Commissariat
à la protection de
la vie privée du Canada

Les courtiers en données

Regard sur les paysages canadien et américain

Rapport préparé par le Groupe de recherche du Commissariat à la protection de la vie privée du Canada

Septembre 2014

Table des matières

Résumé

Le but du présent rapport est de donner une vue d'ensemble des courtiers en données et de leurs activités dans le contexte de la protection de la **vie privée** au Canada et aux États-Unis.

Introduction

La pratique des courtiers en données consistant à recueillir et à vendre des renseignements personnels, à des fins de marketing ou autres, suscite des inquiétudes sur le plan du droit à la vie privée. Ces inquiétudes découlent en partie d'un manque de transparence et d'ouverture ainsi que des difficultés auxquelles se heurtent les personnes qui tentent d'exercer un contrôle sur les renseignements qui les concernent.

Les préoccupations et les risques d'atteinte à la vie privée vont au-delà des enjeux qui viennent spontanément à l'esprit lorsque l'on pense aux répercussions d'une atteinte à la sécurité des renseignements personnels stockés dans de grandes bases de données. Comme l'a signalé Daniel J. Solove, le problème avec les bases de données et les pratiques connexes actuelles, c'est qu'elles rendent les intéressés impuissants. Elles rendent les gens vulnérables en les empêchant d'exercer un contrôle sur leurs renseignements personnels[1].

Le présent rapport vise à fournir aux individus et aux entreprises un examen de l'environnement de réglementation en matière de protection de la vie privée au Canada et aux États-Unis ainsi que des exigences liées à la conformité en la matière que doivent observer les courtiers en données de l'étranger qui font affaire au Canada. Ainsi, ces derniers pourront prendre des décisions plus éclairées concernant le consentement et le contrôle. En outre, puisque les courtiers en données comprendront mieux leurs responsabilités, il leur sera plus facile de mettre au point des pratiques favorisant le contrôle par les consommateurs, la confiance et la transparence.

Le rapport s'inspire en partie de la recherche concernant les courtiers en données financée par le Programme des contributions du Commissariat à la protection de la vie privée du Canada.

A. Qu'est-ce qu'un courtier en données? Définition de son champ d'activité

Comme on l'a récemment montré lors d'un sommet sur la protection de la vie privée tenu en décembre 2012 aux États-Unis, qui réunissait la Federal Trade Commission (FTC), des législateurs et des représentants de l'industrie, il est difficile de définir de façon catégorique l'expression « courtier en données »[2]. Ces courtiers sont-ils les organisations qui font le commerce des renseignements personnels sans jamais traiter directement avec les consommateurs? Et qu'en est-il des entreprises qui ont établi une relation directe avec les gens et utilisent leurs renseignements pour créer des bases de données à des fins de marketing ou autres[3]?

Étant donné la gamme des organisations et des modes de fonctionnement qui participent au commerce de l'information, nous nous limiterons dans le présent rapport à la définition retenue par la FTC : [traduction] « Les courtiers en données sont des entreprises qui recueillent des renseignements personnels sur les consommateurs auprès de diverses sources publiques et non publiques et les revendent à d'autres entreprises »[4].

B. Le contexte américain

Législation et surveillance – analyse de la conjoncture

Ces dernières années, on a observé aux États-Unis un intérêt croissant pour les pratiques des courtiers en données[5]. Cet intérêt est attribuable à un manque de transparence concernant les pratiques de ces organisations, au fait que les consommateurs sont peu conscients de la portée et de l'existence de ces pratiques et à la progression exponentielle de la capacité des organisations, grandes et petites, à recueillir, à stocker et à analyser les données hors ligne et en ligne pour établir des profils extrêmement détaillés.

Aux États-Unis, la protection des renseignements personnels dans le secteur privé n'est régie par aucune législation nationale exhaustive. On observe plutôt au niveau des États et de l'administration fédérale une multitude de lois, de règlements et de délits en common law qui parfois se chevauchent et créent une mosaïque complexe d'exigences en matière de protection de la vie privée et de sécurité des données. Cependant, aucune législation exhaustive ne couvre *tous les types possibles de renseignements personnels* ou *toutes les activités commerciales* des courtiers en données. Par exemple, pratiquement tous les États américains se sont dotés d'une loi sur la notification des atteintes à la vie privée et l'administration fédérale impose des exigences concernant cette notification pour certains renseignements médicaux et financiers personnels. En outre, la plupart des États ont des lois exigeant une sécurité raisonnable de l'information et sont assujettis à des lois s'appliquant à plusieurs États qui régissent l'utilisation de certains renseignements, par exemple ceux sur la santé, les numéros de sécurité sociale, les renseignements financiers ou les données biométriques, ou encore qui confèrent certains droits en ce qui a trait aux avis de confidentialité dans un contexte en ligne. Au niveau fédéral, le droit à la vie privée semble éparpillé de façon similaire dans différentes lois sectorielles, comme la *Fair Credit Reporting Act* (FCRA), la *Gramm Leach-Bliley Act* (GLBA), la *Health Insurance Portability and Accountability Act* (HIPAA) et la *Health Information Technology for Economic*

and Clinical Health Act (HITECH), qui renferment toutes des dispositions se rapportant à la protection de la vie privée et des renseignements personnels.

