Médias sociaux, données volumineuses et respect de la vie privée : Protéger les droits des citoyens à l'ère de l'interconnectivité

Mémoire au Comité de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le 13 décembre 2012

B.C. Freedom of Information and Privacy Association
1093, rue West Broadway, bureau 103
Vancouver (Colombie-Britannique) V5N 1E2
Téléphone : 604-739-9788 | Télécopieur : 604-739-9148
Courriel : fipa@fipa.bc.ca

La B.C. Freedom of Information and Privacy Association tient à remercier la Law Foundation of British Columbia, qui, par son appui constant dans les domaines de la réforme du droit, la recherche et la sensibilisation, lui permet de produire des mémoires comme le présent document.

INTRODUCTION

La B.C. Freedom of Information and Privacy Association (l'Association) est un organisme non partisan et sans but lucratif créé en 1991. Elle milite pour la liberté d'information et les droits à la vie privée au Canada. Elle vise à permettre aux citoyens d'avoir prise sur leur propre vie, par un meilleur accès à l'information et à un plus grand contrôle sur leurs renseignements personnels. Elle s'adresse à un large éventail de particuliers et d'organismes par la voie de programmes de sensibilisation, d'aide, de recherche et de réforme du droit.

L'Association œuvre essentiellement en Colombie-Britannique, mais elle joue aussi un rôle actif sur la scène nationale. Par exemple, en 2009, elle a soumis à votre Comité un mémoire fondé sur les 12 recommandations formulées par l'ancien commissaire à l'information, M. Marleau, concernant la réforme de la *Loi sur l'accès à l'information*. L'Association a également témoigné devant le Comité lors de l'étude sur un gouvernement transparent en 2011 et elle s'est employée, depuis le siècle dernier, à examiner les conséquences sur le respect de la vie privée que pourraient engendrer diverses propositions sur l'accès légal et sur d'autres questions fédérales connexes.

La confidentialité des renseignements personnels à l'ère des médias sociaux devient hautement pertinente pour le travail de l'Association, et elle l'est encore plus pour celui des décideurs comme vous et pour le Canadien moyen. De plus en plus de renseignements personnels circulent sur les réseaux de communications mondiaux d'une grande complexité, par la voie des médias sociaux et des applications, et notre conception de la vie privée, sa protection et son fonctionnement sont donc mis à rude épreuve. Il faut signaler toutefois que, contrairement à ce que prétendent ceux qui diabolisent les médias sociaux, cette mise à l'épreuve ne porte pas atteinte à la valeur démocratique, personnelle et sociale de la vie privée, bien au contraire.

En effet, comme nos vies sont de plus en plus intégrées aux technologies du réseautage social, c'est le coût des incursions non autorisées dans nos vies qui a explosé. Il n'est pas exagéré d'affirmer que notre gagne-pain, notre sécurité et notre bien-être dépendent fortement de la confidentialité de nos renseignements personnels. Il y a donc urgence à adopter un cadre réglementaire et législatif qui régisse les conceptions émergentes de la vie privée, surtout que des lois comme la *Loi sur la protection des renseignements personnels et les documents électroniques* pourraient être modifiées par le projet de loi C-12. L'étude du Comité sur le sujet est une première étape prometteuse de l'établissement d'un tel cadre, et l'Association est fière de pouvoir y contribuer.

UNE NOUVELLE CONCEPTION DE LA CONFIDENTIALITÉ POUR UN NOUVEAU PUBLIC

Le réseautage social, les renseignements personnels et les limites de la méfiance à l'égard des inconnus

Il a été très bien expliqué que les espaces sociaux en ligne menacent la vie privée. Depuis les tout débuts d'Internet, nombreux sont ceux ayant affirmé (avec raison) que les réseaux sociaux numériques ouvrent nécessairement, au moins dans une certaine mesure, la voie aux incursions dans la vie privée et, dans bien des cas, favorisent des comportements prédateurs et dangereux. C'est pourquoi les réseaux sociaux, notamment les précurseurs comme LiveJournal, MySpace et Nexopia, et les plus récents comme Facebook, Twitter, Google+, LinkedIn et Tumblr, demeurent aussi profondément liés, tant dans les contextes stratégiques particuliers que dans les cadres culturels élargis, à ce qu'on appelle « la méfiance à l'égard des inconnus » (Poyntz, à paraître).

