IEDM Des idées pour une société plus prospère

LES NOTES ÉCONOMIQUES

NOVEMBRE 2016

QUI MENACE LE PLUS LA VIE PRIVÉE, LES ENTREPRISES OU LES GOUVERNEMENTS?

Par Mathieu Bédard

Dans le débat sur la collecte, le partage et l'utilisation des renseignements personnels, il existe un préjugé largement répandu selon lequel les entreprises seraient moins respectueuses de la vie privée des citoyens que les gouvernements. Pourtant, les entreprises fonctionnent universellement sur le principe du consentement alors que l'État ne demande que très peu souvent l'accord des personnes concernées pour avoir accès à des informations. Au moment où le Commissariat à la protection de la vie privée appelle à moderniser les lois encadrant les pratiques du gouvernement fédéral et des entreprises[1], il est important de souligner les différences fondamentales entre les deux ainsi que la source des véritables menaces.

LA COLLECTE DE RENSEIGNEMENTS PUBLICS

Il est difficile de cerner le périmètre de la vie privée, puisqu'il varie énormément d'une personne à l'autre. Par exemple, plusieurs personnes n'acceptent de partager leur information médicale qu'avec leur médecin et leur famille rapprochée, tandis que d'autres vont à la télévision pour parler de leur maladie et ainsi aider les gens dans la même situation qu'eux. Le respect de la vie privée doit donc être envisagé non pas comme un niveau absolu et uniforme de secret, mais bien comme un niveau de contrôle par l'individu des informations qui le concernent[2].

Les politiques publiques appropriées sont celles qui contribuent à maintenir ce contrôle en forçant les entreprises et les gouvernements à être transparents et à respecter leurs engagements à propos de l'utilisation des renseignements personnels. Toutes les méthodes de collecte de renseignements personnels n'ont cependant pas les mêmes conséquences sur la vie privée.

Lorsque l'information est déjà publique, bien souvent le principe du consentement ne s'applique pas. Par exemple, des entreprises collectent des renseignements à notre sujet sans notre approbation préalable à partir d'archives et d'autres sources publiques comme les moteurs de recherche.

Cette pratique peut avoir de nombreuses utilisations avantageuses et légitimes. Ces renseignements permettent par exemple à la presse d'enquêter et de dénoncer certains actes répréhensibles. C'est au hasard d'une recherche Internet qu'une Française a découvert que son conjoint était atteint du sida et qu'il avait été condamné pour avoir sciemment infecté plusieurs femmes[3].

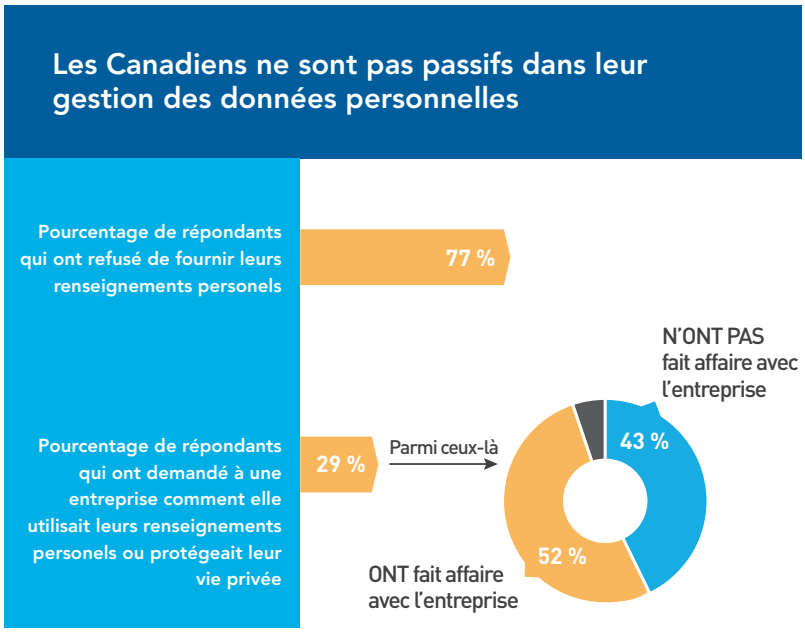
Cette *Note économique* a été préparée par **Mathieu Bédard**, économiste à l'IEDM. Il est titulaire d'un doctorat en sciences économiques d'Aix-Marseille Université et d'une maîtrise en analyse économique des institutions de l'Université Paul Cézanne.

