La Revue du Barreau, tome 74

L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé

Auteur(s) : Aylwin, Antoine

Publié par : Barreau du Québec

Sujet(s) : Droits et libertés -- Droits démocratiques

[+] Table des matières

- Le défi du passage vers la nouvelle culture juridique de la justice participative
  Thériault, Michelle
- Chronique jurisprudentielle sur les sociétés de personnes : histoire d'une anomalie
  Bouchard, Charlaine
- La convocation de témoins extraprovinciaux : vers une meilleure harmonisation avec le reste du Canada?
  Faure, Gabriel ; Zucker, Noah
- Quels changements pour la recherche avec les modifications au Code civil du Québec?
  Shuang, Shuang ; Lévesque, Emmanuelle ; Sénécal, Karine
- La cession de contrats d'assurance par l'assureur : le chaînon manquant
  Prévost, Alain
- L'indépendance des tribunaux administratifs fédéraux et le lien avec le pouvoir exécutif : une relation parfois empreinte de friction
  Chênevert, Paul
- L'interdiction de la discrimination en emploi et les pratiques de recrutement et de sélection des PME assujetties au droit du travail québécois
  Denis, Pascale L. ; Asselin, Sophie ; Simard, Myriam ; Paré, Frédéric ; Benoit-Chabot, Gabrielle
- Le maintien des services essentiels à la lumière de Saskatchewan Federation of Labour
  Talarico, Andrea
- Métadonnées : Plaidoyer pour des mal aimées et des incomprises
  Gingras, Patrick ; Senécal, François
- Étude de la décision Gagné c. Société de l'assurance automobile du Québec : pourquoi la S.A.A.Q. devra modifier ses façons de faire en matière de saisie automobile
  Vigneault, Jean-Gabriel
- La confidentialité du processus de nomination des juges
  Huppé, Luc
- La défense de renonciation au Canada : le legs de l'arrêt Gauthier
  Raymond, Maxime
- La discrimination fondée sur le handicap ou le moyen pour y pallier : concepts fondamentaux et évolution

nécessaire
Drapeau, Maurice ; Aubry, Alexis

- L’obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé
Aylwin, Antoine
  - I. INTRODUCTION
  - II. LIGNES DIRECTRICES AU CANADA
    - 1. Au niveau fédéral
      - A. Limitation dans l'atteinte à la vie privée et évaluation préliminaire
      - B. Évaluation des risques associés à la brèche dans la protection des données
      - C. Notification
      - D. Prévention
    - 2. Au Québec
      - A. Lignes directrices et recommandations de la CAI
      - B. Orientations gouvernementales de 2015
    - 3. Autres provinces
  - III. OBLIGATIONS LÉGISLATIVES AU CANADA
    - 1. La *Personal Information Protection Act* de l'Alberta (« PIPA »)
    - 2. La *Loi sur la protection des renseignements personnels et la prévention du vol d'identité* du Manitoba (« LPRPPVI »)
    - 3. La *Loi sur la protection des renseignements personnels et les documents électroniques* fédérale (« LPRPDE »)
    - 4. Les obligations de notification dans les lois sectorielles sur la santé
      - A. Ontario
      - B. Terre-Neuve-et-Labrador
      - C. Nouveau-Brunswick
  - IV. CERTAINS MODÈLES INTERNATIONAUX
    - 1. La Californie
    - 2. Les autres États américains
    - 3. L'Union européenne
  - V. IMPACTS D'UNE VIOLATION DE LA CONFIDENTIALITÉ
  - VI. LES MODALITÉS POTENTIELLES
  - VII. CONCLUSION

- Pratique du droit et influence du comportement
Allamehzadeh, Mani

- L’art et la science de la négociation à l’ère du Nouveau Code de procédure civile. Les stratégies essentielles pour le juriste
Roberge, Jean-François ; Fraser, Véronique

Chroniques

- Droit international privé. Regards croisés sur l'application de l'entente France-Québec du 9 septembre 1977 en matière de reconnaissance et d'exécution des jugements
Mignon, Natacha ; Vuitton, Xavier Philippe

- Procédure civile. Communications entre avocats et experts : le privilège relatif au litige et les devoirs des experts

Caron, Sébastien C. ; Neelin, Elisabeth ; Rochon, Marie-Noël

L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé

Résumé

Les entreprises privées gèrent une quantité importante de renseignements personnels dans le cadre de leurs activités. Afin de protéger les personnes concernées, plusieurs mesures législatives ont été mises en place. À l'ère des banques de données informatiques connectées, la pression augmente pour une transparence accrue lorsque la confidentialité des renseignements personnels n'est pas préservée.

Le texte s'attarde à l'obligation de notification en cas de violation de la confidentialité des renseignements personnels. Au moment où le législateur québécois se questionne sur l'opportunité d'ajouter une telle obligation pour les organismes publics au Québec, nous abordons certaines lignes directrices et législations au Canada et à l'étranger. Ce texte traite ainsi des différentes modalités potentielles et l'auteur suggère un modèle approprié.

L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé

[Page 469]

I. INTRODUCTION

L'utilisation des technologies de l'information ne cesse de s'étendre et les violations de la confidentialité de renseignements personnels hébergés sur support informatique ont naturellement suivi la même tendance. Il suffit de mentionner la découverte de la vulnérabilité logicielle « Heartbleed » au mois d'avril 2014 pour saisir l'ampleur des risques d'accès aux renseignements personnels recueillis par les entreprises. La faille Heartbleed a affecté les données de millions d'internautes abonnés aux populaires sites web SoundCloud[1] et Reddit[2], ainsi que les utilisateurs des systèmes d'exploitation Android[3].

Plusieurs juridictions légifèrent pour obliger les entreprises à notifier les victimes d'un accès non autorisé à leurs renseignements personnels. De telles obligations commencent à être mises en place au Canada. Toutefois, plusieurs questions concernant les modalités de cette notification demeurent sans réponse. Les violations de la confidentialité devraient-elles être portées à la connaissance des victimes dans tous les cas ? À défaut d'une notification systématique, selon quels critères la violation de la confidentialité devrait-elle être évaluée ? Devrait-on notifier un organisme de réglementation ?

Afin d'approfondir la réflexion sur ces questions, cet article traite des sujets suivants :

- Une révision des lignes directrices au Canada en matière de violation de la confidentialité;
- Un recensement des obligations législatives de notification en cas de violation de la confidentialité existant au Canada;

[Page 470]

- L'identification de certains modèles internationaux sur la notification en cas de violation de la confidentialité;

- Une discussion sur les impacts d'une violation de la confidentialité pour une organisation;
- Un résumé des différentes modalités potentielles et nos commentaires sur le modèle approprié.

II. LIGNES DIRECTRICES AU CANADA

1. Au niveau fédéral

En 2007, le Commissariat à la protection de la vie privée du Canada a publié certaines directives destinées aux entreprises du secteur privé[4]. Pour le Commissariat, il y a atteinte à la vie privée lorsqu'il y a une collecte ou un accès non autorisé de renseignements personnels en violation des lois applicables en la matière[5]. Ces lignes directrices encouragent les organisations à prendre certaines mesures lors d'une violation de la confidentialité.

Les lignes directrices adoptées n'ont aucune portée obligatoire, mais servent de guide sur les meilleures pratiques à adopter selon le Commissariat à la protection de la vie privée du Canada.

Voici les quatre étapes du processus proposé dans ces lignes directrices :

A. Limitation dans l'atteinte à la vie privée et évaluation préliminaire

Le Commissariat recommande tout d'abord aux entreprises de mettre fin le plus rapidement possible à la violation de la confidentialité. Ainsi, la pratique qui a permis l'accès non autorisé aux renseignements personnels doit cesser immédiatement[6]. Les systèmes de sécurité en place doivent être inspectés pour corriger les

[Page 471]

lacunes qui ont permis la violation de la confidentialité. À partir du moment où l'accès non autorisé est arrêté, l'entreprise doit mener un processus d'enquête pour évaluer la situation. À cette fin, il est recommandé de désigner une personne ou une équipe chargée d'enquêter sur les circonstances entourant la violation de la confidentialité. De plus, les personnes concernées au sein de l'organisation devraient être mises au courant de la survenance de la violation de la confidentialité (départements informatique, juridique et de communication par exemple)[7].

Les organismes publics canadiens ont une obligation supplémentaire découlant de la *Trousse d'outils pour la gestion des atteintes à la vie privée* publiée par le Secrétariat du Conseil du Trésor du Canada en 2014[8]. En complément à ce qui précède, ces organismes doivent rédiger un rapport préliminaire dans le cadre de cette première étape[9]. La préparation d'un tel rapport pourrait également être utile pour une entreprise privée, pour mieux documenter la violation de la confidentialité, faciliter les communications avec les autorités de réglementation et les personnes concernées. Un tel exercice est utile dans l'objectif de limiter la responsabilité civile de l'entreprise.

