Identification par radiofréquence et nécessité de protéger les renseignements personnels

par Mavis Taillieu, députée provinciale

L'identification par radiofréquence est une nouvelle technologie qui pourrait permettre une collecte sans précédent de renseignements personnels. Celle-ci, liée à d'autres bases de données de renseignements, dont bon nombre sont utilisées à l'insu des personnes concernées ou sans leur accord, inquiète ceux qui croient qu'il faut protéger les renseignements personnels et la vie privée. Dans ce meilleur des mondes, la technologie progresse à la vitesse de l'éclair, tandis que notre compréhension de ses utilisations croît avec la lenteur d'une tortue. Dans le présent article, l'auteure qu'il est temps que les législateurs se penchent sérieusement sur la technique d'identification par radiofréquence et ses répercussions pour la société canadienne.

En 2004, la commissaire à la protection de la vie privée de l'Ontario, Anne Cavoukian, a publié un rapport mettant en évidence les risques que fait courir à la vie privée l'identification par radiofréquence (IRF). Cette méthode d'identification très spécifique repose sur l'utilisation de dispositifs de stockage de données appelés étiquettes ou transpondeurs ainsi que de dispositifs de lecture à distance appelés interrogateurs ou lecteurs. Les étiquettes sont de petits objets. Les plus grandes mesurent quelques centimètres carrés, tandis que les plus petites ont la taille d'un grain de poivre. On peut les fixer sur un produit, un animal ou une personne ou les incorporer dans l'objet ou l'être récepteur. Les étiquettes IRF contiennent des puces de silicium et une antenne qui leur permettent de recevoir des interrogations en radiofréquence provenant d'un lecteur et d'y répondre. En juin 2006, la commissaire a publié, à l'intention des entreprises utilisant cette technologie, des lignes directrices sur l'identification par radiofréquence qui reposent sur trois principes fondamentaux : se concentrer sur les systèmes d'information fondés sur l'identification par radiofréquence, et non sur les technologies elles-mêmes; intégrer, dès l'étape de la conception, des caractéristiques de protection de la vie privée et de sécurité; assurer une participation maximale des particuliers et obtenir leur consentement.

Ce n'est pas la technologie IRF qui a suscité les préoccupations des défenseurs de la vie privée, mais les possibilités qui s'y rattachent. Les étiquettes IRF sont uniques et spécifiques et, donc, parfaitement identifiables aux produits, aux personnes et aux animaux qui les portent. Elles jouent un rôle analogue à celui des codes à barres, mais sont beaucoup plus sophistiquées. Contrairement au code à barres qui identifie toutes les canettes de cola comme contenant ce produit, l'étiquette IRF peut identifier chaque canette d'une façon unique. La lecture du code à barres se fonde sur l'utilisation d'un faisceau lumineux, alors que l'étiquette IRF reçoit et émet des ondes radio à travers les objets qui l'entourent, que ce soit un sac à main, une poche ou même la carrosserie d'une voiture. Cette technologie est actuellement utilisée dans la gestion de l'offre pour suivre le mouvement des biens dans le monde entier et contrôler les stocks. À ce niveau-là, elle ne représente que peu de dangers, mais l'utilisation d'étiquettes IRF pour des articles de consommation courante, lorsqu'elles sont liées à des renseignements personnels, pourrait faciliter la localisation et la surveillance des personnes. Si chaque objet que vous achetez peut être rattaché à d'autres renseignements, comme votre carte de crédit ou votre téléphone cellulaire, il sera possible d'accéder à vos données bancaires et, en définitive, d'établir

Mavis Taillieu est députée de Morris à l'Assemblée législative du Manitoba. *Le présent article est une version révisée d'une communication faite lors de la 44e Conférence régionale canadienne de l'Association parlementaire du Commonwealth, qui a eu lieu à Gatineau, en juillet 2006.*

vos habitudes d'achat et de dépenses, vos préférences personnelles et le profil de vos déplacements personnels.

L'IRF est actuellement utilisée dans le monde pour plusieurs applications. Elle sert au suivi des livres en bibliothèque et en librairie, au contrôle de l'accès aux bâtiments, au suivi des bagages par les compagnies aériennes, au suivi des vêtements et des produits pharmaceutiques et aux porte-noms des employés. Le bétail porte des étiquettes IRF. Certains pays ont commencé à faire appel à cette technologie pour leurs passeports, mais pas le Canada, pour l'instant. Dans plusieurs États américains, les détenus d'établissements correctionnels portent au poignet un bracelet muni d'étiquettes IRF qui permettent de suivre leurs déplacements. Les postes de péage de l'autoroute 407, au nord de Toronto, font appel à l'IRF pour facturer automatiquement les comptes des conducteurs qui franchissent le poste, les cartes à étiquettes IRF pouvant être déchiffrées à distance. Les cartes Nexus que l'on propose pour assurer la sécurité des passages à la frontière canado-américaine comportent des étiquettes de ce type. L'Université du Manitoba est en train d'étudier cette nouvelle technologie.