Empêcher cette collecte d'information, par exemple par la création d'un « droit à l'oubli » comme il existe en Europe, aiderait des personnes malintentionnées à se dérober à leurs responsabilités et aux criminels à récidiver.

De même, les agences d'évaluation de crédit utilisent les archives publiques et les moteurs de recherche pour compléter les données que leurs clients consentent déjà à leur divulguer par l'entremise de leurs institutions financières. Cela leur permet de préserver les bonnes cotes de crédit de nombreuses personnes, tout en protégeant les prêteurs et les propriétaires de logements.

Tant que les organisations qui s'adonnent à ces pratiques sont transparentes et donnent aux personnes visées un accès aux renseignements qui sont colligés et la possibilité de corriger des erreurs, cela est compatible avec le respect de la vie privée[4]. Le gouvernement, contrairement aux entreprises, ne respecte pas souvent ces conditions.

Figure 1



Source : Phoenix SPI, *Sondage auprès des Canadiens sur la protection de la vie privée de 2014*, Document préparé pour le Commissariat à la protection de la vie privée du Canada, décembre 2014, p. 34.

UN VASTE SYSTÈME DE VIOLATION DE LA VIE PRIVÉE

Selon le Commissariat à la protection de la vie privée, « l'appétit des institutions fédérales pour les renseignements personnels de la population a crû en corrélation directe avec la facilité avec laquelle il était possible de les recueillir »[5].

Le respect de la vie privée doit être envisagé non pas comme un niveau absolu et uniforme de secret, mais bien comme un niveau de contrôle par l'individu des informations qui le concernent.

Et en effet, en même temps que les nouvelles technologies prenaient leur essor, il se mettait en place à l'insu du public un système de violation de la vie privée d'une ampleur que personne ne pouvait suspecter, révélé en juin 2013 par le lanceur d'alerte Edward Snowden. Appels téléphoniques, courriels, vidéos conférences, réseaux sociaux… la quasi-totalité des communications en ligne sont maintenant interceptées par les gouvernements[6].

Bien que les révélations d'Edward Snowden concernent surtout le gouvernement américain, les Canadiens sont aussi visés par ce système. D'une part, Internet et les télécommunications ne connaissent pas de frontières et les Canadiens utilisent aussi ces moyens de communications. D'autre part, la plupart des gouvernements du monde, dont le Canada, ont des programmes de surveillance semblables ou collaborent au programme américain[7]. Même au niveau provincial, la Sûreté du Québec a récemment annoncé la création d'un tel programme[8].

Des journalistes ont ainsi découvert que la Gendarmerie royale du Canada avait accès aux communications privée et cryptées de la plupart des téléphones intelligents BlackBerry et avait décrypté approximativement un million de messages privés[9].

On ignore l'ampleur de ces programmes de surveillance. On sait cependant que le nombre d'appels et de communications interceptés a été multiplié par 26 en 2015, sans que les autorités n'en dévoilent les raisons[10]. Plusieurs experts suspectent fortement que le gouvernement canadien utilise des instruments qui captent les appels et communications de tous les appareils cellulaires d'une zone et pas seulement des personnes sous surveillance[11]. Ces suspicions se heurtent au manque de transparence du gouvernement.

De plus, les gouvernements forcent les entreprises à espionner pour eux. Plusieurs d'entre elles ont subi des pressions de la part des autorités, au Canada et aux États-Unis, pour partager des données et des renseignements privés. La responsabilité de cette violation de la vie privée repose entièrement sur le gouvernement puisqu'il ne leur laisse pas le choix[12].

Ces programmes représentent une menace pour la vie privée des individus, mais ce n'est pas le seul type de menace. Comme l'attestent les révélations récentes concernant la surveillance policière dont ont fait l'objet des journalistes au Québec, la menace s'étend aussi aux médias[13]. L'espionnage industriel, pratiqué par les gouvernements mais aussi par des pirates informatiques ayant

mis la main sur les outils d'espionnage des gouvernements, constitue par ailleurs un risque réel auquel sont confrontées les entreprises[14].

