

Commissariat à la
protection de la vie privée
du Canada



Office of the
Privacy Commissioner
of Canada

Sommaire des projets de recherche financés dans le cadre du Programme des contributions de 2004 à 2007

Septembre 2007

Table des matières

Introduction	1
Vie privée des consommateurs et conformité des entreprises privées	
Le respect des lois canadiennes en matière de protection des données : Les commerçants se conforment-ils? (rapport en anglais seulement) <i>Clinique d'intérêt public et de politique d'Internet du Canada (deux rapports distincts), avril 2006.....</i>	2
Suivre la piste des renseignements : De quelle manière des renseignements détaillés à votre sujet se retrouvent-ils entre les mains d'organismes avec lesquels vous n'avez aucun lien? Un rapport sur l'industrie canadienne du courtage de données (rapport en anglais seulement) <i>Clinique d'intérêt public et de politique d'Internet du Canada (deux rapports distincts), avril 2006.....</i>	3
Les consommateurs tirent-ils profit de l'échange de renseignements personnels? <i>L'Union des consommateurs, avril 2007</i>	4
Application de la LPRPDÉ : Examen des énoncés de confidentialité sur Internet et des pratiques en ligne (rapport en anglais seulement) <i>Université de Toronto, mai 2005</i>	6
Des modèles de protection de la vie privée qui fonctionnent : Un guide pour les organisations canadiennes	
Pratiques exemplaires de gestion des données : Un guide pour les spécialistes du marketing (rapport en anglais seulement)	
Conformité des petites entreprises aux règlements en matière de protection de la vie privée – Résultats de recherche (rapport en anglais seulement) <i>Association canadienne du marketing (trois rapports distincts), juin 2005</i>	8
Assurer le respect des principes relatifs à la protection de la vie privée : Projet de recherche sur l'évaluation de l'application de la LPRPDÉ <i>British Columbia Civil Liberties Association, mars 2006</i>	10
Directives à l'intention des professionnels de la protection de la vie privée et des entreprises	
Projet de normes de certification professionnelle (rapport en anglais seulement) <i>Canadian Association for Professional Access and Privacy Administrators et Association canadienne d'accès à l'information et de la protection des renseignements personnels, mars 2007.....</i>	11
Stratégies de formulation de politiques sur la protection de la vie privée compréhensibles pour les enfants (rapport en anglais seulement) <i>Université de Western Ontario, mars 2007</i>	12
Information sur la santé	
Directives sur la dépersonnalisation des renseignements personnels sur la santé pour l'ensemble du Canada (rapport en anglais seulement) <i>Institut de recherche du Centre hospitalier pour enfants de l'est de l'Ontario, avril 2007.....</i>	14

Dossiers de santé électroniques et la <i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (rapport en anglais seulement) <i>Université de l'Alberta et Université de Victoria, avril 2005</i>	16
Utilisation secondaire des renseignements personnels consignés dans des systèmes nationaux de dossiers électroniques de santé : Développements clés et enjeux <i>Centre de bioéthique, Institut de recherches cliniques de Montréal, juin 2007</i> ,.....	18
Les usages sociaux de l'ADN dans le processus de formulation des politiques : Analyse de deux projets de loi sur l'identification par les empreintes génétiques <i>Université d'Ottawa, avril 2006</i>	20
Choix de technologies et politiques sur la protection de la vie privée dans le secteur de la santé (rapport en anglais seulement) <i>Université Memorial de Terre-Neuve, avril 2007</i>	21

Protection de la vie privée et technologie

Analyse des répercussions juridiques et technologiques sur la protection de la vie privée des technologies d'identification par radiofréquence (rapport en anglais seulement) <i>Université Dalhousie, avril 2005</i>	23
Le défi de l'identification des consommateurs dans le cadre de nouveaux mécanismes de paiement électronique <i>Option consommateurs, août 2006</i>	25
Technologies de gestion des droits numériques et protection de la vie privée des consommateurs : Étude du marché canadien et évaluation des facteurs relatifs à la vie privée (rapport en anglais seulement) <i>Clinique d'intérêt public et de politique d'Internet du Canada, avril 2007</i>	26
Le droit à la vie privée et les services de communications payés d'avance : Enquête sur les politiques relatives à la réglementation et à l'enregistrement touchant les services de téléphones cellulaires payés à l'avance au sein des États membres de l'OCDE (rapport en anglais seulement) <i>Université Simon Fraser, mars 2006</i>	28
Technologies à bord des véhicules et protection de la vie privée des consommateurs (rapport en anglais seulement) <i>Automobile Consumer Coalition, mars 2007</i>	30

Surveillance

Services basés sur l'emplacement : Analyse des répercussions sur la vie privée dans le contexte canadien (rapport en anglais seulement) <i>Université de Victoria, juin 2005</i>	32
Les technologies de localisation : Mobilité, surveillance et protection de la vie privée (rapport en anglais seulement) <i>Université Queen's, mars 2005</i>	33
L'utilisation des caméras de surveillance dans les lieux à accès public au Canada <i>École nationale d'administration publique, décembre 2005</i>	35

Protection de la vie privée en milieu de travail

Examen préliminaire des enjeux relatifs à la protection de la vie privée en milieu de travail au Canada (rapport en anglais seulement) <i>Université de la Colombie-Britannique, avril 2006</i>	36
Dans la ligne de mire? Le point de vue de l'employeur concernant la protection de la vie privée en milieu de travail (rapport en anglais seulement) <i>Université Ryerson, juin 2006</i>	38

Autres

La LPRPDÉ et le vol d'identité : Des solutions pour protéger les Canadiennes et les Canadiens (rapport en anglais seulement) <i>B.C. Freedom of Information and Privacy Association, avril 2005</i>	40
Protection de la vie privée au sein du système de justice pénale : Utilisation d'échantillons d'ADN dans le cadre d'enquêtes (rapport en anglais seulement) <i>Université d'Ottawa, avril 2007</i>	42
Visions du Canada : Prévisions relatives aux politiques sur l'identité, et politiques de rechange (rapport en anglais seulement) <i>Université de Toronto, avril 2007</i>	44

Introduction

Le Commissariat à la protection de la vie privée du Canada est fier de présenter les résumés des 25 études de recherche relatives à la protection de la vie privée que nous avons financées depuis 2004 par l'entremise de notre Programme des contributions.

Notre mandat consiste en partie à favoriser la compréhension et la sensibilisation des Canadiennes et des Canadiens à l'égard des enjeux liés à la protection de la vie privée. Le Programme des contributions permet de financer et de publier de la recherche utile, réalisée au Canada par des universitaires, des défenseurs de la vie privée et le milieu des affaires. Soulignons qu'il s'agit souvent de travaux de pointe, reconnus mondialement et pertinents à l'échelle internationale.

Nous n'avons jamais eu autant besoin de recherche de ce genre. En outre, les sujets d'étude sur la protection de la vie privée ne manquent pas. Pour tout dire, bon nombre d'experts dans le domaine sont d'avis que les tendances politiques, économiques et technologiques exercent d'implacables pressions sur notre vie privée et nos autres droits et libertés.

Au cours des trois premières années, les chercheurs financés dans le cadre du Programme des contributions ont examiné la mise en œuvre de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ). Ils ont étudié les enjeux liés à la protection des renseignements médicaux, notamment dans le domaine de la génétique et des dossiers automatisés sur les soins de santé. Ils se sont penchés sur un éventail d'autres nouvelles technologies pour connaître la manière dont elles sont susceptibles de « s'insinuer » dans nos vies privées. Enfin, ils ont fouillé les enjeux touchant la protection de la vie privée en milieu de travail selon le point de vue des employés et des employeurs.

En 2007, le Commissariat oriente la recherche effectuée dans le cadre du Programme des contributions vers la confidentialité sur l'Internet, particulièrement chez les jeunes qui semblent trop disposés, trop souvent, à prendre des risques avec leur sécurité et leur réputation pour des raisons de commodité. Nous tournons notre attention également vers les défis que pose la préservation de l'identification et de l'authentification dans un monde où il nous faut de plus en plus renoncer à l'anonymat – jadis tenu pour acquis –, pour se déplacer ou communiquer. Le troisième volet de recherche portera sur le point de convergence des secteurs privé et public en matière de collecte et d'utilisation de renseignements personnels, comme l'accessibilité croissante dont jouissent les autorités gouvernementales à l'égard de nos dossiers de consommation.

Nous encourageons les défenseurs, les universitaires, les décideurs et les chefs d'entreprise à utiliser et mettre à profit le corpus de recherches existant, à entreprendre de nouveaux travaux de recherche de même qu'à collaborer au développement et à la mise en commun de pratiques exemplaires en matière de protection de la vie privée. La protection de la vie privée est une valeur de base de notre société et, pour tout dire, elle fait partie des droits fondamentaux de la personne. Il nous faut protéger ce droit pour le bien-être de tous les citoyens du monde et pour les générations futures.

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada
Septembre 2007

Le respect des lois canadiennes en matière de protection des données : Les commerçants se conforment-ils?

Clinique d'intérêt public et de politique d'Internet du Canada, avril 2006, 110 pages

Cette étude visait à examiner la mesure dans laquelle les organisations respectent la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)* en évaluant la conformité des détaillants à certaines dispositions clés de la *LPRPDÉ*.

Au moyen d'un processus de sélection impartial, les auteurs ont recensé 64 détaillants en ligne pour évaluer leur conformité aux prescriptions de la *LPRPDÉ* en ce qui a trait à la transparence, à la responsabilisation et au consentement. Ils communiquaient avec les détaillants en composant leur numéro de téléphone principal pour poser quelques questions normalisées, examiner la politique de l'entreprise en matière de protection de la vie privée et commander un produit ou un service en ligne. Un deuxième groupe de 72 détaillants en ligne et traditionnels ont fait l'objet d'une évaluation par rapport aux prescriptions de la *LPRPDÉ* concernant l'accès aux renseignements personnels. Le processus consistait notamment à envoyer une lettre type aux entreprises et à examiner les réponses.

Les résultats de l'étude révèlent une non-conformité généralisée dans les quatre domaines et laissent entendre qu'il faut prendre en considération des solutions de rechange à l'application actuelle de la *LPRPDÉ*. Bien que la plupart des entreprises évaluées disposaient d'une politique sur la protection de la vie privée et, par le fait même, étaient au courant de la nécessité de respecter la confidentialité du client, bon nombre n'ont pas su se conformer ne serait-ce qu'aux prescriptions réglementaires de base, par exemple fournir les coordonnées d'une personne responsable de la politique concernant la protection de la vie privée, expliquer clairement ce qu'ils font avec les renseignements personnels des clients, et répondre aux demandes d'accès à l'information. Les résultats démontrent clairement que les lois canadiennes sur la protection des données n'incitent pas suffisamment les entreprises à faire en sorte que les consommateurs exercent un contrôle valable de leurs renseignements personnels et à parler ouvertement de leurs pratiques de gestion des données.

On peut consulter le rapport à l'adresse suivante : <http://www.cippic.ca/en/bulletin/>

Suivre la piste des renseignements : De quelle manière des renseignements détaillés à votre sujet se retrouvent-ils entre les mains d'organismes avec lesquels vous n'avez aucun lien? Un rapport sur l'industrie canadienne du courtage de données

Clinique d'intérêt public et de politique d'Internet du Canada, avril 2006, 64 pages

Le rapport décrit la façon dont des renseignements personnels détaillés sur les Canadiennes et les Canadiens aboutissent entre les mains d'agents de vente directe et autres. De façon plus précise, on y examine l'industrie du courtage de données dont les activités ont des répercussions importantes sur la vie privée des personnes. Il s'agit d'un document descriptif, qui explique la façon dont les courtiers de données prétendent se conformer aux lois canadiennes sur la protection de la vie privée. Toutefois, il n'évalue pas à proprement dit la conformité des courtiers aux lois sur la protection de la vie privée.

La recherche s'est déroulée au moyen de diverses méthodes, y compris des analyses documentaires, des examens de sites Web, la consultation auprès d'experts, des demandes d'accès à l'information et des suivis sélectifs auprès de gestionnaires et de compilateurs de données. Les chercheurs ont examiné les directives industrielles et les politiques sur la protection de la vie privée pour mieux comprendre la façon dont les entreprises qui échangent des renseignements personnels se conforment aux lois relatives à la protection de la vie privée.

Il existe un marché vaste et fécond concernant les renseignements personnels des consommateurs canadiens. Le moteur de ce commerce est l'industrie de la vente directe. Ce commerce est facilité par un éventail de compagnies qui se spécialisent, entre autres choses, dans la gestion et le courtage de listes, l'établissement de profils géodémographiques, l'analyse de base de données, l'établissement du profil de consommateurs individuels, la cueillette de données au moyen d'enquêtes et le forage de données issues de multiples sources.

Bien qu'une bonne partie des données prennent la forme de listes normalisées et de profils de groupes, on trouve de nombreuses preuves d'établissement de profils de consommateurs individuels. 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. On souhaite que ce rapport fournisse aux chercheurs, aux protecteurs des consommateurs, aux décideurs et à d'autres de l'information utile pouvant servir de base à des lois et à des politiques efficaces pour protéger les renseignements personnels dans le secteur privé.

Le rapport est affiché à l'adresse suivante : <http://www.cippic.ca/en/bulletin/>.

Les consommateurs tirent-ils profit de l'échange de renseignements personnels?

L'Union des consommateurs, avril 2007, 73 pages

Marie-Ève Rancourt

Ce projet de recherche vise essentiellement à savoir si l'échange de renseignements personnels entre les entreprises est profitable aux consommateurs.

En abordant cette question, l'auteure prend en considération les avantages des pratiques de traitement des données suivantes et nous présente ces conclusions.

Établissement de profils : Bien que certains consommateurs puissent apprécier la personnalisation des services et la publicité qui découle de la capacité des spécialistes du marketing de créer un profil personnalisé du consommateur, rien ne garantit la précision de l'information contenue dans un profil qui peut servir à des fins préjudiciables à la personne concernée (par exemple, les décisions relatives à l'octroi de crédits ou à l'embauche). De plus, l'établissement de profils mène à la création de catégories différentes de consommateurs (les « bons » et les « mauvais » consommateurs) et ouvre la porte aux pratiques discriminatoires – notons que la Cour suprême de la France a décidé qu'une telle caractérisation du consommateur était illégale dans ce pays. L'établissement de profils peut également mener à un marketing ciblé de plus en plus envahissant qui peut changer la nature des rapports avec Internet et encourager les gens à surconsommer.

