Pour discussion

Règlement sur la notification et la déclaration des atteintes à la protection des données

Innovation, Sciences et Développment économique Canada

Mars 2016

Page intentionnellement vide

Table des matières

Préface

Le 18 juin 2015, la *Loi sur la protection des renseignements personnels numériques* (aussi dite projet de loi S-4) a reçu la sanction royale au Parlement du Canada. La *Loi sur la protection des renseignements personnels numériques* a modifié la loi canadienne régissant la protection des renseignements personnels dans le secteur privé, c'est-à-dire la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ). En général, la LPRPDÉ définit les règles applicables à la collecte, à l'utilisation et à la communication des renseignements personnels par les organisations du secteur privé dans le cadre d'activités commerciales. Elle établit les exigences juridiques de base auxquelles les organisations du secteur privé doivent se conformer pour veiller à ce que les Canadiens aient l'assurance qu'on respecte leur vie privée quand des entreprises détiennent leurs renseignements personnels.

Entre autres modifications importantes, la *Loi sur la protection des renseignements personnels numériques* a modifié la LPRPDÉ pour exiger des organisations du secteur privé d'aviser les Canadiens touchés par une perte ou un vol de renseignements personnels risquant de leur porter préjudice. Ces organisations sont aussi tenues de signaler ces atteintes à la protection des données potentiellement préjudiciables au commissaire à la protection de la vie privée du Canada.

Les nouvelles exigences de la LPRPDÉ en cas d'atteinte à la protection des données entreront en vigueur quand le gouvernement aura édicté le règlement, ce qui leur conférera davantage de clarté et de précision. Le but du présent document de discussion est de solliciter l'avis et le point de vue des intervenants sur ce règlement. Les commentaires reçus seront pris en compte dans la préparation du projet de règlement.

Les parties intéressées sont encouragées à étudier les questions soulevées dans le présent document de consultation ainsi qu'à faire parvenir par écrit leurs commentaires et réponses aux questions d'ici le 31 mai. Prière de transmettre vos observations sous forme électronique (en format Microsoft Word ou Adobe PDF) par courriel à l'adresse ic.ised.breach-atteinte.isde.ic@canada.ca ou en version papier par la poste à l'adresse suivante : Consultations sur les atteintes à la protection des données, Direction de la politique sur la sécurité et la protection des renseignements personnels, Innovation, Sciences et Développement économique Canada, 235, rue Queen, Ottawa (Ontario) K1A 0H5.

Il convient de noter que tout au long du présent document il est fait référence aux lois et règlements d'autres juridictions ayant cours en date du 17 décembre 2015. Ainsi, tout développement concernant ces juridictions ayant lieu après cette date n'y sont pas reflétés.

Innovation, Sciences et Développement économique Canada remercie tous les intervenants de l'aide précieuse qu'ils lui ont peut-être déjà fournie dans l'élaboration des exigences de notification en cas d'atteinte à la protection des données de la LPRPDÉ et de leur participation continue à la préparation de la présente proposition.

Introduction

En général, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) définit les règles applicables à la collecte, à l'utilisation et à la communication des renseignements personnels dans le cadre d'activités commerciales par les organisations du secteur privé qui lui sont assujetties. Elle établit les exigences juridiques de base auxquelles les organisations du secteur privé doivent se conformer pour veiller à ce que les Canadiens aient l'assurance qu'on respecte leur vie privée quand des entreprises détiennent leurs renseignements personnels.

La LPRPDÉ s'inspire des dix principes internationalement reconnus sur lesquels se fonde le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, une norme nationale qui a été élaboré en 1996 par des groupes de consommateurs et d'entreprises ainsi que par des représentants du gouvernement. Conformément à son article 3, la Loi a pour objet est de créer un équilibre entre le droit d'une personne à la vie privée et le besoin légitime des entreprises de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins raisonnables. La LPRPDÉ propose une approche souple et non prescriptive pour atteindre cet objectif.

La Loi prévoit un processus indépendant de supervision et de réparation par le truchement du Commissariat à la protection de la vie privée du Canada et de la Cour fédérale. Le commissaire à la protection de la vie privée du Canada peut résoudre les conflits en matière d'atteinte à la protection des renseignements personnels en recourant à divers mécanismes de règlement des différends, tandis que la Cour fédérale a le pouvoir d'ordonner aux organisations de modifier leurs pratiques afin de se conformer à la loi, pouvant aussi accorder des dommages-intérêts aux personnes ayant subi des préjudices du fait de l'atteinte à la protection de leurs renseignements personnels en violation de la LPRPDÉ.

La LPRPDÉ s'applique aux entreprises fédérales à l'échelle du pays et à toute organisation exerçant des activités commerciales, sauf celles assujetties aux lois provinciales essentiellement similaires[1].

[1] Les lois provinciales considérées comme essentiellement similaires à la LPRPDÉ sont : la *Personal Information Protection Act* de la Colombie-Britannique; la *Personal Information Protection Act* de l'Alberta; la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec; la *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario (dépositaires de renseignements sur la santé); la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick (dépositaires de renseignements sur la santé); et la *Personal Health Information Act* de Terre-Neuve-et-Labrador (dépositaires de renseignements sur la santé).

La Loi sur la protection des renseignements personnels numériques

Le 18 juin 2015, la *Loi sur la protection des renseignements personnels numériques* (aussi dite projet de loi S-4) a reçu la sanction royale, apportant d'importantes modifications à la LPRPDÉ afin de mieux protéger les renseignements personnels, de simplifier les règles applicables aux entreprises et d'en accroître le respect. Le projet de loi donnait suite à la réponse du gouvernement au premier examen prévu par la loi de la LPRPDÉ, réalisé en 2007[2].

Au nombre des modifications apportées par la *Loi sur la protection des renseignements personnels numériques* figure l'établissement d'exigences obligatoires de notification des atteintes à la protection des données. Les exigences sont énoncées à la section 1.1 de la LPRPDÉ. En résumé, en cas d'intrusion dans leurs données – appelée dans la Loi « atteinte aux mesures de sécurité » –, les organisations doivent :

- déterminer si l'atteinte présente un « risque réel de préjudice grave » à l'endroit de tout individu dont les renseignements personnels sont en cause;
- aviser le plus tôt possible les individus de toute atteinte présentant un « risque réel de préjudice grave » à leur endroit;
- signaler le plus tôt possible au commissaire à la protection de la vie privée toute atteinte à la protection des données présentant un « risque réel de préjudice grave »;

Qu'entend-on par « atteinte aux mesures de sécurité »?

Les nouvelles exigences de signalement des atteintes à la protection des données prévues par la LPRPDÉ s'appliquent à toute « atteinte aux mesures de sécurité ». D'où la nécessité de bien comprendre ce terme.

Le paragraphe 2(1) de la LPRPDÉ définit une « atteinte aux mesures de sécurité » comme suit :

> *Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues à l'article 4.7 de l'annexe 1 ou du fait que ces mesures n'ont pas été mises en place.*

La définition vise à inclure deux éléments, le premier étant la perte de renseignements personnels ou l'accès non autorisé à ceux-ci (par suite de leur vol ou de leur communication illicite) et le second, que cette perte et cet accès non autorisé résultent d'une atteinte aux mesures de sécurité d'une organisation (ou de la non-mise en place de telles mesures par l'organisation).