B. Évaluation des risques associés à la brèche dans la protection des données

Afin de déterminer si les victimes doivent être notifiées, la deuxième étape propose l'identification des éléments suivants :

- **L'évaluation de la sensibilité des renseignements personnels en cause.** Certains renseignements sont plus sensibles que d'autres, tels que les données sur la santé, les pièces d'identité émises par le gouvernement ainsi que les numéros de comptes financiers[10]. Toutefois, une analyse contextuelle s'impose puisque le même type d'information pourrait être considéré plus ou moins sensible selon le contexte. Par exemple, la liste des noms et adresses des abonnés d'un journal ne serait pas

aussi sensible que la liste des abonnés qui ont demandé une interruption de service pendant une période donnée pour leurs

[Page 472]

vacances[11]. En matière de violation de la confidentialité, plus l'information est sensible, plus les risques de préjudice augmentent.

- **La cause et l'étendue de l'accès aux renseignements personnels.** La découverte de la cause et de l'étendue pourrait servir à déterminer s'il y a un risque que la violation de la confidentialité se reproduise dans le futur[12]. Dans le cas d'un problème systémique, le risque de récidive est beaucoup plus prononcé que dans les cas d'incidents isolés.

- **Les personnes concernées par l'accès.** Il faut identifier les renseignements personnels compromis et déterminer qui sont les personnes touchées par cette divulgation : des employés de l'entreprise, des fournisseurs de services, des clients ou d'autres individus.

- **Les préjudices prévisibles découlant de la violation de la confidentialité.** Est-ce que la violation de la confidentialité peut entraîner des risques pour la sécurité de la victime, des pertes financières ou bien une atteinte à sa réputation ? Le contexte peut aider à évaluer les préjudices potentiels plus précisément. Par exemple, la perte d'une liste d'abonnés à une publication spécialisée pour les personnes atteintes d'une maladie causerait un préjudice plus important que la perte d'une liste similaire d'abonnés à un journal national[13]. Les dirigeants de l'entreprise concernée doivent aussi anticiper la réaction du public au moment où les victimes seront notifiées de la divulgation non autorisée. Dans les cas extrêmes, les dirigeants doivent déterminer si la notification en elle-même poserait un risque pour la santé ou la sécurité publique.

C. Notification

Le Commissariat ne suggère aucune obligation systématique de notifier les personnes victimes d'une violation de la confidentialité. Il recommande plutôt de traiter la notification des violations de la confidentialité au cas par cas. Toutefois, le Commissariat demande à être avisé par l'entreprise dans tous les cas, même si les victimes ne sont pas notifiées[14].

[Page 473]

Afin de déterminer s'il faut notifier les individus victimes de violations de la confidentialité, les entreprises doivent considérer plusieurs facteurs. Tout d'abord, dans les cas où l'entreprise a une obligation contractuelle de notification, elle doit respecter cette obligation. Le Commissariat recommande également de notifier les personnes visées dans les cas où il existe un risque raisonnable de vol d'identité ou de fraude et lorsque la personne concernée risque de subir un dommage physique[15]. Un autre facteur identifié par le Commissariat est la capacité de l'individu, une fois informé de la violation de la confidentialité, d'éviter ou d'atténuer les dommages éventuels. Ainsi, dès que la violation de la confidentialité cause tous les dommages prévisibles avant que la victime puisse en être informée, la notification subséquente par l'organisation privée n'aurait aucun effet de prévention.

Lorsque l'entreprise décide d'informer les victimes de la violation de la confidentialité, la notification devrait être effectuée le plus rapidement possible afin que ces victimes puissent prendre les mesures nécessaires pour se protéger[16]. Il est à noter que dans les cas de vols ou d'activités criminelles présumés, le Commissariat suggère à l'entreprise d'aviser les services policiers de la faille de sécurité informationnelle.

Dans certaines circonstances, le Commissariat est d'avis que les organisations privées peuvent avoir tout intérêt à notifier les victimes d'une violation de la confidentialité, puisque le fait pour une entreprise de procéder à la notification des personnes concernées lui permet de démontrer sa transparence dans la gestion de l'incident. Ces actions pourraient ainsi avoir un impact favorable sur l'opinion et la confiance du public envers l'entreprise en question. L'opinion publique étant susceptible d'influencer concrètement les résultats financiers d'une entreprise, une notification rapide et efficace aux victimes pourrait s'avérer bénéfique pour l'entreprise[17].

Finalement, la notification est un mécanisme approprié afin de réduire la responsabilité civile de l'entreprise. Il est raisonnable

[Page 474]

de penser qu'à partir du moment où l'entreprise divulgue la violation de la confidentialité, les individus ne pourront plus se plaindre devant le tribunal d'avoir été laissés dans l'ignorance, sans pouvoir agir.

D. Prévention

Une fois la violation de la confidentialité contenue et les victimes informées, le Commissariat suggère l'élaboration d'un plan de prévention. Ce plan pourrait contenir plusieurs éléments tels qu'une vérification de la sécurité physique et technique de l'entreprise, un examen des pratiques de formation des employés ou une inspection des prestataires de services[18]. Il serait également pertinent pour les entreprises de mettre en place un registre des divulgations non autorisées afin de compiler les atteintes à la vie privée et d'atténuer les risques de récidive.

Ceci étant dit, il nous semble évident que la mise en place d'un plan de prévention proactive avant l'existence d'une violation de la confidentialité s'impose pour le prévenir, plutôt que la prise de mesures réactives après un tel événement.

2. Au Québec

Deux lois québécoises réglementent la protection des renseignements personnels, soit la ***Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels***[19] et la ***Loi sur la protection des renseignements personnels dans le secteur privé***[20]. Ces lois ne comportent pas actuellement d'obligation de notification aux victimes d'une violation de la confidentialité. La Commission d'accès à l'information (« **CAI ») invite** toutefois le gouvernement québécois à ajouter une telle obligation de notification dans la législation.

Dans l'intervalle, la CAI a publié en avril 2009 des lignes directrices sous la forme d'un « Aide-mémoire ».

[Page 475]

A. Lignes directrices et recommandations de la CAI

Les entreprises au Québec ont l'obligation de prendre les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels qu'elles détiennent[21]. Lorsque ces mesures de sécurité ne parviennent pas à prévenir une violation de la confidentialité, la CAI identifie six étapes pour réagir à la situation :

i. évaluation préliminaire de la situation;

ii. limiter l'atteinte à la vie privée;

iii. évaluer les risques;

iv. aviser les organisations et les personnes concernées;

v. évaluation approfondie de la situation et prévention; et

vi. suivi[22].

Les entreprises et les organismes peuvent également, sur une base volontaire, aviser la CAI de la survenance d'une violation de la confidentialité impliquant des renseignements personnels[23].

L'évaluation préliminaire se veut une étape d'enquête pour identifier les renseignements personnels concernés, les victimes, le contexte et les circonstances entourant la violation de la confidentialité. À cette étape, les autorités externes (service de police, la CAI) ainsi que les intervenants concernés à l'interne (dirigeants de l'entreprise, conseillers juridiques, etc.) peuvent être informés de la violation de la confidentialité[24]. En parallèle et en utilisant les résultats de l'enquête, la violation de la confidentialité doit être arrêtée. Ensuite, les risques d'effets préjudiciables sont évalués et l'entreprise doit décider s'il convient d'informer les personnes concernées de la violation de la confidentialité. La CAI recommande que les victimes reçoivent une notification dans les

[Page 476]

cas où la perte ou le vol de renseignements personnels présente un risque de préjudice[25]. Le terme « préjudice » n'est cependant pas défini dans cet *Aide-mémoire.* La Commission recommande d'envisager d'entrer en contact avec certains autres intervenants, tels que les agences de crédit, un cocontractant, ou un ordre professionnel[26]. Suite aux diverses notifications, il importe d'approfondir l'analyse des circonstances entourant la perte ou le vol, de formuler des recommandations relatives aux stratégies de prévention et de prévoir le suivi devant être effectué[27].

La CAI aborde la question de la notification des violations de la confidentialité de manière plus précise dans son rapport quinquennal publié en 2011[28]. Elle propose l'adoption d'une obligation de déclaration des violations de la confidentialité à la CAI et, dans certaines circonstances, aux victimes[29]. L'obligation de déclarer les violations de la confidentialité aurait un caractère curatif et renforcerait l'obligation préventive de mise en place des mesures de sécurité adéquates[30]. Pour la CAI, l'instauration de cette obligation aurait plusieurs effets bénéfiques tels que la réduction des répercussions négatives relatives au vol d'identité et l'amélioration de la confiance des citoyens envers les entreprises qui collectent leurs renseignements personnels[31].

La Commission propose un mécanisme en deux étapes. En premier lieu, la *Loi sur l'accès* et la *Loi sur le secteur privé* créeraient l'obligation de déclarer à la Commission toute violation de la confidentialité présentant un risque pour des renseignements personnels[32]. En deuxième lieu, la CAI déterminerait si les victimes doivent être notifiées compte tenu des mesures prises pour limiter la violation de la confidentialité et de la sensibilité des renseignements personnels en question[33]. Seule la CAI serait habilitée à ordonner une telle notification; les entreprises et organismes conserveraient par contre la liberté de notifier les victimes de leur propre chef.