En octobre 2004, la Food and Drug Administration des États-Unis a approuvé les premières puces IRF à implanter dans des humains. Ces dispositifs, fabriqués par la VeriChip Corporation, filiale d'Applied Digital Solutions Inc., peuvent stocker des renseignements médicaux, des données personnelles sur les comptes bancaires et les comptes-cartes de crédit, des codes et des mots de passe ou, de fait, toute information personnelle. En Espagne, il existe un club sur plage dont les clients se font implanter une puce dans la main qui contient leur numéro de carte de crédit pour qu'ils n'aient pas à porter d'argent sur eux. En février de cette année, une compagnie de surveillance de Cincinnati est devenue la première entreprise américaine à utiliser des VeriChip implantés dans ses employés pour qu'ils aient accès à son centre de données. La Direction des produits thérapeutiques de Santé Canada n'a pas encore approuvé la technologie IRF implantable au Canada, mais VeriChip a ouvert des bureaux à Vancouver et à Ottawa. Selon Ian Kerr, titulaire de la Chaire de recherche du Canada en éthique, en droit et en technologie et professeur agrégé de la Faculté de droit de l'Université d'Ottawa, ces puces sont faciles à copier. Deux questions se posent, à son avis : « Faut-il réglementer cette technologie? » et « Qui devrait s'en charger? » La commissaire à la vie privée du Canada, Jennifer Stoddard, a entrepris une étude de l'utilisation de l'IRF au Canada en 2005 et conclu : « Il est essentiel de travailler maintenant à mieux informer le grand public et les intervenants politiques sur le danger que pose la nature envahissante de l'IRF. » Elle a précisé que la technologie IRF était déjà utilisée à d'autres fins que la simple localisation de marchandises et qu'elle servait à établir des liens avec des renseignements personnels et parfois à suivre le déplacement de personnes.

Nous vivons à une époque de collecte et de partage excessifs des renseignements personnels. Depuis plusieurs dizaines d'années, la façon dont nous faisons nos emplettes, menons nos activités bancaires et vaquons à nos occupations quotidiennes s'est transformée radicalement, ce qui a abouti à une prolifération sans précédent de dossiers et de données. D'après l'auteur Daniel Solove, des petits détails qui restaient avant enterrés dans les mémoires ou consignés sur des petits bouts de papier dont l'écriture s'effaçait avec le temps sont désormais préservés dans les mémoires numériques des ordinateurs, dans de vastes bases de données comportant des champs fertiles de données personnelles.

À l'heure actuelle, trois grands groupes recueillent des renseignements personnels : les gouvernements, les organismes sans but lucratif et les entreprises commerciales. La collecte, l'échange, la location et la vente de renseignements personnels constituent des affaires lucratives. L'Association canadienne du marketing estime qu'il y a environ 480 000 emplois qui génèrent 51 milliards de dollars de ventes par an et qui touchent à la collecte d'informations sur les consommateurs, à l'analyse des bases de données relatives à ceux-ci et au courtage des renseignements personnels.

> ***Les mégabases de données constituent les nouvelles banques dans lesquelles les renseignements personnels sont la nouvelle devise.***

Délibérément ou non, les gens donnent leurs renseignements personnels quand ils font des achats, s'abonnent à une revue, s'inscrivent à une conférence, deviennent membres d'un club, obtiennent une carte, font un don, participent à un concours, répondent à un sondage ou demandent simplement des renseignements. L'accumulation croissante de renseignements personnels et le regroupement des bases de données exposent les gens à des abus de la part de ceux qui ont accès à cette information. L'utilisation de celle-ci n'est limitée que par la loi et l'éthique.