Toutefois, de façon générale, les lois américaines ne protègent les consommateurs que dans certaines situations. Par exemple, la FCRA – loi fédérale américaine qui régit actuellement un segment appréciable de l'industrie des mégadonnées – ne s'applique qu'aux renseignements que les entreprises reçoivent dans le rapport de solvabilité des consommateurs, entre autres l'information sur le crédit, les assurances, le logement et l'emploi, et elle ne couvre pas nécessairement toutes les activités de marketing des courtiers en données[6]. En outre, la GLBA se limite aux institutions financières et à certaines activités bancaires et activités de prêt traditionnelles.

Les plus vastes protections offertes aux États-Unis sont prévues par l'article 5 de la *Federal Trade Commission Act*, qui confère à la Federal Trade Commission le pouvoir de prendre des mesures à l'encontre des organisations qui se livrent à des manœuvres ou à des pratiques déloyales ou frauduleuses dans le domaine du commerce[7]. La FTC a eu recours à ce pouvoir dans des affaires qui mettaient en cause les pratiques d'organisations concernant des renseignements personnels[8]. En vertu de ses pouvoirs quant à l'aspect frauduleux, elle a appliqué la loi à l'encontre d'entités qui avaient fait de fausses promesses concernant leurs pratiques de gestion des renseignements personnels, par exemple dans leur politique de confidentialité. Par ailleurs, en vertu de ses pouvoirs concernant l'aspect déloyal, la FTC a pris des mesures contre des pratiques préjudiciables en matière de gestion des renseignements, mais ses pouvoirs dans le domaine sont limités par un triple critère :

- la manœuvre ou la pratique a causé ou pourrait causer un préjudice appréciable aux consommateurs;
- le préjudice n'a pas été compensé par des avantages suffisants pour les consommateurs ou la concurrence;
- les consommateurs ne pouvaient raisonnablement pas échapper au préjudice[9].

Même si les pouvoirs d'application de la loi dévolus à la FTC lui donnent une marge de manœuvre en ce qui touche la portée de son mandat pour protéger les consommateurs contre les manœuvres ou les pratiques déloyales ou frauduleuses et que la FCRA couvre déjà les pratiques d'un segment appréciable de l'industrie des mégadonnées, le régime de réglementation américain ne prend pas expressément en compte toute l'envergure de l'industrie des mégadonnées à l'ère des flux de données constants et des utilisations possibles apparemment illimitées. Signalons en outre que plusieurs projets de loi ciblant précisément l'industrie du courtage de données ont été déposés au Congrès, mais qu'aucun n'a été adopté ou ne semble en voie de l'être au moment de la rédaction du présent rapport.

Il faut considérer que tous ces projets de loi et ces lois sont limités par les notions fortes de liberté d'expression qui, selon la Cour suprême des États-Unis, englobe expressément la vente, la communication et l'utilisation de renseignements dans le contexte particulier des documents concernant les habitudes des médecins en matière d'ordonnances[10]. Cet arrêt fondé sur la Constitution a fait comprendre aux courtiers en données des États-Unis que les efforts visant à réglementer la façon dont ils utilisent les renseignements feront l'objet d'un contrôle judiciaire accru compte tenu de leur droit à la liberté d'expression.

Rapports, audiences et études sur les courtiers en données

Les défenseurs du droit à la vie privée n'ont pas été les seuls à observer que l'industrie du courtage de données aux États-Unis n'est pas soumise à une surveillance exhaustive. Selon un rapport publié en 2005 par le service de recherche du Congrès, les États n'ont pratiquement aucune loi régissant les courtiers en

données[11]. Les auteurs du rapport soulignent également que les inquiétudes suscitées par l'industrie du courtage de données sont attribuables en partie aux grandes quantités de renseignements personnels que détiennent les courtiers, aux atteintes à la vie privée associées à certains d'entre eux ainsi qu'aux répercussions sur le plan du vol d'identité. L'année suivante, le Government Accountability Office (GAO) des États-Unis a publié un rapport où l'on peut lire :

> [traduction] « En obligeant les revendeurs de renseignements à prendre des mesures pour empêcher l'accès non autorisé à tous les renseignements personnels délicats qu'ils détiennent, on aiderait à faire en sorte que les exigences explicites relatives à la sécurité des renseignements s'appliquent plus intégralement à une catégorie d'entreprises qui détiennent de grandes quantités de ce type de renseignements. En outre, aucune loi fédérale n'oblige les entreprises à déclarer les atteintes à la sécurité des renseignements personnels délicats, même si une exigence en ce sens pourrait les inciter à mieux protéger les renseignements et à communiquer des renseignements utiles aux consommateurs vulnérables au vol d'identité ou à d'autres préjudices connexes »[12].

En 2012, Edward Markey (représentant démocrate du Massachusetts) et Joe Barton (représentant républicain du Texas) ont piloté une initiative bipartisane du Congrès et écrit à neuf organisations faisant le commerce de renseignements pour leur demander d'indiquer l'ampleur et la portée de leurs pratiques de collecte de renseignements, les sources qu'elles utilisaient, leurs champs d'activité, les mesures de sécurité mises en place ainsi que leurs pratiques en matière d'accès et de correction[13]. Insinuant que les pratiques des organisations manquaient de transparence, leurs lettres laissaient entendre qu'elles avaient constitué des dossiers secrets sur pratiquement tous les clients américains[14] et que le regroupement de tous les renseignements en ligne et hors ligne aux fins de marketing pouvait mettre en danger tous les Américains, y compris les enfants.