Dans cette optique, on se représente les réseaux sociaux comme de possibles moyens de prédation sociale qui exploitent nos renseignements personnels pour les raisons les plus viles (extorsion, chantage, usurpation d'identité, cyberintimidation). C'est qu'on transforme l'incursion dans la vie privée en problème individualisé et quelque peu aléatoire, causé de façon imprévisible par de mystérieux personnages difficiles, voire impossibles à retracer. Comme l'avancent Livingstone et Helsper (2011), cette optique a amené des universitaires, des leaders d'opinion et des décideurs à se pencher sur la question du respect de la vie privée sur les médias sociaux, particulièrement sur la régulation des comportements d'individus par le blocage, la restriction et l'interdiction d'accès à un site.

Comme la popularité des services de réseautage social n'a cessé d'augmenter au cours des dix dernières années, les gens ont été inondés de guides, de dépliants, de politiques et de programmes éducatifs sur les pratiques à suivre, qui insistent tous sur les stratégies de préservation des renseignements personnels. Par exemple, quand il s'agit de protéger leur vie virtuelle, les enfants et les adolescents se font souvent dire que la meilleure stratégie est de carrément éviter les réseaux sociaux qui encouragent l'autopromotion. Une chose est certaine, ces stratégies importantes ont le mérite bien réel d'expliquer comment notre personnalité publique en ligne peut être exploitée, et elle l'est souvent, à nos dépens. En novembre 2012, le suicide d'Amanda Tood, adolescente de Vancouver victime d'une campagne de cyberintimidation sans merci, constitue un rappel tragique des risques considérables que l'on court à publier des renseignements personnels dans les médias sociaux.

Cela dit, en matière de politiques visant à protéger les renseignements personnels des citoyens dans les médias sociaux, encourager simplement la non-divulgation et l'abandon des réseaux sociaux constitue une stratégie inopérante pour deux raisons :

1. Elle sous-estime l l'interconnectivité entre les réseaux numériques et nos vies sociale, politique, culturelle, civique et économique. Surtout pour les jeunes, les espaces sociaux en ligne servent, dans le meilleur des cas, aussi de sites d'apprentissage non conventionnel, et de lieux de discussion démocratique et décontractée sur divers sujets

(Poyntz, à paraître). En plus, si le Canada veut devenir un chef de file dans la nouvelle économie de l'information, il faut être disposé à tirer parti des réseaux favorables aux idées novatrices. Il ne semble pas raisonnable sur plusieurs plans de simplement se retirer de lieux d'échange et de création au riche potentiel. Comme l'a bien résumé dans son article paru dans *Maclean's* en novembre 2011 Emma Teitel, journaliste primée, « le seul moyen de ne pas être sur les photos d'une fête publiées sur Facebook, c'est de ne pas aller à la fête. Mais qui veut faire ça? » [traduction]

2. Si on conçoit les comportements intrusifs surtout comme des actes individuels et si on relie constamment ces actes à l'ombre menaçante d'un cybercriminel, on oublie qu'il existe des structures de grande échelle dans lesquelles les renseignements personnels sont recueillis, utilisés et publiés, et on écarte complètement les **données volumineuses**, ce moteur qui stimule le réseautage social en ligne.

Les données volumineuses et les métadonnées : évolution de l'identification et des renseignements personnels

> Jay Stanley (2012), analyste principal des politiques du Speech, Privacy and Technology Project de l'American Civil Liberties Union, a expliqué l'origine des **données volumineuses :** la poussée exponentielle de la puissance informatique combinée à l'expansion des réseaux de communications numériques dans le monde et à la chute du coût d'entreposage des données permettent désormais de colliger et d'entreposer des quantités prodigieuses de données. Une fois saisies, les données sont analysées selon un processus appelé **exploration des données**, en général au moyen de systèmes et de processus automatisés (comme des algorithmes) pour passer au crible des quantités phénoménales de données pour faire ressortir des répétitions subtiles, des corrélations ou des relations dans un ensemble de données (Stanley, 2012). L'exploration de données fait apparaître des choses auparavant invisibles (*ibid*.), et comme Bigus (1996) et Cavoukian (1998) l'ont expliqué, l'exploration sert souvent des intérêts commerciaux. Même si elles se révèlent d'un grand intérêt sur les plans de la recherche et des affaires, la collecte et l'analyse de données sur grande échelle soulèvent de graves préoccupations quant à la confidentialité et à la protection des renseignements personnels. Ces dernières ouvrent la voie à d'autres formes de surveillance inquiétantes qui, selon M. Stanley, seraient confiées à de grosses institutions plutôt qu'à des individus.