[Page 477]

B. Orientations gouvernementales de 2015

En 2015, le gouvernement québécois a diffusé de nouvelles orientations relatives au respect du droit à la vie privée[34]. Ce communiqué expose uniquement les positions du gouvernement quant aux devoirs des organismes publics en matière de protection des renseignements personnels. Le gouvernement mentionne qu'il entend poursuivre sa réflexion au sujet d'une modification éventuelle de la *Loi sur le secteur privé* afin de moderniser le régime de protection des renseignements personnels détenus par les entreprises[35]. Nous croyons que certaines orientations

relatives aux organismes publics indiquent les approches que le gouvernement provincial risque de favoriser lors de sa réflexion sur la législation du secteur privé.

La 17e recommandation des orientations gouvernementales est la suivante : « Obliger les organismes publics à gérer de façon transparente les incidents de sécurité portant sur des renseignements personnels »[36]. Plus précisément, le gouvernement annonce vouloir inclure une nouvelle section dans la *Loi sur l'accès* qui porterait sur la déclaration des violations de la confidentialité ainsi que des dispositions pour obliger les organismes publics à informer les victimes et la CAI de la survenance de tels événements[37]. Les individus victimes d'une violation de la confidentialité seraient ainsi notifiés dès que l'incident pose un risque d'atteinte à la vie privée et à la protection des renseignements. La Commission aurait de son côté l'obligation de publier un répertoire des violations de la confidentialité présentant un risque d'atteinte significative aux droits des victimes sur son site Web[38]. Ainsi, le gouvernement ne semble pas retenir la possibilité d'imposer une notification automatique.

Le Québec semble donc être sur le point d'adopter des modifications législatives qui s'inscrivent dans un courant de transparence

[Page 478]

modelé sur la législation albertaine[39], qui prévoit une obligation de divulgation des violations de la confidentialité des renseignements détenus par les entreprises du secteur privé. Un projet de loi est attendu dans les prochains mois pour en dévoiler les modalités particulières, suite aux travaux de la Commission des institutions, qui a tenu des consultations publiques tenues durant le mois de septembre 2015.

3. Autres provinces

D'autres provinces ont publié des directives destinées tant aux organismes publics qu'aux entreprises du secteur privé relativement aux étapes à suivre lors d'une violation de la confidentialité. En général, les orientations des gouvernements provinciaux en question s'inspirent des directives publiées par le Commissariat fédéral en 2007. Par exemple, la Colombie-Britannique identifie les mêmes quatre étapes : (i) limitation de la violation de la confidentialité, (ii) évaluation des risques y associés, (iii) notification, et (iv) prévention[40]. Cependant, le gouvernement de la Colombie-Britannique fournit des explications supplémentaires relatives aux cas où la notification des victimes affectées devient nécessaire. Les lignes directrices prévoient une notification obligatoire (« notification of the individuals affected *must occur »)* dans tous les cas où la loi ou un contrat impose une telle notification[41]. En l'absence d'une obligation légale ou contractuelle, les organisations ont le choix de faire une notification ou non. Pour prendre cette décision, l'organisation devrait évaluer la possibilité d'un risque de vol d'identité, de préjudice physique, d'humiliation, d'atteinte à la réputation, ou de perte d'opportunités d'affaires.

Quant à lui, le gouvernement ontarien identifie seulement deux étapes à suivre en cas de violation de la confidentialité : (i) maîtrise de la situation, et (ii) notification[42]. Le contenu de ces

[Page 479]

deux étapes reflète grandement les étapes correspondantes dans les lignes directrices exposées jusqu'à présent. Toutefois, lorsque des informations financières sont concernées, les directives ontariennes prévoient que l'entreprise encourage les individus affectés à contacter leurs institutions financières directement[43]. En Colombie-Britannique, les orientations gouvernementales suggèrent aux entreprises de contacter les assureurs et les institutions financières des victimes[44], et cela même à l'insu de celles-ci. L'approche de l'Ontario semble reposer davantage sur le consentement des victimes et leur donner un rôle actif dans la réparation.

Certaines juridictions ont décidé d'introduire des obligations légales afin d'encadrer le processus de notification des personnes concernées par les violations de la confidentialité. C'est ce que nous allons voir dans la prochaine section.

III. OBLIGATIONS LÉGISLATIVES AU CANADA

1. La *Personal Information Protection Act* de l'Alberta (« PIPA »)

L'Alberta est la première juridiction canadienne à avoir implanté en mai 2010 une obligation de notification des violations de la confidentialité. La PIPA prévoit un mécanisme en deux étapes. En premier lieu, l'entreprise doit en informer le commissaire à la vie privée de l'Alberta, lorsqu'il y a un « réel risque de préjudice grave » :

> 34.1 (1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure[45], (nos soulignements)

En deuxième lieu, dès que l'entreprise avise le commissaire à la vie privée de l'Alberta de la violation de la confidentialité, ce dernier doit décider s'il convient d'obliger l'entreprise en question

[Page 480]

à notifier les victimes[46]. Le législateur albertain a décidé de renforcer cette obligation avec la possibilité d'imposer une pénalité pouvant s'élever à 100 000 $ dans les cas où les entreprises manquent à leur devoir d'informer le commissaire à la vie privée[47]. Les entreprises peuvent également décider d'informer les victimes de la violation de la confidentialité avant même de notifier le commissaire à la vie privée de l'Alberta[48].

Afin d'interpréter le critère de « réel risque de préjudice grave », le gouvernement albertain a publié des directives d'interprétation.

D'une part, le préjudice grave (« significant harm ») réfère à un préjudice qui a des conséquences importantes pour la victime, notamment une perte de revenus, un vol d'identité, une atteinte à l'intégrité physique, ou une atteinte à la réputation personnelle ou professionnelle[49]. Par exemple, le préjudice qui pourrait découler de la perte d'un numéro d'assurance sociale (NAS) peut être considéré comme grave, puisque la victime s'expose à un risque de fraude ou de vol d'identité. Le paragraphe 34.1(1) prévoit un critère objectif pour déterminer si la violation de la confidentialité doit être communiquée au commissaire : une personne raisonnable considérerait-elle que le préjudice en question comporte des conséquences graves pour les victimes[50] ? Puisqu'il s'agit d'un critère objectif, l'identité de la victime importe peu. Cependant, le contexte général et les circonstances de la violation de la confidentialité doivent tout de même être appréciés. Ainsi, la perte d'une liste de clients appartenant à un refuge pour femmes victimes de violence conjugale comporterait des conséquences beaucoup plus importantes que la perte d'une liste de membres d'un centre de conditionnement physique[51].

D'autre part, le concept du risque réel (« real risk ») équivaut à un degré raisonnable de probabilité que le préjudice grave en question surviendra. Par exemple, dans la mesure où les données

[Page 481]

sont recouvrées avant qu'un tiers puisse y accéder, ce critère ne serait pas rempli. Le risque réel ne peut être

hypothétique, théorique ou spéculatif[52]. Tout comme le critère pour la gravité du préjudice, il s'agit d'un critère objectif. Les dirigeants de l'entreprise concernée doivent se demander si une personne raisonnable considérerait que la divulgation des renseignements en question comporte un risque réel d'occasionner un préjudice grave[53].

Entre mai 2010 et avril 2012, le commissaire à la vie privée de l'Alberta a reçu un total de 151 déclarations de violation de la confidentialité. 63 de ces violations de la confidentialité présentaient un risque réel de préjudice grave et ont nécessité la notification des victimes[54]. Les motifs soutenant les décisions du commissaire de traiter ces violations de la confidentialité varient selon les circonstances. Cependant, dans la plupart des cas où l'information divulguée était hautement sensible, notamment la perte d'un NAS en combinaison avec un autre identifiant personnel, le commissaire a décidé qu'il existait un risque réel de préjudice grave et a ordonné que les victimes soient informées[55]. Au contraire, dans le cas de renseignements sensibles cryptés ou protégés d'une manière similaire, le commissaire a généralement conclu qu'il n'y avait aucun risque réel de préjudice grave[56].

2. La *Loi sur la protection des renseignements personnels et la prévention du vol d'identité* du Manitoba (« LPRPPVI »)

En 2013, la *Loi sur la protection des renseignements personnels et la prévention du vol d'identité* du Manitoba a reçu la sanction royale, mais n'est toujours pas en vigueur à ce jour. Cette loi contient une obligation de notification des violations de la confidentialité pour les entreprises privées. L'obligation contenue dans la LPRPPVI diffère de celle contenue dans la PIPA de l'Alberta :

> 34. (2) Une organisation doit, dès que possible et de la manière prescrite, aviser un particulier si des renseignements personnels le

[Page 482]

> concernant et qui relèvent d'elle sont volés ou perdus ou si ces renseignements font l'objet d'un accès non autorisé[57].

Il appert que la législation manitobaine n'impose aucun devoir de notification à un organisme de réglementation, tel le Bureau de l'Ombudsman de la province. La disposition prévoit plutôt l'obligation de l'organisation privée de notifier directement les victimes.