Par exemple, le fait pour des employés contractuels non autorisés d'avoir eu accès à une base de données renfermant les renseignements personnels des clients d'une organisation, parce qu'un employé de celle-ci a omis de protéger cette base de données par un mot de passe (ainsi que l'exige la politique de sécurité de l'organisation) répondrait à la définition d'atteinte à la protection de la LPRPDÉ. Par contre, le simple fait de ne pas avoir protégé cette base de données par un mot de passe même sans qu'il y ait eu accès non autorisé à ses données, ne répondrait pas à la définition d'« atteinte aux mesures de sécurité » de la Loi.

[2] Réponse du gouvernement au Quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique : Examen, prévu par la loi, de la LPRPDÉ.

- aviser s'il y a lieu, tout tiers qu'elle croit être en mesure d'atténuer le risque de préjudice;
- tenir un registre des atteintes à la protection des données et donner accès à ce registre au commissaire à la protection de la vie privée à la demande de celui-ci.

Règlement sur la notification et la déclaration des atteintes à la protection des données

Le gouvernement a le pouvoir d'établir des règlements afin de conférer davantage de clarté et de précision aux exigences de déclaration des atteintes à la protection des données prévues par la Loi. Cela comprend le pouvoir d'établir les modalités et le contenu des avis et déclarations, les facteurs additionnels à considérer dans la détermination du risque, les exigences de tenue de registres et d'autres éléments.

Les nouvelles exigences de notification en cas d'atteinte à la protection des données entreront en vigueur quand le gouvernement aura adopté le règlement définitif. Le but de la présente consultation est de solliciter l'avis et le point de vue des intervenants sur ce règlement. Leurs commentaires reçus seront pris en compte dans la préparation du projet de règlement.

À l'issue de ce processus de consultation, le gouvernement publiera le projet de règlement dans la Partie I de la *Gazette du Canada* aux fins de consultation et d'observation du public. Une fois toutes les observations reçues, le règlement définitif sera publié dans la Partie 2 de la *Gazette du Canada* et les nouvelles dispositions de notification en cas d'atteinte à la protection des données de la LPRPDÉ seront mises en vigueur.

Ce qui se fait dans d'autres juridictions

Un certain nombre d'organisations responsables de la protection des données ont établi ou proposé que soient établis des cadres de signalement (obligatoire et volontaire) des atteintes à la protection des données. Il est révélateur pour le gouvernement du Canada d'étudier les exigences précises de ces cadres afin de mieux harmoniser la réglementation et d'alléger le fardeau administratif des organisations, d'une part, et d'adopter les meilleures pratiques avérées, d'autre part.

Commissariat à la protection de la vie privée du Canada : déclaration volontaire des atteintes à la protection des données

Le programme existant de signalement volontaire des atteintes à la protection des données qu'a instauré le Commissariat à la protection de la vie privée (CPVP)[3] du Canada en 2007, revêt une importance particulière pour les organisations assujetties à la LPRPDÉ, bon nombre d'entre elles, en ayant fait une pratique exemplaire. Le programme sera mis à jour dès la mise en œuvre des dispositions impératives de la *Loi sur la protection des renseignements personnels numériques*.

Le programme volontaire encourage les organisations à signaler au CPVP toute atteinte « substantielle » à la protection des données et d'en aviser leurs clients ou employés concernés en cas de « risque de préjudice ». Les documents d'orientation à l'appui tels que *Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée*[4] suggèrent et recommandent des pratiques exemplaires, par exemple l'évaluation du risque associé à l'atteinte à la protection des données, le quand et le comment notifier ainsi que les renseignements à inclure dans un avis. Il s'ensuit que le programme volontaire du CPVP constitue une bonne base pour l'élaboration du règlement sur la notification et la déclaration des atteintes à la protection des données.

Politique du Conseil du Trésor sur la déclaration des atteintes à la protection des données

En 2014, le gouvernement a mis en œuvre une nouvelle politique sur le signalement obligatoire des atteintes à la vie privée dans la fonction publique fédérale. La Directive modifiée sur les pratiques relatives à la protection de la vie privée du Secrétariat du Conseil du Trésor oblige l'ensemble des institutions fédérales à déclarer certaines atteintes à la protection des renseignements personnels auprès du Secrétariat du Conseil du Trésor et du Commissariat à la protection de la vie privée, et aussi d'en aviser les personnes touchées.

[3] https://www.priv.gc.ca/resource/pb-avp/index_f.asp
[4] https://www.priv.gc.ca/information/guide/2007/gl_070801_02_f.asp

La politique et le projet de loi S-4 concordent en ce que les deux emploient un critère de signalement fondé sur le risque, définissent globalement le préjudice de manière semblable et prévoient un délai d'avis souple.

Provinces canadiennes

Au Canada, l'Alberta est, à l'heure actuelle, la seule province à obliger toutes les organisations du secteur privé à signaler les atteintes à la protection des données, et ce, en vertu de sa *Personal Information Protection Act* (PIPA)[5]. Les lois en matière de protection des renseignements personnels en santé des provinces de l'Ontario, du Nouveau-Brunswick et de Terre-Neuve--et-Labrador prévoient également des exigences en la matière pour le secteur des soins de santé[6].

États-Unis

Depuis plusieurs années, les lois de la majorité des États américains obligent à déclarer toute atteinte à la protection des données, et certains États commencent à mettre à jour leurs exigences à la lumière des règles existantes.

Aux États-Unis, des lois propres aux secteurs des finances et de la santé obligent également ceux-ci à signaler de telles atteintes. Il s'agit de la *Gramm-Leach-Bliley Act*[7], qui s'applique au secteur financier, ainsi que de la *Health Insurance Portability and Accountability Act* [8] et de l'*American Recovery and Reinvestment Act*[9], qui s'appliquent toutes deux au traitement des **d**onnées électroniques en santé.

---

[5] On peut consulter la *Personal Information Protection Act* de l'Alberta à l'adresse suivante : http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507.

[6] On peut consulter la *Loi de 2004 sur la protection des renseignements personnels sur la santé de l'Ontario* à l'adresse suivante : http://www.ontario.ca/fr/lois/loi/04p03, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick, en suivant le lien http://laws.gnb.ca/fr/showfulldoc/cs/P-7.05/20121030, et la *Personal Health Information Act* de Terre-Neuve-et-Labrador, en se rendant à l'adresse suivante : http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm.

[7] Voir la *Safeguards Rule* de la *Gramm-Leach-Bliley Act* à l'adresse suivante : http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.

[8] Voir la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante: http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6.

[9] On peut consulter la *Health Breach Notification Rule* de l'*American Recovery and Reinvestment Act* à l'adresse suivante: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART.

Au niveau fédéral, plusieurs projets de loi ont été mis de l'avant pour fixer des règles nationales, bien qu'aucun n'ait encore été adopté. Le plus récent, proposé par la Maison-Blanche, s'intitule *Personal Data Notification and Protection Act*[10].

Union européenne

En Europe, la *Directive vie privée et communications électroniques* de la Commission européenne[11] oblige actuellement les fournisseurs de services de télécommunications à notifier les violations de données. Les exigences précises en vertu de la Directive sont énoncées dans le règlement (UE) n° 611/2013[12] de la Commission. L'Union européenne a publié un projet de *Règlement général sur la protection des données*, qui propose d'étendre ces exigences à toutes les organisations.