LES DIFFÉRENCES FONDAMENTALES ENTRE LES GOUVERNEMENTS ET LES ENTREPRISES

Les entreprises et les agences du gouvernement ont des approches totalement différentes du respect de la vie privée. Les entreprises doivent, dans le système américain comme dans les systèmes canadien et européen, informer les utilisateurs de la façon dont leurs renseignements seront utilisés et demander leur consentement explicite[15]. À l'inverse, les gouvernements ont recours à des méthodes de collecte et une utilisation des données privées qui ignorent le principe du consentement et sont souvent secrètes.

Une autre différence importante est que les interactions des individus avec les entreprises peuvent être évitées relativement facilement. Il est toujours possible de ne pas utiliser de téléphone intelligent, de ne pas s'inscrire sur les réseaux sociaux, ou encore d'utiliser de l'argent comptant plutôt qu'une carte de crédit pour éviter de partager des données, bien qu'on renonce alors à de nombreux bienfaits et avantages associés à la modernité.

Les sondages démontrent que les Canadiens ne sont pas passifs dans la gestion de leurs données personnelles. Ils s'informent à propos de l'utilisation des données faites par les entreprises et, lorsque les réponses ne leur conviennent pas, refusent de faire affaire avec elles (voir Figure 1).

Plusieurs entreprises ont subi des pressions de la part des autorités, au Canada et aux États-Unis, pour partager des données et des renseignements privés.

Les gouvernements ne donnent pas aux citoyens le même niveau de contrôle sur leurs renseignements personnels que ce que leurs offrent les entreprises. D'abord parce que, dans beaucoup de cas, le partage d'information est obligatoire, souvent pour des raisons évidentes. C'est le cas pour les rapports d'impôts, les cadastres, les permis de conduire, les dossiers criminels, les historiques des différents programmes sociaux, etc. Mais aussi parce qu'ils n'ont pas les mêmes garde-fous contre l'abus que les entreprises.

Le premier garde-fou vient du fait que les entreprises sont en concurrence et que par conséquent, elles doivent donner aux utilisateurs ce qu'ils désirent. Les changements entraînés par la pression des consommateurs sont fréquents. On peut penser à l'annulation de Facebook Beacon et Google Buzz, ou encore aux modifications apportées à la façon dont la géolocalisation est stockée sur les appareils Apple[16].

De plus, les deux grandes familles de téléphones intelligents utilisent des paramètres de respect de la vie privée qui sont de plus en plus fins et adaptables aux limites personnelles de chacun avec chaque nouvelle version de leur système d'exploitation. Les résultats d'un sondage commandé par le Commissariat à la protection de la vie privée démontrent que les Canadiens sont conscients de l'existence de ces paramètres et les utilisent (voir Tableau 1).

Un autre garde-fou existe dans le cas du secteur privé : le fait que les renseignements personnels collectés par les grandes entreprises du Web soient trop précieux pour être vendus[17]. En effet, la publicité ciblée rendue possible par cette information représente une valeur pouvant aller jusqu'à 1200 $US par utilisateur, contre aussi peu qu'un demi cent par utilisateur si les renseignements étaient vendus. Conserver un accès exclusif à cette information pour cibler la publicité est donc beaucoup plus rémunérateur que la vendre.

Dans le cas des gouvernements, il existe peu de garde-fous. Même les révélations d'Edward Snowden et l'indignation de la communauté internationale n'ont pas provoqué de modification substantielle dans la politique de collecte de données des États-Unis. Tout récemment encore, il a été révélé que le gouvernement américain

Tableau 1

Les Canadiens connaissent et utilisent les paramètres de respect de la vie privée de leurs téléphones intelligents

	2011	2012	2014
Part des répondants qui déclarent avoir ajusté les paramètres de leur téléphone mobile pour limiter le partage d'information	40 %	53 %	72 %
Part des répondants qui déclarent avoir décidé de ne pas installer une application en raison de préoccupations au sujet des renseignements personnels demandés	nd	55 %	75 %
Part des répondants qui déclarent avoir désactivé la fonctionnalité de suivi de l'emplacement sur un appareil mobile en raison de préoccupations au sujet de l'accès par d'autres personnes à cette information	nd	38 %	58 %