L'obligation de divulgation proposée par la LPRPPVI ne comporte aucune balise quant au type de violation de la confidentialité qui doit faire l'objet d'une notification. Ainsi, le critère du risque réel de préjudice grave contenu dans la PIPA de l'Alberta n'est pas été repris par le législateur manitobain, ce dernier optant plutôt pour une obligation générale de notification. Les entreprises seraient alors contraintes de notifier les victimes de façon systématique.

La législation prévoit toutefois une exception à cette obligation de notification. Si l'entreprise privée « est convaincue que l'utilisation illégale des renseignements personnels est pratiquement impossible », elle n'est pas obligée de déclarer la violation de la confidentialité aux victimes[58]. Compte tenu du vocabulaire utilisé dans cette disposition, il est probable que l'emploi de cette exception pour éviter l'obligation de divulgation soit peu fréquent. Ainsi, la grande majorité des violations de la confidentialité devraient être communiquées aux victimes. On peut se questionner sur l'effet désensibilisant d'une obligation aussi étendue de notification auprès de la population de la province. De plus, l'utilisation d'un critère différent d'une province à l'autre risque de causer des maux de tête aux entreprises ayant des activités à l'échelle canadienne.

3. La *Loi sur la protection des renseignements personnels et les documents électroniques*

fédérale (« LPRPDE »)

Le 18 juin 2015, la *Loi sur la protection des renseignements personnels numériques* a reçu la sanction royale. Cette loi modifie

[Page 483]

plusieurs dispositions de la ***Loi sur la protection des renseignements personnels et les documents électroniques***[59]. Entre autres, le gouvernement fédéral a instauré une obligation de notification des violations de la confidentialité pour les entreprises privées. À l'instar de la loi manitobaine, les dispositions relatives à cette obligation ne sont pas en vigueur à ce jour. Les dispositions relatives à l'obligation de notification entreront en vigueur à une date ultérieure proclamée par décret.

Le législateur fédéral s'est inspiré du texte de la PIPA de l'Alberta pour élaborer le processus de notification de la **LPRPDE** :

> 10.1 (1) L'organisation déclare au commissaire toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu[60].

Ainsi, nous retrouvons le même critère du « risque réel de préjudice grave » pour baliser l'obligation de notification. Contrairement à la législation albertaine, la notion du « préjudice grave » est définie à même la loi fédérale. Il est indiqué qu'un tel préjudice vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation, la perte financière, le vol d'identité ainsi que la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles[61]. Le législateur fédéral a donc cru bon d'adopter une définition étendue afin d'assujettir les entreprises privées à une obligation de notification étendue.

Les facteurs servant à établir si une violation de la confidentialité présente un « risque réel » de préjudice grave sont identifiés comme étant : le degré de sensibilité des renseignements personnels en question, la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être, ainsi que tout autre élément prévu par règlement[62].

[Page 484]

Bien que l'obligation de notification contenue dans la **LPRPDE** soit similaire à celle de la PIPA de l'Alberta, elle comporte néanmoins quelques différences :

- La loi énonce deux obligations de notification distinctes et indépendantes. Le premier paragraphe de l'**article 10.1** de la **LPRPDE** prévoit que l'entreprise victime de l'atteinte aux mesures de sécurité doit notifier le Commissariat à la protection de la vie privée dans les cas où elle juge qu'il existe un risque réel de préjudice grave à l'endroit des individus concernés. En parallèle, l'entreprise doit également notifier directement les victimes, à moins qu'une règle de droit ne l'interdise[63];

- La **LPRPDE** prévoit une obligation de notification sous-jacente à des tiers. Lorsque l'entreprise est d'avis que la violation de la confidentialité présente un risque réel de préjudice grave et notifie les victimes, elle doit également aviser toute autre organisation ou institution gouvernementale susceptible d'être en mesure de réduire le risque ou d'atténuer le préjudice en question[64]. D'autres organisations, notamment les agences de crédit et les institutions financières, pourront alors avoir accès à certains renseignements personnels de la victime sans consentement;

- La **LPRPDE** oblige les entreprises à tenir un registre de toutes ses violations de la confidentialité[65]. Cette disposition ne fait aucune distinction entre les violations de la confidentialité comportant des risques réels de préjudice grave et les événements ne satisfaisant pas ce critère. Ainsi, l'organisation doit cataloguer chaque violation de la confidentialité qu'elle subit, peu importe son importance à l'égard des victimes. On peut penser que le contenu de ce registre pourrait être potentiellement invoqué contre l'entreprise dans le cadre d'un litige portant sur une atteinte aux mesures de sécurité dans la mesure où l'avocat du plaignant requiert la production du registre pendant le processus de communication de la preuve[66].

[Page 485]

4. Les obligations de notification dans les lois sectorielles sur la santé

Afin de faire un tour d'horizon complet des obligations de notification de violation de la confidentialité, nous tenons à mentionner au passage les trois lois sectorielles provinciales qui s'appliquent à des renseignements sur la santé principalement détenus par des organismes du secteur public.

A. Ontario

La *Loi de 2004 sur la protection des renseignements personnels sur la santé*[67] de l'Ontario prévoit une obligation de notification à son article 16(2) :

> 16(2) Le dépositaire de renseignements sur la santé qui utilise ou divulgue des renseignements personnels sur la santé sans le consentement du particulier qu'ils concernent d'une manière qui ne correspond pas à l'exposé de ses pratiques relatives aux renseignements visés à l'alinéa (1)a) prend les mesures suivantes :
>
> a) il informe le particulier des utilisations et des divulgations à la première occasion raisonnable, sauf si, en application de l'article 52, le particulier n'a pas le droit d'avoir accès à un dossier des renseignements;
>
> b) il prend note des utilisations et des divulgations;
>
> c) il verse la note aux dossiers de renseignements personnels sur la santé concernant le particulier, dont il a la garde ou le contrôle, ou la consigne sous une forme qui est liée à ces dossiers.

Il est intéressant de noter que ce mécanisme prévoit une notification systématique de toute utilisation ou divulgation des renseignements personnels sans consentement. C'est le mécanisme le plus étendu dans les obligations législatives recensées. La loi ne prévoit aucun critère relatif à l'existence d'un préjudice et on inclut sans ambiguïté l'utilisation sans consentement pour déclencher l'obligation de notification. De plus, une autre obligation s'ajoute, soit celle de documenter au dossier du patient la violation de la confidentialité. Cette obligation peut se comprendre dans un contexte de dossier de santé, mais est probablement difficilement applicable en dehors de ce contexte.

[Page 486]

B. Terre-Neuve-et-Labrador

La *Personal Health Information Act*[68] de Terre-Neuve-et-Labrador adoptée en 2008 prévoit ce qui suit à son article 15(3) à (7) au sujet de l'obligation de notification :

(3) Except as otherwise provided in subsections (6) and (7), a custodian that has custody or control of personal health information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is

(a) stolen;

(b) lost;

(c) disposed of, except as permitted by this Act or the regulations; or

(d) disclosed to or accessed by an unauthorized person.

(4) Where a custodian reasonably believes that there has been a material breach as defined in the regulations involving the unauthorized collection, use, or disclosure of personal health information, that custodian shall inform the commissioner of the breach.

(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by a custodian is not required, the commissioner may recommend that the custodian, at the first reasonable opportunity, notify the individual who is the subject of the information.

(6) Where a custodian is a researcher who has received personal health information from another custodian under section 44, he or she may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the custodian who provided the information to the researcher first obtains the individual's consent to contact by the researcher and informs the researcher that the individual has given consent.

(7) Subsection (3) and subsection 20(3) do not apply where the custodian reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal health information will not have an adverse impact upon

[Page 487]

(a) the provision of health care or other benefits to the individual who is the subject of the information; or

(b) the mental, physical, economic or social well-being of the individual who is the subject of the information.

La notion de « material breach » est définie à l'article 5 du *Personal Health Information Regulations*[69] *:*

5. The factors that are relevant to determining what constitutes a material breach for the purpose of subsection 15(4) of the Act include the following:

(a) the sensitivity of the personal health information involved;

(b) the number of people whose personal health information was involved;

(c) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and

(d) whether the cause of the breach or the pattern of breaches indicates a systemic problem.

Nous notons que la liste des incidents donnant lieu à une obligation de notification est spécifiquement prévue. On prévoit une notification à la personne concernée à la première éventualité et la notification au Commissaire à la vie privée provincial en cas de « material breach », tel que défini par règlement. Il est intéressant de noter les quatre critères retenus : la sensibilité des renseignements, le nombre de victimes, le risque d'utilisation préjudiciable et la présence d'un problème systémique. On peut toutefois critiquer le fait que la pondération de ces différents critères ouvre la porte à des difficultés d'application pratique afin de savoir quelle combinaison de ces facteurs entraîne l'obligation de notification.

Il y a une exception à l'obligation de notification en l'absence de préjudice. Le Commissaire à la vie privée se réserve toutefois la discrétion de recommander la notification aux victimes de la violation de la confidentialité.