Éléments du règlement

Déterminer le risque réel de préjudice grave

En vertu des nouvelles dispositions sur l'atteinte à la protection des données, les organisations qui prennent connaissance d'une atteinte à leurs mesures de sécurité sont tenues d'effectuer une analyse de situation pour déterminer si ladite atteinte présente un « risque réel de préjudice grave » occasionné à l'individu dont les renseignements personnels sont en cause. L'organisation décide, à l'issue de cette analyse, des mesures additionnelles qu'il y a lieu de prendre.

L'article 10.1(8) exige que l'analyse tienne compte, à tout le moins, de la nature délicate des renseignements personnels mis en cause par l'atteinte et de la probabilité que les renseignements aient été ou seront utilisés à mauvais escient pour causer un préjudice.

L'article 10.1(8) accorde au gouvernement le pouvoir de spécifier d'autres facteurs servant à déterminer s'il y a risque réel de préjudice grave par suite d'une atteinte.

---

[10] On peut consulter la *U.S. Personal Data Notification and Protection Act* se trouve à l'adresse suivante: *https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf*

[11] On peut consulter la Directive 2002/58/EC (Directive vie privée et communications électroniques) à l'adresse suivante : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32002L0058; cette dernière est modifiée et complétée par la Directive 2009/136/CE et peut être consultée à l'adresse suivante : http://eur-lex.eurpa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:fr:PDF.

[12] On peut consulter le règlement (UE) n° 611/2013 de la Commission à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

***10.1*(*8*)** *Les éléments servant à établir si une atteinte aux mesures de sécurité présente un risque réel de préjudice grave à l'endroit de l'intéressé sont notamment le degré de sensibilité des renseignements personnels en cause, la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être et tout autre élément prévu par règlement.*

Considérations

L'objectif global des exigences de signalement des atteintes à la protection des données de la LPRPDÉ est de veiller à ce qu'on informe les personnes dont on a violé les renseignements personnels de cette atteinte et du risque consécutif de préjudice à leur endroit, de façon à ce qu'elles puissent agir pour se protéger et atténuer ce préjudice. D'où l'établissement dans la Loi d'un cadre fondé sur le risque.

L'un des principes fondamentaux en protection de la vie privée est l'importance du contexte. Dans certains cas l'accès non autorisé aux renseignements personnels sera parfois sans gravité, mais la perte ou le vol des mêmes renseignements personnels pourrait être extrêmement préjudiciable dans d'autres circonstances. Il n'est donc pas pratique de détailler les types de renseignements personnels ou de dresser une liste précise des circonstances qui obligent à déclarer et à notifier. La LPRPDÉ exige plutôt des organisations qu'elles fassent une analyse de situation tenant compte de la nature délicate des renseignements personnels en cause selon le contexte, d'une part, et de la probabilité que les renseignements aient été ou seront utilisés à fins préjudiciables, d'autre part.

Les organisations sont déjà tenues en vertu de la LPRPDÉ de déterminer si un renseignement donné est de nature délicate dans les circonstances. Par exemple, les organisations doivent tenir compte de la sensibilité des renseignements dans l'obtention du consentement, conformément aux articles 4.3.4 et 4.3.6 de l'annexe 1 de la Loi, et dans l'établissement de mesures de sécurité appropriées, conformément à l'article 4.7.2 de la même annexe.

À l'obligation d'envisager la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être s'ajoute l'examen d'un certain nombre de sous-facteurs selon les circonstances. Les données étaient-elles chiffrées? Combien de temps s'est-il écoulé entre l'atteinte et sa détection? Qui a eu accès aux données?

En vertu des lignes directrices facultatives *Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée* du CPVP, les organisations sont encouragées à tenir compte des facteurs suivants dans l'évaluation des risques :

- les renseignements personnels en cause, y compris leur degré de sensibilité, s'ils sont encodés ou dépersonnalisés, et s'ils peuvent servir à des fins préjudiciables;
- la cause et l'étendue de la brèche;

- les personnes concernées par la brèche, y compris leur nombre et s'il s'agit de clients ou d'employés de l'organisation;
- les préjudices prévisibles de la brèche.

En Alberta, ni la *Personal Information Protection Act* ni son règlement ne prévoient de critère pour déterminer s'il y a risque réel de préjudice grave.

Aux États-Unis, le règlement d'application de la *Health Insurance Portability and Accountability Act* oblige à tenir compte des facteurs de risque suivants pour déterminer s'il y a eu violation de la confidentialité des renseignements :

- la nature et l'étendue des renseignements en santé protégés en cause, y compris les types d'identificateurs et la probabilité de réidentification;
- la personne non autorisée qui a utilisé les renseignements en santé protégés ou à qui ceux-ci ont été communiqués;
- si les renseignements ont bel et bien été acquis ou consultés;
- le degré d'atténuation du risque de violation des renseignements en santé protégés[13].

En vertu de la *Personal Data Notification and Protection Act*, un projet de loi américain, une organisation pourrait présumer qu'aucun risque n'existe à l'issue d'une atteinte quand les renseignements ont été rendu inutilisables, illisibles ou indéchiffrables au moyen d'une technologie ou d'une méthode de sécurité généralement acceptée par les experts du domaine de la sécurité de l'information. Le projet de loi précise toutefois que cette présomption sera présumée réfutable en cas de violation avérée de ces mesures[14].

Dans l'Union européenne, la *Directive vie privée et communications électroniques* exige qu'il y ait notification quand « une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une personne ». Le règlement d'application de la Directive exige que soient pris en compte les facteurs suivants pour déterminer la probabilité d'effets adverses :

- la nature et la teneur des données concernées, y compris des renseignements spécifiques tels que des informations financières, les données de localisation, les fichiers journaux et les historiques de sites consultés;

---

[13] Voir la partie 164.402 de la *Health Breach Notification Rule*, 45 CFR §§ 164.400-414, de l'ARRA à l'adresse suivante : http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6.

[14] Voir l'article 102(b) de la *Personal Notification and Protection Act* (États-Unis) à l'adresse suivante : https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

- les conséquences vraisemblables de la violation, notamment les cas où cette violation pourrait entraîner un vol ou une usurpation d'identité, un préjudice physique, une humiliation, etc.;

- les circonstances de la violation, en particulier l'endroit où les données ont été volées et si on sait ou non que les données sont en possession d'un tiers qui n'est pas autorisé à y avoir accès[15].

En outre, la Directive ajoute que « la notification d'une violation de données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité nationale compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation de sécurité. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès »[16].

Questions à débattre

Première question : Faut-il préciser d'autres facteurs d'évaluation du risque dans le règlement? Ou ceux énumérés dans la loi sont-ils suffisamment clairs?

Deuxième question : Quels facteurs additionnels devrait-on prescrire, le cas échéant?

Troisième question : Le règlement devrait-il spécifier que le risque de préjudice est présumé faible lorsqu'une méthode appropriée de chiffrement a été utilisée? Si oui, comment, à votre avis, devrait-on définir ce qu'est un niveau approprié de protection?