Témoins : Les fichiers témoins (ou « cookies ») facilitent l'utilisation d'Internet, mais sont souvent installés sans le consentement de l'utilisateur et recueillent sur ce dernier des renseignements à son insu. En particulier, les témoins persistants (ceux qui demeurent sur le disque dur même après la fin d'une séance sur Internet) font en sorte que le consommateur perd toute prise sur ses renseignements personnels – avec les risques concomitants que sont l'établissement de profils et le vol d'identité.

Logiciels espions : Dans les cas où les entreprises incluent des logiciels espions dans leur logiciel, qui se télécharge automatiquement lorsque l'utilisateur accepte le contrat de licence, un tel logiciel recueille des renseignements personnels, le plus souvent sans consentement explicite, consomme de l'espace sur la mémoire vive et le disque dur, et mobilise des ressources du processeur, ce qui peut avoir une incidence négative sur d'autres applications logicielles. En outre, seule l'industrie tire profit de la collecte de renseignements par logiciel espion, habituellement dans des circonstances où elle craint que le consommateur refuse de communiquer ces renseignements si on lui donnait le choix.

Pourriel : Certains milieux défendent les pourriels qu'ils considèrent comme une forme de publicité économique et inoffensive sur le plan écologique, qu'il est facile de supprimer ou de n'en pas tenir compte, et qui permet aux petites compagnies de faire concurrence aux plus grandes. Cependant, l'auteure ne voit dans cette forme de publicité aucun avantage pour le consommateur compte tenu du facteur élevé de désagrément et du fait que le pourriel offre rarement des produits susceptibles d'intéresser les consommateurs.

Cartes de fidélité : L'auteure décrit les préoccupations liées à la vie privée que représentent ces cartes, comme l'impressionnante quantité de renseignements que peuvent recueillir les entreprises, le manque de transparence entourant la collecte et l'impossibilité des consommateurs de profiter des avantages d'une carte de fidélité sans accepter cette collecte de renseignements personnels.

Période de conservation et mesures de sécurité : Les pratiques actuelles portent préjudice aux consommateurs en raison des risques pour la protection de la vie privée que posent la période de conservation prolongée des données et les mesures de sécurité médiocres.

Circulation transfrontalière des données : Contrairement aux lois européennes, les lois canadiennes n'interdisent pas la transmission transfrontalière ni ne l'assujettissent à des

conditions de protection équivalente. L'auteure laisse entendre que l'exportation de données personnelles des Canadiennes et des Canadiens permet aux entreprises de se soustraire aux normes canadiennes et de profiter de lois moins contraignantes.

L'auteure intègre de nouveaux éléments de recherche sur le terrain en s'appuyant sur une enquête et une analyse des politiques en matière de protection de la vie privée sur Internet de dix entreprises. Elle tente, notamment, de savoir si les entreprises s'efforcent d'obtenir un consentement explicite à la collecte et à l'utilisation des renseignements personnels. L'enquête, qui s'est déroulée entre le 10 et le 20 avril 2007, comporte une grille de résultats et une discussion sur les points saillants des conclusions.

On peut consulter le rapport à l'adresse :

http://www.consommateur.qc.ca/union/docu/vieprivee/info_perso_f.pdf

Application de la *LPRPDÉ* : Examen des énoncés de confidentialité sur Internet et des pratiques en ligne

Université de Toronto, mai 2005, 43 pages.

Rajen Akalu, Barbara Bressolles, Sapna Mahboobani, Aniz Alani, Andrew Clement

Les auteurs de ces quatre études évaluent l'efficacité avec laquelle divers commerces de détail, entreprises de télécommunications, entreprises bancaires et transporteurs aériens canadiens se conforment au principe de transparence de la *LPRPDÉ* et, dans le cas des transporteurs aériens et des banques, à l'opinion sur les avis d'information du groupe de travail sur la protection des données de la Commission européenne (*Data Protection Working Party Opinion on information notices*). Ils ont examiné les politiques sur la protection de la vie privée en ligne des entreprises selon ces critères, en combinant leur recherche avec des enquêtes, des entrevues et des interactions en ligne auprès des chefs de la protection des renseignements personnels et d'autres experts.

L'étude sur les télécommunications est un sommaire de l'affaire *Englander c. Telus Communications Inc.* portée devant la Cour d'appel fédérale. M. Englander prétendait que Telus avait contrevenu aux prescriptions de la *LPRPDÉ* concernant les connaissances et le consentement (qui devraient refléter le principe de transparence), et que l'imposition de frais pour obtenir un numéro de téléphone non publié transgressait l'esprit, sinon la lettre de la Loi. La Cour a approuvé le premier point, mais pas le second. Les frais de service des entreprises de télécommunications sont réglementés par un autre organisme fédéral.

Le second document examine les déclarations de confidentialité en ligne de quatre transporteurs aériens, soit Air Canada, WestJet, CanJet et Jetsgo, pour déterminer leur conformité à la *LPRPDÉ* et à l'opinion du groupe de travail. La conformité à l'opinion du groupe de travail donne un aperçu des processus politiques de la Commission européenne visant à assurer une protection adéquate des renseignements personnels sur les passagers et les équipages arrivant d'Europe. L'Agence des services frontaliers du Canada se sert de ces renseignements pour repérer les éventuelles menaces terroristes. Les engagements de l'Agence en matière de confidentialité envers le groupe de travail ont reçu un accueil positif et ont permis d'en déduire que la protection était adéquate. Toutefois, l'étude fait état d'un manque d'uniformité dans les déclarations de confidentialité en ligne des transporteurs aériens et proposent que le Commissariat à la protection de la vie privée y donne suite au moyen de vérifications ou d'activités de sensibilisation.

Le troisième document explique plus en détail l'opinion du groupe de travail sur l'harmonisation des avis de confidentialité et évalue la mesure dans laquelle deux grandes banques canadiennes (CIBC et la Banque Scotia) répondent aux normes en question. L'auteur reconnaît que l'harmonisation favorisera vraisemblablement une plus grande facilité de comparaison entre les déclarations, y compris la mise en lumière des omissions. Il recommande un système d'avis en trois volets, le premier fournissant de l'information de base, et les deuxième et troisième, apportant de l'information plus pertinente requise par la Commission et la loi nationale. Ensemble, ils constituent un avis juridique. Dans les circonstances, on estime que les déclarations de confidentialité de la CIBC et de la Banque Scotia sont insuffisantes, bien que la déclaration de la Banque Scotia soit assortie de passerelles qui la rendent plus conviviale.

Le dernier document comporte un examen des déclarations de confidentialité dans le secteur du commerce de détail qui relèvent des compétences provinciales. L'auteur conclut que le fait que ce secteur suive généralement l'exemple des entreprises fédérales telles que les banques et les transporteurs aériens (qui ont été assujetties aux lois sur la protection des renseignements personnels trois ans avant les commerces de détail) n'est peut-être pas une si bonne chose en soi. La publication de renseignements plus détaillés donnerait aux consommateurs une base appropriée sur laquelle évaluer les pratiques des entreprises en matière de confidentialité et demander des comptes à ces dernières.

Vie privée des consommateurs et conformité des entreprises privées

Dans l'ensemble, les auteurs observent une conformité adéquate, et concluent que les entreprises semblent davantage disposées à communiquer leurs politiques sur la protection de la vie privée par mesure de précaution que par respect pour la vie privée. Il y a place à l'amélioration.

On peut consulter le rapport à l'adresse suivante :

http://pipedaproject.atrc.utoronto.ca/index.php?option=com_content&task=view&id=1&Itemid=1

Des modèles de protection de la vie privée qui fonctionnent : Un guide pour les organisations canadiennes

Pratiques exemplaires de gestion des données : Un guide pour les spécialistes du marketing

Conformité des petites entreprises aux règlements en matière de protection de la vie privée – Résultats de recherche

Association canadienne du marketing (trois rapports distincts), juin 2005

En 2005, l'Association canadienne du marketing a produit deux guides et mené une enquête portant sur les lois en matière de protection de la vie privée et sur les questions de conformité.

Des modèles de protection de la vie privée qui fonctionnent : Un guide pour les organisations canadiennes (13 pages) – Ce document examine les modèles de gestion de la protection de la vie privée dans les organisations canadiennes. La prémisse de l'étude est que la fonction de gestion de la protection de la vie privée est relativement nouvelle, et qu'il n'existe pas encore une « bonne façon », qui soit généralement acceptée ou uniforme, de mettre en place, d'organiser et de gérer la fonction de protection de la vie privée dans les entreprises. Les auteurs s'appuient sur des entrevues menées auprès de plus d'une douzaine d'organisations canadiennes de premier plan pour regrouper les approches utilisées sous trois principaux modèles, auxquels s'ajoute un modèle de rechange pour les petites organisations – des modèles qui, d'après les auteurs, fonctionnent pour les organisations canadiennes.

Le rapport décrit brièvement chacun des modèles et renferme des observations d'agents de protection de la vie privée sur les forces de leur modèle. On y résume également les avantages et les inconvénients de diverses structures de protection de la vie privée, les principaux rôles et responsabilités de ces agents, les processus de gestion de la conformité en matière de protection de la vie privée et les processus de vérification, le tout s'accompagnant dans chaque cas d'une petite liste non numérotée des éléments qui fonctionnent. Le rapport se termine par un court texte sur l'intégration de la protection de la vie privée dans une stratégie opérationnelle globale.

Pratiques exemplaires de gestion des données : Un guide pour les spécialistes du marketing (13 pages) – Ce document renferme un ensemble de lignes directrices axées sur le consommateur et portant sur les quatre principaux domaines d'intérêt pour les spécialistes du marketing, soit la collecte de renseignements, l'obtention du consentement, la protection des données et l'échange de données avec des partenaires.

Dans chacun de ces domaines d'intérêt, le document fournit des conseils précis, détaillés et pratiques, fondés sur les principes de confidentialité de l'Association canadienne du marketing qui aideront ces spécialistes à appliquer les pratiques exemplaires.

À titre d'exemple, la section sur le consentement explique les différentes formes de consentement et aborde neuf points particuliers dont les spécialistes du marketing devraient tenir compte au moment d'obtenir un consentement. On trouve des lignes directrices semblables dans chacune des autres sections. Le rapport se termine par un sommaire d'une page sur les pratiques exemplaires.

Conformité des petites entreprises aux règlements en matière de protection de la vie privée – Résultats de recherche (23 pages) – Ce document se fonde sur une enquête en ligne à laquelle ont participé 157 entreprises (275 entreprises ont pris part à l'enquête, mais 118 ne l'ont pas terminée, principalement parce que les lois sur la protection de la vie privée ne s'appliquaient pas à leurs activités commerciales).

L'enquête comportait des questions sur le traitement des renseignements personnels au sein des entreprises, le comportement des entreprises à l'égard des lois en matière de protection de la vie privée, les mesures que prennent ces entreprises pour assurer la conformité à ces lois, le classement de divers points à considérer quant aux risques pour la vie privée (par exemple, ce

qui porte atteinte à la réputation d'une entreprise), les mesures de protection en place, les obstacles à l'entière conformité aux lois sur la protection de la vie privée ainsi que les ressources supplémentaires nécessaires.

Le manque d'information était considéré comme le principal obstacle à la conformité (51 p. 100). Le second obstacle en importance était le temps qu'exigeaient la mise en place de nouvelles lois et la mise à jour des processus (43 p. 100).

En ce qui concerne les ressources supplémentaires, les trois principales réponses étaient, par ordre d'importance, la nécessité de comprendre les lois sur la protection de la vie privée du point de vue de l'industrie, le besoin en information simplifiée et plus accessible, et la nécessité d'améliorer les pistes pour trouver de l'information en ligne.

Le rapport se terminait par des recommandations où l'on invitait le Commissariat à la protection de la vie privée à aider les petites entreprises à se conformer aux lois sur la protection de la vie privée (y compris la nécessité de rejoindre plus d'entreprises). Il lui faudrait, suggère-t-on, commencer par les rudiments, reconnaître les similitudes et les différences entre les industries, créer un site Web consacré uniquement à la conformité aux lois sur la protection de la vie privée et aider les entreprises à élaborer une politique en la matière.

On peut consulter les rapports à l'adresse suivante :
<http://www.the-cma.org/?WCE=C=47|K=224334>.

Assurer le respect des principes relatifs à la protection de la vie privée : Projet de recherche sur l'évaluation de l'application de la LPRPDÉ

British Columbia Civil Liberties Association, mars 2006, 91 pages

Chercheur principal : Kirk Tousaw, avocat

Ce rapport examine les mécanismes d'application de la LPRPDÉ par opposition à d'autres modèles appliqués dans les provinces du Québec, de l'Alberta et de la Colombie-Britannique, ainsi qu'en Australie et en Nouvelle-Zélande, et deux modèles non liés à la protection de la vie privée au Canada qui réglementent les droits de la personne et les télécommunications.

La recherche combine des analyses documentaires et des interviews menées auprès de responsables de la protection de la vie privée, de défenseurs et d'agents des parties réglementées, pour analyser les répercussions pratiques de différents choix dans les modèles d'application. La recherche met en lumière les pouvoirs ayant été accordés et utilisés afin de cerner les mécanismes politiques et juridiques les plus susceptibles d'améliorer la conformité.

Selon l'étude, le rôle d'ombudsman que joue le Commissariat à la protection de la vie privée (CPVP) en vertu de la LPRPDÉ suscite davantage d'insatisfaction que de bons commentaires, et il faudrait modifier la loi pour l'assortir de mesures d'application plus efficaces. Le CPVP dispose de solides pouvoirs d'enquête (en plus de ses rôles de vérification et de sensibilisation), mais ne peut rendre des ordonnances ni accorder des dommages-intérêts. La seule voie de redressement passe par la Cour fédérale, un état de choses qu'on considère comme un obstacle considérable à l'accès à la justice. L'auteur fait valoir que le modèle d'ombudsman a pu s'avérer approprié pour obtenir le consensus des parties réglementées lors de l'adoption de la LPRPDÉ. Il reconnaît le vif engagement du CPVP à améliorer l'application en vertu du modèle existant. Toutefois, il conclut que, après cinq ans, le Commissariat a besoin de plus d'outils pour faire évoluer les parties réglementées vers une conformité accrue.