Au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régit la collecte, l'utilisation et la divulgation des renseignements personnels dans le contexte d'activités commerciales. Cette loi n'est cependant pas très respectée. Philippa Lawson, directrice générale et avocate générale de la Clinique d'intérêt public et de politique d'Internet du Canada, a publié une étude qui révèle que les détaillants, en particulier ceux dont les activités se font en ligne, ne respectent pas la loi. « Notre étude montre tout à fait clairement qu'il y a très peu de respect dans le milieu lorsqu'il s'agit du type de choses dont les consommateurs n'ont pas conscience. Il y a partage et utilisation de leurs données personnelles en coulisses. Les entreprises ne sont pas aussi transparentes à ce sujet et ne donnent pas aux consommateurs un choix réel. »

De plus, on ne devrait pas nous faire croire que cette sécurité est infaillible. Entre le 15 février 2005 et le 30 juin 2006, il y a eu, aux États-Unis, 222 violations de la sécurité touchant plus de 88 millions de dossiers contenant des renseignements personnels délicats. La majorité de ces incidents est attribuable à des pirates informatiques, au vol d'ordinateurs portables ou à

des employés malhonnêtes. L'année dernière, plus de 10 millions d'Américains ont été victimes d'usurpation d'identité. Deux grandes agences canadiennes d'évaluation du crédit, Equifax et TransUnion, signalent qu'elles reçoivent, chaque mois, entre 1 400 et 1 800 plaintes d'usurpation d'identité qui proviennent surtout de l'Ontario. Equifax a été elle-même victime de violations de la sécurité au cours desquelles des renseignements ont été volés.

Mary Kirwan, avocate, écrivaine et experte en sécurité des TI, a déclaré qu'il n'est pas facile de devancer les escrocs virtuels. Les enregistreurs de frappe sont des mécanismes que peuvent utiliser les parents pour suivre les habitudes de consultation d'Internet de leurs enfants et les employeurs, celles de leurs employés. Lorsque ces dispositifs tombent en de mauvaises mains, ce sont de parfaits outils d'espions, qui permettent à des criminels de prendre des instantanés d'écran et d'enregistrer les touches utilisées de manière à saisir des données protégées, comme les mots de passe pour accéder à un compte bancaire et les numéros d'identification personnels. Il y a une foule de données personnelles à voler, et le public connaît très mal les lacunes de la sécurité en ligne.

Le non-respect de la loi et le manque de sécurité accroissent les risques d'usurpation d'identité, crime qui connaît le plus grand essor au Canada aujourd'hui.

De façon générale, l'usurpation d'identité désigne toutes les infractions dans lesquelles une personne obtient et utilise illégalement des renseignements identifiant une autre personne à des fins frauduleuses ou à d'autres fins criminelles, notamment pour en tirer un avantage économique. Ces renseignements peuvent comprendre le nom, la date de naissance, le nom de jeune fille de la mère, le numéro d'assurance sociale, le numéro d'assurance-santé, les numéros de carte de crédit et l'information qui figure sur l'acte de naissance, le passeport ou le permis de conduire. Une fois volés, ils peuvent servir à ouvrir des comptes, à faire des virements bancaires, à présenter une demande de prêt ou de crédit ou à acheter des biens et des services, ou, en fait, à voler une identité.

Les renseignements sont dérobés de différentes sources : dans le courrier, des membres de la famille, dans les domiciles privés et même dans les sacs de déchets domestiques. Toutefois, les voleurs deviennent beaucoup plus expérimentés. Ils utilisent des explorateurs de données, recourent à la piraterie informatique ou se servent d'ordinateurs ou de portables branchés sur d'énormes bases de données. Les nouveaux usages des technologies comme l'IRF pourraient accroître la collecte et l'utilisation malveillante de données, et l'usurpation d'identité risque d'être plus fréquente et plus facile.

Les législateurs devraient prendre l'initiative de discuter, d'éduquer et, peut-être, de légiférer à propos de la protection des renseignements personnels, compte tenu des progrès des technologies, dont le public n'a généralement pas conscience. Si les gens consentent en toute connaissance de cause à communiquer leurs renseignements personnels en sachant qu'ils serviront aux fins indiquées, qu'ils ne seront pas communiqués et qu'ils seront protégés, il y a plus de chances qu'ils acceptent de le faire. Avant d'adopter une nouvelle technologie, il faudrait toujours l'évaluer sous l'angle du respect de la vie privée, et la participation et le consentement du public devraient être acquis.

Dans son rapport annuel 2005 qu'elle a remis au Parlement en mai 2006, Jennifer Stoddard, commissaire à la protection de la vie privée du Canada, précise deux points : « J'aimerais pouvoir dire que dans le domaine de la protection de la vie privée au Canada, tout va pour le mieux dans le meilleur des mondes possible. Malheureusement, ce n'est pas encore le cas. Plus que jamais, les Canadiennes et les Canadiens s'inquiètent du sort de leur vie privée et du risque que leurs renseignements personnels soient utilisés à mauvais escient. Leurs inquiétudes sont le fruit de menaces toujours plus nombreuses surgissant à l'ère électronique de la circulation massive et continue de données ».