Mais d'où viennent toutes ces données? Quelles activités produisent autant de données pour qu'autant d'efforts soient consacrés à les colliger et à les entreposer? Hormis la simple croissance de la quantité de données échangées par les internautes, un facteur important de la multiplication des données est l'expansion et l'intensification sans pareil au cours des trente dernières années de la vidéosurveillance et de l'écoute électronique qu'effectuent les institutions pour assurer la sécurité des infrastructures, ainsi que de la surveillance volontaire ou spontanée des citoyens à l'aide de téléphones cellulaires munis d'un appareil photo et de réseaux de partage de photographies (comme Instagram). Cependant, la plus grande source d'information dans le domaine des données volumineuses, sensiblement plus importante que les précédentes, provient des données *sur* les données, communément appelées **métadonnées**.

À chaque interaction sur un média social, même si elle est infime, banale ou faible en contenu, le média social produit, à l'aide d'algorithmes complexes d'agrégation de données, des quantités massives de données *sur* l'interaction : le lieu, le moment, les utilisateurs connectés, l'appareil et le système d'exploitation utilisés, la durée, etc. Une fois réunies, ces données permettent de dresser un portrait très précis de l'utilisateur, avec ses préférences, ses réseaux et ses habitudes. M. Stanley l'a bien résumé : « quand on combine les renseignements personnels d'un individu à de vastes ensembles de données externes, on crée de nouvelles données sur cet individu ». Par conséquent, même si des utilisateurs ne fournissent *pas* volontairement de données précises, complètes ni factuelles sur eux-mêmes, les médias sociaux recueillent tout de même de vastes quantités de *métadonnées*, qui rendent possible de bien des manières l'identification des utilisateurs. Dans les médias sociaux, l'identification des individus est étroitement liée à leur interactivité tout comme à leur définition conventionnelle de la divulgation des renseignements. La commissaire à la protection de la vie privée, Jennifer Stoddard l'a expliqué dans son témoignage devant le Comité :

> « En un tour de main, les entreprises de médias sociaux parviennent à réunir une quantité astronomique de renseignements personnels. En plus des préférences, des habitudes et des interactions sociales des utilisateurs, elles recueillent une foule de renseignements de base qui ne figurent pas dans le profil public, notamment l'historique des recherches, les achats effectués, les sites Web consultés et le contenu des messages privés. En recueillant ces milliards de points de données, les entreprises de médias sociaux peuvent analyser le comportement des utilisateurs au moyen d'algorithmes évolués dans le but de personnaliser leurs services et de trouver des façons de générer des revenus. »

Dans l'univers des données volumineuses, des métadonnées et des médias sociaux, le paradigme de la « méfiance à l'égard des inconnus », selon lequel la confidentialité des renseignements personnels repose sur les choix des gens sur ce qu'ils divulguent et sur ce qu'ils gardent confidentiel, est donc incomplet. Les utilisateurs ont beau utiliser pseudonymes, fausses dates de naissance et villes d'origine imaginaires, les médias sociaux parviennent néanmoins à les identifier, car les vastes ensembles de métadonnées sont liés différemment. Autrement dit : si les pratiques d'interactivité permettent l'incursion des médias sociaux dans la vie privée des utilisateurs (soit la capacité d'identifier les utilisateurs), et si les médias sociaux sont créés de manière à faciliter lesdites pratiques, les médias sociaux contiennent donc tous un élément propice à la violation de la confidentialité des renseignements.