On recommande notamment au CPVP d'instaurer plusieurs réformes sans modifier la loi ou le modèle d'ombudsman, par exemple :

- 1) Mettre en place des normes d'enquête améliorées, comme le recours à des exposés convenus des faits, en s'assurant que chaque partie a toute liberté de répondre et que les rapports qu'elles reçoivent sont analogues.
- 2) Obtenir des fonds supplémentaires pour offrir de l'aide juridique, effectuer des visites sur les lieux afin d'examiner les politiques sur la protection de la vie privée, et fournir davantage d'information sur support papier et électronique.
- 3) Mettre en place des processus de vérification et d'examen permanents pour mesurer la conformité, dont les résultats seraient publiés dans le rapport annuel de la commissaire et où on indiquerait notamment les entreprises non conformes.

L'auteur recommande également d'apporter des modifications à la LPRPDÉ, en concluant que des outils d'application plus solides existants et utilisés dans d'autres juridictions amélioreront la conformité tout en maintenant le modèle de l'ombudsman pour la résolution des conflits. Ces nouveaux outils feraient en sorte que la commissaire pourrait notamment : rendre des ordonnances pouvant être présentées à la Cour fédérale et qui seraient applicables sur-le-champ; attribuer une indemnité aux plaignants et, dans les cas flagrants, réclamer à l'intimé des dommages-intérêts punitifs; permettre à des représentants de déposer des plaintes auprès du CPVP (par un tiers au nom d'une personne); enfin, permettre à des plaignants de faire un recours collectif devant la Cour fédérale.

On peut consulter le rapport à l'adresse suivante :

<http://www.bccla.org/othercontent/FINAL%20REPORT.APRIL06.pdf>.

Projet de normes de certification professionnelle

Canadian Association for Professional Access and Privacy Administrators, et Association canadienne d'accès à l'information et de la protection des renseignements personnels, mars 2007, 65 pages

Ce rapport est le résultat final de la première phase d'une initiative permanente de l'Association canadienne d'accès à l'information et de la protection des renseignements personnels (ACAP) et de la Canadian Association for Professional Access and Privacy Administrators (CAPAPA) visant à établir des normes à l'intention des professionnels de l'accès à l'information et de la protection de la vie privée au Canada.

Ce projet a entraîné la mise sur pied d'un groupe de travail présidé par Frank Work, commissaire à l'information et à la protection de la vie privée de l'Alberta, et composé de représentants principaux de l'ACAP, de la CAPAPA et de l'Association sur l'accès et la protection de l'information (AAPI) du Québec, de cadres supérieurs du Commissariat à l'information du Canada, de la commissaire à la protection de la vie privée du Canada, ainsi que des universitaires, des consultants et des représentants des industries concernés par la question.

L'objectif de ce rapport consistait à dégager et à établir des normes professionnelles à l'intention des professionnels de l'accès à l'information et de la protection de la vie privée (PAIPVP). Les normes constitueront des critères pratiques de niveau minimal pour évaluer les compétences que possède un PAIPVP qui tente d'obtenir une certification.

Les auteurs font valoir qu'on a vivement besoin de normes professionnelles et qu'il faudrait, au cours de phases subséquentes de ce travail, créer un organisme de certification et de surveillance. Ils soulignent que les PAIPVP peuvent être considérés, dans certains contextes, comme des responsables quasi judiciaires faisant respecter des droits juridiques d'une nature quasi constitutionnelle. Ils décrivent de tels professionnels comme les gardiens d'une fiducie d'intérêt public qui sous-tend nos libertés démocratiques et économiques. Ils soutiennent que le travail de tels professionnels nécessite des qualités spéciales et un comportement professionnel de haut niveau.

Le rapport décrit les trois aspects interdépendants du travail des PAIPVP, soit l'administration, l'exécution et la consultation, qui exigent tous une orientation différente. Les auteurs indiquent que l'ordonnancement de ces aspects est une considération importante dans la conception et la classification des descriptions d'emploi, dans l'organisation des groupes de travail de PAIPVP et dans la conception de structures de carrière.

Les compétences requises pour les trois aspects sont énoncées dans le profil de compétences du PAIPVP, qui indique le niveau de maîtrise nécessaire pour réussir à entrer dans la profession par le biais d'un processus de certification officiel. Un total de 24 compétences particulières sont recensées sous les trois aspects, y compris l'interprétation des lois, le développement de relations et d'un climat de confiance, l'acquisition de connaissances technologiques et la prestation d'activités de formation et de sensibilisation. Les auteurs ajoutent que ce modèle de compétences prévoit un éventuel perfectionnement et des améliorations personnalisées afin d'établir des niveaux d'expertise plus pointue dans chaque compétence. L'annexe C du rapport contient une liste d'indicateurs d'accomplissement pour chacune des 24 compétences, ce qui en fait une matrice extrêmement utile pour toute évaluation des qualifications des PAIPVP.

Le rapport contient également une proposition de code d'éthique en six points pour les PAIPVP, qui vise à définir leurs obligations professionnelles et à établir, pour les clients, les intervenants et les membres du public, les attentes envers les PAIPVP et les comptes qu'ils doivent rendre.

Les auteurs concluent en énonçant des critères de certification que pourrait appliquer un organe de certification professionnel et en présentant une liste de publics cibles en matière de certification et un sommaire du travail qu'il reste à terminer. Les prochaines étapes du travail comprennent un modèle de certification recommandé (exécution en août 2007) et un modèle de gouvernance recommandé, à terminer d'ici la fin de novembre 2007.

On peut consulter le rapport à l'adresse suivante : <http://www.capa.ca/Main%20certification.html>.

Stratégies de formulation de politiques sur la protection de la vie privée compréhensibles pour les enfants

Université de Western Ontario, mars 2007, 119 pages

Jacquelyn Burkell, Valerie Steeves et Anca Micheti

Cette recherche visait à dégager des directives pour la rédaction de politiques sur la protection de la vie privée que les enfants et les adolescents pourraient interpréter avec relativement d'aisance et de précision. La poursuite de cet objectif nécessitait une stratégie en trois volets. En premier lieu, les auteures ont analysé la documentation pertinente sur la capacité de lecture et la compréhension de texte au sein des groupes d'âge cibles. En deuxième lieu, elles ont créé des groupes de discussion avec des enfants et des adolescents pour examiner leur expérience et leur pratique de consultation et d'interprétation de politiques en matière de protection de la vie privée sur les sites préférés qui leur étaient destinés. À partir des résultats obtenus, les auteures ont établi un ensemble de directives éventuelles pour la rédaction de politiques sur la protection de la vie privée, dont on a fait l'essai empirique dans la troisième phase de la recherche. Le résultat final est un ensemble de directives pour la rédaction de politiques sur la protection de la vie privée qui, selon les auteures, améliore la donne en rehaussant fortement l'intelligibilité des politiques sur la protection de la vie privée dont prennent connaissance les enfants et adolescents canadiens lorsqu'ils naviguent sur Internet.

La recherche que les auteures et d'autres ont menée antérieurement indique qu'il est difficile de trouver des politiques sur la protection de la vie privée, que ces dernières sont longues et souvent écrites à un niveau d'intelligibilité non accessible à la plupart des adultes. Cette recherche antérieure a permis aux auteures d'apprendre que 49 des 50 principaux sites pour les enfants contiennent des politiques sur la protection de la vie privée. Toutefois, il est souvent difficile de trouver ces politiques. En outre, elles tendent à être longues (1 902 mots en moyenne) et leur niveau de lecture moyen est à mi-chemin entre la 11^e et la 12^e année. (Le niveau de 8^e année est celui qu'on recommande pour les documents destinés aux adultes, selon le test Flesch.)

Bien qu'on ait habituellement recours aux formules de lisibilité pour évaluer le niveau d'intelligibilité des politiques sur la protection de la vie privée, les auteures préviennent que la rédaction de politiques en fonction des formules de lisibilité n'est pas en soi une garantie de compréhension. L'essentiel du rapport porte sur un ensemble de directives proposées pour aborder la rédaction des politiques sur la protection de la vie privée, la structure du texte et la conception globale des politiques. Il existe 14 directives précises regroupées sous ces trois catégories. À titre d'exemple, l'une des directives fait valoir qu'il faudrait éviter la construction avec double négation. Ces directives reposent sur la rétroaction du lecteur et la recherche antérieure concernant les facteurs qui influent sur la compréhension de textes. La description prolongée de chaque directive comporte des constatations de recherche pertinentes, des observations formulées par des jeunes qui sont pertinentes à la directive, et des exemples pratiques d'application positive et négative de la directive. Pour tester l'efficacité des directives, les auteures ont comparé les versions originales et révisées des politiques mêmes en ligne (avec des dénominations maquillées). En tout, 35 participants âgés de 11 à 17 ans ont participé au test. Les politiques révisées ont amélioré le degré de compréhension, et les participants étaient mieux en mesure de faire rapport avec précision sur l'information recueillie par l'entremise du site. En outre, les participants ont très majoritairement préféré les versions remaniées. Le rapport inclut un tableau utile résumant les directives.

Les auteures se sont également rendu compte que les jeunes se souciaient de la protection de leur vie privée. Dans les groupes de discussion dirigés par les auteures, il est devenu évident que, bien que la protection de la vie privée ne soit pas un objectif premier de l'activité en ligne (à cet égard, les auteures considèrent que les enfants ne sont pas différents des adultes), il va de soi que les enfants et les adolescents ne se sentent pas à l'aise avec l'omniprésence de la surveillance en ligne, mais ont le sentiment de n'avoir aucune prise sur la question. Comme le disait si bien une jeune fille: « Il y a des portes sur Internet, mais elles sont brisées ».

Directives à l'intention des professionnels de la protection de la vie privée et des entreprises

Les auteures ont également constaté que les enfants et les adolescents se méfient généralement des organisations qui recueillent des renseignements personnels sur Internet, et que cette méfiance imprègne leurs attentes vis-à-vis des politiques sur la protection de la vie privée dont ils prennent connaissance en ligne. Selon eux, ces politiques visent à compliquer les efforts pour découvrir ce qui se produit avec leurs renseignements, et ils prêtent aux rédacteurs de ces lois une mauvaise volonté. Selon un adolescent de 17 ans, ils exploitent les jeunes parce qu'ils savent qu'ils n'ont pas une capacité de lecture de niveau universitaire.

On peut consulter le rapport à l'adresse suivante : <http://idtrail.org/content/view/684/42/>.

Directives sur la dépersonnalisation des renseignements personnels sur la santé pour l'ensemble du Canada

Institut de recherche du Centre hospitalier pour enfants de l'est de l'Ontario, avril 2007, 83 pages

Khaled El Emam, Elizabeth Jonker, Scott Sams, Emilio Neri, Angelica Neisa, Tianshan Gao et Sadrul Chowdhury

Cette étude porte sur les risques de repersonnalisation des renseignements personnels sur la santé anonymisés lorsque ces renseignements sont combinés à de l'information issue de bases de données publiques ou à des données obtenues par déduction (par exemple, la prédiction du sexe et de l'année de naissance à partir des prénoms et des années d'obtention des diplômes). L'étude a permis d'apprendre que, dans certaines circonstances, le taux de succès d'une tentative de repersonnalisation de données de santé anonymisées peut être très élevé. L'étude a également révélé que de tels risques de repersonnalisation ne sont pas négligeables, particulièrement parmi les chercheurs d'emploi qui peuvent afficher suffisamment de renseignements personnels sur des sites Web publiquement accessibles pour permettre quelques tentatives simples de repersonnalisation.

Fortes de ces conclusions, l'équipe de recherche a élaboré des lignes directrices pratiques et un outil concret d'anonymisation des données qui permettront aux gardiens des données sur la santé de gérer les risques de repersonnalisation liés à leurs activités de diffusion des données et de protéger la vie privée des Canadiennes et des Canadiens. L'accent est principalement mis sur l'anonymisation des quasi-identificateurs tels que le sexe, la date de naissance et les codes postaux ou de zone.

Les auteurs citent la recherche américaine effectuée par Latanya Sweeney, selon laquelle il est possible d'identifier 87 p. 100 de la population américaine uniquement à partir de sources de données publiques, en utilisant les trois variables quasi-identificatrices du code de zone, du sexe et de la date de naissance. Le sexe, la date de naissance et la ville ou la municipalité de résidence permettent à eux seuls d'identifier 53 p. 100 de la population américaine.

Les auteurs ont cherché à déterminer à quoi ressemblerait une situation parallèle dans laquelle on mettrait à profit les quasi-identificateurs et les bases de données accessibles en Ontario. Afin de cerner les bases de données d'identification dont pourrait se servir une personne qui tente de procéder à une repersonnalisation, les chercheurs ont examiné les ensembles de données accessibles auprès de 29 ministères de l'Ontario, de courtiers de renseignements commerciaux, de sources généalogiques, de sociétés professionnelles, de Statistique Canada et d'Élections Canada. Ils ont également testé la capacité de relier les données sur les personnes par le biais de diverses sources publiquement accessibles, ce qui a permis de tirer certaines conclusions statistiques incontestables sur la capacité de relier les listes des médecins et avocats de l'Ontario à des codes postaux domiciliaires et dates de naissance, et sur la capacité également d'obtenir la date de naissance, les numéros de téléphone à domicile et le sexe des propriétaires occupants à Ottawa et à Toronto. Les auteurs du rapport se penchent également sur les tentatives par inférence – particulièrement la précision avec laquelle on peut faire des déductions sur le sexe et l'année de naissance au moyen d'un logiciel permettant d'établir le sexe et d'autres méthodes prédictives. On trouve également une analyse détaillée de la capacité de prédire le code postal domiciliaire d'une personne à partir d'un autre code postal – par exemple, une adresse de travail ou une adresse de médecin. Les chercheurs ont pris en considération des codes postaux urbains et ruraux en Alberta, en Ontario et en Nouvelle-Écosse.

En s'appuyant sur les résultats de cette recherche, les auteurs ont conclu que la région seule (code postal), le sexe seul, l'année de naissance seule et la combinaison du sexe et de la région constituaient des quasi-identificateurs représentant de façon générale un faible risque de repersonnalisation de données gardées anonymes. Toutefois, ils préviennent que cela s'applique uniquement aux circonstances précises de leurs scénarios de tentatives et de leurs hypothèses

sur le seuil de risques. Ils sont d'avis que le travail ultérieur sur ces questions devrait viser à consigner le niveau des risques de repersonnalisation.

L'étude contient des résultats de recherche récente sur l'ampleur des renseignements personnels (nom, adresse, code postal, numéro de téléphone et un indicateur de l'âge) que les Canadiennes et les Canadiens sont disposés à afficher sur Internet lorsqu'ils envoient leur curriculum vitae, et aussi les renseignements personnels qu'on peut récupérer à partir des disques durs vendus.

