OSLER

La protection des renseignements personnels, une préoccupation importante en 2017

13 DÉCEMBRE 2017 8 MIN DE LECTURE

Expertises Connexes

- Respect de la vie privée et gestion de l'information

Auteurs(trice): Joanna Fine, Adam Kardash, Christopher Naudie, John Salloum

Des menaces sophistiquées à la cybersécurité, des incidents très médiatisés relatifs aux données et une explosion du nombre de programmes d'analyse de données ont fait en sorte que les problèmes liés à la protection des renseignements personnels sont devenus prioritaires pour les organisations de tous les secteurs. De plus, l'année 2017 s'est révélée riche en nouveautés législatives et réglementaires importantes sur le plan de la protection des renseignements personnels et des données au Canada, surtout en ce qui concerne les régimes législatifs portant sur les avis d'atteinte aux mesures de sécurité, la *Loi canadienne anti-pourriel* (la LCAP) et la gouvernance relative aux données.

Security breach notification

La *Loi sur la protection des renseignements personnels et les documents électroniques* (la LPRPDE), loi fédérale régissant la protection des renseignements personnels dans le secteur privé au Canada, prévoit un nouveau mécanisme de déclaration et de notification d'incidents liés à la sécurité, qui entrera en vigueur une fois que le règlement aura été achevé.

Le nouveau mécanisme comprend une exigence unique d'avis en trois volets. Lorsqu'une organisation subit une atteinte aux mesures de sécurité qui donne lieu à un « risque réel de préjudice grave » dans les circonstances, l'organisation doit i) déclarer l'incident au Commissariat à la protection de la vie privée du Canada (le CPVP); ii) aviser les personnes touchées et iii) aviser les tiers qui seraient en mesure d'atténuer le risque de préjudice pour les personnes touchées.

Fondamentalement, le nouveau mécanisme d'avis d'atteinte aux mesures de sécurité de la LPRPDE impose également l'exigence de tenue de registres aux termes de laquelle les organisations doivent tenir un registre de tous leurs problèmes liés à la sécurité des données. En vertu de la loi, les organisations sont tenues de donner accès à ce registre au CPVP s'il en fait la demande.

Un projet de règlement sur l'atteinte aux mesures de sécurité a été rendu public en septembre dernier. Il devrait être achevé en 2018 et entrer en vigueur par la suite, après une courte période de transition.

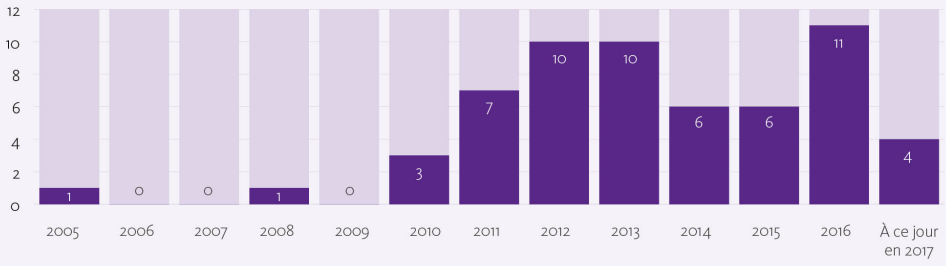
Nous nous attendons à ce que ce mécanisme d'avis ait une incidence importante sur l'environnement des données au Canada. Selon l'expérience que nous avons acquise dans la mise en œuvre de mécanismes d'avis d'atteinte aux mesures de sécurité dans des États américains il y a plusieurs années, après la modification de la *Personal Information Protection Act* (Alberta) pour y inclure une règle de déclaration des incidents, et après l'introduction de

règles de notification dans différentes lois provinciales sur la protection des renseignements personnels sur la santé (y compris des règles accentuées dans la législation ontarienne en matière de protection des renseignements personnels sur la santé qui sont entrées en vigueur cette année), nous nous attendons à ce que le nouveau mécanisme de déclaration et d'avis prévu par la LPRPDE ait les effets suivants :

- Davantage de transparence au sujet des incidents d'atteinte aux mesures de sécurité des données et de la déclaration de ceux-ci au sein des organisations, et une meilleure connaissance générale de la portée, du niveau de sophistication et du nombre croissant des menaces à la sécurité.
- Davantage d'avis envoyés aux personnes touchées et aux autres organisations au sujet des incidents de sécurité.
- Davantage de couverture médiatique, ou au moins une intensification des informations relayées par les médias, et une sensibilisation accrue du public sur les pratiques de mise en place de mesures de sécurité des renseignements (ou sur la perception d'absence de celles-ci).
- Davantage d'enquêtes, de décisions publiées et de demandes réglementaires par des autorités de réglementation en matière de protection des renseignements personnels, entraînant un perfectionnement accru des autorités de réglementation en matière de protection des renseignements personnels, ce qui aura pour conséquence de susciter des attentes en matière de réglementation.
- Un risque plus élevé d'actions collectives.