Les réponses fournies par les organisations ont révélé toute une gamme d'activités et de pratiques de collecte de renseignements, notamment l'obtention d'information auprès de sources publiques, au moyen de sondages et de fiches de produit, et dans certains cas, l'obtention de données sur des achats ou des permis auprès de tiers (par exemple d'autres courtiers en données) et la collecte de renseignements dans les sites de réseaux sociaux. La gamme de renseignements et les catégories étaient larges et approfondies, et comprenaient des identifiants comme la race et la religion, et parfois le classement des individus à des fins de marketing.

À la suite de cette initiative, les représentants Markey et Barton, en concertation avec la FTC, des défenseurs du droit à la vie privée et plusieurs courtiers en données, ont tenu en décembre 2012 une réunion sur la protection des renseignements personnels dans l'industrie du courtage de données[15]. Les participants ne sont pas parvenus à un consensus sur la façon de définir la notion de « courtiers en données » ou d'apaiser les inquiétudes suscitées par leurs pratiques, mais l'événement n'en a pas moins fait date, car il s'agissait de la toute première audience du Congrès sur ce sujet[16].

Précédemment, en mars 2012, la FTC avait publié un rapport final[17] sur la protection de la vie privée des consommateurs, dans lequel elle recommandait d'adopter un cadre de protection de la vie privée plus exhaustif pour améliorer les pratiques de collecte et d'utilisation des renseignements. En outre, le rapport renfermait des recommandations précises à l'intention de l'industrie du courtage de données – en particulier pour améliorer la transparence des mégadonnées. Le rapport s'inspire d'un rapport préliminaire publié par la FTC en décembre 2010.

La FTC a demandé au Congrès d'adopter une loi de base sur la protection de la vie privée, mais les auteurs du rapport final lui ont aussi demandé d'envisager l'adoption d'une loi s'appliquant expressément aux courtiers en données pour accroître la transparence de leurs pratiques et le contrôle exercé sur celles-ci[18].

Pour remédier au manque de transparence des courtiers, la FTC a aussi formulé des recommandations précises à l'industrie des mégadonnées pour améliorer la transparence même en l'absence de législation. Elle a notamment exhorté les courtiers en données qui se livrent au marketing à créer un site Web centralisé afin que les consommateurs connaissent leur identité, et à décrire leur accès aux renseignements personnels et aux choix des consommateurs concernant le contrôle de leurs renseignements. Ces recommandations visaient à promouvoir l'accès et à améliorer la transparence des activités des courtiers[19].

Le cadre de protection de la vie privée établi par la FTC recommande également que les organisations soient tenues d'obtenir un consentement explicite si elles ont l'intention d'utiliser l'information « à une fin sensiblement différente » de celle indiquée au moment de la collecte ou dans certaines situations où il s'agit de renseignements délicats. Pour faciliter cette démarche, la FTC a recommandé que les organisations améliorent et normalisent leur politique de confidentialité. L'amélioration des politiques de confidentialité a également été préconisée comme moyen de promouvoir la transparence[20].

La FTC a aussi recommandé d'inciter les organisations à se limiter aux renseignements qui concordent avec le contexte d'une transaction donnée, d'établir des limites pour la conservation des données, de prendre des mesures pour assurer l'exactitude de l'information et de considérer les tiers comme des sociétés affiliées à moins que la relation ne soit claire pour les individus[21].

D'après les auteurs du rapport, le cadre devrait s'appliquer aux organisations qui utilisent des renseignements permettant d'identifier un consommateur ou un appareil en particulier, mais non à celles i) qui s'assurent que les renseignements sont dépersonnalisés et qui sont raisonnablement convaincues qu'il sera impossible de les repersonnaliser, ii) qui s'engagent publiquement à tenir à jour et à utiliser des renseignements dépersonnalisés ou iii) qui interdisent par contrat la repersonnalisation par l'autre organisation dans les cas où des renseignements dépersonnalisés sont mis à la disposition d'autres organisations[22].

Compte tenu des pouvoirs d'application de la loi conférés à la FTC, ses recommandations constituent souvent des suggestions très convaincantes en ce qui concerne les pratiques des courtiers en données. D'ailleurs, après avoir publié son rapport, la FTC a pris certaines mesures d'application. En mai 2013, à la suite d'un ratissage en ligne mené sous l'égide du Global Privacy Enforcement Network (activité conjointe des autorités de protection des données de différents pays organisée par le Commissariat à la protection de la vie privée du Canada aux fins de l'application de la loi), la FTC a envoyé à dix entreprises de courtage de données des lettres les avisant que leurs pratiques pourraient contrevenir à la FCRA[23].

Le leadership exercé par la FTC a également continué de mettre ces enjeux en évidence. En particulier, la commissaire Julie Brill a été le fer de lance de l'initiative « Reclaim Your Name » visant à donner aux consommateurs une plus grande maîtrise des mégadonnées[24]. Edith Ramirez, présidente de la FTC, a aussi beaucoup parlé de ces enjeux, indiquant aux courtiers en données qu'ils doivent se conformer à la réglementation actuelle qui vise à protéger les données et à assurer leur sécurité, et leur rappelant les pouvoirs d'application de la loi dévolus à la Commission[25].

