'élaboration d'un système de carte d'identité nationale pourrait coûter extrêmement cher et réduire les fonds accordés à la mise en œuvre de mesures de sécurité plus efficaces et moins envahissantes;
- Même un pourcentage d'erreurs minime dans la production des cartes pourrait fausser les données d'un grand nombre de personnes;

- Tout d’abord, le processus d’authentification de l’identité pourrait s’avérer lent et difficile. Dans certains cas, les demandeurs pourraient se trouver dans l’impossibilité de trouver les documents « fondateurs » comme le certificat de naissance et de citoyenneté nécessaires – par exemple, si les documents sont volés ou détruits ou s’ils se trouvent dans un autre pays;
- La technologie nécessaire au fonctionnement d’un système de carte d’identité nationale pourra être insuffisante et devra, de toute façon, être mise à niveau régulièrement, au moins pour contrer les tentatives de piratage du système. Le fait que le Canada est une fédération constitutionnelle ne fait qu’ajouter à la complexité d’une telle proposition, car elle exigerait une activité conjointe des gouvernements fédéral, provinciaux et territoriaux pour concevoir et administrer le système;
- Toute mesure proposée devrait répondre à quatre critères : la nécessité, l’efficacité, la proportionnalité et l’absence d’autres moyens portant moins atteinte à la vie privée.

Annexe B : Évaluations des facteurs relatifs à la gestion de l'identité

Les questions politiques et techniques qui suivent peuvent servir de point de départ à l'évaluation de l'incidence des systèmes d'identité actuels ou proposés sur la vie privée. Elles sont directement tirées ou inspirées du rapport de 2002 du Computer Science and Telecommunications Board des États-Unis intitulé *IDs – Not That Easy: Questions About Nationwide Identity Systems*. Ces questions ne s'appliquent pas à tous les systèmes d'identité, mais elles peuvent néanmoins servir de guide. De plus, les lecteurs peuvent examiner les recommandations sur l'authentification dans la partie intitulé *Who Goes There? Authentication Through the Lens of Privacy*[28]*.* Les principales recommandations se trouvent à la fin de la présente annexe.

Questions politiques

- À quoi sert le système?

- Combien de personnes recevraient une carte d'identité et seraient inscrites dans les dossiers du système? Comment prouverait-on l'identité de ces personnes?

- Quelles seraient les données recueillies sur les personnes inscrites au système et couplées avec leur identité nationale? Ces données porteraient-elles uniquement sur l'identité (et qu'entend-on par ce terme)? D'autres données seraient-elles aussi recueillies, stockées et analysées? Quelle degré de confiance pourrait-on accorder à l'exactitude et à la qualité de ces données?

- Qui seraient les utilisateurs du système (par opposition à ceux qui y seraient inscrits)? On semble dire que l'administration publique et le secteur public en seront les principaux utilisateurs, mais de quels organismes parle-t-on exactement, dans quel contexte et dans quelle mesure? Dans quelle partie de la sphère publique le système serait-il utilisé? Les États et les gouvernements locaux auraient-ils accès au système? Le secteur privé pourrait-il y accéder? Quels organismes des

[28] Stephen T. Kent et Lynette I. Millett, éditeurs, Committee on Authentication Technologies and Their Privacy Implications, National Research Council (Washington, D.C., The National Academies Press, 2003).

secteurs public et privé y auraient accès? Qui pourrait inscrire ou modifier des données dans le système ou les consulter?

- Quels types d'utilisations seraient autorisés? Qui pourrait demander à voir la carte d'identité et dans quelles circonstances? En supposant que des ensembles de données soient associés à l'identité des personnes, quels types de questions seraient permis (p. ex. « Cette personne est-elle autorisée à voyager? » et « Cette personne a-t-elle un casier judiciaire? »). Outre les questions simples, l'analyse et le forage de données seraient-ils permis? Si oui, qui serait autorisé à le faire et à quelles fins?

- La participation au système et l'identification par le système seraient-elles facultatives ou obligatoires? En outre, devrait-on informer les participants ou obtenir leur consentement avant de consulter leurs données d'identification (par opposition, par exemple, à une simple reconnaissance du visage)?

- Quelles structures juridiques protégeraient l'intégrité du système et la confidentialité des données personnelles, le droit à une application régulière de la loi et le degré de responsabilité des gouvernements et des parties associées si le système est utilisé à des fins illicites ou s'il tombe en panne?