Déclaration au commissaire – Modalités de l'avis

L'organisation concluant qu'une atteinte à ses mesures de sécurité présente un risque réel de préjudice grave est tenue, en vertu de l'article 10.1(1), de la déclarer au commissaire à la protection de la vie privée du Canada.

L'article 10.1(2) confère au gouvernement le pouvoir d'énumérer les types de renseignements devant figurer dans une telle déclaration et d'en préciser les modalités.

***10.1*(2)** *La déclaration contient les renseignements prévus par règlement et est faite, selon les modalités réglementaires, le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte.*

[15] Voir l'article 3.2 du Règlement (UE) 611/2013/CE.
[16] Voir l'article 4.1 du Règlement (UE) 611/2013/CE.

Considérations

Signaler les atteintes au CPVP permet à celui-ci de remplir son mandat de surveillance et de veiller à ce que les organisations respectent l'obligation qui leur est faite d'aviser les intéressés. Cela permettra aussi de normaliser le suivi des atteintes graves à la protection des données au Canada. Par conséquent, les déclarations doivent renfermer suffisamment d'information pour atteindre ces objectifs tout en imposant un fardeau de déclaration minimal aux organisations.

Contenu de la déclaration

Le formulaire type *Rapport d'atteinte à la vie privée*[17] du programme de signalement volontaire du CPVP demande aux organisations de fournir l'information suivante dans leur déclaration au commissaire :

- la date et le lieu de l'incident et la date de sa découverte;
- une description de l'incident;
- sa cause;
- une estimation du nombre d'individus affectés;
- la relation de ces individus avec l'organisation (p. ex., des employés ou des clients);
- la catégorie de renseignements personnels en cause;
- les mesures prises par l'organisation pour contenir l'atteinte;
- si d'autres personnes ont été notifiées de l'incident (p. ex., les individus en cause et la police) et quand elles l'ont été.

En Alberta, le règlement *Personal Information Protection Regulation*[18] spécifie les modalités de déclaration des atteintes à la protection des renseignements personnels au commissaire à la vie privée de l'Alberta conformément à l'obligation de signalement prévue à la *Personal Information Protection Act*[19]. En vertu de ce règlement, la déclaration doit être faite par écrit et renfermer, à tout le moins :

- une description des circonstances de l'atteinte;
- la date (ou période) de l'atteinte;
- une description des renseignements en cause;

[17] https://www.priv.gc.ca/resource/pb-avp/index_f.asp
[18] Voir le règlement 366/2003 de l'Alberta (y compris toutes les modifications jusqu'au règlement de l'Alberta 51/21 010) à l'adresse suivante : http://www.qp.alberta.ca/documents/Regs/2003_366.pdf.
[19] http://www.qp.alberta.ca/documents/Acts/P06P5.pdf.

- une évaluation du risque de préjudice aux intéressés pouvant résulter de l'atteinte;
- une estimation du nombre d'individus en cause;
- les mesures prises par l'organisation afin de réduire le risque de préjudice pour les individus;
- les coordonnées d'un représentant de l'organisation qui peut répondre aux questions du commissaire au sujet de l'atteinte.

Il convient de noter qu'en vertu de ce régime, la décision d'aviser les individus relève du commissaire. L'organisation doit tout de même fournir une évaluation du risque de préjudice auquel l'atteinte expose les intéressés. Ces éléments correspondent assez fidèlement, à quelques exceptions près, aux exigences d'autres régimes de notification des atteintes à la vie privée.

Aux États-Unis, les organisations qui signalent des atteintes en vertu de la *Health Insurance Portability and Accountability Act* sont également tenues d'identifier les organismes d'application de la loi qu'elles ont informés de l'incident et d'indiquer si les intéressés ont été avisés.

En vertu de la *Directive vie privée et communications électroniques* de l'Union européenne, la notification à l'autorité compétente doit contenir 17 points de données, dont : l'identification de l'organisation; les informations initiales sur la violation des données (telles que la date et l'heure de l'incident ainsi que la nature et la teneur des données à caractère personnel en cause); les informations supplémentaires sur la violation des données (telles que le nombre de particuliers concernés et un résumé de l'incident à l'origine de la violation); la notification supplémentaire éventuelle aux particuliers (telle que le contenu de la notification et les moyens de communication utilisés); et les questions transnationales éventuelles (telles que la notification à d'autres autorités nationales compétentes)[20].

Questions à débattre

Quatrième question : a) Y aurait-il lieu d'exclure de toute déclaration obligatoire des renseignements requis en vertu du rapport volontaire du CPVP en vigueur? Si oui, lesquels? b) Y aurait-il lieu d'exiger des renseignements additionnels? Si oui, lesquels?

Cinquième question : Les organisations devraient-elles joindre à leurs déclarations au commissaire une évaluation du type de préjudice susceptible de résulter de l'atteinte et de l'éventualité d'un tel préjudice?

[20] Voir l'annexe 1 du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

La LPRPDÉ met l'accent sur la nécessité de déclarer rapidement les atteintes à la protection des données auprès du commissaire, les organisations étant tenues de présenter une déclaration « le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte ». Cela accorde une certaine latitude aux organisations en leur permettant de régler des questions plus urgentes – comme contenir l'atteinte – avant de faire leur déclaration. Cependant, il sera peut-être plus facile aux organisations de recueillir certains éléments de données demandés que d'autres. De plus, après étude plus poussée de l'atteinte, certaines informations pourraient changer. Il faudra par conséquent trouver un équilibre entre l'exigence de produire une déclaration rapidement et l'impératif de fournir des renseignements complets et exacts.

En vertu de la *Directive vie privée et communications électroniques* de l'Union européenne, les organisations doivent notifier la violation auprès de l'autorité compétente au plus tard 24 heures après l'avoir constatée. Le règlement prévoit que si les informations ne sont pas toutes disponibles et si une enquête plus approfondie est nécessaire, l'organisation fera une première notification dans les 24 heures du constat et, le plus rapidement possible, une seconde notification renfermant les informations manquantes et actualisant au besoin les informations déjà fournies[21].

Questions à débattre

Sixième question : Dans quelle mesure une organisation devrait-elle être tenue de fournir et de valider tous les éléments de la déclaration auprès du CPVP pour qu'elle soit réputée s'être conformée aux exigences?

Septième question : Le règlement devrait-il exiger d'une organisation qu'elle actualise les renseignements qu'elle avait d'abord fournis au commissaire après avoir constaté qu'ils étaient inexacts ou incomplets ou qu'ils ont changé?

Modalités de déclaration

Le CPVP permet actuellement, en vertu de son programme de signalement volontaire, que les atteintes lui soient signalées par courriel, par courrier ou par téléphone. En Alberta, le commissaire ne peut accepter de déclaration que par courriel ou courrier ordinaire. C'est aussi le cas en vertu de la plupart des lois des États américains. La *Health Information Portability and Accountability* des États-Unis fait toutefois exception à la règle, n'autorisant le signalement électronique d'infractions aux données que par le truchement d'un portail Web conçu à cette fin.

[21] Voir le paragraphe 2.3 du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

Dans le même ordre d'idées, le règlement d'application de la *Directive vie privée et communications électroniques* de l'Union européenne oblige l'autorité compétente à mettre à la disposition des autorités de chaque État membre concerné « un moyen électronique sécurisé de notification des violations de données à caractère personnel »[22]. En voici un exemple sur le site Web du commissaire à la protection des données de l'Irlande : (https://www.dataprotection.ie/secur-breach/form.asp).