En mai 2014, la FTC a publié le rapport intitulé *Data Brokers: A Call for Transparency and Accountability*[26], qui fait suite à l'étude menée par la FTC concernant neuf courtiers en données. La FTC y révèle un manque de transparence dans l'industrie du courtage de données et demande au Congrès de promulguer une loi qui

améliorerait la transparence et le contrôle par les consommateurs. Entre autres, le rapport souligne ce qui suit :

- Les courtiers en données recueillent des données sur les consommateurs à partir de diverses sources en ligne et hors ligne, principalement à l'insu des consommateurs. Il peut s'agir de données sur leurs achats, leurs activités dans les médias sociaux, leurs enregistrements de garantie, leurs abonnements à des magazines, leurs affiliations religieuses ou politiques et d'autres détails sur leur quotidien.
- Les courtiers en données combinent et analysent les données concernant les consommateurs pour établir des inférences à leur sujet, y compris des inférences potentiellement délicates touchant l'ethnicité, le revenu, la religion, les allégeances politiques et l'âge. Parmi les autres catégories potentiellement délicates, notons ce qui touche à la santé, par exemple la grossesse, le diabète ou un haut taux de cholestérol.
- Bon nombre des raisons pour lesquelles les courtiers en données recueillent et utilisent des données représentent un risque pour les consommateurs, notamment une utilisation non prévue de l'information.
- Si l'on considère la mesure dans laquelle les courtiers en données offrent actuellement des choix aux consommateurs concernant leurs données, ces choix sont principalement invisibles et incomplets[27].

Si l'on considère la portée, l'ampleur et le volume des renseignements que détiennent les courtiers en données aux États-Unis, la fusion des activités hors ligne et en ligne ainsi que les solutions analytiques et technologiques complexes qui existent, les courtiers en données établissent de plus en plus des profils aboutis brossant un portrait plus contextuel et exact des consommateurs.

Le volume de renseignements en ligne et la puissance de l'analyse informatique démontrent clairement que l'information concernant les activités en ligne des individus va bien au-delà du profil sommaire. Le portrait d'un internaute devient moins opaque et plus révélateur lorsque l'on ajoute les activités hors ligne pour étoffer son profil. Il est même possible d'affiner les traits lorsque les renseignements viennent d'un large éventail d'industries et de secteurs avec lesquels l'individu interagit depuis des jours, des semaines, voire des années. Dans le meilleur des cas, la ligne de démarcation entre les renseignements permettant d'identifier un individu et les renseignements dépersonnalisés est floue.

C. Législation canadienne sur la protection des renseignements personnels

Il existe une différence nette entre les régimes de réglementation américain et canadien. Aux États-Unis, différentes lois sur la protection des renseignements personnels s'appliquent uniquement à certains types d'organisations ou d'activités, tandis qu'au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régit toutes les organisations qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre d'activités commerciales, sauf dans les provinces ayant adopté une loi essentiellement similaire. La LPRPDE s'applique à la circulation transnationale des renseignements et à tous les renseignements personnels détenus par les entreprises fédérales, y compris ceux concernant leurs employés.

L'objectif de la LPRPDE consiste à établir des règles régissant la collecte, l'utilisation et la communication des renseignements personnels d'une manière qui reconnaît le droit des individus à la vie privée et le besoin pour les organisations de recueillir, d'utiliser et de communiquer ce type de renseignements aux fins de leurs activités commerciales légitimes. Cette loi crée donc un équilibre entre les besoins des entreprises et le droit des individus à la vie privée.

La LPRPDE n'interdit pas les pratiques commerciales comme le marketing direct, mais elle veille à ce que les organisations donnent aux individus la possibilité d'exercer un contrôle sur la collecte, l'utilisation et la communication de leurs renseignements. De même, dans la mesure où les entreprises qui achètent des renseignements auprès de courtiers en données sont régies par la LPRPDE, elle les oblige aussi à respecter la législation. Compte tenu de la portée de son application, seule ou de concert avec des lois essentiellement similaires, la LPRPDE assure que les courtiers en données et les acheteurs tiers protégeront les renseignements sur leur cycle de vie.

De cette façon, la LPRPDE, les lois provinciales sur la protection des renseignements personnels essentiellement similaires et les lois sur la protection des renseignements personnels dans le secteur public ont créé un contexte de protection de la vie privée très différent de celui que l'on observe aux États-Unis.

Si certains renseignements réglementés accessibles au public peuvent être soustraits à l'obligation d'obtenir le consentement de l'intéressé pour les recueillir, les utiliser et les communiquer, d'autres exigences imposées par la LPRPDE continuent de s'appliquer. Par exemple, on peut lire dans les conclusions du Commissariat à la protection de la vie privée du Canada portant sur les pratiques d'une organisation : « […] si les renseignements personnels étaient certes accessibles au public, ils demeuraient des renseignements personnels. Afin que l'organisation se conforme au principe de transparence, la commissaire adjointe a proposé certaines modifications à apporter à ses politiques et pratiques »[28].

Au moment de la rédaction du présent rapport, le projet de loi S-4[29], *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence*, avait été déposé. Le projet de loi prévoit entre autres la modification de la LPRPDE pour y ajouter un nouvel article 7.2 afin de permettre à des organisations qui envisagent des « transactions commerciales » d'utiliser et de communiquer sans le consentement de l'intéressé, sous réserve de certaines conditions et mesures de protection. Le paragraphe 7.2(4) prévoit une autre limite concernant le recours à ces dispositions, soit qu'elles ne s'appliquent pas dans le cas d'une transaction commerciale « dont l'objectif premier ou le résultat principal est l'achat, la vente ou toute autre forme d'acquisition ou de disposition de renseignements personnels, ou leur location ». Il semble que cette mesure empêcherait, par exemple, un courtier en données souhaitant acheter une autre entreprise de courtage d'utiliser ces dispositions.