Lors d'un sondage entrepris par la commissaire à la protection de la vie privée, les Canadiens ont fait savoir que le respect de la vie privée constitue l'un des plus importants dossiers dont le pays doit s'occuper. La population appuie des lois rigoureuses et judicieuses sur le respect de la vie privée qui visent les secteurs public et privé. Soixante- dix pour cent (70 %) des personnes sondées se sont dites convaincues que les renseignements personnels étaient moins bien protégés. Une bonne majorité des personnes interrogées ont déclaré qu'il n'y avait aucune réelle protection de la vie privée, parce que les gouvernements peuvent trop facilement suivre la population grâce aux nouvelles technologies.

Par suite de la multiplication des violations de la sécurité et des pertes de renseignements personnels aux États-Unis, 23 États ont inscrit dans leurs lois l'« obligation de notification », qui impose aux entreprises d'avertir les gens touchés de la compromission possible de leurs renseignements personnels. Jusqu'à il y a deux ans, la Californie était le seul État américain à avoir adopté une loi en ce sens. Une douzaine d'États ont emboîté le pas en légiférant le recours à l'IRF, sous une forme ou une autre. Ces mesures législatives s'échelonnent entre la création d'un groupe de travail chargé d'étudier la technologie au Maryland et l'interdiction au gouvernement d'imposer aux gens l'implantation d'une étiquette IRF dans leur corps au Wisconsin, dans le Dakota du Sud et au New Hampshire.

Au Canada, d'après la commissaire à la protection de la vie privée du Canada, les principes de la LPRPDE s'appliquent à l'utilisation de l'IRF et au couplage des données. Cette loi fait actuellement l'objet d'un examen. L'une des recommandations à cet égard est d'en renforcer l'exécution.

> ***À ma connaissance, il n'y a pas au Canada de lois concernant exclusivement l'IRF.***

La Colombie-Britannique, l'Alberta, le Québec et l'Ontario (pour les renseignements médicaux seulement) ont adopté des lois contenant à peu près les mêmes dispositions que la LPRPDE et sont donc régis par leur propre législation. Brian Bowman, éminent avocat winnipégois spécialiste des

questions de protection de la vie privée, estime que les lois provinciales devraient précipiter un meilleur respect des dispositions légales, parce que les entreprises reconnaîtraient et accepteraient la législation locale.

J'ai moi-même proposé un projet de loi d'initiative parlementaire intitulé *Loi sur la protection des renseignements personnels et la prévention du vol d'identité*, qui a pour objet de mettre en vigueur des dispositions législatives à peu près semblables au Manitoba. Il comprend une disposition sur l'obligation de notification qui est, je crois, la première de son genre au Canada. Le projet de loi a été rejeté par l'actuel gouvernement néo-démocrate, comme la quasi totalité des projets de loi d'initiative parlementaire. Je suis persuadée que des dispositions sur l'« obligation de notification » figureront dans les projets de loi futurs sur la protection des renseignements personnels et pourraient même être envisagées dans le cadre de l'examen de la LPRPDE fédérale.

Les renseignements personnels qui vous concernent vous définissent. Il ne s'agit pas juste de votre nom, de votre adresse, de votre numéro de téléphone, de votre adresse électronique, de votre numéro d'assurance sociale, des numéros de vos comptes bancaires, de vos numéros d'identification personnels, de votre date de naissance, de votre permis de conduire, mais également de votre appartenance à un groupe ethnique, de votre religion, de votre orientation sexuelle, de votre affiliation politique et de vos associations et préférences personnelles ainsi que de vos voyages. Ces renseignements comprennent également les données biométriques comme les photographies, les empreintes digitales et palmaires, les empreintes faciales et la lecture de l'iris ainsi que l'ADN. Chacun doit protéger ses renseignements personnels et savoir pourquoi il doit le faire, avant de les perdre au nom de la commodité et de la sécurité. Lorsque nous fournissons nos renseignements personnels, nous sommes à la merci des progrès technologiques et de tous ceux qui savent comment en abuser. Lorsque nous abandonnons nos renseignements personnels, nous abandonnons notre droit à la vie privée.