À partir d'un utilitaire de récupération des fichiers, les chercheurs ont pu récupérer de l'information personnelle dans 39 des 60 unités de lecture qu'ils s'étaient procurés auprès de vendeurs de matériel informatique usagé, en dépit de la répartition et du reformatage. La grande majorité des unités de lecture avec des données récupérées contenaient des renseignements personnels, notamment sur les salaires et les déclarations de revenus, de la correspondance personnelle, de l'information sur les polices d'assurance-vie et les héritages, des données sur la liste de paie, des vérifications des casiers judiciaires, des documents de divorce ainsi que des renseignements personnels sur la santé. Il y avait même une unité de lecture avec de l'information très délicate sur la santé mentale d'un certain nombre de personnes.

Devant un tel état de choses, les auteurs recommandent un processus décisionnel pour rendre anonyme un ensemble de données, et fournissent une liste non numérotée de certaines considérations utiles et détaillées pour différents quasi-identificateurs.

On peut consulter le rapport à l'adresse suivante :
<http://www.ehealthinformation.ca/documents/OPCReportv11.pdf>.

Dossiers de santé électroniques et la *Loi sur la protection des renseignements personnels et les documents électroniques*

Université de l'Alberta et Université de Victoria, avril 2005, 100 pages

Nola Ries, Elizabeth Robertson, Fiona Moore et Jane Steblecki

Ce rapport porte sur les questions de vie privée, de confidentialité et de sécurité dans le contexte des renseignements personnels sur la santé et des dossiers de santé électroniques (DSE). On y lit que la demande de progrès rapides dans les systèmes de gestion des DSE peut être quelque peu prématurée, et qu'il faudrait attendre que des discussions pertinentes aient eu lieu en ce qui touche la protection de la vie privée, la confidentialité et la sécurité.

La première partie est une enquête sur certains des enjeux liés aux systèmes de DSE, y compris les défis que pose l'établissement de tels systèmes, les concepts de protection de la vie privée, de confidentialité et de sécurité dans le cadre des soins de santé, l'état des systèmes de DSE au Canada et la complexité du paysage canadien en matière de protection de la vie privée. Cette partie se termine par une observation de la professeure Elaine Gibson, selon laquelle la protection des renseignements personnels ne devrait pas être considérée comme un obstacle à la mise en place d'une infrastructure de santé pancanadienne. Elle ajoute qu'il faut toutefois comprendre que des régimes rigoureux de protection des renseignements personnels et de sécurité sont essentiels si l'on veut préserver la confiance des membres de la société canadienne, qui s'attendent à ce que leurs renseignements personnels sur la santé reçoivent le plus haut niveau de protection.

La deuxième partie est un examen détaillé des règles de la *LPRPDÉ* dans le contexte des DSE, ainsi que des règles concernant les DSE dans les lois relatives à l'information sur la santé au Manitoba, en Saskatchewan, en Alberta et en Ontario.

Les auteures accordent une attention particulière à la question du consentement aux termes de la *LPRPDÉ* dans le contexte des DSE. Elles se penchent sur les défis que pose l'obtention d'un consentement éclairé de la part des patients pour utilisation ou communication futures des renseignements sur un DSE, en soulevant le problème que pose l'impossibilité de prévoir les utilisations futures des renseignements lorsque ceux-ci sont initialement entrés dans le système. Elles abordent également le concept du « cercle de soins » et la capacité de se fier au consentement tacite pour des utilisations relatives aux traitements ou la communication de renseignements personnels, ainsi que la notion de ce qui constitue, dans les faits, un consentement éclairé. Il y est également question de l'utilisation de recherche secondaire, et les auteures font référence à des études sur des patients qui acceptent l'utilisation secondaire de leur DSE à des fins de recherche.

L'examen des lois provinciales sur la protection des renseignements sur la santé offre des analyses détaillées des dispositions relatives aux DSE, y compris la façon dont certaines de ces dispositions se sont modifiées avec le temps. Les auteures concluent cette partie en indiquant que les entités du secteur de la santé assujetties aux lois provinciales sur la protection des renseignements sur la santé pourraient également avoir à se conformer à la *LPRPDÉ* si elles s'engagent dans des activités commerciales. Elles ajoutent, par contre, que dans certaines situations, une organisation trouvera impossible de se conformer aux prescriptions de la *LPRPDÉ* et des lois provinciales. Le cas échéant, les auteures estiment que l'organisation devrait chercher à obtenir des directives supplémentaires de la part des commissaires provinciaux ou de la commissaire fédérale et que les situations où les règles législatives entravent la prestation des soins de santé aux patients doivent également être déclarées aux commissaires à la protection de la vie privée ainsi qu'aux ministères concernés qui supervisent l'application des lois.

La troisième partie renferme un examen détaillé des initiatives liées aux DSE en Australie, au Royaume-Uni et aux États-Unis, des environnements législatifs et des problèmes à résoudre, y compris des enjeux tels que le couplage des données, le détournement d'usage et le soutien à la baisse des médecins (au R.-U.) en ce qui concerne les systèmes de dossiers électroniques.

Le rapport comporte trois annexes : 1) un tableau des lois actuelles régissant les secteurs public, privé et de la santé, et les situations où elles s'appliquent; 2) des résumés de cas d'utilisation des DSE par quatre agences : la BC Cancer Agency, l'Alberta Capital Health Region, le projet d'information pharmaceutique de la Saskatchewan (*Saskatchewan Pharmacy Information Project*) et le système d'information hospitalier de la Nouvelle-Écosse (*Nova Scotia Hospital Information System*); 3) une liste de pratiques exemplaires dans l'élaboration d'un système de DSE, fondé sur les principes de protection de la vie privée appliquée par la CSA. Cette annexe peut se révéler l'un des volets les plus importants du rapport pour les décideurs dans le domaine des renseignements personnels sur la santé.

On peut consulter le rapport à l'adresse suivante :
<http://www.law.ualberta.ca/centres/hli/pdfs/ElectronicHealth.pdf>.

Utilisation secondaire des renseignements personnels consignés dans des systèmes nationaux de dossiers électroniques de santé : Développements clés et enjeux

Centre de bioéthique, Institut de recherches cliniques de Montréal, juin 2007, 93 pages

David J. Roy et François Fournier avec l'aide technique de Thierry Hurlimann

Cette étude vise à attirer l'attention sur les perspectives, possibilités et préoccupations que les systèmes nationaux de dossiers de santé électroniques (DSE) soulèveront à l'égard des utilisations secondaires de renseignements personnels sur la santé. La recherche est extrêmement bien documentée et à jour, et comporte une analyse approfondie des préoccupations entourant les utilisations secondaires.

Selon les auteurs, la confiance du patient envers la relation thérapeutique établie avec les professionnels de la santé est en jeu si les renseignements personnels sur la santé sont utilisés d'une manière qui a peu ou qui n'a rien à voir avec les soins directs du patient. Les utilisations secondaires peuvent également menacer l'autonomie du patient – si les patients subissent des contrariétés quant à la prise qu'ils peuvent exercer sur leurs renseignements personnels sur la santé – et la fidélité (intégrité) des professionnels de la santé. En outre, de telles utilisations peuvent susciter de lourdes préoccupations sociales, culturelles et démocratiques qui sont d'une importance cruciale.

Les utilisations secondaires des renseignements personnels sur la santé se définissent généralement comme des utilisations non directes en matière de soins, et incluent des fins liées aux soins de santé (comme la gestion des soins de santé, la santé publique, la recherche médicale) et des buts non liés à la santé (comme l'application de la loi, l'immigration). Les limites actuelles entre les utilisations primaires et secondaires sont contestées par certains utilisateurs secondaires, comme les chercheurs en médecine, qui souhaitent être reconnus à titre d'utilisateurs primaires et, en conséquence, être exemptés de processus de consentement plus rigoureux, entre autres choses.

Les auteurs décrivent les DSE comme des registres axés sur le patient qui découlent des dossiers électroniques médicaux (DEM). Les DSE sont donc des sous-ensembles de l'information contenue dans les DEM, qui est téléchargée vers les sites centraux et utilisée pour un éventail de fins relatives aux services axés sur le patient et à des améliorations dans la prestation des soins de santé. Bien que certains pays ainsi que le Québec et d'autres provinces du Canada aillent de l'avant avec des systèmes provinciaux de DSE, aucun système national du genre n'est encore intégralement mis en place et opérationnel à l'échelle nationale. Par conséquent, le rapport de recherche est un aperçu d'une situation fluide et évolutive, qui offre un témoignage des enjeux liés aux utilisations secondaires futures des renseignements personnels sur la santé dans un système national de DSE.

Dans la première partie du rapport, les auteurs se penchent sur le système de DSE proposé par Inforoute Santé du Canada et examinent les trois principaux aspects des utilisations secondaires des renseignements personnels sur la santé dans les systèmes nationaux de DSE, à savoir : 1) les éléments intégrés aux DSE nationaux qui améliorent ou limitent les utilisations secondaires des renseignements personnels sur la santé; 2) le cadre de gouvernance des systèmes nationaux de DSE concernant les utilisations secondaires des renseignements personnels sur la santé, y compris des questions se rapportant au consentement; 3) les attentes et les préoccupations des intervenants à l'égard des utilisations secondaires des renseignements personnels sur la santé stockés dans les systèmes nationaux de DSE.

La deuxième partie est une étude de cas extrêmement détaillée et bien documentée du registre national des services de santé au Royaume-Uni. Au cours des dix dernières années, ce système évolutif a fait l'objet d'un débat soutenu et souvent acharné sur les utilisations secondaires des renseignements personnels sur la santé. Le rapport aborde le cadre juridique des utilisations secondaires de renseignements personnels sur la santé au sein de ce système, les types

d'utilisations secondaires envisagées et les préoccupations qui ont découlé de ces utilisations. On y décrit également plusieurs améliorations proposées et demandes d'éclaircissements soulevées par divers intervenants.

La troisième partie est un sommaire et une synthèse des entrevues approfondies réalisées en mai 2007 dans le cadre de conférences téléphoniques avec une douzaine d'experts canadiens bien connus (les noms sont fournis) sur des questions liées aux utilisations secondaires de renseignements personnels sur la santé. S'y ajoute une discussion détaillée concernant le cercle grandissant des utilisations secondaires, les questions qu'il faudrait mettre en lumière dans les discussions sur les systèmes nationaux de DSE (par exemple, les valeurs de la vie privée, de l'autonomie et de la dignité), la recherche sur la santé comme utilisation secondaire (ce qui a soulevé plusieurs préoccupations), le défi posé par le consentement, et les enjeux liés à la gouvernance.

On peut consulter le rapport à l'adresse suivante :

http://www.ircm.qc.ca/bioethique/english/whatsnew/DES_Secondary_Use_Report.pdf.

Les usages sociaux de l'ADN dans le processus de formulation des politiques : Analyse de deux projets de loi sur l'identification par les empreintes génétiques

Université d'Ottawa, avril 2006, 74 pages

Dominique Robert et Martin Dufresne, en collaboration avec Alain Lachapelle et Marie-Lyne Vachon

Ce rapport traite principalement des utilisations de l'ADN dans le système de justice criminelle et de la compréhension des tensions sociales en cause, au moyen d'une analyse comparative des mémoires soumis au Parlement par divers groupes d'intérêt. Le tout s'est déroulé lors du processus législatif qui a mené à la promulgation de deux projets de loi sur l'ADN (C-3 et C-13). Le premier de ces projets de loi a permis la création d'une base de données nationale sur l'ADN, et le second a allongé la liste des infractions pour lesquelles l'obtention d'échantillons d'ADN est permise.

Les auteurs font état des trois manières dont le sujet de l'ADN est abordé dans la documentation concernant son utilisation dans le système de justice criminelle. L'ADN est défini comme : 1) une substance chimique à traiter sous un angle médico-légal; 2) un outil d'enquête à utiliser de manière stratégique; 3) une manifestation sociologique de la façon dont les cultures modernes redéfinissent la relation entre les sciences et le droit.

L'analyse des rapports présentés par les groupes et associations en cause dans l'étude du projet de loi C-3, qui a mené à la création de la base de données nationale sur l'ADN, démontre que les divers acteurs politiques s'entendent généralement sur l'utilité de créer une base de données génétiques. Toutefois, ils sont en désaccord sur au moins cinq questions majeures : l'utilité de l'ADN au sein du système de justice criminelle; la similarité entre les empreintes digitales et les empreintes génériques; l'ampleur du pouvoir discrétionnaire dont devrait disposer un juge en ordonnant la prise d'un échantillon; la rétroactivité des échantillons; enfin, la nécessité de conserver des échantillons d'ADN.

Lors du dépôt du projet de loi C-13, dans lequel on proposait en 2005 l'élargissement du système d'empreintes génétiques existant, les divers rapports et arguments ont fait ressortir six points importants. Certains points étaient déjà présents dans les derniers débats alors que d'autres étaient nouveaux : l'expansion des listes d'infractions primaires et secondaires de même que les critères connexes; le moment où il faudrait prendre un échantillon d'ADN; l'ampleur de la rétroactivité de la loi; le pouvoir discrétionnaire des juges en matière d'ordonnance de la prise d'un échantillon; le traitement des personnes qui ne sont pas jugées responsables d'un crime; enfin, la conservation des échantillons.

Les débats entourant ces projets de loi ont mené à des résultats concrets. Non seulement ont-ils influé sur la rédaction des textes juridiques, mais ils ont aussi donné naissance à des symboles puissants et les ont alimentés. L'analyse révèle deux résultats interdépendants : 1) les contrevenants sont transformés en monstres criminels; 2) les objectifs du système pénal ont été modifiés – le système n'est plus conçu de manière à rechercher la justice, mais plutôt la vérité. Les effets combinés tendent à renforcer la notion selon laquelle les garanties procédurales sont des obstacles à une lutte efficace au crime.

En dernier lieu, les auteurs ont le sentiment qu'il faut tenir un débat pour répondre à des questions telles que : Quelle est l'efficacité du système pénal? Comment mesurer cette efficacité? Pour qui est-il efficace?

On peut consulter le rapport à l'adresse suivante : <http://www.saea.uottawa.ca/index.php?lang=fr>.