D. Les courtiers en données au Canada

La différence au chapitre du contexte de réglementation a été mentionnée comme l'une des raisons expliquant pourquoi certains courtiers en données aux États-Unis ne font pas affaire au Canada ou y ont modifié leurs pratiques opérationnelles. Selon un rapport de recherche financé par le Programme des contributions du Commissariat à la protection de la vie privée du Canada, un courtier en données américain a affirmé avoir cessé de faire le commerce des renseignements personnels des Canadiens après l'entrée en vigueur de la LPRPDE[30]. Les auteurs du rapport indiquent également qu'en raison des exigences de la législation canadienne sur la protection des renseignements personnels, les courtiers en données canadiens utilisent généralement moins d'ensembles de données que leurs homologues américains, assurant ainsi aux Canadiens une meilleure protection des renseignements personnels.

D'après les auteurs du rapport, les renseignements disponibles sur le marché américain du courtage de données ont une portée et une ampleur beaucoup plus vastes que ceux offerts sur le marché canadien, puisque davantage de données permettant de dresser des listes de consommateurs sont émises aux États-Unis, et qu'il y a davantage d'information accessible au public sur les Américains que sur les Canadiens.

Les différences observées dans la législation entre les deux pays en matière de protection de la vie privée reflètent les différences quant aux exigences de conformité imposées aux organisations, mais les courtiers en données peuvent exercer leurs activités au Canada et ils ne s'en privent pas. Sans évaluer la conformité à la loi des courtiers en données, le rapport de recherche financé par le Programme des contributions n'en illustre pas moins le large éventail de produits, de sources et de services de données offerts. L'information ci-après concernant certains courtiers en données canadiens est tirée du rapport et a été mise à jour à la lumière d'un examen des renseignements affichés sur le site Web des organisations.

Cornerstone Group of Companies (Cornerstone)

D'après l'information affichée sur son site Web[31], Cornerstone offre un éventail de services de données, par exemple la gestion des listes de consommateurs établies par les organisations, des solutions de marketing, des solutions d'amélioration des données, des services d'annuaire, des analyses géodémographiques et des analyses de données. On trouve dans le lot les fiches de données[32] qui permettent de dresser des listes de consommateurs en fonction de plusieurs sous-ensembles démographiques différents. Les chercheurs ont constaté que l'information provient de diverses sources, par exemple les annuaires téléphoniques, les données géodémographiques, les données en réponse directe et les listes numérisées provenant de listes de tiers gérées à l'interne[33].

En ce qui a trait aux fiches de données, la politique de confidentialité de Cornerstone indique expressément que sa liste est régie par la *Loi sur la protection des renseignements personnels et les documents électroniques* et qu'elle s'y conforme[34]. Elle précise en outre que l'entreprise se conforme à la LPRPDE et veille à ce que les renseignements figurant sur les listes soient recueillis, utilisés et communiqués en conformité avec cette loi[35].

InfoCanada

InfoCanada regroupe par couches les renseignements des annuaires avec l'information de Statistique Canada et propose des listes de consommateurs ainsi que des solutions d'analyse de données. Au moment de la rédaction de notre rapport, son site Web affirme que l'organisation possède de l'information provenant de plus de 12 millions de Canadiens et propose des catégories démographiques, par exemple la fourchette de revenu, le type d'habitation et sa valeur, l'état matrimonial, le sexe, l'origine ethnique et la religion[36]. À l'instar de celle de Cornerstone, la politique de confidentialité d'InfoCanada indique qu'elle se conforme à la LPRPDE et précise que l'information recueillie auprès de Statistique Canada ne constitue pas des renseignements personnels et que celle tirée des annuaires est entièrement accessible au public[37].

Agences d'évaluation du credit

Les deux principales agences d'évaluation du crédit en activité au Canada, soit Equifax et TransUnion, sont régies non seulement par la LPRPDE, mais aussi par les lois provinciales qui s'appliquent aux rapports de solvabilité des consommateurs. Les agences d'évaluation du crédit se livrent aussi à la vente de données agrégées pour des solutions commerciales (par exemple le marketing ainsi que la gestion du risque, de la fraude et de l'identité) et recueillent de l'information dans les documents publics et auprès des fournisseurs de crédit. En outre, elles sont de plus en plus appelées à confirmer l'identité d'individus. Experian exerçait autrefois des activités au Canada, mais on peut lire dans des rapports de 2009 qu'elle avait l'intention de fermer son agence canadienne d'évaluation du crédit en raison du climat financier mondial de l'époque[38].

Récemment, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a appris qu'Acxiom avait modifié ses activités sur le marché canadien. Acxiom a comparu devant le Comité en décembre 2012 dans le cadre de l'examen de la protection de la vie privée dans les médias sociaux. Le Comité a alors appris qu'au Canada, l'entreprise se limitait à fournir des annuaires téléphoniques d'entreprises et de particuliers[39]. Signalons qu'Acxiom ajoute des données du recensement aux listes figurant dans les annuaires téléphoniques[40]. En outre, Acxiom a indiqué n'avoir nullement l'intention d'accroître les services qu'elle offre au Canada[41] et de repérer les données canadiennes dans les listes qu'elle obtient[42].