Les Canadiens perçoivent le droit à la vie privée sous de multiples angles : le droit d'être laissé en paix, celui de contrôler ce que les autres savent à leur sujet, celui de s'attendre que l'information personnelle ne soit recueillie qu'à une fin précise et qu'elle ne soit utilisée que dans ce seul but. À leur avis, il s'agit là d'une valeur sociale commune.

On peut ne penser à la vie privée qu'après l'avoir perdue. Quand cela se produit, elle est perdue à jamais.

Sources

Rapport annuel au Parlement sur la *Loi sur la protection des renseignements personnels*, passages sur la technologie d'identification par radiofréquence (IRF). Internet : <www.privcom.gc.ca/information/ar/200506/2005_pipeda_f.asp>

RPP 2005-2006 – Commissariats à l'information et à la protection de la vie privée. Internet : <www.tbs-sct.gc.ca/est-pre/20052006/IPC-CIP/IPC-CIPr5602_f.asp>

Industrie Canada, *Identification par radio-fréquence [*sic*] (RFID) : Au-delà du mandat des clients*. Internet : <http://strategis.ic.gc.ca/epic/internet/indsib-logi.nsf/fr/h_pj00115f.html>

Compliance with Canadian Data Protection Laws, Are retailers measuring up?, avril 2006; *On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship*, avril 2006, Clinique d'intérêt public et de politique d'Internet du Canada, Faculté de droit, Université d'Ottawa (en anglais seulement)

Tag, You're it: Privacy Implications of Radio frequency Identification (RFID) Technology; « RFIDs: Homing in on Privacy Information », dans *Annual Report 2004*, « La commissaire Cavoukian publie des lignes directrices sur l'identification par radiofréquence pour assurer la protection de la vie privée » (communiqué), *Guidelines for Using RFID Tags in Ontario Public Libraries*. Internet : <www.ipc.on.ca>

Kirk J. Nahra et John W. Kuzin, « RFID vendors need a privacy strategy », *RFID Journal*, 19 juin 2006. Internet : <www.rfidjournal.com/article/articleview/2428/1/128/>. Voir aussi des articles connexes. (en anglais seulement)

Katherine Albrecht et Liz McIntyre, « RFID: The Big Brother Bar Code ». Internet : <www.spychips.com/alec-big-brother-barcode-article.html> (en anglais seulement)

« Two U.S. Employees Injected With RFID Microchips at Company Request », RFID Nineteen Eight-Four. Internet : <www.spychips.com/press-releases/us-employees-verichipped.html>. Voir aussi des articles connexes. (en anglais seulement)

« Radio-identification », dans *Wikipédia*. Internet : <http://fr.wikipedia.org/wiki/Radio-identification>

« VeriChip », dans *Wikipédia*. Internet : <http://fr.wikipedia.org/wiki/VeriChip>

Mary Kirwan, « The horns of a security dilemma », *Globe and Mail Update*, 16 mai 2005. Internet : <www.theglobeandmail.com/servlet/story/RTGAM.20050512.gtkirwanmay12/BNStory/Tech> (en anglais seulement)

« Usurpation d'identité », dans *Wikipédia*. Internet : <http://fr.wikipedia.org/wiki/Usurpation_d%27identit%C3%A9>

« National Identity Cards – The Next Step? », *Mapleleafweb*. Internet : <www.mapleleafweb.com/features/privacy/id_cards/cards.html> (en anglais seulement)

« What About the Right to Privacy? », *Mapleleafweb*. Internet : <www.mapleleafweb.com/features/privacy/id_cards/privacy.html> (en anglais seulement)

« The Year of RFID Legislation? ». Internet : <www.cephas-library.com/nwo/nwo_the_year_of_rfid_legislation.html> (en anglais seulement)

Ileiren Byles, « Health-care chips could get under your skin », *Express News*, Université de l'Alberta, 9 juin 2006. Internet : <www.expressnews.ualberta.ca/article.cfm?id=7633> (en anglais seulement)

Sarah Lysecki, « Federal Privacy Commissioner to tackle RFID », *ITBusiness.ca*, 30 mai 2006. Internet : <www.itbusiness.ca/it/client/en/ComputerCanada/News.asp?id=39586&cid=3> (en anglais seulement)

« RFID Passports », *Schneier on Security*, 4 octobre 2004. Internet : <www.schneier.com/blog/archives/2004/10/rfid_passports.html> (en anglais seulement)

« Choicepoint », Electronic Privacy Information Center. Internet : <www.epic.org/privacy/choicepoint/> (en anglais seulement)« A Chronology of Data Breaches », Privacy Rights Clearinghouse. Internet : <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (en anglais seulement)