Questions techniques

- Plans de conception, de fabrication, de distribution, de mise à niveau ou d'entretien des cartes et des lecteurs de cartes;

- Plans de conception des bases de données correspondantes; degré de centralisation des bases de données sous-jacentes, lieu et coût du stockage des données, du traitement informatique et de la communication. Par exemple, comment les organismes autorisés obtiendraient-ils les données dont ils ont besoin, dans quelles circonstances et dans quelle mesure? Y aurait-il des téléchargements quotidiens ou hebdomadaires de dossiers choisis à des médias de stockage plus permanents?

- Méthodes de vérification de l'authenticité des cartes d'identité et de l'identité des détenteurs de carte;

- Conception de moyens de déceler, de signaler, de vérifier et de corriger les erreurs;

- Conception de mesures de sécurité pour que le système de carte d'identité atteigne ses objectifs et ne soit pas vulnérable à des opérations

de fraude ou à des dénis de service pouvant entraîner des atteintes à la vie privée;

- Établissement du besoin d'une alimentation réseau en temps réel (peut-être semblable à celle des systèmes d'autorisation de crédit en temps réel) et évaluation de la sécurisation de cette alimentation.

Recommandations tirées de *Who Goes There? Authentification Through the Lens of Privacy*:

Il existe des façons de réduire l'incidence des systèmes d'authentification sur la vie privée. Voici certaines des lignes directrices à ce propos :

Recommandation : La conception et le choix d'un système d'authentification doivent reposer sur les principes suivants :

- Authentifier uniquement si nécessaire et à des fins très précises;
- Réduire au minimum l'éventail des données recueillies;
- Réduire au minimum l'intervalle de conservation des données recueillies;
- Établir quels organismes auront accès aux données recueillies;
- Définir les types d'accès et d'utilisation des données qui seront permis;
- Réduire au minimum le degré d'envahissement du processus;
- Faire participer la personne concernée au processus d'identification;
- Réduire au minimum le caractère personnel des données recueillies;
- Vérifier l'utilisation du système et veiller à ce que le registre de vérification ne puisse être modifié ou détruit;
- Fournir aux personnes des moyens de vérifier et de corriger les renseignements servant à l'authentification.

De façon plus générale, les systèmes doivent être conçus, développés et mis en œuvre en portant davantage attention à la conciliation des objectifs de vérification de l'identité et de protection de la vie privée.

Recommandation : Avant de concevoir ou de choisir un système d'authentification, on doit établir un modèle de menace afin de faire un choix éclairé entre des technologies concurrentes et élaborer des politiques et des stratégies de gestion. Le modèle de menace doit tenir compte de toutes les menaces possibles au système. Les principaux aspects à prendre en considération sont les conséquences des technologies sur la vie privée.

Glossaire

Attribut – information de tout type relative à une personne. Un attribut décrit une propriété associée à une personne[29].

Authentification (et authentificateur) – le fait de fournir des preuves d'identité. Par exemple, un certificat de naissance peut être utilisé comme preuve pour appuyer l'allégation d'une personne concernant son lieu de naissance. Le certificat de naissance est un « authentificateur », un document qui aide à prouver une affirmation. Un authentificateur est une preuve qui est soumise pour soutenir l'authentification d'une allégation. Il renforce L'authentificateur renforce la crédibilité d'une allégation. [30]

Base de données – ensemble de données. Certaines bases de données, dont celles qui servent à établir l'identité, contiennent des renseignements personnels.

Biométrie – identification automatique ou vérification de l'identité des personnes d'après leurs caractéristiques comportementales ou physiques[31].

Couplage de données – comparaison informatisée de deux ensembles de données ou plus sur la même personne. Le couplage de données met souvent en relation des dossiers personnels servant à des fins différentes[32].

Cryptage – conversion de données sous forme de cryptogramme qui ne peut être déchiffré que par les personnes autorisées. Le décryptage est la conversion de données cryptées à leur forme originale pour en permettre la lecture[33].

Document de base – document ou justificatif source spécial, car il n'est pas obtenu en présentant d'autres documents source. Il se trouve essentiellement au début de la « chaîne » des renseignements. Voir aussi « document / justificatif source ».