E. Les courtiers en données au Canada – Quelles pourraient être les inquiétudes en matière de vie privée?

Si l'on considère les inquiétudes que peuvent susciter les organisations qui font le commerce de l'information, les enjeux comme les mégadonnées, les risques associés à la protection de grandes quantités de renseignements personnels et les répercussions d'une atteinte à la sécurité des renseignements personnels sont pertinents alors que le stockage et la compilation des données sont devenus plus faciles et moins coûteux. Dans le monde actuel de solutions technologiques d'analyse très poussées, la nécessité de prendre en compte ces solutions, de même que les mégadonnées et les profils étoffés et contextuels détenus par les courtiers en données, pour déterminer de façon responsable le risque de repersonnalisation, ajoute à la complexité de la tâche.

En outre, on utilise les mégadonnées pour la découverte de connaissances grâce à l'application de techniques d'extraction. Comme son nom l'indique, la découverte de connaissances consiste à acquérir des connaissances nouvelles. Or, lorsque cette découverte fait appel à des renseignements concernant un individu et que ces renseignements sont utilisés à une fin non indiquée auparavant et sans le consentement de l'intéressé, il y a un problème de protection de la vie privée. La découverte de connaissances peut poser de graves problèmes en raison du fait que l'intéressé même peut ne pas connaître l'existence de ces renseignements et encore moins savoir que d'autres les analysent et les utilisent. Illustrons cette réalité au moyen d'un exemple simple : « Alice achète toujours une automobile une année paire lorsque la Lune se trouve le plus près de la Terre. » Dans ce cas, il est fort possible qu'Alice ne se soit pas rendu compte qu'elle avait cette habitude ou qu'elle ignore que cette information est utilisée pour établir son profil ou la cibler.

À première vue, l'utilisation de renseignements en apparence dépersonnalisés ou consolidés pourrait ne pas sembler relever de la portée de la LPRPDE, car les renseignements anonymes, par définition, ne sont pas considérés comme des renseignements personnels au sens de la Loi[43]. Toutefois, le Commissariat adopte généralement une approche contextuelle pour évaluer si des renseignements sont personnels ou non[44]. Les tribunaux ont également jugé que les renseignements concernent « un individu identifiable » lorsqu'il y a une forte possibilité qu'ils permettent de l'identifier, qu'ils soient utilisés seuls ou combinés avec d'autres renseignements[45]. Cela dit, il demeure possible que les listes de consommateurs soient dépersonnalisées et disponibles à la vente. Cette pratique n'en doit pas moins être indiquée clairement dans la politique de confidentialité des organisations, mais le risque de repersonnalisation de renseignements dépersonnalisés constitue une source d'inquiétude constante.

El Emam et Kosseim mentionnent dans un rapport[46] que le risque de repersonnalisation (dans le contexte des renseignements sur le commerce de détail et les pharmacies d'hôpital transmis aux courtiers en données) est bien réel et qu'il dépend de plusieurs variables, dont la quantité de renseignements communiqués et le degré de « motivation » de l'intrus. On ne peut donc présumer que les renseignements dépersonnalisés demeureront anonymes.

En outre, l'utilisation de l'infonuagique suscite des inquiétudes quant à la capacité des courtiers en données de faire preuve de responsabilité, de protéger l'information et de gérer les risques associés à la circulation transfrontière des données ainsi qu'à l'accès régi par un organisme étranger. En outre, il peut être difficile de gérer plusieurs copies de documents, en particulier quand il s'agit d'assurer l'exactitude des renseignements, de répondre aux demandes d'accès et de donner suite aux plaintes.

Enfin, l'interconnexion au sein de l'économie numérique a élargi la portée des organisations à l'étranger. La conformité à la LPRPDE est requise dans les cas où il y a un lien réel et appréciable avec le Canada, mais la mesure dans laquelle les organisations établies à l'étranger connaissent ces obligations, s'y conforment – ou y contreviennent délibérément – demeure en grande partie inconnue.

Sans être propres à l'industrie du courtage de données, les risques susmentionnés sont plus complexes et ont une plus grande incidence sur la protection de la vie privée des Canadiens que dans d'autres secteurs en raison de la portée, de l'ampleur et de la nature des champs d'activité des courtiers en données.

F. Conclusion

L'environnement en ligne et numérique a profondément changé la façon dont les individus et les entreprises communiquent. En plus de remettre en question la manière dont la communication se déroule, les plateformes en ligne et numériques ont permis à certains courtiers en données de combiner les sphères hors ligne et en ligne pour établir un profil abouti et contextuel des individus.

Le cadre exhaustif de conformité aux exigences de protection de la vie privée et à la réglementation dans lequel l'industrie du courtage de données au Canada exerce ses activités est différent du contexte observé aux États-Unis. Néanmoins, les difficultés associées aux tendances et aux enjeux qui se dessinent dans le domaine de la protection de la vie privée demeurent une notion importante dans la recherche d'un équilibre entre les besoins commerciaux légitimes et le droit des Canadiens à la vie privée.

De surcroît, dans une économie numérique intégrée, on franchit aisément les frontières et il n'a jamais été aussi facile d'avoir accès aux renseignements personnels. Il reste à déterminer si les courtiers en données établis à l'étranger connaissent la LPRPDE et s'y conforment lorsqu'ils exercent des activités au Canada. C'est pourquoi il faut constamment faire connaître les exigences et les expectatives de la LPRPDE aux courtiers en données canadiens et américains qui veulent faire affaire au Canada.

Notes

[1] Clinique d'intérêt public et de politique d'Internet du Canada. *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*, 2006, p. 2. http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Résumé en français : https://www.cippic.ca/sites/default/files/May1-06/ExecSum_DB_FR.pdf. Cité par Daniel J. Solove dans la note 3 de *The Digital Person: Technology and Privacy in the Information Age*, New York University Press.