Questions à débattre

Huitième question : Les organisations devraient-elles être tenues de ne déclarer les atteintes auprès du commissaire à la protection de la vie privée que par écrit (sous forme électronique ou sur papier) par souci d'efficacité? Si non, pourquoi?

Neuvième question : Devrait-on établir un moyen électronique sécurisé pour informer le commissaire à la vie privée de violations à la protection des données?

Avis aux intéressés – Contenu

En vertu de l'article 10.1(3) de la Loi, « l'organisation est tenue d'aviser l'intéressé de toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels le concernant » et qui « présente un risque réel de préjudice grave à son endroit ». L'article 10.1(4) stipule que l'avis doit contenir « suffisamment d'information » pour permettre à l'intéressé de comprendre le risque de préjudice pouvant résulter de l'atteinte et de prendre, si cela est possible, des mesures pour réduire ce risque ou pour l'atténuer.

L'article 10.1(4) confère aussi au gouvernement le pouvoir de spécifier tout autre renseignement réglementaire devant figurer dans l'avis à l'intéressé.

***10.1*(4)** *L'avis contient suffisamment d'information pour permettre à l'intéressé de comprendre l'importance, pour lui, de l'atteinte et de prendre, si cela est possible, des mesures pour réduire le risque de préjudice qui pourrait en résulter ou pour atténuer un tel préjudice. Il contient aussi tout autre renseignement réglementaire.*

[22] Voir le paragraphe 2.4 du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

Considérations

Une étude de consommation[23] sur l'impact des notifications d'atteinte à la protection des données menée aux États-Unis en 2012 conclut à l'existence d'un lien direct entre le type d'information fournie dans un avis aux intéressés et l'efficacité de la notification. Selon l'étude, la plupart des intéressés notifiés étaient déçus de la façon dont les organisations avaient géré l'incident, en retenant surtout que l'avis ne les avait pas aidés à comprendre l'importance de l'atteinte. Plus particulièrement, les destinataires de ces avis trouvaient ceux-ci truffés de « jargon juridique » et trop longs.

Pour améliorer l'efficacité des avis, l'étude recommandait qu'on y spécifie la cause de l'atteinte et les types de données perdues ou volées. Elle recommandait en outre que l'organisation explique aux intéressés les risques ou préjudices pouvant découler de l'atteinte.

- Le programme de signalement volontaire des atteintes à la protection des données du CPVP suggère d'inclure les renseignements suivants dans l'avis envoyé aux personnes concernées :

- un « aperçu » de l'incident et le moment où il s'est produit;

- une description des renseignements personnels en cause et des mesures prises pour contrôler ou réduire les préjudices résultant de l'atteinte;

- ce que l'organisation compte faire pour aider les personnes, et les mesures que ces dernières peuvent prendre pour éviter ou réduire les préjudices à leur endroit;

- les sources de renseignements visant à les aider;

- les coordonnées d'une source à l'intérieur de l'organisation pouvant répondre aux questions ou fournir davantage d'explications;

- les coordonnées du commissaire à la protection de la vie privée compétent (fédéral ou provincial).

Les exigences des cadres de signalement des atteintes à la protection des données varient d'une province à l'autre. Par exemple, le règlement d'application de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick stipule que l'avis doit contenir : le nom de l'organisation; le nom et les coordonnées d'une personne de l'organisation pouvant répondre aux demandes de renseignements; une description de la nature

[23] Ponemon Institute Research Report 2012 Consumer Study on Data Breach Notification, juin 2012

de la violation de la vie privée; les date et lieu de la violation; et la date à la laquelle l'organisation en a pris connaissance[24].

En Alberta, en vertu de la *Personal Information Protection Act*, il appartient au commissaire de déterminer s'il y a lieu d'aviser les personnes concernées et quand le faire. Le règlement connexe, le *Personal Information Protection Regulation*[25], spécifie toutefois les renseignements à inclure dans le libellé d'un avis s'il y a lieu :

- une description des circonstances de l'atteinte;
- la date (ou période) de l'atteinte;
- une description des renseignements en cause;
- les mesures prises par l'organisation pour réduire le risque de préjudice à l'endroit des individus;
- les coordonnées d'un représentant de l'organisation qui peut répondre aux questions du commissaire au sujet de l'atteinte.

Certaines lois américaines exigent des renseignements additionnels, par exemple la date à laquelle l'atteinte a été découverte (en sus de la date présumée de son occurrence), conformément à la *Health Information Portability and Accountability*[26], ainsi qu'un numéro de téléphone sans frais et une adresse de courriel pour permettre aux gens de mieux se renseigner, ainsi que l'exige la *US Personal Data Notification and Protection Act*[27] (projet de loi).

En vertu de la *Directive vie privée et communications électroniques* de l'Union européenne, les fournisseurs de services de télécommunications sont tenus de spécifier neuf catégories d'informations dans les notifications aux particuliers. Outre les renseignements à leur propre sujet et sur la violation même (date, résumé de l'incident, nature des données à caractère personnel concernées), les organisations doivent décrire les mesures qu'elles ont prises pour col-

[24] Voir l'article 19(2) du *Règlement du Nouveau-Brunswick pris en vertu de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* à l'adresse suivante : https://www.canlii.org/fr/nb/legis/regl/regl-du-n-b-2010-112/derniere/regl-du-n-b-2010-112.html.
[25] http://www.qp.alberta.ca/documents/Regs/2003_366.pdf.
[26] Voir l'article 164.404 de la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante: http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6.
[27] Voir l'article 104 du projet de loi *US Personal Data Notification and Protection Act* à l'adresse suivante : https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

mater l'atteinte, les « conséquences vraisemblables » de celle-ci pour l'intéressé et les « mesures recommandées par le fournisseur pour atténuer les préjudices potentiels »[28].

> **Questions à débattre**
>
> **Dixième question :** Est-il nécessaire que le règlement spécifie les renseignements à inclure dans les notifications aux personnes concernées? Ou la loi est-elle suffisamment claire?
>
> **Onzième question** : Quels renseignements y aurait-il lieu de spécifier, le cas échéant?

Notification aux intéressés – Modalités de l'avis

L'élément primordial du cadre est de veiller à ce que la personne touchée soit avisée en cas d'atteinte à la protection de ses renseignements personnels et comprenne clairement qu'elle risque d'en subir un préjudice. Il est par conséquent exigé à l'article 10.1(5) de la Loi que l'avis soit donné à l'intéressé directement pour éviter qu'on le confonde avec du « pourriel » ou qu'il passe inaperçu dans d'autres documents commerciaux.

Toutefois, dans certaines circonstances, une organisation pourrait être dans l'incapacité d'aviser directement les personnes touchées, par exemple si elle n'a pas leurs coordonnées de contact direct. Il lui faudra peut-être alors envisager des moyens indirects de le faire.

L'article 10.1(5) confère au gouvernement le pouvoir de spécifier dans le règlement : i) les modalités obligatoires de notification directe; ii) les circonstances justifiant la notification indirecte plutôt que directe; et iii) les modalités éventuelles de notification indirecte.