Comme il a été dit plus tôt, le simple retrait des médias sociaux pourrait avoir des effets néfastes sur l'économie, la présence sociale en ligne et même sur la démocratie. Comment doit-on procéder? Comment peut-on saisir et adopter des pratiques sur la confidentialité de façon à profiter des avantages d'être connecté tout en étant conscient des nouvelles méthodes d'identification des citoyens canadiens utilisées non seulement par des cybercriminels, mais aussi par des algorithmes, des codes et des métadonnées et en se protégeant contre elles?

Confidentialité selon le contexte : distinguer le « social » dans « média social »

Si les métadonnées rendent possible l'identification des utilisateurs à partir de leurs interactions dans les médias sociaux, c'est-à-dire si l'identification et l'atteinte à la vie privée reposent sur la

socialité au sein d'un réseau, notre définition de la confidentialité des renseignements personnels et les politiques qui doivent la protéger doivent elles aussi reposer sur l'aspect social. Comme l'indiquait Valerie Steeves (2009), professeur de criminologie à l'Université d'Ottawa, l'explosion des violations de la vie privée, comme l'usurpation d'identité, à l'ère des réseaux sociaux n'est pas le simple résultat d'une politique sur le respect de la vie privée mal appliquée. Elle s'est produite parce que la définition de la vie privée pose problème, car elle ne tient *pas compte du contexte social* (p. 193). Selon Mme Steeves, la vie privée dans le monde d'aujourd'hui s'étend bien au-delà « d'étroites considérations procédurales sur la confidentialité des renseignements personnels », qui sont renforcées par le paradigme de la « méfiance à l'égard des inconnus ».

Dans un article, le corédacteur en chef du blogue *Public Policy and Governance Review*, Max Greenwald a donné un compte-rendu du discours prononcé lors de la remise des Prix du magazine canadien de 2012 par Emma Teitel, dont a été cité plus tôt l'essai sur la confidentialité des renseignements personnels dans les médias sociaux, *The New Paparazzi*, publié récemment dans *Maclean's*. La journaliste a commencé son allocution en lisant à haute voix certains renseignements personnels sur des membres de l'auditoire qu'elle avait trouvés sur leur profil Facebook. Même si les renseignements personnels avaient été sciemment rendus publics, l'expérience a quand même fait son effet : un sentiment d'atteinte à sa vie privée. Elle a montré que la divulgation de renseignements et le sentiment d'envahissement de sa vie privée sont beaucoup plus complexes, modulables et dépendants du contexte qu'une coupure nette entre vie privée et vie publique.

Voilà pourquoi la confidentialité, de l'avis de M^{me} Steeves, doit être comprise et considérée comme une balise protection des liens amicaux, familiaux et sociaux *en général* contre l'exploitation, l'usurpation et l'incursion. Si les renseignements utilisés pour porter atteinte au droit à la vie privée proviennent de plus en plus de ses connaissances dans l'espace numérique, et non pas uniquement de ses habitudes *personnelles* de divulgation, il faudra adopter une réglementation visant à protéger la vie privée qui contienne vraiment les notions d'interaction et de socialité. La réglementation devra aussi aborder le concept de vie privée en des termes suffisamment larges et souples pour pouvoir « s'interroger sur – l'incidence néfaste de la surveillance sur les relations sociales et démocratiques – et la limiter – » (p. 193) [traduction]. M^{me} Steeves a résumé son point de vue en citant *Regulating Privacy* (1995), de Priscilla Regan :

> « La confidentialité des renseignements personnels représente plus qu'un droit individuel; il s'agit aussi d'un bien commun en soi qui "sert les autres fonctions [sociales] au-delà de celles inhérentes à un individu". Si la valeur sociale n'est pas prise en considération par les décideurs, la confidentialité des renseignements personnels continuera à perdre du terrain face aux impératifs contraires que sont la sécurité et la commodité » (p. 194)[traduction].

Si, comme M. Stanley en fait état, les institutions déjà puissantes peuvent tirer profit des données volumineuses pour s'approprier davantage de pouvoir aux dépens des citoyens en explorant et en exploitant des métadonnées tirées de la vie virtuelle des gens, les politiques sur la vie privée

doivent alors tenir compte de cette asymétrie croissante et la contrer. Cela suppose l'éloignement par rapport à la socialité, à l'interconnectivité et au partage et la prise en compte de ces phénomènes.