[2] David Leduc. *Data Broker Briefing Reveals Complex Data Ecosystem,* The Software & Information Industry Association, 18 décembre 2012. http://www.siia.net/blog/index.php/2012/12/data-broker-briefing-reveals-complex-data-ecosystem/

[3] David Leduc. *Data Broker Briefing Reveals Complex Data Ecosystem*, The Software & Information Industry Association, 18 décembre 2012. http://www.siia.net/blog/index.php/2012/12/data-broker-briefing-reveals-complex-data-ecosystem/

[4] Federal Trade Commission. « FTC to Study Data Broker Industry's Collection and Use of Consumer Data », communiqué, 18 décembre 2012. http://www.ftc.gov/opa/2012/12/databrokers.shtm

[5] Par exemple, Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, mars 2012. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Sénat des États-Unis, Comité du commerce, de la science et des transports. Lettre à Acxiom, 9 mai 2012. http://commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c. Lettre d'Edward Markey (représentant démocrate du Massachusetts) et Joe Barton (représentant républicain du Texas) à neuf courtiers en données, 24 juillet 2012. En ligne : http://markey.house.gov/content/letters-major-data-brokers. Ce lien n'est plus disponible, mais la page peut être consultée au : http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers. Avis de la Federal Trade Commission qui annonçait une étude portant sur les courtiers en données et ordonnances envoyées aux courtiers en données, décembre 2012. http://www.ftc.gov/opa/2012/12/databrokers.shtm

[6] Maeve Z. Miller. « Why Europe Is Safe From ChoicePoint: Preventing Commercialized Identity Theft Through Strong Data Protection And Privacy Laws », *The George Washington International Review*, vol. 39, 2007, p. 402-403.

[7] 15 *United States Code,* § 45(a)(1); voir aussi Daniel J. Solove et Paul Schwartz. « Privacy Law Fundamentals 2013 », 2013, p. 137-138 (ventilation des interventions de la FTC). Chaque État a aussi sa « petite loi de la FTC » dont l'application est assurée par le procureur général.

[8] Federal Trade Commission. *Making Sure Companies Keep Their Privacy Promises to Consumers*, ressources pour les journalistes. http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml

[9] 15 *United States Code*, § 45(n); *FTC v. NHS Sys., Inc.,* n° 08-2215, 2013 WL 1285424, par. *5 (E.D. Pa. 28 mars 2013). [traduction] « Le critère du préjudice pour le consommateur constitue la définition la plus précise de l'injustice énoncée par la Commission ou le Congrès. » *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) (rejetant l'argument selon lequel la FTC n'est pas habilitée à interdire les « types » de pratiques ou à empêcher les « types » de préjudice pour les consommateurs qui posent problème dans cette affaire.)

[10] *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653 (2011).

[11] Nathan Brooks. *Data Brokers: Background, Industry and Overview,* Service de recherche du Congrès, Bibliothèque du Congrès, code de commande RS 221377, mai 2005, p. 1. http://assets.opencrs.com/rpts/RS22137_20050505.pdf

[12] Government Accountability Office. *AO-06-674, A Report to the Committee on Banking, Housing and Urban Affairs, U.S. Senate: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data,* juin 2006. http://www.gao.gov/assets/260/250627.html

[13] Lettre d'Edward Markey (représentant démocrate du Massachusetts) et Joe Barton (représentant républicain du Texas) à neuf courtiers en données, 24 juillet 2012. En ligne : http://markey.house.gov/content/letters-major-data-brokers. Ce lien n'est plus disponible, mais la page peut être consultée au : http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers

[14] Lettre d'Edward Markey (représentant démocrate du Massachusetts) et Joe Barton (représentant républicain du Texas) à neuf courtiers en données, 24 juillet 2012. En ligne : http://markey.house.gov/content/letters-major-data-brokers. Ce lien n'est plus disponible, mais la page peut être consultée au : http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers

[15] Site Web d'Edward Markey (représentant démocrate du Massachusetts), page de nouvelles, 12 décembre 2012. En ligne : http://markey.house.gov/press-release/markey-barton-ftc-study-data-brokers. Ce lien n'est plus disponible, mais la page peut être consultée au : http://web.archive.org/web/20130220162934/http://markey.house.gov/press-release/markey-barton-ftc-study-data-brokers

[16] Alston and Bird LLP. « Congressional Bi-Partisan Privacy Caucus Holds Roundtable Briefing on Data Broker Practices », *Alston Privacy + Security Blog*, 14 décembre 2012. http://www.alstonprivacy.com/?entry=4765

[17] Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, mars 2012. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[18] Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, mars 2012, p. iv. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[19] L'information figurant dans ce paragraphe est tirée de *Protecting Consumer Privacy in an Era of Rapid Change* de la Federal Trade Commission, mars 2012, p. viii. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[20] L'information figurant dans ce paragraphe est tirée de *Protecting Consumer Privacy in an Era of Rapid Change* de la Federal Trade Commission, mars 2012, p. viii. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[21] L'information figurant dans ce paragraphe est tirée de *Protecting Consumer Privacy in an Era of Rapid Change* de la Federal Trade Commission, mars 2012, p. 26-41. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[22] Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, mars 2012, p. iv. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[23] Federal Trade Commission. « FTC Warns Data Broker Operations of Possible Privacy Violations: Letters Issued as Part of Global Privacy Protection Effort », 7 mai 2013. http://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations

[24] Julie Brill, commissaire de la Federal Trade Commission. « Reclaim Your Name », allocution prononcée lors de la 23rd Computers Freedom and Privacy Conference, 26 juin 2013. http://www.ftc.gov/public-statements/2013/06/reclaim-your-name.