> ***10.1*(5)** *L'avis est manifeste et est donné à l'intéressé directement, selon les modalités réglementaires. Dans les circonstances prévues par règlement, il est donné indirectement, selon les modalités réglementaires.*

Considérations

Notification directe

Compte tenu du large éventail d'organisations assujetties à la LPRPDÉ et de la variabilité des circonstances pouvant donner lieu à des atteintes à la protection des données, il est souhaitable que les organisations jouissent d'une certaine latitude quant à la façon d'aviser les personnes touchées. Par exemple, le courriel est un moyen efficace et peu coûteux de communiquer avec

[28] Voir l'annexe II du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

une multitude de gens, mais là n'est peut-être pas le meilleur moyen de transmettre un avis traitant de la perte d'information de nature très délicate, telle que des renseignements sur la santé ou des informations financières. Dans le même ordre d'idées, la tenue de rencontres en personne pourrait convenir à des organisations devant aviser d'importants clients ou des employés, mais cela ne serait pas pratique pour communiquer avec un grand nombre de personnes.

Dans tous les cas, il importe que l'avis soit manifeste et clair et que les personnes concernées en comprennent la teneur et l'importance. Quelle que soit la méthode de notification directe (courriel, poste ordinaire, téléphone, rencontre en personne, etc.), il est important que l'avis soit distinct des autres communications entre l'organisation et les personnes touchées. Par exemple, il serait inopportun de joindre un avis d'atteinte à la protection des données à une facture courante ou à un état de compte.

En vertu de son programme de signalement volontaire des atteintes à la protection des données, le CPVP recommande d'aviser les intéressés par voie d'appel téléphonique, de lettre, de courriel ou de rencontre en personne.

Les règles des cadres de signalement des atteintes à la protection des données varient quelque peu d'une province à l'autre selon. Par exemple, le règlement d'application de la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick requiert d'aviser « par téléphone ou par écrit » la personne visée. La *Personal Information Protection Act* de l'Alberta est muette quant aux moyens précis à prendre pour aviser les personnes concernées, si ce n'est de dire « qu'il faut le faire directement »[29].

En revanche, la *Personal Data Notification and Protection Act* que se propose d'adopter les États-Unis, ne permettrait pas la notification en personne et rend conditionnel l'usage d'autres méthodes. Par exemple, l'avis par courrier ordinaire doit être envoyé à la dernière adresse postale connue de la personne touchée. La notification par téléphone doit se faire personnellement (c'est-à-dire qu'on ne peut laisser de message donnant l'information). La notification par courriel n'est permise qu'avec le consentement préalable de la personne, et le courriel doit respecter les normes techniques prescrites par la Loi[30].

Aux États-Unis, la *Health Insurance Portability and Accountability Act* n'autorise que deux méthodes de notification écrite, l'avis devant être envoyé à la personne concernée par courrier de

[29] Voir le paragraphe 19.1 (1) du *Personal Information Protection Act Regulation* à l'adresse suivante : http://www.qp.alberta.ca/documents/Acts/P06P5.pdf.
[30] Voir l'article 103 de la *Personal Data Notification and Protection Act* à l'adresse suivante : https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

première classe à sa dernière adresse connue ou par courriel si la personne a choisi de ne *pas* recevoir de notification par la poste[31].

Les lois de la majorité des États américains exigent que les avis soient expédiés par courrier de première classe. Celles qui autorisent la notification téléphonique requièrent des organisations qu'elles tiennent un registre de leurs appels téléphoniques. Dans les États où l'utilisation du courriel est permise, celle-ci est généralement conditionnelle à ce que la personne ait consenti expressément à recevoir ce type d'avis sous forme électronique et à ce que l'organisation tienne un registre de toutes leurs notifications.

La *Directive vie privée et communications électroniques* de l'Union européenne ne spécifie aucune méthode de notification si ce n'est d'exiger qu'elle se fasse « par des moyens de communication qui garantissent une réception rapide de l'information et qui sont sécurisés conformément aux règles de l'art. Les informations concernant la violation se limitent à celle-ci et ne sont pas associées à des informations concernant autre chose »[32].

Questions à débattre

Douzième question : Quelles devraient être les méthodes de notification directe permises?

Treizième question : Le règlement devrait-il assujettir à des conditions ou limites le recours à toute méthode de communication directe? Si oui, à quelles conditions ou limites?

Quatorzième question : Le règlement devrait-il spécifier que les notifications doivent être manifestes et distinctes des autres communications?

Notification indirecte – Circonstances la justifiant

Ainsi que nous le précisions, la LPRPDÉ reconnaît qu'il n'est parfois ni pratique ni possible d'aviser directement les personnes en cause d'une atteinte à la protection de leurs données. Dans ces circonstances, les notifications doivent alors être faites par des moyens indirects.

En vertu du programme de signalement volontaire des atteintes à la protection des données du CPVP, les organisations sont invitées à ne recourir à la notification indirecte que si :

[31] Voir la partie 164.404 de la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante : http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6.

[32] Voir le paragraphe 3.6 du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.

- la notification directe causait davantage de préjudices aux personnes concernées;
- les coûts de la notification directe sont excessifs;
- elles n'ont pas les coordonnées des personnes concernées.

Il convient de noter qu'aucun document d'orientation du CPVP ne définit le terme « excessifs ». Puisqu'il s'agit d'un terme subjectif, peut-être faudra-t-il le définir pour l'utiliser dans le règlement. Par exemple, alors qu'une organisation jugera inabordable le coût d'aviser toutes les personnes touchées par une atteinte importante, une autre le trouvera tout à fait abordable.

En Alberta, la *Personal Information Protection Act* autorise également la notification indirecte si le commissaire juge la notification directe déraisonnable dans les circonstances.

Le règlement d'application de la Directive vie privée et communications électroniques de l'Union européenne est moins souple. Une organisation ne peut utiliser de moyens indirects que si elle n'est pas en mesure d'identifier dans le délai fixé toutes les personnes lésées par une violation. Elle peut alors informer ces personnes par des avis dans de grands médias nationaux ou régionaux[33].

Aux États-Unis, des lois semblables s'appliquant au secteur des soins de santé ne permettent de notifier indirectement les personnes affectées que si leurs coordonnées ne sont pas disponibles. La *Health Insurance Portability and Accountability Act* permet de recourir à la « notification de substitution » si les coordonnées des personnes concernées sont insuffisantes ou périmées[34]. L'*American Recovery and Reinvestment Act* va dans le même sens tout en spécifiant que l'organisation doit d'abord s'efforcer raisonnablement de communiquer avec les intéressés avant de recourir à la notification de substitution[35].

[33] Voir l'article 3.7 du règlement (UE) n° 611/2013 à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF.
[34] Voir la partie 164.404 de la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante : http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6.
[35] Voir la partie 318.5 de la *Health Breach Notification Rule* de l'ARRA à l'adresse suivante : http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART.

Questions à débattre

Quinzième question : Dans quelles circonstances devrait-on permettre aux organisations d'aviser indirectement les personnes touchées en cas d'atteinte à la protection de leurs données?

Seizième question : Si le coût est un facteur dont il faut tenir compte pour autoriser ou non le recours à la notification indirecte, comment le règlement devrait-il fixer le seuil approprié?