Numéro de l'étudiant : ADN2007; mot de passe : ADN2007

Choix de technologies et politiques sur la protection de la vie privée dans le secteur de la santé

Université Memorial de Terre-Neuve, avril 2007, 130 pages

Edward Brown, Todd Wareham, Gerald Farrell, Theodore Hoekman, Rhonda Chaytor, Jennifer Barrigar, Tracy Ann Kosa, Carla Barton, Neil Barrett, Chris Mercer et Andree Thoms

Les auteurs de ce rapport critiquent les technologies liées à la protection de la vie privée et à la sécurité, ainsi que les hypothèses et les partis pris que les technologies accessibles peuvent engendrer à l'égard des choix législatifs et politiques dans le domaine des soins de santé au Canada. Ils se fondent sur de la recherche approfondie et de nombreuses entrevues réalisées avec des universitaires et des professionnels des soins de la santé, de la technologie de l'information et de la protection de la vie privée.

Les auteurs trouvent qu'il existe un important parti pris en faveur des technologies de sécurité des données ou d'un modèle périmétrique visant à prévenir l'accès non autorisé, au détriment de la prise en considération d'approches différentes des technologies de protection de la vie privée. Même les technologies de protection telles que la gestion du consentement, qui transcendent la sécurité puisqu'elles sont conçues pour restreindre les buts réels pour lesquels sont utilisées les données, peuvent être vues comme étant des mesures de contrôle d'accès plus perfectionnés au sein du même modèle. Le contrôle même que les patients exercent sur leurs renseignements personnels sur la santé est au mieux imparfait puisque leur consentement peut être implicite, qu'il existe tellement d'exceptions au consentement, et qu'ils ne peuvent retirer ces renseignements personnels du système de soins de santé. Ils doivent faire confiance aux autres et se fier aux mécanismes de surveillance et d'application.

Les auteurs s'inquiètent du fait que l'on accorde une confiance excessive au modèle périmétrique pour le système de soins de santé du Canada. Les technologies de contrôle d'accès fondé sur le rôle, et les technologies de gestion du consentement et de gestion du droit à la vie privée nécessitent des mécanismes d'ingénierie qui sont essentiellement des choix politiques en matière d'accès à l'information. Cet état de choses peut créer une infrastructure héritée qu'il est difficile et coûteux de modifier lorsqu'une plus grande fluidité dans l'échange de renseignements personnels sur la santé est essentielle à la prestation de soins de qualité aux patients.

Les auteurs se penchent sur les lois canadiennes relatives à la protection des renseignements personnels et, de façon plus particulière, sur quatre lois provinciales relatives au secteur de la santé ainsi que sur la notion de protection des données comme forme de protection de la vie privée. Ils décrivent la mise en place de dépositaires ou de fiduciaires de renseignements personnels sur la santé, avec des règles permettant l'échange de données, ce qui a mené à une mosaïque de dispositions sur la communication, d'exceptions aux consentements et d'obligations contractuelles concernant des professionnels en soins de santé primaire, les entreprises de TI, les administrateurs, les agences de surveillance et autres. Ils examinent également les règlements d'application des lois orientées vers la protection des renseignements personnels sur la santé, ainsi que le rôle des évaluations des facteurs relatifs à la vie privée dans l'environnement des soins de santé.

Les auteurs recommandent de poursuivre les discussions quant à connaître les règles qui seront appliquées ou contrôlées au moyen d'approches technologiques par opposition aux approches non technologiques (humaines). Les médecins et patients ne comprennent pas entièrement l'infrastructure qui protège leur information, mais ils doivent néanmoins l'accepter. Les mesures de sécurité peuvent créer une illusion de protection alors qu'on se contente de faire passer les aspects vulnérables et le processus décisionnel d'un ensemble d'humains à un autre, et même qu'on détourne le tout du « cercle de soins » – ceux qui sont directement concernés par la prestation de soins aux patients – pour le confier aux fournisseurs de services et administrateurs.

Le rapport comprend des entrevues avec des intervenants, qui confirment les préoccupations liées aux risques inhérents à l'automatisation des renseignements personnels sur la santé, les

faiblesses de certaines technologies axées sur la sécurité et la protection de la vie privée, les limites de la conception du contrôle d'accès fondé sur les rôles, et la question de savoir s'il existe réellement un contrôle valable du patient offert par le biais de mécanismes de consentement (à la fois législatifs et technologiques). Les auteurs en concluent que la protection de la vie privée va bien au-delà de la protection des données, car elle englobe les enjeux de dignité et de confiance, pour lesquels il reste encore à trouver des solutions technologiques.

On peut consulter le rapport à l'adresse suivante : <http://cpig.cs.mun.ca/TechnologyChoices.pdf>.

Analyse des répercussions juridiques et technologiques sur la protection de la vie privée des technologies d'identification par radiofréquence

Université Dalhousie, avril 2005, 64 pages

Teresa Scassa, Theodore Chiasson, Michael Deturbide, Anne Uteck

Les étiquettes d'identification par radiofréquence (IRF) sont destinées à remplacer le code à barres CUP comme mécanisme pour le contrôle des stocks de gros et de détail. Pourtant, les puces minuscules offrent un éventail d'utilisations possibles qui supplantent le code à barres. Ce qui a été conçu comme dispositif supérieur de contrôle des stocks pourrait devenir une puissante technologie de couplage des données et, en fin de compte, une technologie de surveillance.

Les médias ont eu tendance à concentrer leur attention sur les préoccupations des consommateurs à l'égard de l'utilisation de la technologie d'IRF dans le commerce de détail, particulièrement les manières dont on s'en sert pour alimenter la demande sans cesse croissante de renseignements personnels en échange de produits et services sur le marché de détail ordinaire. Toutefois, les préoccupations relatives à la protection de la vie privée débordent du contexte commercial. Les applications que l'on peut faire des dispositifs d'IRF sont pratiquement sans limites, et on songe à les utiliser – si tant est qu'elles ne sont pas déjà en place – dans un éventail de contextes, allant de la prestation de soins de santé à la gestion des collections de bibliothèque en passant par le contrôle des approvisionnements alimentaires et la surveillance des employés ou la surveillance qu'effectue le gouvernement dans le cadre d'initiatives de sécurité nationale.

Les auteurs commencent par examiner la technologie qui sous-tend l'IRF et font un survol des usages actuels et prévus dans ce domaine. Ils abordent ensuite les répercussions de l'utilisation de cette technologie sur la protection de la vie privée. Prenant en compte qu'on peut recourir aux lois sur la protection des renseignements personnels de façon formative ou réactive pour faire face aux enjeux que posent les nouvelles technologies, les auteurs observent diverses initiatives juridiques lancées aux États-Unis et à l'étranger au moyen desquelles on tente de donner suite aux répercussions de la technologie de l'IRF sur la vie privée. Ils font également état des démarches effectuées par les activistes soucieux de la défense des consommateurs et de la protection de la vie privée.

En mettant particulièrement l'accent sur la *LPRPDÉ*, les auteurs examinent la mesure dans laquelle les lois existantes sur la protection des renseignements personnels dans le secteur privé au Canada contiennent des dispositions utiles ou pratiques pour composer avec la technologie de l'IRF, et relèvent les lacunes sur le plan juridique.

Bien que ce rapport porte sur l'utilisation et la mise en place de l'IRF dans le secteur privé, les auteurs examinent également son application dans un contexte public élargi. L'adoption ou l'utilisation par le gouvernement des dispositifs d'IRF pour ses programmes soutiendra la mise en place de ces technologies dans le secteur privé, et pourrait limiter la réaction de l'État. Qui plus est, les possibilités de voir les renseignements personnels migrer avec une facilité relative du secteur privé vers le gouvernement ajoute une dimension publique aux développements de cette technologie dans le secteur privé.

Les auteurs concluent en formulant un ensemble de recommandations précises sur les points suivants : la nécessité d'élaborer des normes et des directives concernant expressément l'IRF; la sensibilisation des consommateurs à l'effet que les ministères et organismes gouvernementaux pourraient chercher à obtenir les données recueillies par le secteur privé, et pourraient les obtenir sans que les personnes concernées ne le sachent ou n'y aient consenti; les évaluations des facteurs relatifs à la vie privée que doivent obligatoirement réaliser les organismes gouvernementaux à l'égard des nouveaux programmes ou initiatives mettant à profit l'IRF; les lois

ou règlements qui obligerait les fabricants ou détaillants à utiliser des dispositifs d'IRF uniquement sur des étiquettes volantes détachables ou pour l'emballage des produits.

On peut consulter le rapport à :

[http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2\(Single\).pdf](http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf).

Le défi de l'identification des consommateurs dans le cadre de nouveaux mécanismes de paiement électronique

Option consommateurs, août 2006, 61 pages

Jacques St-Amant

Ce rapport offre un examen des méthodes de confirmation de l'identité dans le cadre des transactions électroniques, du caractère sécuritaire de ces transactions et de la conformité des nouvelles technologies d'identification biométrique aux cadres législatifs régissant la protection des renseignements personnels.

Après analyse de la tendance actuelle vers l'utilisation de méthodes biométriques pour identifier le consommateur, l'auteur en déduit que les systèmes d'authentification biométriques ne seront vraisemblablement pas plus sécurisés que les systèmes actuels, en plus du fait qu'ils poseront des défis pour la protection de la vie privée du consommateur.

La biométrie est efficace uniquement si le système peut vérifier que les attributs biométriques provenaient de la personne au moment de la vérification et concordent avec les données biométriques maîtresses sur fichier. Il existe des raisons pour lesquelles les systèmes n'y parviennent pas. En outre, bien que la biométrie comporte des identificateurs uniques, ces derniers ne sont pas secrets et n'offrent pas de sécurité intégrée en tant qu'identificateurs uniques.

L'auteur conclut en disant que l'utilisation des technologies d'authentification biométrique présente des risques juridiques et financiers supérieurs à ce qu'elles valent. Il indique que la biométrie complète d'autres technologies existantes et qu'aucun système n'est en lui-même entièrement fiable.

En ce qui concerne la confidentialité du consommateur, il mentionne que l'industrie démontre une propension de plus en plus grande à recueillir des renseignements personnels dans une tentative de gérer les risques juridiques et financiers. L'augmentation rapide de l'utilisation de la carte de transaction électronique combinée à celle des numéros d'identification personnels (NIP) a mené à une redéfinition des responsabilités respectives du consommateur et des établissements financiers. Bien qu'on ait toujours considéré que la sécurité était une responsabilité partagée, la banque devait en pratique s'assurer que la signature qu'elle acceptait était vraiment celle du client en question. Selon l'auteur, les banques tentent de faire porter au consommateur une plus grande partie du fardeau.

L'auteur a le sentiment que les consommateurs ont peu de prise sur ce qui est fait ou sera fait avec les renseignements communiqués en retour de produits et services. Les concepteurs des systèmes prétendent que le respect de la vie privée est nécessaire à la sécurité, de sorte qu'ils adoptent une philosophie du type *sécurité dans l'obscurité*. L'auteur avance des preuves selon lesquelles cette approche est depuis longtemps discréditée et que tous les intervenants profiteraient d'une franche discussion sur ces questions. Il faudrait concevoir des systèmes d'authentification de manière à ce que les risques posés aux banques et à leurs clients commerciaux contrebalancent ceux que courent les consommateurs. L'auteur craint que ce ne soit pas le cas et que ce déséquilibre favorise les banques, bien que ces dernières s'efforcent à l'occasion, sans trop d'efficacité, de gérer les risques.

Le rapport est accessible à l'adresse suivante : http://www.option-consommateurs.org/documents/principal/fr/File/rapports/renseignements_personnels/oc_rr_rens_pers_biometrie_200608.pdf.

Technologies de gestion des droits numériques et protection de la vie privée des consommateurs : Étude du marché canadien et évaluation des facteurs relatifs à la vie privée

Clinique d'intérêt public et de politique d'Internet du Canada, avril 2007, rapport intégral, 213 pages

David Fewer, Philippe Gauvin et Alex Cameron

La gestion des droits numériques (GDN), telle que définie dans cette étude, est un système comportant des outils technologiques et une politique d'utilisation, qui vise à gérer de manière sécuritaire l'accès à l'information numérique et l'utilisation de cette information. Les auteurs observent le comportement de plusieurs technologies de GDN dans le but d'évaluer les répercussions de ces technologies sur la protection de la vie privée des consommateurs et de connaître la conformité de la GDN à la *LPRPDÉ*.

Les chercheurs divisent en deux catégories les technologies de GDN analysées dans le cadre de l'étude : la GDN autonome et la GDN cyberdépendante. La GDN autonome ne nécessite aucune interaction externe pour fonctionner (par exemple, les logiciels qui ont besoin d'une clé de DC pour être exploitables ou qui se désactivent après un certain nombre d'utilisations). La GDN cyberdépendante, au contraire, implique l'authentification sur Internet ou la cybersurveillance des utilisations, comme la cybervalidation logicielle ou des services d'abonnement de musique en ligne qui offrent des licences numériques pour accéder au contenu verrouillé. Toutes les technologies de GDN cyberdépendantes supposent une interface avec des ordinateurs externes.

Les chercheurs examinent la façon dont la GDN modifie les rapports des personnes avec le contenu numérique en faisant le suivi et le contrôle de l'accès aux œuvres protégées ainsi que de l'utilisation qui en est faite. En cours de route, ils se penchent également sur l'érosion de la protection de la vie privée qu'engendre ce processus. Ils évaluent l'utilisation de la GDN sur le marché canadien et la façon dont la *LPRPDÉ* pourrait s'appliquer à la GDN. Enfin, ils étudient l'effet inquiétant que la GDN, comme forme de surveillance, pourrait avoir sur l'accès des gens à de l'information controversée ou non conventionnelle, et sur le droit légitime de s'exprimer ou de recevoir de l'information de manière anonyme – ce qui est primordial à l'exercice efficace de la liberté d'expression.

En s'appuyant sur une enquête du marché canadien, les chercheurs ont réalisé une évaluation technique de 18 applications sélectives de la GDN dans différents secteurs du marché entre janvier et mars 2007. Il s'agissait entre autres des commerces suivants : *iTunes Music Store* et *iTunes Video Store* d'Apple, *Zudeo* d'Azureus, *eReader (The Da Vinci Code)*, *InterActual (Pirates of the Caribbean* de Disney), *QuickTax* d'Intuit, *Office Video* de Microsoft, *Napster*, *Norton SystemWorks 2006* de Symantec et *Spark* de Telus Mobilité.

Les évaluations se sont déroulées au moyen d'un banc d'essai contrôlé comportant un ordinateur d'essai et un ordinateur passerelle dont la configuration visait à imiter un environnement d'utilisateur type. Des étudiants en droit de l'Université d'Ottawa et un avocat de la CIPPIC, faisant office d'utilisateurs ordinaires, ont réalisé les essais.