[Page 488]

C. Nouveau-Brunswick

En 2010, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*[70] du Nouveau-Brunswick est entrée en vigueur avec une obligation de notification prévue à l'article 49(1)c) :

> 49(1)c) de notifier, la personne physique visée par les renseignements personnels sur la santé et le commissaire, à la première occasion raisonnable et conformément aux règlements, que ces renseignements ont été :
>
> (i) volés,
>
> (ii) perdus,
>
> (iii) éliminés, sauf dans les cas permis par la présente loi,
>
> (iv) communiqués par une personne non autorisée ou que celle-ci y a eût accès; »

Cette disposition est complétée par l'article 19 *du Règlement général*[71] adopté en vertu de cette loi :

> 19(1) Si survient un cas de violation de la vie privée mentionnée au sous-alinéa 49(1)c)(i), (ii) ou (iii) de la Loi, le dépositaire des renseignements personnels sur la santé en avise à la première occasion raisonnable les personnes suivantes :
>
> a) celle qui est visée par les renseignements, que ce soit en personne, par téléphone ou par écrit;
>
> b) le commissaire.
>
> 19(2) Lorsqu'il donne un avis en vertu du paragraphe (1), le dépositaire fournit les renseignements suivants :
>
> a) le nom du dépositaire;
>
> b) le nom et les coordonnées de la personne désignée par le dépositaire pour répondre aux demandes de renseignements concernant les pratiques relatives aux renseignements qu'a adoptées le dépositaire;

[Page 489]

c) une description de la nature de la violation de la vie privée;

d) la date et le lieu de la violation de la vie privée;

e) la date à la laquelle le dépositaire a pris connaissance de la violation de la vie privée.

Dans cette obligation, on note une obligation systématique de notification, sans exception, dans des cas prévus spécifiquement à la loi. La notification se fait à la fois à la victime et au Commissaire à l'accès aux renseignements personnels sur la santé et à la protection de la vie privée de la province. Il est intéressant de noter que le règlement prévoit le contenu de l'avis envoyé aux victimes.

Il est légitime de se questionner sur la nécessité d'assujettir les organismes publics à une obligation de notification similaire à celle des entreprises privées. Il faut également se rappeler que les renseignements visés par ces lois sont sensibles, puisqu'ils portent sur la santé des personnes concernées. Nous retenons toutefois que ces trois mécanismes sont intéressants et ajoutent à la réflexion sur les modalités potentielles de la mise en place d'une obligation de déclarer les violations de la confidentialité.

IV. CERTAINS MODÈLES INTERNATIONAUX

1. La Californie

En 2002, la Californie fait figure de pionnière en se dotant d'une législation qui impose aux organismes publics et aux entreprises une obligation de notification des violations de la confidentialité aux victimes. En effet, le *California Civil Code* prévoit que toute entreprise qui détient des renseignements personnels numériques doit déclarer toute violation de la confidentialité aux personnes qui en sont victimes[72]. Le législateur californien y précise également les renseignements personnels assujettis à l'obligation de notification. L'entreprise doit informer une victime d'une violation de la confidentialité si son nom, en combinaison avec un autre élément d'information confidentielle (son numéro d'assurance sociale, son permis de conduire, ses données médicales, etc.), fait l'objet d'une violation de la confidentialité[73].

[Page 490]

Bien que la loi impose une obligation de notification au bénéfice de toutes les victimes de toute violation de la confidentialité, il est à noter que les autorités publiques sont informées uniquement dans certains cas. Seules les violations de la confidentialité affectant plus de 500 résidents californiens doivent être signalées au procureur général de la Californie[74]. La loi prévoit la notification du public en général dans les trois éventualités suivantes : la notification individuelle des victimes excède un coût de 250 000 $, le nombre de personnes à être notifiées dépasse 500 000, ou l'entreprise ne possède pas les informations de contact suffisantes[75]. Ces cas sont identifiés par le Code civil californien comme des incidents de notification alternative (« substitute notice »). La notification au public doit se faire à la fois par : (i) courriel aux personnes concernées, (ii) avis sur le site Web de l'entreprise affectée, (iii) déclaration de la violation de la confidentialité aux médias californiens d'envergure, et (iv) envoi de l'avis au *California Office of Privacy Protection*[76].

Chaque année, le procureur général, en collaboration avec le *California Office of Privacy Protection,* recense les données recueillies en vertu de l'obligation de notification des violations de la confidentialité. En 2013, la procureure générale de la Californie a reçu un total de 167 notifications de violation de la confidentialité impliquant les

renseignements personnels de plus de 500 résidents californiens[77], ce qui représente une augmentation de 28 % par rapport aux données de l'année précédente. Le nombre de déclarations auprès de la procureure générale en 2014 a totalisé 187, une augmentation supplémentaire de 12 %[78]. Les violations de la confidentialité demeurent un problème important en Californie, plus de 10 ans après la mise en place d'une obligation de notification. Le bureau de la procureure générale recommande l'implantation de mesures de sécurité plus efficaces et des solutions de cryptage plus avancées pour encoder les données personnelles recueillies. Il est également proposé à la législature

[Page 491]

californienne d'étendre l'obligation de notification des violations de la confidentialité à la procureure générale[79].

2. Les autres États américains

Depuis l'instauration du régime californien en 2002, 47 États américains ont adopté des lois similaires visant à encadrer la procédure appropriée de notification des violations de la confidentialité aux victimes. En général, les standards édictés par chacune des législatures ne diffèrent pas de façon importante. Toutefois, certains législateurs préfèrent l'adoption d'un standard d'application générale qui remplacerait les procédures de notification propres à chaque État. Lors du discours de janvier 2015 sur l'état de l'Union des États-Unis, le président Obama a incité le Congrès américain à adopter un règlement fédéral pour encadrer les violations de la confidentialité :

> No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids [...] I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks.[80]

Le gouvernement américain a présenté un projet de loi au mois de mars 2015 intitulé *Personal Data Notification and Protection Act of 2015* (« PDNPA »). La PDNPA est présentement à l'étude par le sous-comité de la Constitution et de la justice civile. Il est proposé dans ce projet de loi de contraindre toute entreprise qui recueille des données personnelles d'au moins 10 000 personnes au cours d'une période donnée de 12 mois d'informer les victimes de toute violation de la confidentialité[81]. La PDNPA prévoit également plusieurs exceptions à l'obligation de notification, telle que l'inexistence d'un risque raisonnable de préjudice à l'endroit des victimes[82], ou l'implantation par l'entreprise d'un programme de sécurité qui bloque la transmission non autorisée de renseignements personnels[83].

[Page 492]

Les partisans de la PDNPA font valoir que la mise en place d'un standard national pour la gestion des violations de la confidentialité aura des effets bénéfiques pour les entreprises qui desservent des clients domiciliés dans plusieurs États[84]. Bien que les différentes lois étatiques sont souvent similaires, il existe plusieurs différences au niveau pratique. Par exemple, les entreprises localisées à Washington D.C. qui recueillent les informations de clients résidant au Maryland ou en Virginie, des États voisins, doivent être au courant de trois régimes législatifs comportant tous leurs propres exigences réglementaires. En effet, le *District of Columbia Official Code* ne donne aucune indication quant au contenu de la notification à être faite aux victimes d'une violation de la confidentialité[85]. Au contraire, la *Personal Information Protection Act* du Maryland[86] et le *Code of Virginia*[87] prévoient des exigences précises quant au contenu de l'avis à être communiqué aux victimes (l'inclusion des détails de la violation de la confidentialité et des renseignements divulgués, les coordonnées de l'entreprise, le numéro de téléphone de la Federal Trade Commission, etc.). Le projet de loi fédérale, quant à lui, exige un contenu prédéterminé, de manière semblable aux lois du Maryland et de la Virginie. Ainsi, l'instauration d'un seul régime de notification des violations de la confidentialité uniformiserait les pratiques commerciales dans chaque État, ce qui créerait sans doute des gains en efficacité pour les entreprises.

3. L'Union européenne

Le système de protection de la vie privée présentement en vigueur dans l'Union européenne (« l'UE ») occasionne certains problèmes pour les entreprises assujetties. En raison de la proximité des pays, les entreprises européennes doivent connaître et s'adapter à chacun des 27 différents régimes et organismes de réglementation nationaux. Sur un territoire géographique restreint, cette fragmentation de la réglementation applicable entre les pays membres de l'UE entraîne des coûts administratifs importants pour les petites et moyennes entreprises (« PME »)

[Page 493]

ainsi qu'une difficulté supplémentaire pour ces dernières lorsque vient le temps de percer de nouveaux marchés[88]. En parallèle, les données révélées par la plus récente étude ordonnée par la Commission européenne indiquent un sérieux manque de confiance à l'endroit des compagnies qui détiennent les renseignements personnels de leur clientèle. En effet, les deux tiers (67 %) des personnes sondées se disent préoccupées par le manque de contrôle qu'elles peuvent exercer au niveau des renseignements communiqués sur l'Internet[89]. Qui plus est, sept citoyens sur dix (70 %) craignent que leurs renseignements personnels soient utilisés à des fins différentes de celles auxquelles ils ont consenti[90].