Notification indirecte

Le programme de signalement volontaire des atteintes à la protection des données du CPVP encourage les organisations qui doivent aviser indirectement les personnes concernées à le faire par l'entremise de sites Web ou des médias afin d'en informer le public.

En Alberta, bien que la *Personal Information Protection Act* permette bel et bien de substituer la notification indirecte à la notification directe dans certaines circonstances, ni la Loi ni son règlement d'application n'en spécifient les moyens.

Dans le secteur américain des soins de santé, tant la *Health Insurance Portability and Accountability Act* que l'*American Recovery Reinvestment Act* permettent de recourir à la notification indirecte (appelée « notification de substitution ») si l'organisation notifiante n'arrive pas à trouver les coordonnées des personnes concernées. Si l'atteinte touche moins de dix personnes, l'organisation peut choisir un autre moyen raisonnablement susceptible de les joindre. Dans le cas de dix personnes ou plus, l'avis peut :

- être publié bien en vue pendant 90 jours sur la page d'accueil du site Web de l'organisation;
- paraître dans les grands médias imprimés et électroniques des régions géographiques où les personnes concernées sont susceptibles d'habiter. Cet avis doit inclure un numéro de téléphone sans frais où les citoyens peuvent savoir si la sécurité de leurs renseignements pourrait avoir été violée[36].

[36] Voir la partie 164.404 de la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante: http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6 et l'article 318.5 de la *American Recovery and Reinvestment Act Health Breach Notification Rule* à l'adresse suivante : http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART.

Dans l'Union européenne, les organisations qui avisent indirectement les personnes concernées par l'entremise des grands médias nationaux ou régionaux doivent, et si nécessaire sous une forme condensée, inclure les mêmes informations que celles requises pour la notification directe. Elles sont également tenues de continuer à déployer tous les efforts raisonnables pour identifier les personnes non avisées directement et les contacter dès que possible.

Questions à débattre

Dix-septième question : Quelles méthodes de notification indirecte aux intéressés devrait-on permettre?

Dix-huitième question : Le règlement devrait-il assujettir à des conditions ou limites le recours à toute méthode de communication indirecte? Si oui, à quelles conditions ou limites?

Notification à d'autres organisations

L'objectif premier du nouveau cadre de déclaration et de notification des atteintes à la protection des données de la LPRPDÉ est de prévenir le risque de préjudice à l'endroit d'individus par suite d'une atteinte ou d'atténuer ce préjudice. L'on peut parfois réaliser cet objectif en exigeant d'une organisation qu'elle avise d'autres organisations en mesure de prévenir le risque de préjudice ou d'atténuer ce préjudice. L'organisation est par conséquent tenue en vertu de l'article 10.2(1) d'aviser tout tiers de la possibilité d'une atteinte préjudiciable à la protection des données si elle croit l'autre organisation en mesure de réduire le risque de préjudice pouvant résulter de l'atteinte ou d'atténuer ce préjudice.

De plus, l'article 10.2 (1) confère au gouvernement le pouvoir de spécifier les circonstances rendant la notification à un tiers obligatoire.

***10.2*(1)** *L'organisation qui, en application du paragraphe 10.1* (*3*)*, avise un individu d'une atteinte aux mesures de sécurité est tenue d'en aviser toute autre organisation, ou toute institution gouvernementale ou subdivision d'une telle institution, si elle croit que l'autre organisation, l'institution ou la subdivision peut être en mesure de réduire le risque de préjudice pouvant résulter de l'atteinte ou d'atténuer ce préjudice, ou si tout autre condition précisée par règlement est satisfaite.*

Considérations

Le programme de signalement volontaire des atteintes à la protection des données du CPVP recommande aux organisations de se demander s'il y aurait lieu de notifier les organisations suivantes de l'atteinte dans certaines circonstances :

- les policiers en cas de vols ou d'activités criminelles présumés;
- les compagnies d'assurances si les obligations contractuelles l'exigent;
- les ordres professionnels ou d'autres organismes de réglementation si les normes professionnelles ou d'application de la réglementation l'exigent;
- les compagnies émettrices de cartes de crédit, les institutions financières ou les agences d'évaluation du crédit si leur aide est requise pour communiquer avec les personnes concernées ou pour atténuer les préjudices;
- les syndicats ou d'autres unités de négociation si l'atteinte touche leurs membres.

En Alberta, il appartient au commissaire provincial de déterminer s'il y a lieu d'aviser d'autres organisations, et lesquelles. Rien n'indique dans la loi et les documents d'orientation connexes comment le déterminer.

Aux États-Unis, la plupart des lois des États exigent des organisations qu'elles informent les organismes d'application de la loi en cas de violation d'informations financières. De plus, de nombreuses lois d'États exigent la notification aux agences d'évaluation du crédit de toute atteinte à la protection des données d'un grand nombre de personnes, de 1 000 à 10 000 en l'occurrence.

La directive d'interprétation de la *Gramm-Leah-Bliley Act*[37] exige d'aviser les organismes d'application de la loi compétents en cas de soupçon d'activité criminelle dans une atteinte ou de preuve d'usurpation d'identité résultant de celle-ci.

La *Personal Data Notification and Protection Act*, à l'état de projet aux États-Unis, exigerait des organisations qu'elles informent les agences nationales d'évaluation du crédit de toute atteinte affectant plus de 5 000 personnes. Elles seraient également tenues d'aviser les autorités policières en cas d'atteinte affectant :

- plus de 500 000 personnes;
- toute base de données appartenant au gouvernement fédéral;

[37] Voir *Supplement A to Appendix B to Part 570 – Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* à l'adresse suivante: https://www.law.cornell.edu/cfr/text/12/part-570/appendix-B.

- les renseignements concernant les fonctionnaires fédéraux travaillant dans les domaines de la sécurité nationale ou de l'application de la loi.

Questions à débattre

Dix-neuvième question : Le règlement devrait-il spécifier les circonstances obligeant les organisations à systématiquement aviser les tiers d'une atteinte? Si oui, quelles sont ces circonstances?

Tenue de registres

En vertu de l'article 10.3 (1) de la LPRPDÉ, les organisations qui découvrent une atteinte aux mesures de sécurité doivent tenir et conserver un registre de toutes les atteintes ainsi découvertes, et ce, qu'elles concluent à l'issue de leur analyse situation que cette atteinte pose ou non un « risque réel de préjudice grave ».

L'article 10.3 (1) confère au gouvernement le pouvoir de spécifier les critères applicables à ce registre.

> ***10.3*(1)** *L'organisation tient et conserve, conformément aux règlements, un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elle a la gestion.*

Considérations

L'obligation pour une organisation d'ainsi tenir un registre de toutes les atteintes à la protection des données dont elle a la gestion vise un double objectif majeur. D'abord, cela permettra au commissaire de surveiller la conformité aux exigences de signalement et de notification énoncées à l'article 10.1 de la Loi. L'article 10.3(2) de celle-ci exige qu'à la demande du commissaire, l'organisation lui donne accès à son registre des atteintes à la protection des données ou lui en remette une copie.