Le rapport contient une analyse de recherche détaillée de chaque application de GDN ainsi qu'une évaluation détaillée, en fonction des prescriptions de la *LPRPDÉ*, de 12 technologies de la GDN cyberdépendantes qui réalisaient des communications automatiques des renseignements par le biais de la GDN. Dans leur travail, les chercheurs prenaient en compte les politiques sur la protection de la vie privée, la documentation qui s'y rapporte ainsi que les réponses des organisations aux demandes d'accès. Ils en sont venus à la conclusion qu'aucune des organisations n'était conforme aux principes de la CSA en matière de vie privée.

La recherche a également permis de découvrir que plusieurs tiers, notamment Akamai Technologies, Omniture et Doubleclick, étaient fréquemment en cause dans les applications de la GDN qui étaient testées. Ces tiers recueillent beaucoup de renseignements sur

les utilisateurs, y compris des adresses IP, le type de fureteur, le système d'exploitation, le fournisseur d'accès Internet, la largeur de bande et le moment d'exploitation dans la journée. Dans le cas d'au moins deux de ces entreprises, les chercheurs indiquent qu'elles n'étaient pas au fait de leur existence ou de leur rôle dans le système de la GDN. Au moins une organisation n'a pas réussi à protéger correctement les renseignements personnels, et a communiqué le nom de l'utilisateur, son mot de passe et son adresse de courriel sur Internet sans cryptage des données.

On peut consulter le rapport à l'adresse suivante :

http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf.

Le droit à la vie privée et les services de communications payés d'avance : Enquête sur les politiques relatives à la réglementation et à l'enregistrement touchant les services de téléphones cellulaires payés à l'avance au sein des États membres de l'OCDE

*Centre for Policy Research on Science and Technology (CPROST),
Université Simon Fraser, mars 2006, 80 pages.*

Gordon Gow et Jennifer Parisi

Ce rapport de recherche constitue une enquête sur les politiques entourant la réglementation des services de téléphones cellulaires payés à l'avance dans les pays de l'OCDE. L'objet du rapport était de contribuer au processus de délibérations politiques fondées sur des preuves et concernant le dossier du droit à la vie privée et des services de communication payés à l'avance au Canada et ailleurs. Ce faisant, les auteurs ont examiné les positions stratégiques et les expériences des pays visés par l'enquête. Comme le rapport a pour objet de fournir des preuves empiriques qui serviront à prendre des décisions éclairées sur le sujet, on n'y trouve pas de recommandations précises sur la façon dont le Canada et d'autres pays devraient réagir dans ce dossier.

Les services de téléphones cellulaires payés à l'avance intéressent habituellement les clients qui ont fait l'acquisition d'un combiné et de crédits pour l'utilisation du réseau, suite à quoi ils obtiennent des notes de crédit supplémentaire ou achètent des cartes à valeur stockée avec des transactions au comptant ou au moyen de cartes de débit ou de crédit. Dans certains pays, les gens peuvent obtenir des services payés à l'avance de manière tout à fait anonyme sans avoir à présenter de pièce d'identité. Dû à la préoccupation croissante que les services téléphoniques payés à l'avance de façon anonyme servent à des fins criminelles ou terroristes, plusieurs pays ont adopté des lois exigeant des exploitants de la téléphonie cellulaire qu'ils recueillent des renseignements sur les consommateurs souhaitant obtenir des services payés à l'avance.

Selon les auteurs, bien que le Canada ne dispose pas d'une réglementation du genre, la possibilité qu'une telle chose se produise dans l'avenir devrait intéresser la commissaire à la protection de la vie privée compte tenu de l'incertitude entourant les répercussions juridiques et éthiques. Le débat public a été entravé par un manque d'information sur les objectifs qu'il serait réaliste de poursuivre ou sur la façon dont on pourrait mettre en œuvre et appliquer une réglementation.

Le rapport jette un éclairage sur cette question en présentant les conclusions d'une enquête des pays de l'OCDE concernant des enjeux tels que les politiques gouvernementales, les préoccupations de l'industrie et d'autres éléments de preuve sur l'utilisation des services payés à l'avance et les abus qu'on en fait, ainsi que les forums et les possibilités de débats publics sur cette question. La recherche, qui s'est déroulée entre avril et octobre 2005, reposait sur de nombreuses sources d'information publiées ainsi que sur des questionnaires expédiés aux autorités de protection des données et à d'autres agences dans les pays de l'OCDE. Environ 25 des 30 pays de l'OCDE, ainsi que l'Afrique du Sud, ont fourni de l'information plus ou moins détaillée.

Le rapport contient un sommaire détaillé des positions de chaque pays sur l'enregistrement des services de communications payés à l'avance. Parmi les pays interrogés, l'Australie, le Canada, l'Allemagne, les Pays-Bas, la Norvège, la République slovaque, la Suisse, le Royaume-Uni et les États-Unis sont ceux qui offrent les discussions et analyses les plus détaillées concernant leur position sur la question, les raisons favorables ou défavorables à l'enregistrement, les particularités de la réglementation, la réponse du marché et les aspects logistiques.

Le rapport comprend quelques observations sommaires sur les justifications et contre-justifications des enregistrements prépayés, la faisabilité de la mise en œuvre et de

l'application des mesures réglementaires et, enfin, le recours possible à des mesures de rechange.

Les auteurs proposent un test de « pertinence raisonnable » au moment d'examiner la collecte de renseignements sur les abonnés des services de communication sans fil payés à l'avance, et proposent trois manières de régler la question : présenter des preuves empiriques selon lesquelles l'enregistrement a un effet dissuasif sur le crime et le terrorisme; démontrer le caractère acceptable, sur les plans politique et social, de l'enregistrement des clients des services téléphoniques prépayés selon l'interprétation des pouvoirs législatifs existants; ou par le biais d'une argumentation efficace faisant valoir qu'une telle réglementation améliorera l'efficacité de l'application des lois et la sécurité du public.

On peut consulter le rapport à l'adresse suivante : <http://www.sfu.ca/cprost/prepaid/>.

Technologies à bord des véhicules et protection de la vie privée des consommateurs

Automobile Consumer Coalition/Car Help Canada, mars 2007, 74 pages

Paul Coninx

Ce rapport examine la croissance rapide des technologies en Amérique du Nord et en Europe qui enregistrent les mouvements et les emplacements des véhicules privés, leurs répercussions sur la vie privée des automobilistes, et des manières de s'attaquer à ces questions. Au nombre des technologies examinées, mentionnons les suivantes : les enregistreurs de données de conduite (EDC), les systèmes mondiaux de localisation (GPS), la télématique pour véhicule (appareils de communication), l'identification par radiofréquence (IRF) et la reconnaissance automatique de la plaque d'immatriculation.

L'auteur en arrive à la conclusion que les comportements des automobilistes seront de plus en plus surveillés en raison de la sécurité routière, de l'engorgement des routes, des préoccupations environnementales ainsi que de l'efficacité et de l'utilité de ces technologies de moins en moins coûteuses. Les tiers intéressés sont les services de transport et la police, les fabricants d'automobiles, les fournisseurs de services et les compagnies d'assurance.

Les automobilistes font depuis longtemps des demandes de permis de conduire et d'immatriculations et, avec le temps, les services de transport ont élaboré de vastes bases de données sur les propriétaires actuels et précédents qui sont devenues trop accessibles. L'auteur recommande un accès plus restreint en raison des risques de préjudice personnel, de vol d'identité, de sollicitations non souhaitées et d'organismes d'État trop entreprenants.

Les EDC sont utiles dans les enquêtes sur les accidents, sauf que certains fabricants d'automobiles s'y opposent puisque les automobilistes pourraient se servir de leurs propres véhicules pour témoigner contre eux. L'auteur n'est pas d'accord, car les automobilistes se trouvent sur les voies publiques, et il recommande d'améliorer les EDC et de les rendre obligatoires et accessibles aux parties intéressées, y compris les automobilistes. Toutefois, il faudrait strictement limiter le temps de consignation de tels dispositifs à quelques secondes au plus avant et après un accident. L'auteur est également favorable au diagnostic (mais non à l'enregistrement) de l'état du conducteur pour avertir ce dernier qu'il est somnolent et qu'il louvoie.

L'auteur en déduit que c'est aux automobilistes que devrait revenir le choix d'utiliser le GPS et les technologies connexes, en ayant en mains toutes les informations voulues concernant les répercussions éventuelles sur la protection de la vie privée, puisqu'il est possible qu'un tiers accède aux données sur leur emplacement, leur direction, leur vitesse et même leurs conversations. Les automobilistes devraient toujours avoir le droit de faire enlever sur demande de tels appareils de leur véhicule. L'auteur reconnaît les possibilités réelles et éventuelles d'abus associés aux appareils-photos automatiques et au système de reconnaissance automatique de la plaque d'immatriculation, mais il concède qu'ils apportent une sécurité sur la route dans certaines circonstances et qu'ils ne portent pas davantage atteinte à la vie privée que le fait d'être arrêté par la police. Il recommande plusieurs mesures de protection pour prévenir les abus, par exemple en n'imputant pas des points d'inaptitude lorsque le conducteur est inconnu.

L'auteur signale que les tribunaux canadiens et américains ne considèrent pas comme une priorité le droit à la vie privée lorsqu'une personne se trouve à bord d'un véhicule, en dépit de la *Charte canadienne des droits et libertés* et de la constitution des États-Unis. Il fait également valoir que l'utilisation accrue des transpondeurs et des dispositifs d'IRF est inévitable pour contrôler les rues embouteillées et percevoir les péages et frais de stationnement. Ces technologies posent la menace la plus lourde à la protection de la vie privée si elles débouchent sur de vastes bases de données centralisées que se partagent différentes compagnies et juridictions. On pourrait atténuer cette menace en utilisant des transpondeurs intelligents prépayés qui ne nécessiteraient pas le stockage de données personnelles. Il faudrait mettre en

place une telle technologie décentralisée avant qu'une technologie centralisée ne devienne la norme.

L'auteur formule en conclusion plusieurs recommandations concernant la collecte de renseignements personnels par ces nouvelles technologies. Il suggère notamment de chiffrer les données, de restreindre l'accès, d'éviter le couplage de données et de fournir toute l'information voulue aux automobilistes.

On peut consulter le rapport à l'adresse suivante: <http://www.carhelpcanada.com>.

Services basés sur l'emplacement : Analyse des répercussions sur la vie privée dans le contexte canadien

Université de Victoria, juin 2005, 44 pages

Colin J. Bennett et Lori Crowe

Ce rapport examine les technologies de surveillance du télécommerce mobile, à savoir les produits existants, l'accessibilité aux produits courants, les applications réelles et possibles, et les groupes cibles. Les auteurs discutent de la couverture médiatique ambiguë des enjeux liés à la surveillance du télécommerce mobile et posent les questions suivantes : De quelle façon les dispositifs de suivi sont-ils utilisés ou mal utilisés, et par qui? Quels sont les avantages attribués à de tels appareils? Sont-ils légitimes? Qui risque de subir une atteinte à sa vie privée et de quelle façon? Comment protéger le droit à la vie privée? Enfin, les auteurs visent à mieux cerner les répercussions sur la vie privée du télécommerce mobile qui a cours sur le marché canadien, et se penchent sur les défis particuliers qui risquent de se poser au Commissariat à la protection de la vie privée du Canada et aux organismes provinciaux équivalents.

Les auteurs fournissent de l'information sur les produits et font état des exigences opérationnelles et des limites de diverses technologies, comme celles exploitées pour le service d'urgence 911 (connexion avec ou sans fil); les dispositifs d'identification par radiofréquence (IRF); les enregistreurs de données de conduite (EDC), utilisés comme « boîtes noires » pour automobiles; et les appareils personnels de localisation (APL). Plus important encore, ils en cernent les avantages et les inconvénients. À titre d'exemple, bien qu'un APL ou un dispositif d'IRF puisse aider des parents à retrouver leurs enfants dans un parc d'attractions, il peut également servir à localiser, traquer et enlever ces mêmes enfants. Les EDC installés dans bon nombre de nouvelles automobiles (à l'insu du conducteur) peuvent aider les services d'urgence à retrouver un véhicule au besoin. D'un autre côté, les employeurs peuvent recourir à l'EDC pour suivre à la piste sans aucun scrupule leurs employés itinérants (comme les chauffeurs-livreurs), et des procureurs l'ont utilisé avec succès dans des affaires judiciaires.

Parmi les groupes cibles recensés, il y a les travailleurs mobiles, les aînés, les personnes handicapées, les patients et les aidants naturels, les enfants et les adolescents, les chauffeurs et les personnes effectuant des activités professionnelles et récréatives, ainsi que les prisonniers et les contrevenants. Toutefois, ces technologies peuvent être utilisées à la fois par et contre n'importe quelle personne. Les données de localisation peuvent se révéler extraordinairement sensibles, en ce sens qu'on peut les contrôler à distance sans que la personne en cause ne le sache ou n'ait donné son consentement. Elles peuvent être recueillies de façon continue et conservées indéfiniment. Le niveau de sensibilisation et d'expérience des consommateurs est faible, et la valeur potentielle de tels renseignements pour le gouvernement et les entreprises est énorme.

En conclusion, les auteurs affirment que la situation pourrait poser des défis aux cadres de réglementation existants en matière de protection de la vie privée, et qu'on recense peu de tentatives d'appliquer les principes normalisés de protection des renseignements personnels aux données de localisation. Au Canada, les commissaires fédéral et provinciaux à la protection de la vie privée doivent envisager plusieurs moyens de sensibiliser le grand public à la saisie, l'utilisation et la communication des données de localisation. Ils pourraient également examiner des façons de jouer un rôle plus actif dans les processus d'établissement de normes qui ont des répercussions aussi profondes et à long terme sur les pratiques de surveillance.

On peut consulter le rapport à l'adresse suivante :
<http://web.uvic.ca/polisci/bennett/pdf/LBSFINAL.pdf/>.

Les technologies de localisation : Mobilité, surveillance et protection de la vie privée

*Projet de surveillance, sous la direction du département de sociologie,
Université Queen's, Kingston (Ontario), mars 2005, 74 pages*

David Lyon, Stephen Marmura, Pasha Peroff

Ce rapport examine les nouvelles préoccupations à l'égard de la protection de la vie privée qui découlent des services axés sur l'emplacement, les technologies sous-jacentes à ces derniers et l'avènement du repérage en temps réel. L'objet de la recherche est d'attirer l'attention sur les préoccupations courantes que suscitent la localisation des personnes utilisant de telles technologies, y compris les mesures que prennent les fabricants et les fournisseurs de services pour assurer la conformité aux lois sur la protection de la vie privée au Canada. Les auteurs se penchent également sur la question de savoir si les stratégies intégrées répondent aux attentes du public à l'égard de tels services.