Document / Justificatif source – document qui sert à obtenir d'autres documents d'identité[34]. Un certificat de naissance peut servir à obtenir un

[29] Stephen T. Kent et Lynette I. Millett, *éditeurs*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).
[30] *Ibid*.
[31] *Ibid*.
[32] Simon Rogerson, publication originale sous ETHIcol dans le IMIS Journal, volume 7 n° 1 (février 1997): http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv7no1.html (consulté le 5 mars 2007).
[33] http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci212062,00.html (consulté le 5 mars 2007)
[34] http://www.ssa.gov/history/reports/ssnreportc4.html (consulté le 5 mars 2007).

passeport. Le certificat de naissance est le justificatif ou le document source. Le passeport est le document d'identité. Veuillez noter que le justificatif ou le document source – dans le cas présent le certificat de naissance – peut aussi constituer un document d'identité.

Hameçonnage – technique de fraude qui consiste à usurper l'identité d'une organisation, généralement sur Internet. L'hameçonnage est la version électronique du faux-semblant. Par exemple, le fraudeur envoie un courriel au client d'une banque en se faisant passer pour un de ses représentants. Le courriel demande à la personne d'envoyer de l'information sur son compte et son mot de passe à une adresse qui semble être celle du site Web de la banque, mais qui est en réalité celle du fraudeur. Ce dernier utilise ensuite l'information obtenue pour accéder au compte bancaire de la personne.

Identificateur – élément d'information qui distingue une personne d'une autre. Par exemple, le nom courant, le nom ou le code d'utilisateur[35]; ou encore le nom ou le signe utilisé par une personne et connu des autres[36]. L'identificateur désigne une personne. Il peut s'agir d'un nom, d'un numéro de série ou de tout autre moyen d'identification[37].

Identificateur commun – habituellement un numéro (comme un numéro d'assurance sociale) utilisé dans plusieurs bases de données pour classer l'information recueillie. Dans le cas présent, il s'agit d'information sur une personne. Quand plusieurs bases de données utilisent un identificateur commun, comme un numéro d'assurance sociale, il est très simple de relier les renseignements qui s'y trouvent. L'utilisation d'identificateurs communs dans plusieurs bases de données permet de dégager des profils de comportement basés sur l'information qu'on y a inscrit.

Identification – processus d'établissement de l'identité d'une personne[38].

Identité – ensemble d'attributs relatifs à une personne stockés ensemble. Par exemple des profils, des dossiers et des comptes.

Interconnexion des ordinateurs – voir « couplage de données ».

---

[35] Roger Clarke, « Identification and Authentication Fundamentals » (version du 8 mai 2004): http://www.anu.edu.au/people/Roger.Clarke/DV/IdAuthFundas.html (consulté le 10 avril 2006).

[36] Stephen Kent et Lynette Millett, éds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002

[37] Stephen T. Kent et Lynette I. Millett, *éditeurs*, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (Washington, D.C., The National Academies Press, 2003).

[38] Stephen Kent et Lynette Millett, éds., National Academy of Sciences, Computer Science and Telecommunications Board, *IDs – Not That Easy: Questions About Nationwide Identity Systems* (Washington, DC: National Academy Press) 2002, p. 12.

Justificatif – élément d'information attestant de l'exactitude de certaines affirmations. Un justificatif sert principalement à l'authentification et est souvent intégré à un symbole d'authentification – par exemple, une carte à puce ou une carte bancaire[39].

Politique sur l'identité – politique sur le rôle approprié des divers moyens d'identification ou d'autorisation des personnes.

Profilage – collecte et analyse de données relatives à une personne dans le but d'établir son profil[40].

Symbole – peut être une carte bancaire, un billet d'autobus ou tout autre objet servant à établir le droit à un service (le droit de monter à bord d'un autobus, par exemple), ou le droit d'effectuer une transaction. Un symbole peut être un objet réel ou virtuel qui permet de faire une transaction. Il peut s'agir d'un élément matériel ou logiciel qui comprend des justificatifs liés aux attributs sous forme de données numériques, de carte à puces ou de téléphone mobile. On peut l'utiliser à des fin d'autorisation (« symbole d'autorisation »)[41].

Vol d'identité – usurpation de l'identité d'une personne par une autre pour effectuer des transactions en son nom. Le vol d'identité survient quand une personne peut éviter ou tromper un système d'authentification, par exemple en raison d'une faiblesse des authentificateurs.

[39] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc (consulté le 5 mars 2007).
[40] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf (consulté le 6 mars 2007).
[41] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc (consulté le 5 mars 2007).