Source : Phoenix SPI, *Sondage auprès des Canadiens sur la protection de la vie privée de 2014*, Document préparé pour le Commissariat à la protection de la vie privée du Canada, décembre 2014, p. 30-31.

demandait à Yahoo d'intercepter tous les courriels entrants, une politique que le président Obama et un comité de supervision de la NSA avaient pourtant juré que le gouvernement n'utilisait pas[18].

MODERNISER LES LOIS

La prévention du terrorisme et de la criminalité sont évidemment des objectifs légitimes. Le gouvernement s'est armé de lois musclées pour lutter contre le terrorisme et par conséquent épie les communications privées en collaboration avec des puissances étrangères pour déjouer les attentats. Il faut toutefois reconnaître qu'il s'agit de circonstances exceptionnelles. Ces pouvoirs doivent être bien encadrés, se limiter à ces objectifs et ne pas être banalisés.

Ottawa impose des règles beaucoup plus strictes au secteur privé qu'il ne s'impose à lui-même quant à la collecte, l'utilisation, la communication et la conservation des renseignements personnels.

Ce n'est malheureusement pas le cas. Il est alarmant de constater que les limites que le gouvernement canadien impose à ses agences de surveillance sont floues, en particuliers lorsqu'il s'agit de partager des banques de données entre agences du gouvernement et avec les États étrangers[19]. Un jugement de la Cour fédérale nous apprenait récemment que le Service canadien du renseignement de sécurité avait agi dans l'illégalité en conservant des données personnelles pendant 10 ans[20]. Ottawa impose des règles beaucoup plus strictes au secteur privé qu'il ne s'impose à lui-même quant à la collecte, l'utilisation, la communication et la conservation des renseignements personnels, tel que l'a reconnu le Commissaire à la protection de la vie privée et d'autres observateurs[21].

Si le gouvernement devait moderniser les lois sur la protection de la vie privée, il faudrait avant tout s'attaquer aux deux principales menaces à la vie privée au Canada : les pratiques de l'État qui limitent le contrôle des individus sur leur propre partage d'information et l'opacité de la collecte et du partage de données des agences gouvernementales. Le « Big Brother » qui menace la vie privée au Canada n'est pas une entreprise, mais bien le gouvernement.