En 2012, la Commission européenne a entrepris un processus de modernisation du régime de protection de la vie privée avec un projet de règlement. Il y est proposé de réunir toutes les juridictions membres de l'UE sous une seule législation. Pareillement, les entreprises européennes seraient redevables à une seule entité de réglementation, soit celles du pays où est situé leur siège social[91]. De cette manière, les coûts administratifs et les délais de nature bureaucratique attribuables à une violation de la confidentialité touchant des victimes résidant dans plusieurs pays membres de l'UE seraient réduits considérablement. Il est estimé que cette harmonisation représenterait une épargne de 2,3 milliards d'euros par année[92]. À ce jour, le projet de règlement n'est pas en vigueur. Věra Jourová, Commissaire à la Justice, les Consommateurs et l'Égalité des Genres, annonçait en juin 2015 que la réforme sur la protection des renseignements personnels en question sera adoptée avant la fin de l'année 2015[93], ce qui n'est pas le cas.

La réglementation proposée inclut un nouveau régime de notification des violations de la confidentialité. En effet, l'article

[Page 494]

31 de la proposition de règlement présentée en janvier 2012 énonce :

> 31 (1) En cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 24 heures, la notification comporte une justification à cet égard[94].

Le règlement identifie le « responsable du traitement » comme étant la personne, l'entreprise ou l'agence qui détient les renseignements personnels et qui en détermine la finalité[95]. Pareillement, 1'« autorité de contrôle » est définie comme l'organisme de réglementation responsable de l'application de la législation dans le pays où se trouve le siège social de l'entreprise[96]. Il semble que l'obligation de notification proposée indique alors que *toute* violation de la confidentialité doit être communiquée à l'autorité compétente du pays où est domiciliée la compagnie. En effet, le modèle européen ne prévoit ni une balise au niveau du préjudice subi par la victime ni une au niveau de la sensibilité des renseignements concernés.

Une violation de la confidentialité ne devrait pas faire l'objet d'une notification systématique aux victimes. Le législateur européen n'impose ce fardeau aux entreprises que dans le cas où la violation de la confidentialité pose un risque pour la protection des renseignements personnels en question :

> 32 (1) Lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement, après avoir procédé à la notification prévue à l'article 31, communique la violation sans retard indu à la personne concernée[97].

Le critère proposé par le projet de règlement semble difficile d'interprétation. La méthode d'évaluation de la possibilité qu'une violation de la confidentialité porte atteinte à la protection des

[Page 495]

renseignements ou à la vie privée d'un individu n'est pas définie au règlement. Qui plus est, certains pourraient même considérer que toute violation de la confidentialité peut « potentiellement porter atteinte aux données à caractère personnel ». Si la volonté du législateur européen est en fait d'obliger une notification systématique aux victimes, les conséquences pourraient être importantes pour les PME.

L'expérience aux États-Unis et au Canada semble démontrer que l'imposition de cette obligation vient augmenter le nombre de notifications, le risque de poursuites et de recours collectifs intentés par les victimes, ainsi que la demande pour des produits d'assurance en cyber-responsabilité[98]. Par ailleurs, l'instauration d'une telle obligation de divulgation pourrait même aller à l'encontre de l'objectif général de la réforme du régime de protection de la vie privée, soit la réduction d'obstacles administratifs et bureaucratiques imposés aux entreprises. Il est à noter que le projet de règlement prévoit une exception particulière à l'obligation de notifier les victimes. Si l'entreprise peut démontrer, à la satisfaction de l'autorité de réglementation, qu'elle a mis en œuvre des mesures de protection technologiques et que les renseignements divulgués bénéficient de ces mesures, la communication d'une violation de la confidentialité aux personnes concernées ne serait pas nécessaire[99]. Ce critère risque de poser de sérieux défis d'application.

V. IMPACTS D'UNE VIOLATION DE LA CONFIDENTIALITÉ

La notification d'une violation de la confidentialité aux victimes est une arme à double tranchant pour les entreprises. D'une part, une réaction rapide et efficace peut avoir pour effet de mitiger les dommages, notamment en communiquant aux victimes les mesures de prévention nécessaires afin d'éviter un préjudice.

D'autre part, la notification donnera bien souvent des munitions à qui souhaite intenter une action en justice contre l'entreprise, y compris une action collective. Au cours des dernières années, plusieurs actions en justice relatives à l'accès

[Page 496]

inapproprié à des renseignements personnels ont été intentées devant les tribunaux, incluant dans les circonstances suivantes :

1. En décembre 2006, l'accès sans autorisation aux numéros de carte de crédit de près de 2 millions de Canadiens détenus par les compagnies TJX (Winners, HomeSense, TJ Maxx)[100];

2. Entre 2011 et 2012, un conseiller de la Banque de Nouvelle-Écosse aurait transmis des

renseignements confidentiels de 643 clients à sa copine[101];

3. Entre 2011 et 2012, l'accès sans autorisation à 280 dossiers de patients du Peterborough Regional Health Center et la communication de certaines informations à des tiers[102];

4. En novembre 2012, le gouvernement fédéral aurait perdu un disque dur non crypté contenant les informations personnelles de 583 000 étudiants participant au programme de prêts et bourses. L'information contenue dans le disque dur inclut notamment les noms, dates de naissance et numéros d'assurance sociale des victimes[103];

5. Entre 2009 et 2013, près de 8 300 patients de l'hôpital Rouge Valley (en majorité des mères venant d'accoucher) ont vu leurs informations personnelles transmises à des entreprises privées impliquées dans la vente de régimes enregistrés d'épargne-étude[104];

6. À partir de novembre 2013, Bell Canada aurait recueilli les renseignements personnels et les données relatives à la navigation Internet de ses clients de téléphonie cellulaire sans leur consentement. Bell aurait ensuite procédé à la vente de ces informations à des compagnies publicitaires[105];

[Page 497]

7. À la fin 2013, la compagnie Target a subi une violation de la confidentialité impliquant les numéros de carte de crédit et de débit de près de 40 millions de ses clients[106]. Un règlement a été entériné le 19 mars 2015 pour un montant de 10 millions de dollars[107];

8. En avril 2014, des pirates informatiques ont accédé à l'information associée aux cartes de crédit et de débit de près de 4 millions de clients de Home Depot[108];

9. Durant l'été 2015, les renseignements personnels et financiers de 1,2 million d'utilisateurs du site Web controversé **AshleyMadison.com** ont été rendus publics sans consentement par des pirates informatiques[109].

Des actions collectives ont été intentées dans tous ces dossiers pour des montants de plusieurs millions de dollars.

L'obligation de notifier devrait ainsi normalement mettre de la pression sur les entreprises pour les forcer à exercer une meilleure prévention des risques de violation de la confidentialité. Cela s'applique dans un domaine où la jurisprudence n'est pas encore fixée sur la part de responsabilité que l'entreprise doit assumer dans le cadre d'une action en dommages.

D'un autre côté, il serait important de réfléchir à la façon appropriée de favoriser la collaboration des entreprises par certains incitatifs, afin d'éviter qu'elles fassent le calcul qu'il serait plus « payant » de ne pas divulguer une violation de la confidentialité, étant donné les conséquences potentielles au niveau civil.

VI. LES MODALITÉS POTENTIELLES

En résumé de ce qui précède, nous avons tenté de rassembler dans le tableau suivant les différentes modalités possibles d'une obligation de notification potentielle et nous avons indiqué en

caractère gras les modalités qui nous semblent les plus intéressantes :

QUAND notifier ?	• Tous les cas • Lorsque l'autorité de réglementation l'ordonne • Si la divulgation est utile • Risque de préjudice • Lorsque des renseignements sensibles sont en cause (selon une liste précise) • **Risque sérieux de préjudice grave** • Préjudice spécifique prévu : financier/physique/réputation • Lorsqu'il y a une obligation contractuelle
	• Et lorsque les démarches de confinement n'ont pas permis de limiter substantiellement les risques • Et critère de balance des inconvénients de la divulgation
A QUI notifier ?	• Registre interne • Organisme de réglementation • Institutions gouvernementales • Tiers privés (assureur, banque, agence de crédit) • **Victimes** • Grand public
QUOI notifier ?	• L'existence du bris • **Transparence sur la nature du bris et les informations connues** • Instructions pour réduire les impacts (banque, dossier de crédit, etc.)

	• Coordonnées pour avoir plus d'informations
COMMENT notifier ?	• Lettre • **Courriel** • Téléphone • Avis public

[Page 499]

À l'instar de la législation albertaine et de la législation fédérale, nous privilégions l'option prévoyant que l'obligation de notification existe lorsque la violation de la confidentialité donne lieu à un risque sérieux de préjudice grave. Tout d'abord, nous ne croyons pas qu'il soit opportun qu'une entreprise doive notifier les victimes en l'absence de préjudice. Considérant les ressources nécessaires pour respecter cette obligation, cela nous semble un mauvais investissement. Ensuite, nous croyons utile de noter l'existence d'un risque sérieux, encore une fois afin d'éviter de créer un sentiment de panique chez les victimes, alors que la survenance d'un préjudice éventuel serait au mieux hypothétique. Étant donné que chaque violation de confidentialité diffère, il nous semble hasardeux de vouloir définir plus précisément le type de bris donnant lieu à une obligation de notification. L'expérience albertaine paraît fonctionner, ce qui démontre que ce critère semble un bon équilibre afin d'atteindre l'objectif poursuivi. Toutefois, pour des considérations pratiques, notamment au niveau du délai, nous croyons que l'entreprise devrait être en mesure de prendre la décision de notifier elle-même, sans attendre la décision d'un organisme de réglementation.