CONSIDÉRATIONS D'ORDRE STRATÉGIQUE

La B.C. Freedom of Information and Privacy Association (l'Association) propose que le Comité étudie les points suivants lors de son examen du dossier concernant les données volumineuses, les politiques et le respect de la vie privée dans le contexte canadien actuel.

1. **Revoir et élargir la définition de « renseignements personnels » inscrite dans la *Loi sur la protection des renseignements personnels et les documents électroniques.***

   La *Loi* définit les renseignements personnels comme suit : « Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ». Cette définition ne tient pas compte du fait qu'un utilisateur d'un média social en particulier n'est pas forcément identifiable uniquement à l'aide de données faisant l'objet d'une collecte traditionnelle, étant donné que même les données prétendument anonymes, comme les métadonnées recueillies à l'aide d'algorithmes, servent désormais à identifier les individus.

   En outre, dans la définition actuelle, on présume de l'existence d'un « individu identifiable » et la *Loi* établit seulement des restrictions sur la collecte de données *après* que l'individu a été identifié et ne couvre donc pas le moment de l'identification. Ainsi, la *Loi* ne tient pas compte du fait que les gens *deviennent identifiables* à partir du moment où ils discutent et échangent avec les autres usagers. La fonction première des réseaux sociaux est précisément d'identifier les gens; les entreprises et systèmes propriétaires ne peuvent fonctionner ni collecter des métadonnées sans que les utilisateurs ne s'identifient tout d'abord (et de manière très approfondie). Cet acte d'identification est donc inhérent à la transaction entre les utilisateurs et les propriétaires d'un média social, et devrait donc être couvert par la *Loi*.

   À la lumière de l'explication sur la confidentialité selon le contexte, la protection des renseignements personnels à l'ère des médias sociaux ne devrait pas se limiter à protéger les données sur les individus identifiables. Elle devrait englober les processus, pratiques et interactions sociales propices à l'*identification*, surtout dans la mesure où celle-ci est nécessaire au fonctionnement des réseaux sociaux.

   Par conséquent, l'Association propose de modifier la définition des « renseignements personnels » de telle sorte que celle-ci tienne compte des processus et pratiques liés à l'interactivité qui permettent d'identifier les utilisateurs de médias sociaux.

2. **S'opposer au régime de divulgation volontaire qui serait créé par les modifications à la *Loi* proposées dans le projet de loi C-12.**

   On devrait simultanément réviser la définition des « renseignements personnels » inscrite dans la *Loi* et s'opposer vertement aux dispositions du projet de loi C-12 sur l'incursion dans la vie privée. Comme Tamir Israel de la Clinique d'intérêt public et de politique d'Internet du Canada l'a écrit, le projet de loi C-12 se trouverait à instaurer un régime de divulgation volontaire auquel échapperait ne serait-ce que la plus rudimentaire des surveillance et géolocalisation généralement associées aux fonctions policières. En permettant à davantage d'entités de mettre la main sur les renseignements personnels détenus par des entreprises privées (dont les propriétaires de réseaux sociaux) sous prétexte d'« exercice des fonctions de police », le projet de loi C-12 entamerait la protection des renseignements personnels établie par la *Loi* et augmenterait de beaucoup la capacité de surveillance d'imprécises « autorités légitimes », au moment où, pour reprendre les propos de Jay Stanley, les données volumineuses exacerbent déjà le déséquilibre du pouvoir entre les citoyens et les autorités.

   Plus important encore, si le projet de loi C-12 est adopté, on s'éloigne davantage d'un cadre réglementaire qui reconnaisse la confidentialité des renseignements comme une valeur commune résultant des interactions entre utilisateurs, on permet aux forces policières d'obtenir des renseignements personnels détenus, entreposés et transmis par les sociétés de télécommunications, les médias sociaux et les fournisseurs de services Internet, ce qui porte atteinte à la protection de l'interactivité et de la socialité et soumet les médias sociaux à une surveillance accrue. Combiné à l'éventualité que l'on établisse, à l'aide de métadonnées sur la géolocalisation et la proximité, des liens entre des interactions anodines et non compromettantes entre utilisateurs de médias sociaux et des activités suspectes sans aucun rapport, le régime de divulgation volontaire préconisé dans le projet de loi C-12 menace d'impliquer à tort des Canadiens innocents dans des enquêtes criminelles.