Les actions collectives pour atteinte à la vie privée au fil du temps

Le nombre d'actions collectives pour atteinte à la vie privée a augmenté rapidement entre 2010 et 2016. Avant 2010, seulement deux actions collectives pour atteinte à la vie privée avaient été intentées. En 2010, il y en a eu trois, sept en 2011 et dix pour chacune des années 2012 et 2013. Après un léger recul en 2014 et 2015, il y en a eu onze en 2016. Jusqu'à ce jour, en 2017, nous savons que quatre nouvelles actions collectives pour atteinte à la vie privée ont été intentées.



- Davantage de préoccupations et d'attention au sujet des risques accrus sur le plan juridique et celui de la réputation au niveau des cadres supérieurs et du conseil d'administration.
- Davantage d'efforts proactifs de la part des organisations pour dissiper les inquiétudes en matière de sécurité des renseignements personnels, en se concentrant d'abord, notamment, sur ce qui suit :
  - l'élaboration ou l'amélioration des plans et protocoles de préparation aux incidents de sécurité et sur leur mise en œuvre appropriée ;
  - une surveillance accrue des tiers fournisseurs qui ont la garde des données des

organisations, notamment des pratiques améliorées de gestion des fournisseurs, comme une vérification diligente précontractuelle renforcée, des obligations contractuelles de protection des données plus rigoureuses imposées aux fournisseurs, une plus grande attention sur la répartition appropriée du risque et plus particulièrement sur la vérification de conformité postcontractuelle.

- D'une manière générale, des coûts plus élevés pour les organisations en raison de tous ces facteurs.

La Loi canadienne anti-pourriel

La LCAP est possiblement la législation anti-pourriel la plus stricte au monde. La loi impose des exigences strictes et normatives en matière de consentement, d'avis, d'envoi de messages électroniques commerciaux et d'installation de programmes informatiques.

À ce jour, le Conseil de la radiodiffusion et des télécommunications canadiennes (le CRTC), organisme principal responsable de l'application de la LCAP, a reçu plus d'un million de plaintes concernant de prétendues violations de la LCAP. Les sanctions en cas de non-conformité peuvent être sévères : les organisations peuvent se voir imposer des amendes maximales de 10 millions de dollars et faire l'objet de poursuites en dommages-intérêts dans le cadre du droit privé d'action pouvant atteindre 200 $ par courriel commercial (ou autre type de message électronique) envoyé en contravention de la loi, jusqu'à concurrence d'un million de dollars par jour de durée de la contravention.

Le droit privé d'action devait initialement entrer en vigueur le 1er juillet 2017. Toutefois, à la suite d'un fait important survenu en juin 2017, le gouvernement fédéral canadien a annoncé qu'il suspendait l'entrée en vigueur de ces dispositions, indiquant qu'il demanderait à un comité parlementaire de passer la LCAP en revue.

Le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes a entrepris l'examen parlementaire en septembre dernier et a avancé rapidement dans ses travaux. Au début de novembre, le Comité avait entendu des douzaines de témoins et avait reçu des douzaines de mémoires écrits, dont la très grande majorité préconisait des modifications importantes de la LCAP. La réponse du gouvernement fédéral au rapport de ce comité parlementaire est prévue pour 2018.

Dans l'intervalle, des sociétés demeurent confrontées à la possible application de la loi par le CRTC en cas de violation de la LCAP. Le CRTC a conclu plusieurs enquêtes en 2017 et il en a de nombreuses autres en cours.

L'orientation vers la gouvernance de données

Les données sont maintenant considérées comme un actif commercial crucial pour bon nombre d'organisations et d'importantes ressources d'analyse sont retenues pour tirer parti des avantages de la grande quantité (en croissance rapide) de renseignements qu'elles possèdent et contrôlent.

Les sociétés de tous les secteurs sont en voie de s'adapter aux risques nuancés en matière de protection des renseignements personnels, de droit, d'éthique et de réputation qui émergent de leurs analyses (p. ex. initiatives au sujet des « données volumineuses »). S'inscrivant dans une grande tendance visant à cerner et à atténuer ces risques, davantage d'organisations ont élaboré ou amélioré des cadres rigoureux de gouvernance des données, qui intègrent des programmes de protection des renseignements personnels, une gouvernance en

matière de sécurité de l'information et des processus sur les risques d'entreprise.

En 2017, les autorités de réglementation canadiennes en matière de protection des renseignements personnels ont également tourné davantage l'éclairage sur les programmes des organisations en matière de protection des renseignements personnels, la gouvernance des données et une « responsabilité démontrable ». Dans des décisions réglementaires et dans certaines déclarations publiques, des autorités de réglementation en matière de protection des renseignements personnels ont davantage mis l'accent sur la nécessité pour les organisations de démontrer l'efficacité des politiques, des pratiques et des procédures qui régissent leurs pratiques en matière de renseignements personnels.

Avec l'arrivée de 2018, nous prévoyons que la « responsabilité démontrable » demeurera au cœur des préoccupations des autorités de réglementation canadiennes en matière de protection des renseignements personnels. Les organisations canadiennes devraient s'assurer qu'elles sont en mesure de démontrer qu'elles disposent de cadres de gouvernance des données à jour et suffisamment rigoureux.