Nous estimons que les victimes devraient être notifiées en premier lieu. En effet, nous croyons que l'obligation de notification doit d'abord servir à notifier ces personnes, afin qu'elles puissent prendre les mesures qui s'imposent et être sur leurs gardes, et ainsi réduire tout potentiel de préjudice, dans la mesure du possible. Puisque la prévention du préjudice (fonction curative) est selon nous au cœur de l'obligation de notification, nous ne croyons pas que cet objectif pourrait être rempli de façon aussi efficace autrement.

Nous sommes d'avis que la notification devrait être suffisamment détaillée afin que les personnes concernées comprennent le risque en cause. En effet, une invasion dans une base de données par des pirates qui ont annoncé vouloir utiliser les données à mauvais escient ne comporte pas le même risque que la perte d'une clé USB dans un endroit inconnu. Il nous semble que la transparence sur les informations connues constitue également la meilleure façon de gérer les attentes des personnes concernées envers l'entreprise. À cela peuvent s'ajouter d'autres informations complémentaires afin de réduire les risques ou obtenir des ressources, mais cette portion de la notification peut être appelée à varier selon les circonstances. Nous croyons que des lignes directrices

[Page 500]

pourraient être développées par les organismes de réglementation afin de s'adapter au contexte changeant de la technologie. Nous trouvons intéressante l'approche préconisée au Nouveau-Brunswick et dans certains États américains, où la réglementation prévoit spécifiquement certaines informations à être divulguées dans l'avis de notification.

La notification peut se faire selon les moyens de communication accessibles à l'entreprise, selon les coordonnées qu'elle possède sur le client. Entre différentes options, nous croyons que c'est le moyen le plus rapide qui doit être

privilégié. Considérant l'utilisation importante du courriel dans les affaires, il nous semble que ce moyen serait vraisemblablement approprié dans de très nombreux cas afin d'atteindre l'objectif de célérité désiré.

Bien que certaines modalités doivent être prévues dans la législation, nous croyons important de rappeler que les organisations concernées doivent faire preuve de jugement et évaluer les mesures additionnelles requises dans les circonstances, comparativement au minimum prévu par la loi.

VII. CONCLUSION

La notification des violations de la confidentialité aux victimes de ceux-ci est un enjeu réglementaire pouvant être analysé de plusieurs perspectives. Du point de vue des victimes, toute divulgation des violations de la confidentialité à l'endroit de leurs renseignements personnels est souhaitable. Cette réalité est renforcée par la méfiance du public envers les entreprises qui récoltent des renseignements personnels. Du point de vue de ces entreprises, la notification aux victimes de chaque violation de la confidentialité, indépendamment de la gravité du bris en question, provoquerait des dépenses importantes et augmenterait les risques de poursuites mal fondées.

À notre avis, les modalités de notification doivent plutôt être établies en considérant conjointement les priorités des victimes et des entreprises.

Dans cet ordre d'idées, nous suggérons l'adoption d'une obligation de notification inspirée des différents modèles exposés jusqu'à présent, tant canadiens qu'internationaux. Afin de desservir les intérêts à la fois des victimes et des entreprises, il nous apparaît

[Page 501]

logique d'établir deux critères distincts relatifs à la notification à être faite à un organisme de réglementation et aux personnes victimes de la violation de la confidentialité.

En premier lieu, il reviendrait à l'entreprise d'évaluer non seulement la gravité du préjudice potentiel, mais également son risque de survenance. Tout comme ce que prévoient les modifications récentes à la loi fédérale (**LPRPDE**), l'entreprise informerait directement les victimes de la violation de la confidentialité si elle est d'avis que ce bris peut causer un préjudice grave. Ainsi, l'approche de la Commission d'accès à l'information exposée dans son rapport quinquennal en 2011 nous semble inadéquate. La décision de notifier les victimes de la violation de la confidentialité ne devrait pas incomber à la Commission, mais plutôt à l'entreprise qui a subi le bris en question et qui doit assumer ses responsabilités. De cette manière, l'entreprise pourrait éviter certaines dépenses supplémentaires relatives à la communication du bris à la Commission (temps consacré à la compilation de documents à être envoyés, obtention de rapports d'experts en cyber-technologie, autres coûts administratifs, etc.). Qui plus est, la notification directe aux victimes par l'entreprise serait nécessairement plus rapide que de passer par l'intermédiaire de la Commission, notamment dans un contexte où les ressources allouées aux activités de la Commission sont limitées. L'efficacité qui en résulterait s'inscrit dans un des objectifs identifiés par la Commission, soit celui de minimiser les conséquences qu'une violation de la confidentialité pourrait avoir pour les victimes et donner une chance à ces dernières de prévenir toute aggravation du préjudice déjà subi[110].

Nous sommes également d'avis que les violations de la confidentialité divulguées aux victimes doivent se limiter à ceux qui comportent un risque réel de préjudice grave. Ce critère d'inspiration albertaine représente l'équilibre idéal entre les intérêts des victimes et ceux des entreprises qui détiennent leurs renseignements personnels. Si chaque violation de la confidentialité était communiquée aux victimes, peu importe la gravité des dommages qui pourraient en découler, ces dernières risqueraient de devenir désensibilisées aux violations de la confidentialité qui les concernent,

ce qui constitue une critique fréquente du modèle californien qui prévoit une obligation de notification plus étendue. En

[Page 502]

limitant le nombre de violations de la confidentialité communiqué, le risque de désensibilisation serait donc limité.

Enfin, les violations de la confidentialité représentent un problème important. En raison des développements au niveau des technologies de l'information, l'incitation pour les citoyens de communiquer leurs renseignements personnels sur une plateforme technologique ne cessera d'augmenter dans les prochaines années. Dans cette optique, plusieurs entreprises songent déjà à mettre en œuvre des mesures de sécurité responsables telles que la modernisation de l'infrastructure informationnelle, l'embauche et la formation de personnel qualifié, ainsi que l'élaboration de nouvelles politiques internes[111]. Quoi qu'il en soit, les législatures provinciales devraient songer, lorsqu'elles adoptent des modifications à la réglementation en matière de protection des renseignements personnels, comme ce sera le cas sous peu au Québec, à y inclure une obligation de notification appropriée à la réalité des entreprises et des citoyens qui y sont assujettis. Finalement, l'harmonisation des dispositions à l'échelle nationale devrait être un objectif sérieusement envisagé pour simplifier et améliorer la conformité à de telles obligations.

---

[*] L'auteur tient à remercier l'étudiant en droit Jonathan Raizenne pour sa contribution dans le cadre de la recherche et de la rédaction du présent article, ainsi que Karl Delwaide et Francis Barragan pour leurs commentaires.

1. Brendan Codey, « Security Update: We're Going to Sign out Everyone, Here's Why » (9 avril 2014), *The SoundCloud Blog* (blogue), en ligne : https://blog.soundcloud.com/2014/04/09/heartbleed/>.

2. alienth, « we Recommend That You Change Your Reddit Password » (14 avril 2014), publié sur *Announcements,* en ligne : Reddit http://www.reddit.com/r/announce_ents/comments/231hl7/we_recommend_that_you_change_your_reddit_password>.

3. Charles Arthur, « Heartbleed makes 50m Android phones vulnerable, data shows » (15 avril 2014), *The Guardian,* en ligne : http://www.theguardian.com/technology/2014/apr/15/heartbleed-android-phones-vulnerable-data-shows>.

4. Canada, Commissariat à la protection de la vie privée du Canada, *Lignes directrices : Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée,* Gatineau, 1er août 2007. Rappelons que la loi fédérale s'applique à toutes les entreprises au Canada, à l'exception des activités d'une entreprise dans une province pour laquelle un décret d'exclusion a été adopté, soit principalement la Colombie-Britannique, l'Alberta et le Québec.

5. *Ibid* à la p 1.

6. *Ibid* à la p 2.

7. *Ibid.*

8. Canada, Secrétariat du Conseil du Trésor du Canada, *Trousse d'outils pour la gestion des atteintes à la vie privée,* Ottawa, SCT, 20 mai 2014, en ligne : http://www.tbs-sct.gc.ca/atip-aiprp/tools/pbmt-togap/pbmt-togappr-fra.asp>.

9. *Ibid.*

10. *Supra* note 4 à la p 3.

11. *Ibid.*

12. *Ibid.*

13. *Ibid* à la p 4.

14. *Ibid.*

15. *Ibid* à la p 5.

16. *Ibid* aux pp 4-5.