3. **Assujettir les partis politiques canadiens à la *Loi sur la protection des renseignements personnels et les documents électroniques.***

   À mesure qu'ils gagnaient en popularité, en complexité technique et en ampleur, les médias sociaux se sont transformés en précieux outils de mobilisation politique. Les pétitions électroniques et autres formes de cyberactivisme sont désormais extrêmement courantes et deviennent souvent virales sur les médias sociaux, ce qui permet de colliger de prodigieuses quantités de renseignements personnels sur les signataires. Ces pétitions sont souvent remises aux politiciens et aux chefs d'État en vue de les pousser à prendre des mesures concernant d'importants dossiers d'intérêt public.

   Cependant, de telles actions constituent une menace unique et étonnante pour la vie privée, puisque les partis politiques canadiens *ne sont pas assujettis* à la *Loi sur la protection des renseignements personnels et les documents électroniques*. Ainsi, les vastes ensembles de données comme les listes de pétitions et même les listes électorales peuvent être utilisés et rendus publics selon le bon vouloir des partis, sans que ceux-ci n'aient à rendre de comptes ni à fournir leurs sources. Sous cet angle, les partis politiques canadiens sont des anomalies. Toutes les autres organisations du pays (privées, publiques,

sans but lucratif, à but commercial, professionnelles ou bénévoles) sont contraintes de protéger dans une certaine mesure les renseignements personnels de leurs membres, que ce soit en vertu d'une loi provinciale ou d'une loi fédérale. L'Association ne voit aucune raison justifiant que les partis politiques, qui figurent sans doute parmi les organisations les plus influentes du pays et qui sont particulièrement présents sur les médias sociaux et dans le cyberespace, fassent exception à la règle.

Les conséquences possibles de cette faille sont importantes. En premier lieu, les Canadiens sont exposés à tous les agissements relevant de l'exploitation et de l'incursion dans la vie privée, comme l'usurpation d'identité, la sollicitation et le télémarketing. Par exemple, en 2009, des journalistes ont découvert que la cellule des Tigres tamouls de Toronto, officiellement déclarée organisation terroriste, avait obtenu des copies de listes électorales canadiennes et l'utilisaient à des fins de financement. Même des ministres membres du Cabinet et des figures de proue du gouvernement utilisent les renseignements personnels tirés de pétitions pour faire la promotion de projets partisans auprès de groupes d'intérêts particuliers. À l'automne de 2012, un certain nombre de gays et lesbiennes qui avaient signé la pétition visant à empêcher la déportation au Nicaragua de l'artiste homosexuel Alvaro Orozco ont reçu un courriel non sollicité du bureau du ministre de l'Immigration Jason Kenney, qui faisait l'apologie des efforts du Parti conservateur en matière de protection d'immigrants ouvertement membres de la communauté LGBT. Or les destinataires de ce message n'avaient pour la plupart jamais voté pour les conservateurs, ni ne les avaient soutenus, ni même eu de contact direct avec eux qui les aurait obligés à indiquer leur orientation sexuelle ou leurs coordonnées. En fait, les renseignements personnels ont été trouvés à l'aide de l'exploration des données sur les signataires de la pétition concernant M. Orozco. De telles prises de contact non sollicitées ne se produisent que parce que les partis politiques ne sont pas assujettis à la *Loi* en ce qui concerne les données sur les électeurs, leur source et leur utilisation.

En deuxième lieu, cette faille pourrait avoir des effets néfastes sur la confiance de l'électorat et dissuader les citoyens de participer à la politique. Comme la vie politique devient de plus en plus présente sur les médias sociaux, environnements qui colligent des quantités phénoménales de données sur les préférences et habitudes de leurs utilisateurs, il est essentiel que les représentants du gouvernement, les bénévoles qui participent aux campagnes électorales et le personnel des partis prennent des mesures pour protéger ces renseignements personnels – surtout s'ils contiennent des détails sensibles comme l'allégeance politique et les préférences de l'électeur. Si les partis politiques utilisaient à mauvais escient ces renseignements, les divulguaient de manière inappropriée ou les exploitaient, les citoyens risqueraient de se désintéresser tout simplement de la chose politique et de se retirer des médias sociaux, outils possibles de renforcement de la démocratie.