L'information provient notamment d'entrevues qui se sont déroulées en 2005, essentiellement en Ontario, avec des experts de l'industrie. Au nombre des sources d'information secondaires, mentionnons les reportages des médias, les sites Web des industries, les enquêtes publiées et les politiques des industries sur la protection de la vie privée.

Les auteurs définissent les technologies de localisation comme celles pouvant dégager des coordonnées de façon continue et en temps réel. Les principales technologies du genre prises en compte dans le rapport sont les technologies de localisation par téléphone cellulaire, dont certaines fonctionnent par réseau et d'autres nécessitent un combiné muni d'un système mondial de localisation (GPS). Les auteurs se penchent également sur d'autres technologies activées par GPS comme les systèmes de navigation automobile. Sont exclues les technologies de repérage comme les étiquettes d'identification par radiofréquence (IRF) et les systèmes de télévision en circuit fermé puisqu'elles ne sont pas en mesure de produire des données de localisation précises, en temps réel et de façon continue sur une personne.

Les auteurs examinent les prévisions du marché, les facteurs du marché et les obstacles à la croissance des services axés sur l'emplacement, de même que les enjeux liés à la protection de la vie privée liés à de tels services. Selon eux, les principaux transporteurs sans fil et fournisseurs de services axés sur l'emplacement au Canada se montreront probablement proactifs en prévoyant et abordant les préoccupations juridiques et publiques à propos de la collecte, de l'utilisation et de la communication pertinentes des renseignements personnels des clients, mais ils pourraient ne pas investir les ressources nécessaires pour parer aux problèmes éventuels en matière de sécurité des données.

Selon les auteurs, la nature des renseignements de localisation permettra de broser un tableau plus détaillé des schémas de mouvement individuels et collectifs lequel invitera à la création de nouveaux algorithmes visant à déduire les rapports possibles entre la mobilité et l'identité. Ils indiquent également que les données de localisation sont stockées à des fins de marketing futur pour cibler des publics de consommateurs et recueillir de l'information concernant la mobilité des populations, ce qui implique bien souvent l'utilisation évoluée de données anonymes et groupées pour classer les consommateurs en groupes cibles précis. Les auteurs soulignent que, même si les lois sur la protection de la vie privée telles que la *LPRPDÉ* sont sans l'ombre d'un doute nécessaires pour protéger les droits des personnes, elles ne sont pas conçues pour donner suite aux pratiques commerciales de tri social rendues possibles par l'utilisation de données groupées anonymes.

Le rapport comporte des recommandations concernant la recherche future sur plusieurs variables qui influent sur les attitudes qu'ont les gens à l'égard des technologies de localisation et de leurs répercussions sur la protection de la vie privée, y compris le rôle joué par le gouvernement, l'industrie et les médias. Les auteurs estiment qu'on a besoin d'études comparatives sur les technologies de localisation pour les mettre en parallèle avec celles d'autres pays ayant des

populations urbaines plutôt denses qui font un usage généralisé des téléphones cellulaires. Ils proposent également de poursuivre les recherches sur la précision des prédictions faites au sujet des développements commerciaux et technologiques par les entreprises de recherche en marketing; les vulnérabilités du stockage et de la gestion des données des secteurs privé et public, y compris les données de localisation; et les enjeux relatifs à la convergence des médias en tenant compte des approches politiques traditionnelles qu'applique le gouvernement devant divers médias de masse et médias des communications.

Le rapport est accessible à l'adresse suivante :
<http://www.surveillanceproject.org/files/loctech.pdf>.

L'utilisation des caméras de surveillance dans les lieux à accès public au Canada

Université du Québec, École nationale d'administration publique, décembre 2005, 66 pages

Christian Boudreau et Monica Tremblay en collaboration avec Paul-André Comeau

Ce rapport est une étude sur les perceptions, les enjeux, les répercussions sur la vie privée et les pratiques exemplaires en matière d'utilisation des caméras de surveillance au Canada. L'étude repose sur un examen de 22 projets de surveillance vidéo dans des endroits publics (la plupart dans des rues du centre-ville et des secteurs commerciaux), de sept publications offrant des directives provinciales sur la vie privée, des opinions de groupes de discussion du Québec et des analyses des médias, à quoi s'ajoute un survol de la documentation.

Les auteurs estiment que les responsables doivent prendre en considération cinq principaux enjeux compte tenu du fait que l'utilisation des caméras de surveillance est de plus en plus répandue au Canada.

Premièrement, d'après leur analyse du contexte canadien, les auteurs en déduisent que, compte tenu du sentiment croissant d'insécurité de la population, la pression exercée pour le recours accru à des caméras de surveillance provient principalement de divers groupes communautaires (propriétaires d'entreprise, citoyens, etc.) plutôt que des institutions gouvernementales et publiques. Bien qu'elle ne constitue pas nécessairement la meilleure approche, la surveillance vidéo est habituellement la première solution qui vient à l'esprit. Il en résulte souvent un déplacement du problème (par exemple, le trafic de drogues, la prostitution) et une menace grandissante pour la vie privée.

Deuxièmement, l'importance accordée aux enjeux relatifs à la protection de la vie privée varie en fonction des événements courants. Les actes de terrorisme ne sont pas les seuls à produire le type de peur qui déclenche la demande accrue de caméras de surveillance. Tout acte criminel ou délinquant peut frapper l'imaginaire collectif selon les victimes et les circonstances. Le danger réside dans la réaction excessive à une situation d'ampleur limitée, puisqu'il est souvent difficile de renverser les décisions.

Troisièmement, la technologie des caméras numériques ouvre la voie à l'identification biométrique généralisée dans les lieux publics. Les auteurs ont le sentiment que cette autre menace à la vie privée pourrait nécessiter de la part des autorités responsables une réglementation et un contrôle plus étroits des systèmes de caméras de surveillance.

Quatrièmement, bien que les caméras de surveillance soient généralement considérées comme un outil de contrôle des éléments criminels et de dissuasion des crimes contre la personne ou la propriété, certains groupes redoutant une discrimination à leur endroit de la part des autorités (pour des raisons d'ethnicité, d'âge, de sexe, etc.) les considèrent comme un outil assurant la transparence et un traitement équitable. Encore une fois, tout est question d'équilibre entre la recherche de sécurité et la nécessité de protéger la vie privée.

Enfin, bien que les groupes communautaires soient souvent ceux qui réclament davantage de caméras de surveillance, ce sont également eux qui souhaitent un contrôle et une réglementation accrus de ces systèmes. Cette position fait en sorte qu'ils sont souvent en désaccord avec les administrateurs des systèmes qui souhaitent maintenir leur autonomie. Une telle tension démontre la nécessité d'établir des règles de gouvernance plus claires et d'intensifier le dialogue entre les intervenants.

On peut consulter le rapport à l'adresse suivante :
<http://archives.enap.ca/bibliotheques/2006/06/24261876.pdf>.

Examen préliminaire des enjeux relatifs à la protection de la vie privée en milieu de travail au Canada

Université de la Colombie-Britannique, avril 2006, 60 pages

Vance Lockton, Richard S. Rosenberg

Les auteurs de ce rapport expliquent l'importance de la vie privée en milieu de travail, se penchent sur le caractère inadéquat des protections juridiques dans les juridictions canadiennes et américaines, examinent des domaines de préoccupation précis et concluent qu'il faut s'attaquer à cinq problèmes. Le document vise à fournir un cadre d'analyse pour les employeurs, les employés et les décideurs.

Les auteurs définissent la protection de la vie privée comme un enjeu de confiance et de dignité humaine. Les employés associent généralement le contrôle en milieu de travail aux mesures d'application et aux mesures disciplinaires qui peuvent engendrer de l'anxiété et de la dépression. De leur côté, les employeurs veulent réduire les vols commis par les employés, assurer la productivité, se protéger contre les litiges en milieu de travail, éviter les tragédies, et prévenir les attaques et les fuites électroniques. Les employeurs ont de plus en plus recours à des vérifications complètes avant l'emploi, à des contrôles d'accès, à des caméras de surveillance ainsi qu'au contrôle d'Internet, du courrier électronique et des réseaux, et ils multiplient les tests et les recherches.

Les auteurs constatent que les lieux de travail s'étendent de plus en plus aux domiciles, aux lieux publics et au cyberspace en raison des appareils électroniques que fournissent les entreprises, et qui peuvent servir à des fins commerciales et personnelles. Cet état de choses a brouillé la démarcation entre les heures de service et l'après-service et a accru les perspectives de surveillance. Pourtant, certaines études donnent à entendre que les entreprises qui s'engagent dans le contrôle électronique et le dépistage des drogues engendrent des milieux de vie plus stressants et moins productifs que celles qui n'appliquent pas de telles mesures.

Le rapport met en lumière plusieurs lacunes dans les lois canadiennes protégeant la vie privée des employés. La *Loi sur la protection des renseignements personnels* ne s'applique qu'aux institutions gouvernementales fédérales, tandis que la *LPRPDÉ* ne vise pas les renseignements personnels des employés dans les entreprises sous réglementation provinciale. La commissaire fédérale à la protection de la vie privée, qui supervise ces deux lois, ne dispose d'aucun pouvoir réparateur et, en vertu de la *LPRPDÉ*, le nom des institutions non conformes n'est pas révélé. En outre, les lois provinciales en matière de protection de la vie privée en Alberta et en Colombie-Britannique appliquent des normes moins rigoureuses en matière de collecte des renseignements concernant les employés du moment qu'on notifie ces derniers. La majorité des conventions collectives du Canada ne prévoient pas de protection supplémentaire.

Par opposition, le *Code civil* du Québec, la *Charte des droits et libertés de la personne* et les lois sur la protection des renseignements personnels qui les accompagnent offrent des protections supérieures à celle de la *LPRPDÉ*. Les auteurs citent la Nouvelle-Galles-du-Sud, en Australie, comme juridiction où la surveillance du milieu de travail est adéquatement réglementée, avec des mesures comme la notification obligatoire, une liste de méthodes de surveillance interdites et des restrictions imposées à la surveillance cachée.

Les auteurs examinent des enquêtes sur des plaintes précises et des cas de jurisprudence, abordant des domaines tels que la télévision en circuit fermé, le dépouillement du courriel, le contrôle au clavier, la surveillance hors des heures de travail et le dépistage des drogues. Ils concluent en disant que le déséquilibre des pouvoirs entre les employeurs et les employés signifie que la vie privée ne sera pas protégée par défaut. Les auteurs font valoir qu'il est nécessaire de mieux comprendre que les enjeux liés à la protection de la vie privée en milieu de travail ne doivent pas être source de conflit étant donné que les employeurs et les employés profitent tous d'un milieu de travail fondé sur la confiance et le respect mutuel; qu'il est nécessaire d'adopter des lois qui protègent les employés dans les provinces et territoires non

visés actuellement par les lois sur la protection de la vie privée au travail; et qu'il est nécessaire de promulguer des lois proactives pour donner suite aux enjeux de la surveillance. Les auteurs recommandent également d'habiliter la commissaire à la protection de la vie privée à identifier publiquement les entreprises contrevenantes, de faire de meilleures prévisions quant aux répercussions des nouvelles technologies sur la protection de la vie privée, et d'approfondir la recherche canadienne pour résoudre ces enjeux.

On peut consulter le rapport à l'adresse suivante : <http://www.cs.ubc.ca/~lockton/workplace.pdf>.

Dans la ligne de mire? Perspective de l'employeur concernant la protection de la vie privée en milieu de travail

Université Ryerson, juin 2006, 22 pages

Avner Levin, Mary Foster, Mary Jo Nicholson et Tony Hernandez

Les employeurs et consommateurs canadiens reconnaissent la nécessité d'établir un équilibre entre la protection de la vie privée au travail et d'autres intérêts pour s'assurer de créer une économie concurrentielle. Ce rapport visait à documenter les pratiques actuelles telles que vues par l'employeur et de comprendre la façon dont un tel équilibre est envisagé et mis en œuvre dans un contexte canadien.

Le projet reposait sur une méthode structurée d'entrevues et d'analyses au moyen d'un échantillonnage représentatif à l'échelle du pays et de l'industrie et en prenant en considération des facteurs tels que la représentation syndicale et la taille de l'employeur. Les entrevues étaient axées sur des indicateurs clés tels que la sensibilisation des employeurs à la protection de la vie privée en milieu de travail; l'existence et les capacités de diverses technologies de contrôle/surveillance; l'objet de la surveillance; les raisons justifiant la protection de la vie privée au travail; les rôles du gouvernement et de l'industrie.

Les lois fédérales et provinciales visant à protéger les renseignements personnels abordent certains aspects de la protection de la vie privée au travail. Le rapport offre une description du paysage juridique au Canada, alors que ses auteurs examinent les lois fédérales et provinciales sur la protection de la vie privée et les répercussions de ces lois sur les pratiques et perspectives commerciales. Cela dit, les approches conceptuelles de la protection de la vie privée en milieu de travail reposent sur les concepts fondamentaux de protection de la vie privée en général.

Les auteurs offrent un cadre se rapportant aux concepts prédominants en matière de vie privée au travail, dont l'un repose sur les *droits* (le modèle européen, fondé sur le droit à la dignité ou à la vie privée) et l'autre sur la *propriété* (le modèle américain, fondé sur le fait que le lieu de travail appartient à l'employeur). Le modèle des *droits* prédomine au Québec et se reflète dans les lois, mais les auteurs ont constaté que les lois fédérales et provinciales sont souvent mal interprétées par les entreprises canadiennes qui font valoir le modèle américain alors que, dans les faits, on impose aux employeurs une norme fondée sur le caractère raisonnable.

Les auteurs ont examiné l'attitude des employeurs à l'égard du rôle du gouvernement et de l'industrie dans la gestion des enjeux liés à la protection de la vie privée en milieu de travail. Les personnes interviewées ont reconnu que la loi liée à la protection de la vie privée motivait les entreprises à prendre des mesures officielles pour se conformer. Cependant, aucun employeur ne voyait la nécessité d'une loi fédérale additionnelle sur la protection de la vie privée en général, et sur la protection de la vie privée au travail en particulier. Par contre, ils seraient ouverts à des directives qui éclairciraient les lois existantes.

Le rapport porte sur les mesures de surveillance et de contrôle déclarées par les employeurs, ainsi que sur les raisons pour lesquels ils les ont mises en place. Les auteurs évaluent ces mesures et ces raisons en fonction des modèles fondés sur les *droits* et la *propriété*, et en tenant compte des exigences législatives.