[25] Edith Ramirez, présidente de la Federal Trade Commission. *The Privacy Challenges of Big Data: A View from the Lifeguard's Chair*, 19 août 2013. http://www.ftc.gov/public-statements/2013/08/privacy-challenges-big-data-view-lifeguard's-chair.

[26] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, 27 mai 2014. http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[27] *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information*, 27 mai 2014. http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

[28] Commissariat à la protection de la vie privée du Canada. *Résumé de conclusions d'enquête en vertu de la LPRPDE n^o^ 2009-004* : *Aucun consentement n'est requis pour l'utilisation de renseignements personnels accessibles au public combinés à des statistiques démographiques propres à un lieu géographique*. http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_f.asp

[29] Voir la Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques

[30] Clinique d'intérêt public et de politique d'Internet du Canada. *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*, 2006, p. 45. http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Résumé en français : https://www.cippic.ca/sites/default/files/May1-06/ExecSum_DB_FR.pdf

[31] L'information est tirée du site Web du Cornerstone Group of Companies. http://www.cstonecanada.com/

[32] Les fiches de données comprennent le nom figurant sur la liste, certaines données, la fréquence des mises à jour, l'utilisation recommandée et d'autres renseignements utiles pour les prospects. Signalé dans *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* de la Clinique d'intérêt public et de politique d'Internet du Canada, 2006, p. 12. http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Résumé en français : https://www.cippic.ca/sites/default/files/May1-06/ExecSum_DB_FR.pdf

[33] Clinique d'intérêt public et de politique d'Internet du Canada. *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*, 2006, p. 19. http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Résumé en français : https://www.cippic.ca/sites/default/files/May1-06/ExecSum_DB_FR.pdf

[34] Une recherche a été menée à titre d'exemple sur les fiches de données du site Web du Cornerstone Group of Companies pour le sujet CANADIAN FAMILY (famille canadienne) en vue de trouver des fiches de données. Cette recherche a mené à http://www.cstonecanada.com/datacards/datacard.aspx?uid=65a701dd-9efa-4d32-a68c-38cb163c0036

[35] Cornerstone Group of Companies. Politique de confidentialité affichée dans le site Web. http://www.cstonecanada.com/privacy/index.asp

[36] Cette information est tirée du site Web d'InfoCanada. http://www.infocanada.ca/main_page_fr.aspx

[37] Cette information est tirée du site Web d'InfoCanada. Politiques de confidentialité. http://www.infocanada.ca/privacy.aspx?bas_session=S688251728274 31&bas_vendor=99911

[38] Tom Drake. « Experian Closes Their Canadian Consumer Credit Bureau », *Canadianfinanceblog*. http://canadianfinanceblog.com/experian-closes-their-canadian-consumer-credit-bureau/

[39] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 41e législature, 1re session. Témoignages, jeudi 6 décembre 2012, Étude de la protection de la vie privée dans les médias sociaux, témoignage de Mme Jennifer Barrett Glasgow, responsable de la protection des renseignements personnels et des politiques publiques, Acxiom, par. 1635. http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=5927254#Int-7842856

[40] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 41e législature, 1re session. Témoignages, jeudi 6 décembre 2012, Étude de la protection de la vie privée dans les médias sociaux, témoignage de

M^me^ Jennifer Barrett Glasgow, responsable de la protection des renseignements personnels et des politiques publiques, Acxiom, par. 1635. http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=5927254#Int-7842856

[41] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 41^e^ législature, 1^re^ session. Témoignages, jeudi 6 décembre 2012, Étude de la protection de la vie privée dans les médias sociaux, témoignage de M^me^ Jennifer Barrett Glasgow, responsable de la protection des renseignements personnels et des politiques publiques, Acxiom, par. 1640. http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=5927254#Int-7842856

[42] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 41^e^ législature, 1^re^ session.Témoignages, jeudi 6 décembre 2012, Étude de la protection de la vie privée dans les médias sociaux, témoignage de M^me^ Jennifer Barrett Glasgow, responsable de la protection des renseignements personnels et des politiques publiques, Acxiom, par. 1655. http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=F&Mode=1&DocId=5927254#Int-7842856

[43] Teresa Scassa, *"Privacy and Open Government"*, (2014) 6. *Future Internet*, 397-413. En ligne : http://www.mdpi.com/1999-5903/6/2/397, et Teresa Scassa, *"Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy"*, (2009) 7:2. Canadian Journal of Law and Technology 193-222. En ligne : http://www.teresascassa.ca/Files/publications/scassa_1.pdf

[44] Commissariat à la protection de la vie privée du Canada. *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique,* 2012. http://www.priv.gc.ca/resource/consultations/report_201105_f.asp

[45] *Gordon c. Canada (Santé),* 2008 CF 258 (CanLII). http://www.canlii.org/fr/ca/cfpi/doc/2008/2008cf258/2008cf258.html

[46] Khaled El Emam et Patricia Kosseim. « Privacy Interests in Prescription Data, Part 2: Patient Privacy », *IEEE Security & Privacy*, vol. 7, n^o^ 2, 2009, p. 75-78. http://www.computer.org/csdl/mags/sp/2009/02/msp2009020075-abs.html