RÉFÉRENCES

1. Commissariat à la protection de la vie privée du Canada, *Rapport Annuel au Parlement 2015-2016 : le temps est venu de moderniser les outils du 20e siècle*, Rapport annuel au Parlement 2015-2016 concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*, 27 septembre 2016.
2. Jim Harper, *Understanding Privacy—and the Real Threats to It*, Policy Analysis, Cato Institute, 4 août 2004.
3. Marine Messina, « Douze ans de prison pour avoir transmis le virus du sida à sa compagne », *Le Monde*, 2 octobre 2014.
4. Les courtiers en données, qui 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, passent parfois outre le consentement et la transparence nécessaire au respect de la vie privée. La nature et l'ampleur du phénomène sont toutefois toujours floues. Pour plus de détails, voir 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.
5. Commissariat à la protection de la vie privée du Canada, *op. cit.*, note 1, p. 14.
6. Glenn Greenwald, « NSA collecting phone records of millions of Verizon customers daily », *The Guardian*, 6 juin 2013; Glenn Greenwald, « XKeyscore: NSA tool collects "nearly everything a user does on the internet" », *The Guardian*, 31 juillet 2013.
7. Colin Freeze, « Data-collection program got green light from MacKay in 2011 », *The Globe and Mail*, 10 juin 2013; Greg Weston, Glenn Greenwald et Ryan Gallagher, « Snowden Document Shows Canada Set up Spy Posts for NSA », *CBC News*, 9 décembre, 2013.
8. Vincent Larouche, « La SQ met sur pied un grand centre de "cybersurveillance" », *La Presse*, 1er novembre 2016.
9. Justin Ling et Jordan Pearson, « Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key », *Vice News*, 14 avril 2016.
10. Ian MacLeod, « Federal spies suddenly intercepting 26 times more Canadian phone calls and communications », *National Post*, 24 août 2016.
11. Matthew Braga, « Why Canada isn't having a policy debate over encryption », *The Globe and Mail*, 23 février 2016; Matthew Braga, « The covert cellphone tracking tech the RCMP and CSIS won't talk about », *The Globe and Mail*, 15 septembre 2014.
12. Aux États-Unis, le processus pour obliger une entreprise à coopérer inclut l'envoi d'une lettre de sécurité nationale. Il s'agit d'une lettre dont le destinataire ne peut parler à personne et qui est très difficile à contester en cour, comme l'atteste l'histoire du fondateur du service de messagerie sécurisée Lavabit, Ladar Levison, dont les tribunaux se sont assurés par des procédures judiciaires controversées que sa cause ne serait jamais entendue par la justice. Pour donner une idée de l'importance du nombre de ces lettres, Google en reçoit chaque semestre entre une et 999. Le Canada est encore moins transparent puisqu'on ignore même les directives qui encadrent ce genre de surveillance. Ladar Levison, « Secrets, lies and Snowden's email: why I was forced to shut down Lavabit », *The Guardian*, 20 mai 2014; Google, Transparence des informations, États-Unis.
13. Philippe Teisceira-Lessard, « Patrick Lagacé visé par 24 mandats de surveillance policière », *La Presse*, 31 octobre 2016; Vincent Larouche et Philippe Teisceira-Lessard, « Six journalistes épiés par la Sûreté du Québec », *La Presse*, 2 novembre 2016.
14. Ce scénario s'est produit en août dernier, lorsque des logiciels de piratage de la National Security Agency ont été volés et ont fait l'objet d'une fuite. Des pirates ont alors presque immédiatement exploité cette fuite pour s'infiltrer dans les systèmes informatiques d'entreprises. Ce risque existe aussi au Canada, mettant à risque la vie privée et les secrets industriels. Lily Hay Newman, « Of course everyone's already using the leaked NSA exploits », *Wired*, 24 août 2016.
15. The Law Library of Congress, *Online Privacy Law: the European Union*, Global Legal Research Center, juin 2012 (mise à jour en mai 2014); Gouvernement du Canada, *Loi sur la protection des renseignements personnels et les documents électroniques*, juin 2015; Practical Law, Data protection in United States: Overview.
16. Louise Story et Brad Stone, « Facebook Retreats on Online Tracking », *The New York Times*, 30 novembre 2007; Joseph Tartakoff, « Google fixes privacy issues in Buzz », *The Guardian*, 15 février 2010; Marguerite Reardon, « Apple: We'll fix iPhone tracking 'bug' », *Cnet*, 27 avril 2011.
17. Alexis C. Madrigal, « How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200 », *The Atlantic*, 19 mars 2012.
18. Joseph Menn, « Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources », Reuters, 4 octobre 2016; Kate Connolly, « Barack Obama: NSA is not rifling through ordinary people's emails », *The Guardian*, 19 juin 2013; Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Gouvernement des États-Unis, 2 juillet 2014, p. 1 et 8.
19. Justin Ling, « Secret Documents Reveal Canada's Spy Agencies Got Extremely Cozy With Each Other », *Vice News*, 20 mai 2015.
20. Colin Freeze, « In scathing ruling, Federal Court says CSIS bulk data collection illegal », *The Globe and Mail*, 3 novembre 2016.
21. Daniel Therrien, « Assurer la protection de la vie privée au 21e siècle », *Options Politiques*, 5 octobre 2016; Jennifer Stoddart, Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique à propos de la Réforme de la *Loi sur la protection des renseignements personnels*; David H. Flaherty, *Reflections on Reform of the Federal Privacy Act*, juin 2008; Colin Freeze, « Watchdog warned of CSIS data access », *The Globe and Mail*, 19 juin 2013.

Institut économique de Montréal 910, rue Peel, bureau 600, Montréal QC H3C 2H8 - T 514.273.0969 F 514.273.2581 **iedm.org**