Selon les auteurs, le Canada serait en train d'élaborer un modèle hybride de gestion des enjeux liés à la protection de la vie privée au travail, et ce modèle repose sur la confiance. Comme le faisait valoir un employeur, « l'intérêt de l'entreprise est indissociable de celui des personnes. Nous avons à cœur d'établir un climat de confiance entre les employés et l'entreprise. »
[Traduction] Tous les employeurs interviewés ont convenu qu'une certaine forme de protection de la vie privée est nécessaire pour le fonctionnement régulier et sans heurt de leur entreprise, et que le tout pourrait favoriser une plus grande productivité.

Cependant, les employeurs interrogés ont unanimement insisté sur le fait que leurs employés ne perçoivent pas la protection de la vie privée en milieu de travail comme un réel enjeu. En

conclusion, les auteurs avancent que les employeurs sont du même avis que leurs employés. De façon plus précise, la question n'entre pas dans la mire de la plupart des employeurs. Par conséquent, les auteurs invitent à approfondir la recherche sur les attitudes des employés à l'égard de la protection de la vie privée en milieu de travail.

On peut consulter le rapport à l'adresse suivante :

<http://ryerson.ca/faculties/business/news/archive/UnderTheRadar.pdf>.

La *LPRPDÉ* et le vol d'identité : Des solutions pour protéger les Canadiennes et les Canadiens

B.C. Freedom of Information and Privacy Association, avril 2005, 73 pages

Stephanie Perrin, Philippa Lawson, Jennifer Manning et Robert Gellman.

Leila Pourtavaf, adjointe de recherche

Ce rapport décrit le vol d'identité comme le crime parfait de nature non violente et néanmoins très lucratif et tente d'évaluer son ampleur au Canada et aux États-Unis, les méthodes utilisées pour voler l'identité, les enjeux juridiques des poursuites, les interventions judiciaires aux États-Unis et la protection offerte par la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)* au Canada. Le rapport se termine par une série de recommandations pour améliorer la protection contre le vol d'identité au Canada.

Le rapport met en lumière des données statistiques de 2002 et 2004 sur la fréquence du vol d'identité au Canada et aux États-Unis. Les auteurs distinguent les vols d'identité des simples fraudes par carte de crédit ou carte bancaire, qui sont des situations où les banques ont pris des mesures afin de limiter la responsabilité individuelle. Il y a vol d'identité lorsqu'une personne usurpe l'identité de quelqu'un d'autre pour ouvrir de nouveaux comptes, une activité qui, selon les auteurs, crée de réels problèmes pour la personne honnête qui doit prouver le bien-fondé de sa propre identité. Le document comporte des descriptions informatives assorties d'exemples non scientifiques de différentes techniques de vol d'identité.

Trois chapitres du rapport portent sur l'environnement juridique lié au vol d'identité aux États-Unis, y compris les enjeux juridiques, les réponses judiciaires et une analyse de ce qu'on appelle « le scandale de ChoicePoint ». Les auteurs examinent les raisons du faible taux de poursuites dans les cas de vols d'identité aux États-Unis, notamment une discussion d'une affaire judiciaire de référence, *Huggins c. Citibank*. On trouve également un répertoire sélectif utile des lois américaines (fédérales et d'État) portant sur le vol d'identité. La discussion sur les États-Unis comporte une description d'un régime modèle de protection de la vie privée, proposé, dans la foulée du scandale de ChoicePoint, par deux avocats spécialisés dans les lois d'intérêt public. Y sont décrites les 16 propositions contenues dans le régime modèle, le tout suivi d'une analyse.

D'un point de vue canadien, l'aspect le plus utile du rapport est l'examen très détaillé des protections contre le vol d'identité qui sont actuellement offertes en vertu de la *LPRPDÉ* du Canada, avec une analyse détaillée des dispositions particulières des dix principes de la CSA où la loi prévoit des mesures de protection précises.

Ce chapitre est utile. En fait, il devrait être lu par toute personne qui se préoccupe des obligations commerciales en matière de prévention du vol d'identité ou qui cherche à comprendre la façon dont la *LPRPDÉ* peut servir à protéger les intérêts des consommateurs, incluant le dépôt d'une plainte en vertu de la loi.

Le rapport se termine par huit recommandations précises, dont la nécessité de poursuivre les recherches sur les pratiques des entreprises et les risques de vol d'identité, l'application de directives particulières pour les entreprises, et une sensibilisation accrue du public en la matière. Il faudrait également encourager la commissaire fédérale à la protection de la vie privée à collaborer avec d'autres commissaires et des agences policières sur des enquêtes, des vérifications et la sensibilisation du grand public, et à présenter des affaires de vol d'identité à la Cour fédérale afin de demander réparation et d'obtenir des dommages-intérêts pour les victimes.

Au nombre des modifications juridiques proposées, mentionnons l'obligation des entreprises de notifier les atteintes à la vie privée dans les cas où les personnes courent le risque de se faire voler leur identité, et des modifications au *Code criminel du Canada* pour donner suite aux problèmes de vol d'identité. Les auteurs demandent également d'accélérer l'établissement d'ententes d'aide mutuelle pour les poursuites judiciaires dans les cas de vol d'identité, et l'aide

mutuelle dans les enquêtes relatives aux atteintes à la vie privée entre le Canada et les États-Unis.

On peut consulter le rapport à l'adresse suivante : http://fipa.bc.ca/home/hot_topics/14.

Protection de la vie privée au sein du système de justice pénale : Utilisation d'échantillons d'ADN dans le cadre d'enquêtes

Université d'Ottawa, avril 2007, 49 pages

Martin Dufresne et Dominique Robert, en collaboration avec Pascal Dominique-Legault, Alain Lachapelle et Marie-Lyne Vachon

Ce rapport replace dans le contexte du débat public élargi la manipulation des échantillons d'ADN, depuis le moment où les échantillons sont recueillis durant une enquête jusqu'à leur utilisation dans les poursuites judiciaires. L'effet « CSI » (*Crime Scene Investigation*) a rendu l'utilisation de l'information génétique dans les enquêtes criminelles aussi connue que les empreintes digitales. Pourtant, il n'y a pas encore eu de débat public sérieux (hormis les groupes d'intérêts spéciaux) sur l'utilisation de l'ADN dans le système de justice pénale.

Le rapport comporte cinq parties, dont la première offre un examen du défi croissant que posent la protection du droit à la vie privée et le flou dans les distinctions entre la « vie privée » et la « vie publique ». Le tout résulte en un nouvel aspect – la « vie privée publique », qui découle des besoins sociaux et de la confluence des technologies de l'information. Dans ce contexte et concernant l'information génétique, les auteurs soulèvent les enjeux de surveillance des données (*dataveillance*), les utilisations secondaires non prévues et la valeur de ces données dans l'économie de l'information.

La deuxième partie porte sur les défis que pose à la « vie privée » l'identification par le biais de la technologie génétique. L'information de type ADN que les gens laissent derrière eux – par exemple, les cellules laissées sur un siège d'aéroport – peut se balader en Chine après que les cellules se soient accrochées à un autre passager, et le reste pourra prendre le chemin de Toronto. Cette dilution de nous-mêmes, par laquelle l'information de type ADN détachable peut aboutir dans de nombreuses bases de données disparates sans qu'on ne le sache, pourrait également mener à l'entreposage, l'examen et la comparaison d'échantillons d'ADN dans le système de justice pénale, avec des répercussions uniques sur le droit à la vie privée.

La troisième partie est une description de la méthode utilisée pour recueillir et analyser les données qui feront l'objet de la partie suivante. Les auteurs ont tenté de décrire l'utilisation que le système de justice fait de l'ADN pour identifier la séquence de données d'ADN recueillies qui serviront de preuves génétiques dans les enquêtes criminelles, les principaux acteurs dans la collecte de ces données et l'utilisation qu'en font les forces de l'ordre et les laboratoires de police. Ils offrent également un aperçu des normes en place et des types de renseignements recueillis à partir des preuves génétiques, en abordant la façon dont elles sont utilisées (la trajectoire des données). Les auteurs ont réalisé huit entrevues d'une durée d'une à trois heures avec des représentants de deux corps de police et de la Banque nationale de données génétiques, ainsi qu'une analyse de la documentation pertinente.

La quatrième partie est une description extrêmement détaillée et révélatrice de la trajectoire que prendra l'ADN dans une enquête criminelle, depuis le moment de la collecte d'un échantillon sur la scène d'un crime jusqu'à son inclusion dans l'un des deux registres de la base nationale de données génétiques. Les auteurs décrivent dix étapes distinctes qui se répartissent en deux catégories. La première catégorie se compose des six étapes allant de la collecte de substance génétique à l'établissement de l'identité d'une personne. La deuxième catégorie inclut les quatre étapes menant à une preuve incriminante ou à l'« identité criminelle ». Dans leur description des diverses étapes, les auteurs soulèvent les ramifications sociales et juridiques possibles pour la protection de la vie privée. Les auteurs signalent que l'ADN peut avoir d'importantes répercussions sur la « vie privée » des gens lorsqu'on peut le relier directement à eux, ou qu'on s'en sert pour dresser le profil de suspects probables dans un crime ou à des fins de suivi biologique ou des fins prédictives.

Dans la cinquième partie, les auteurs présentent certaines conclusions, y compris l'opinion que la création d'une « identité pénale » par le biais de collecte de données génétiques dans une enquête criminelle modifie le paradigme de la « vie privée » et assujettit la personne à un nouveau rapport avec le système de justice pénale dans lequel doivent être expliquées ses actions et la présence de son ADN. Dans ce contexte, le droit au silence d'une personne est atténué, le fardeau de la preuve selon laquelle elle ne serait pas un suspect lui est transféré, et une approche de type « vision en tunnel » pour utiliser des preuves génétiques peut nuire à ses droits juridiques. En résumé, tout cela se traduit par une réorganisation complète de la justice pénale qui remet en question nos notions libérales de la « vie privée ».

On peut consulter le rapport à l'adresse : <http://www.saea.uottawa.ca/index.php?lang=fr>.

Numéro de l'étudiant : ADN2007; mot de passe : ADN2007

Visions du Canada : Prévisions relatives aux politiques sur l'identité, et politiques de rechange

Faculté des sciences de l'information, Université de Toronto, et London School of Economics and Political Science, avril 2007, 114 pages

Krista Boa, Andrew Clement, Simon Davies et Gus Hosein

Les auteurs de ce rapport établissent et analysent le paysage politique actuel en matière d'identité au Canada, particulièrement dans le contexte de la proposition REALID des États-Unis, l'entente sur la frontière intelligente et les plans de l'Initiative relative aux voyages dans l'hémisphère occidental, et ils formulent des recommandations à cet égard. Ils examinent également les plans relatifs aux permis de conduire et à la documentation sur l'identité dans plusieurs provinces canadiennes. Ils mettent à profit l'expérience d'autres pays et étudient les principaux cas de développement des mécanismes d'identité au Canada, ainsi que les résultats de deux ateliers de recherche réunissant des responsables gouvernementaux, des universitaires, des organismes de la société civile et des firmes du secteur privé.

Le rapport qui en découle offre d'abord un examen des rouages des politiques sur l'identité et de plusieurs facteurs stratégiques d'importance. Cela inclut les risques politiques, y compris ceux liés à la façon dont les cartes d'identité en particulier peuvent modifier les relations entre le citoyen et l'État, et créer une source de tension. Les auteurs indiquent que la protection de la vie privée peut cependant engendrer le risque politique le plus lourd dans le contexte canadien. Passant ensuite à l'examen des facteurs de telles politiques, les auteurs préviennent que les principes moteurs d'un mécanisme d'identité pourraient changer en milieu de parcours, ce qui ajoute aux risques politiques. Les auteurs prennent également en considération les défis que pose la conception d'un mécanisme d'identité qui apparie des buts et objectifs énoncés avec des échéanciers réalistes et des technologies raisonnables, et décrivent les difficultés d'agir ainsi dans d'autres juridictions. L'efficacité des choix politiques et les coûts de tels systèmes sont abondamment décrits, et les auteurs prennent en considération les questions de savoir qui paie pour de tels coûts, qui détermine les politiques et qui « possède » le système. Selon les auteurs, il existe au Canada une préoccupation prédominante quant à savoir si une nouvelle politique « appartient » au gouvernement fédéral ou aux provinces.

Les auteurs se penchent ensuite sur les avantages d'un cadre politique national et précisent que, bien que l'établissement d'une infrastructure nationale d'assurance de la qualité puisse se révéler très bénéfique (particulièrement pour les besoins de l'entreprise), il faut du leadership politique pour promouvoir une assurance de l'identité dans l'économie canadienne. Après examen de récents exemples de la Suède, de Hong Kong et de la Malaisie, les auteurs en déduisent qu'il serait avantageux sous bien des angles d'amorcer une discussion nationale concernant le besoin en stratégies d'identité efficaces au Canada, mais qu'une décision centralisée déterminée par le gouvernement pourrait ne pas vraiment produire ces avantages. Ils insistent sur la nécessité de faire davantage de travail de base dans des environnements organisationnels et commerciaux et touchant directement le consommateur et le citoyen.

Dans leur analyse, les auteurs décrivent les risques posés par une mauvaise politique publique de choix axés sur le fournisseur ou l'adoption de technologies propres comme la biométrie sans débat ouvert et prudent, et s'inquiètent du manque de clarté et de transparence des politiques canadiennes en matière d'identité. Ils énoncent les critères nécessaires à une rigoureuse consultation publique et proposent plusieurs ensembles de principes et des tests pour orienter un tel effort. Ils concluent qu'il est faisable d'instituer des mécanismes d'identité nationaux qui abordent simultanément la sécurité légitime et les intérêts en matière d'échange de données du gouvernement ainsi que les intérêts légitimes des citoyens quant à la protection de leur vie privée et à leur autonomie. Le rapport comprend également un résumé de deux ateliers qui se sont déroulés à Vancouver et à Ottawa, auxquels ont participé environ 50 personnes, et qui incluaient une riche discussion sur les préoccupations en matière de protection de la vie privée et sur la question de savoir si un mécanisme devrait impliquer l'utilisation obligatoire ou volontaire des

Autres

services d'identité. On y trouve également une discussion détaillée sur les initiatives provinciales, fédérales et internationales des dernières années, y compris les récentes initiatives canado-américaines en matière de sécurité frontalière.

On peut consulter le rapport à l'adresse suivante : <http://www3.fis.utoronto.ca/research/iprp/>.