Dans tous les domaines, des services sociaux à l'entreprise privée, il est bien connu que la participation et la loyauté du citoyen dépendent fortement de la sécurité et de la confiance dans le rapport entre le citoyen et le prestataire de services. Une étude de l'Association sur le système de gestion de cas intégré de la Colombie-Britannique menée en 2009 a montré, entre autres choses, que les utilisateurs de certains services médicaux

et sociaux sont beaucoup moins susceptibles de recourir à des ressources d'urgence s'ils sentent la sécurité de leur rapport personnel avec le prestataire de services menacée. De même, la protection des renseignements personnels des clients représente un volet essentiel de la stratégie de toute entreprise. Au tout début d'un rapport publié en 2001, l'importante firme d'experts-conseils PricewaterhouseCoopers a mis une déclaration sans équivoque : « La confidentialité des communications électroniques est un élément fondamental du commerce électronique. Loin d'être un obstacle ou un simple coût, elle représente le meilleur moyen pour une entreprise de se démarquer sur le marché numérique – et une condition absolue pour gagner les plus grandes loyauté et confiance du consommateur à son égard, essentielles à la prospérité du commerce électronique ». [traduction]

À l'évidence, la protection des renseignements personnels est primordiale pour le maintien de rapports efficaces dans le cas de la prestation de services. Le même principe s'applique à la participation citoyenne aux partis politiques. En l'absence de lois qui protègent le droit à la vie privée des citoyens et qui tiennent les partis politiques responsables de l'utilisation, de la collecte et de la divulgation de renseignements personnels sur les électeurs, on risque de faire disparaître les citoyens d'un paysage politique de plus en plus numérique.

4. **Respecter les politiques nationales sur la vie privée en garantissant des « exclusions » dans les accords de coopération et de commerce internationaux.**

   L'établissement de toute politique exige un équilibre subtil et des recherches approfondies. L'Association espère avoir très bien expliqué que c'est encore plus vrai lorsqu'il s'agit de la protection des renseignements personnels à l'ère des médias sociaux. Selon elle, il importe que ces initiatives démocratiques prudentes soient, au final, respectées et protégées au sein d'un Canada doté de politiques de vaste portée.

   Plus précisément, il faut empêcher que la portée des politiques nationales sur la vie privée ne soit minée par d'autres accords et engagements du gouvernement fédéral, comme des partenariats commerciaux qui favorisent la libre circulation de données sur les Canadiens entre diverses régions, sans que personne n'en assume la responsabilité. Les projets tels que le Partenariat transpacifique, doivent être adoptés de façon à ce que soit respecté le droit à la vie privée des Canadiens d'après le contexte et les lois nationales. Il faut donc intégrer des « exclusions » dans les accords internationaux et ainsi préserver l'équilibre et les compromis prudemment établis dans les lois sur la vie privée adoptées démocratiquement.

   De telles exclusions sont essentielles puisqu'elles dénotent un respect de l'application régulière de la loi et de la démocratie parlementaire au Canada. Plus important encore, ces exclusions témoignent d'une vision où la vie privée est une valeur commune résistante à l'intégration, sans prise de responsabilité, de la vie virtuelle des gens et des réseaux sociaux à des accords commerciaux de grande ampleur, mais dotés de fondements économiques limités.

5. **Revoir les politiques établissant la vie privée comme valeur commune et s'en inspirer.**

Dans bien des régions, les représentants du gouvernement et les défenseurs de la vie privée ont déjà commencé à élaborer des politiques où les avantages réels de la connectivité par les médias sociaux et la nécessité d'assurer la confidentialité des renseignements personnels comme valeur commune font bon ménage. En voici quelques exemples :