En deuxième lieu, la nécessité de tenir des registres obligera l'organisation à documenter systématiquement les atteintes à la protection des données dont elle fait l'objet, quel qu'en soit le risque de préjudice ou la gravité. Cela lui permettra de déceler dans ses mesures de sécurité toute tendance dénotant l'existence d'un problème ou d'un manquement systémique. Elle sera ainsi à même d'agir pour corriger tout problème systémique afin d'éviter la répétition d'atteintes pouvant causer préjudice à des personnes.

Compte tenu de ce double objectif, le règlement devrait spécifier suffisamment les exigences de tenue de registres pour permettre au commissaire de surveiller efficacement le respect de la Loi et à l'organisation de déceler des difficultés à tendance systémique. En même temps, ces exi-

gences devraient être suffisamment souples et raisonnables afin d'en réduire au minimum le fardeau pour l'organisation.

Contenu des registres

Plusieurs cadres de signalement et de notification des atteintes à la protection des données exigent la tenue de registres. Dans bien des cas, ces registres sont requis pour qu'une organisation puisse justifier le fait de n'avoir pas déterminé nécessaire d'aviser de l'atteinte les personnes concernées.

Au Canada, par exemple, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick oblige l'organisation à tenir « un registre de toutes les atteintes à la sécurité des renseignements en consignant ces atteintes ainsi que les mesures correctives prises pour réduire le risque qu'elles se reproduisent »[38].

Aux États-Unis, les organisations doivent pouvoir démontrer qu'elles respectent les règles de notification en vertu de l'*American Reinvestment and Recovery Act* ou que l'utilisation ou la communication de renseignements non protégés ne constituait pas une atteinte. D'où l'exigence qui leur est faite de conserver des documents à l'appui[39]. Par exemple, une organisation qui a choisi de ne pas aviser les personnes concernées doit avoir au dossier une évaluation démontrant qu'il était peu probable que l'atteinte cause un risque.

En vertu de la *Directive vie privée et communications électroniques* de l'Union européenne[40], les organisations doivent « tenir à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier ». Il y est aussi stipulé que cet inventaire doit comporter « uniquement les informations nécessaires » pour permettre aux autorités nationales compétentes (homologues du commissaire à la protection de la vie privée du Canada) de vérifier le respect des exigences de notification des violations de données de la Directive. Les notes explicatives de cette exigence[41] disent que la tenue à jour de cet inventaire permet aux autorités nationales de vérifier si l'organisation respecte ses obligations en vertu de la Directive.

---

[38] Voir l'article 20(2) du *Règlement du Nouveau-Brunswick pris en vertu de la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* à l'adresse suivante : https://www.canlii.org/fr/nb/legis/regl/regl-du-n-b-2010-112/derniere/regl-du-n-b-2010-112.html.

[39] Voir la partie 164.404 de la *Health Breach Notification Rule* de la *Health Insurance Portability and Accountability Act* à l'adresse suivante : http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6 et la *Breach Notification Rule* du département américain de la Santé et des Services sociaux à l'adresse suivante : http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.

[40] Voir l'article 2 de la Directive 2009/136/CE.

[41] Cinquante-huitième considérant de la Directive 2009/136/CE.

Questions à débattre

Vingtième question : Le règlement devrait-il spécifier les champs de données des registres? Ou devrait--il prévoir une approche plus souple et demander « suffisamment d'information pour indiquer que l'atteinte ne présente pas de risque réel de préjudice grave » ou renfermer un libellé similaire à cet effet?

Vingt-et-unième question : En vertu du règlement, quelle information une organisation serait-elle tenue d'inclure dans un registre sur les atteintes à la protection des données?

Tenue de registres

Durant l'étude parlementaire de la *Loi sur la protection des renseignements personnels numériques*, certains intervenants ont exprimé leur préoccupation au sujet de certaines exigences touchant la tenue de registres sur les atteintes à la protection des données. Au nombre des questions soulevées figuraient :

- la période de conservation des registres;
- si certains membres de l'organisation ont l'obligation de tenir les registres et de les fournir au commissaire à la protection de la vie privée à la demande de celui-ci (soit les personnes que l'organisation a désignées pour veiller au respect de la LPRPDÉ ainsi que l'exige l'annexe A de celle-ci);
- si l'organisation doit tenir des registres sur les atteintes à la protection des données qui ont été signalées au commissaire à la protection de la vie privée;
- si l'obligation de tenir des registres ne s'applique qu'aux atteintes connues à la protection des données ou si elle s'applique aussi aux atteintes présumées (par exemple, les estimations relatives au courrier mal acheminé contenant des renseignements personnels);
- si les registres peuvent prendre la forme de récapitulatifs mensuels, trimestriels ou annuels des atteintes à la protection des données subies par l'organisation (contenant l'information requise pour chaque atteinte).

Questions à débattre

Vingt-deuxième question : Le règlement devrait-il préciser la durée de conservation des registres sur les atteintes à la protection des données? Si oui, quelle serait une période de conservation raisonnable?

Vingt-troisième question : Le règlement devrait-il préciser que les personnes qui sont désignées par l'organisation pour veiller au respect de la LPRPDÉ sont celles qui sont responsables de tenir les registres sur les atteintes à la protection des données et de les fournir au commissaire à la protection de la vie privée à la demande de celui-ci?

Vingt-quatrième question : Le règlement devrait-il préciser qu'une déclaration auprès du commissaire à la protection de la vie privée répond aux exigences de tenue de registres de l'article 10.3(1)?

Vingt-cinquième question : Le règlement devrait-il préciser que l'obligation de tenir un registre sur les atteintes à la protection des données ne s'applique qu'aux atteintes dont une organisation a bel et bien connaissance?

Vingt-sixième question : Le règlement devrait-il permettre que les registres sur les atteintes à la protection des données soient présentés sous forme de récapitulatifs périodiques regroupant l'information sur les atteintes à la protection des données que l'organisation a subies durant la période applicable? Ou devrait-il contraindre celle-ci à préparer un dossier pour chaque atteinte qu'elle a subie?

Autres sujets

Innovation, Sciences et Développement économique Canada (ISDE) vous saurait gré de bien vouloir lui faire part de toute autre question à considérer dans l'élaboration du règlement.

Le Ministère s'intéresse tout particulièrement aux enjeux et questions concernant spécifiquement :

- les secteurs d'activité particuliers;
- les organisations multinationales;
- les organisations exerçant au Canada des activités dans diverses juridictions;
- les petites et moyennes organisations.

Participer à la présente consultation

ISDE vous invite à lui faire parvenir vos avis et commentaires sur la question soulevée dans le présent document d'ici le 31 mai 2016. Vous pouvez acheminer vos observations sous forme électronique (en format Microsoft Word ou Adobe PDF), par courriel, ou en version papier, par la poste, aux adresses ci-dessous. Prière d'indiquer dans votre envoi si vous répondez à titre personnel ou au nom d'une organisation ainsi que le numéro de téléphone et l'adresse de courriel d'une personne-ressource de votre organisation pour toute question au sujet de votre envoi.

Veuillez noter que vos observations ou un résumé de celles-ci pourraient être publiés sur le site Web d'ISDE.

Adresse postale :

Consultations sur les atteintes à la protection des données
Direction de la politique sur la sécurité et la protection des renseignements personnels
Innovation, Sciences et Développement économique Canada
235, rue Queen
Ottawa (Ontario) K1A 0H5

Courriel :

ic.ised.breach-atteinte.isde.ic@canada.ca