17. Éloïse Gratton et Frédérick Néron, « Bris de sécurité informationnelle : étapes à suivre et gestion de risques » dans Service de la formation continue du Barreau du Québec, *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014),* Cowansville, Éditions Yvon Biais, 2014, à la p 45.

18. *Supra* note 4 à la p 8.

19. **RLRQ c A-2.1** *[Loi sur l'accès].*

20. **RLRQ c P-39.1** *[Loi sur le secteur privé].*

21. *Ibid,* art 10.

22. Québec, Commission d'accès à l'information, *Aide-mémoire à l'intention des organismes et des entreprises : Que faire en cas de perte ou de vol de renseignements personnels ?,* Montréal, CAI, 2009.

23. Québec, Commission d'accès à l'information, *Rapport quinquennal 2011 : Technologies et vie privée à l'heure des choix de société,* Montréal, CAI, 2011 à la p 38.

24. *Supra* note 22 à la p 2.

25. *Ibid* à la p 4.

26. *Ibid.*

27. *Ibid* aux pp 5-6.

28. *Supra* note 23.

29. *Ibid* à la p 37.

30. *Ibid* à la p 39.

31. *Ibid* à la p 41.

32. *Ibid* à la p 42.

33. *Ibid.*

34. Québec, Ministère du Conseil exécutif, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels,* Québec, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques, 2015.

35. *Ibid* à la p 8.

36. Québec, Ministère du Conseil exécutif, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels : Synthèse,* Québec, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques, 2015 à la p 24.

37. *Supra* note 34 à la p 109.

38. *Ibid.*

39. *Supra* note 34 à la p 107.

40. Colombie-Britannique, Office of the Information and Privacy Commissioner for British Columbia, *Privacy Breaches: Tools and Resources,* Victoria, OIPC, 2 avril 2012 à la p 3.

41. *Ibid* à la p 21.

42. Ontario, Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Protocole en cas de violation de la vie privée Lignes directrices pour les institutions gouvernementales,* Toronto, CIPVPO, 1er décembre 2006 (révisé mai 2014). Malgré son titre, le commissaire précise que ces directives peuvent être utilisées par toute organisation.

43. *Ibid* à la p 2.

44. *Supra* note 42 à la p 11.

45. *Personal Information Protection Act,* **SA 2003, c P-6.5**, art 34.1.

46. Terry Gao et Rahim Esmail, « Clotting Heartbleed: Guidance on Privacy Brea-ches, Notification Obligations and Proposed Amendments to Privacy Legislation » (6 mai 2014), *Canadian Tech Law Blog* (blogue), en ligne : http://www.canadiantechlawblog.com/2014/05/06/clotting-heartbleed-guidance-on-privacy-breaches-notification-obligations-and-proposed-amendments-to-privacy-legislation>.

47. *Supra* note 45, art 59(1)(e.1), art 59(2)(b).

48. Alberta, Service Alberta, *Notification of a Security Breach : Personal Information Protection Act Information Sheet 11,* Edmonton, avril 2010 à la p 1.

49. *Ibid,* note 48 à la p 2.

50. *Ibid,* à la p 3.

51. *Ibid.*

52. *Ibid.*

53. *Ibid.*

54. Alberta, Office of the Information and Privacy Commissioner of Alberta, *Personal Information Protection Act: A Snapshot – Two Years of Mandatory Breach Reporting (May 2010 to Aprii 2012),* Calgary, OIPCA, 2012 à la p 1.

55. *Ibid,* à la p 3.

56. *Ibid.*

57. *Loi sur la protection des renseignements personnels et la prévention du vol d'identité,* **CPLM c P33.7**, art 34(2).

58. *Ibid,* art 34(3)(b).

59. **LC 2000, c 5**.

60. PL S-4, *Loi sur la protection des renseignements personnels numériques,* 2e sess, 41e parl, 2014, art 10.1(1) (sanction royale le 18 juin 2015).

61. *Ibid,* art 10.1(7).

62. *Ibid,* art 10.1(8).

63. *Ibid,* art 10.1(3).

64. *Ibid,* art 10.2(1).

65. *Ibid,* art 10.3(1).

66. Alex Cameron, Antoine Aylwin et Myriam Robichaud, « Loi sur la protection des renseignements personnels numériques : modifications importantes apportées à la législation canadienne en matière de protection des renseignements personnels » (6 juillet 2015), *Bulletin Protection de l'information et de la vie privée* (blogue), en ligne : http://www.fasken.com/fr/loi-protection-renseignements-personnels-numeriques-modifications-importantes-legislation-canadienne-protection-renseignements-personnels/>.

67. **LO 2004, c 3, ann A**.

68. **SNL 2008, c P-7.01**.

69. **NLR 38/11**.

70. **LN-B 2009, c P-7.05**.

71. **Règl du N-B 2010-112**.

72. Cal. Civ. Code § 1798.82(a) (1872).

73. *Ibid,* § 1798.82(h).

74. *Ibid,* § 1798.82(f).

75. *Ibid,* § 1798.82(j)(3).

76. É.-U., California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information,* janvier 2012, à la p 14.

77. É.-U., Office of the Attorney General, California Department of Justice, *California Data Breach Report : October 2014* à la p iv.

78. É.-U., Office of the Attorney General, *California Data Breach Statistics : January 2015,* à la p 1.

79. *Supra* note 77 à la p v.

80. Le président Barack Obama, allocution sur l'état de l'Union (2015), 20 janvier 2015 [non publiée], en ligne : https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015>.

81. É.-U, Bill HR 1704, *The Personal Data Notification and Protection Act of 2015,* 114e Cong, 2015, § 101(a).

82. *Ibid.*

83. *Ibid,* § 102(c)(1)(A).

84. Karla Grossenbacher, « Businesses need a preemptive federal law on data breach notification » (24 juillet 2015), *The Hill,* en ligne : http://thehill.com/blogs/congress-blog/judicial/248978-businesses-need-a-preemptive-federal-law-on-data-breach>.

85. D.C. Code, tit 28 § 3852.

86. Md. Code, Corn. Law § 14-3504 (2010).

87. Va Code Ann. § 18.2-186.6.

88. CE, Commission, *Comment la réforme de la protection des données dans l'Union sera-t-elle profitable aux entreprises européennes* ?, Bruxelles, CE, à la p 1.

89. CE, Commission, « Data protection Eurobarometer out today » (24 juin 2015), CE, en ligne : http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm>.

90. *Ibid.*

91. *Supra* note 88 à la p 2.

92. *Ibid.*

93. CE, Commission, « Remarks by Commissioner Jourovâ after the launch of the Data protection regulation trilogue » (24 juin 2015), CE, en ligne : http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm>.

94. CE, *Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* [2012], art 31.

95. *Ibid,* art 4(5).

96. *Ibid,* art 4(19).

97. *Ibid,* art 32(1).

98. *Supra* note 76 à la p 2.

99. *Supra* note 76, art 32(3).

100. *Wong v The TJX Companies Inc., Winners Apparel Inc.,* **2008 CanLII 3421 (ON SC)**.

101. *Evans v The Bank of Nova Scotia,* **2014 ONSC 2135 (CanLII)**.

102. *Hopkins v Kay,* **2014 ONSC 321 (CanLII)** et **2015 ONCA 112 (CanLII)**. La demande d'autorisation d'appel à la Cour suprême a été rejetée le 29 octobre 2015.

103. *Condon c. Canada,* 2014 CP 250 et 2015 CAP 159.

104. Commissariat à l'information et à la protection de la vie privée de l'Ontario, *PHIPA Order HO-013,* 16 décembre 2014, https://www.ipc.on.ca/images/Findings/ho-013.pdf>.

105. Commissariat à la protection de la vie privée du Canada, *Résultats de l'enquête sur le Programme de publicité pertinente de Bell lancée par le commissaire,* rapport n^{o} 2015-001, 7 avril 2015 https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_f.asp>.

106. *Zuckerman v Target Corporation,* **2015 QCCS 1285 (CanLII)**.

107. Hiroko Tabuchi, *$10 Million Seulement in Target Data Breach Gets Preliminary Approval,* New York Times, 19 mars 2015 http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html>.

108. *Yves Thériault c. The Home Depot Inc.,* C.S.M. 500-06-000711-149 (désistement entériné par la Cour le 1er septembre 2015).

109. Gabrielle Duchaine, *Affaire Ashley Madison : vers un recours collectif au Québec,* 28 août 2015, LaPresse.ca http://www.lapresse.ca/actualites/justice-et-affai res-criminelles/actualites-judiciaires/2 01508/28/01-4895984-affaire-ashley-madison-vers-un-recours-collectif-au-quebec.php>.

110. *Supra* note 22 à la p 41.

111. Voir Hernan Barros et Walid Hejazi, « 2014 TELUS-Rotman IT Security Study », 2015 [non publié], en ligne : http://business.telus.com/en/campaigns/rotman-study-2014> et Verizon, « 2015 Data Breach Investigations Report », 2015 [non publié], en ligne : http://www.verizonenterprise.com/DBIR/2015/>.

Barreau du Québec La Revue du Barreau est une publication du Barreau du Québec.