- La Californie a récemment adopté un projet de loi (AB-1844) qui interdit aux employeurs d'exiger des justificatifs relativement aux médias sociaux (mots de passe, noms d'utilisateurs, gestion de l'image) des candidats à l'embauche. Une mesure législative complémentaire (SB-1349) énonce des dispositions analogues pour les collèges et universités vis-à-vis de leurs candidats. Ces politiques sont très instructives puisqu'on reconnaît que, même si les gens « publient » des renseignements personnels comme des photos, des habitudes et des préférences dans les médias sociaux, ces actes de divulgation sont faits dans un contexte donné et soumis à des normes de socialité et d'interaction. Les États du Delaware, du Maryland et de l'Illinois ont également adopté des mesures similaires (même si elles sont insuffisantes sous bien des aspects, et le Congrès américain a été saisi en avril 2012 du *Social Networking Online Privacy Act*, qui vise à instaurer des mesures de protection comparables à l'échelon fédéral.
- La commissaire à la protection de la vie privée M^{me} Stoddard a demandé à maintes reprises que soient remaniées la *Loi sur la protection des renseignements personnels et les documents électroniques* et autres lois canadiennes connexes et qu'elles soient adaptées au monde des données volumineuses, de l'exploration de données et à l'infrastructure des médias sociaux. M^{me} Stoddard a tenu des propos lourds de sens sur la confidentialité des renseignements personnels sur les médias sociaux, et les enquêtes menées par son Bureau sur les géants numériques comme Facebook s'avèrent très instructives, car elles montrent les limites et contraintes de la législation canadienne en la matière et soulignent la nécessité de la modifier et de la remanier périodiquement.
- Le cadre sur la « protection intégrée de la vie privée » mis sur pied par la commissaire à l'information et à la protection de la vie privée de l'Ontario se révèle aussi d'un grand secours. On y tente de reconnaître et de préserver les avantages de la connectivité des médias sociaux – croissance économique, innovation, créativité, solidarité et discussion démocratique – ainsi que de défendre la création d'infrastructures technologiques qui tendent à colliger moins de données, au lieu de les colliger par défaut. Le cadre énonce d'autres pistes à suivre en matière de politiques adaptées à l'ère des médias sociaux.

CONCLUSION ET SOURCES

La B.C. Freedom of Information and Privacy Association tient à adresser ses remerciements et ses félicitations au Comité permanent de la Chambre des communes pour avoir accepté les mémoires qui traitent de ce dossier important. La confidentialité des renseignements personnels, surtout dans les médias sociaux, exige études, recherches collaboratives et solutions novatrices. L'Association est heureuse d'avoir pu contribuer à ce processus et espère que le présent mémoire aidera à l'établissement d'un cadre sur la protection des renseignements personnels qui permette

de préserver les avantages économiques et culturels de l'interconnectivité ainsi que de resserrer les engagements en matière de respect de la vie privée comme valeur commune.

***

Cavoukian, A. (2009). *Privacy by Design: Take the Challenge.* http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf.

Cavoukian, A. (1998). *Data Mining: Staking a Claim on Your Privacy*. http://www.ipc.on.ca/images/resources/datamine.pdf.

Bigus, J. (1996). *Data Mining With Neutral Networks: Solving Business Problems from Application Development to Decision Support.* New York, McGraw-Hill.

Greenwald, M. (5 octobre 2012). « Seen and Heard: Social Media and Privacy Legislation », *Public Policy and Governance Review.* http://ppgreview.ca/2012/10/05/seen-and-heard-social-media-and-privacy-legislation/.

Israel, T. (23 mars 2012). *Bill C-12: Safeguarding Canadians' Personal Information Act-Eroding Privacy in the Name of Privacy*. http://www.slaw.ca/2012/03/23/billc12-safeguarding-privacy-by-eroding-it/.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-3

Poyntz, S. (à paraître). *Eyes Wide Open: Stranger Hospitality and the Regulation of Youth Citizenship*.

Steeves, V. (2009). « Reclaiming the Social Value of Privacy. In I. Kerr, V. Steeves & C. Lucock » (dir.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* (p. 191-208). Oxford University Press.

Stanley, J. (2012). « Eight Problems with "Big Data." ». American Civil Liberties Union, consulté le 25 novembre 2012. http://www.aclu.org/blog/technology-and-liberty/eight-problems-big-data.

Teitel, E. (1er novembre 2011). « The New Paparazzi ». *Maclean's*, consulté le 10 décembre 2012. http://www2.macleans.ca/2011/11/01/the-new-paparazzi/.