Le Canada Adopte des Lignes Directrices sur la Déclaration Obligatoire des Atteintes à la Protection des Données

21 mars 2018

Par Amanda Branch

La législation canadienne relative à la protection de la vie privée est à l'aube d'une transformation visant à exiger la notification d'une atteinte à la protection des données. L'objectif du projet de règlement est de guider les entreprises quant au moment et à la façon d'informer les consommateurs et le commissaire à la protection de la vie privée en cas de manquement à la sécurité. Le gouvernement a essayé de trouver un équilibre de façon à ce que les consommateurs soient informés explicitement de toute violation constituant un « risque réel de préjudice grave ». Si un bon équilibre est trouvé, les consommateurs prêteront attention et prendront des mesures pour se protéger et atténuer tout autre dommage. Dans le cas contraire, il y aura un déferlement d'avis, entraînant un véritable risque d'essoufflement du processus de notificatic

La déclaration obligatoire d'une atteinte à la protection des données est attendue depuis 2015, avec les amendements à la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRPDE »), la loi fédérale sur la protection des renseignements personnels qui régit les organismes du secteur privé. Toutefois, les dispositions sur l'avis de violation sont en attente jusqu'à ce que le règlement prenne effet. Le projet a été publié en septembre 2017 et le règlement entrera en vigueur en 2018.

Il existe actuellement dans presque l'ensemble du Canada un système de déclaration volontaire de violation, mais l'Alberta est la seule province à obliger une telle notification dans le secteur privé.

Une fois la nouvelle loi en vigueur, lorsqu'un organisme sera victime d'une atteinte aux mesures de sécurité susceptible de donner lieu à un « risque réel de préjudice grave », l'organisme devra (i) déclarer l'incident au Commissariat à la protection de la vie privée du Canada; (ii) aviser les personnes concernées; et (iii) aviser tout tiers qui est en mesure d'atténuer le risque de préjudice aux personnes concernées. Une telle notification devra être faite dès que possible après que l'organisme aura déterminé qu'une violation s'est produite.

Le règlement exige qu'au moment d'évaluer le risque, l'entreprise doit examiner, entre autres choses, le degré de confidentialité des renseignements et la probabilité que ceux-ci soient mal utilisés. Selon la loi, le « préjudice grave » se définit bien au-delà du simple « vol d'identité ». Il inclut l'humiliation, l'atteinte à la réputation ou aux relations, la perte d'emploi ou d'autres occasions, la perte financière, le vol d'identité, les effets négatifs sur le dossier de crédit et les dommages aux biens ou la perte de ceux-ci. Un « risque réel » peut même s'étendre à une intrusion dans les données chiffrées, une position que le gouvernement justifie par la possibilité que l'information soit déchiffrée.

Les entreprises seront également tenues de conserver un registre de tous les incidents d'infractions aux données pour un minimum de 24 mois (que l'entreprise décide ou non si la violation a généré un risque réel de préjudice grave aux personnes concernées) suivant le jour où l'organisme détermine qu'une violation s'est produite. Le commissaire peut demander et examiner l'historique des violations subies par une entreprise en particulier au cours des 24 mois précédents. Le registre doit contenir suffisamment de renseignements pour permettre au Commissaire de vérifier le respect du système de déclaration des violations.

La mise en œuvre de la notification obligatoire des atteintes à la protection des données vise à harmoniser la législation canadienne avec celle d'autres instances, y compris le Règlement général sur la protection des données (GDRP) de l'Union

européenne, qui entrera en vigueur en 2018, et comprend la déclaration obligatoire de telles atteintes. Plusieurs entreprises ont déjà mis en place des systèmes et des politiques pour contrôler, circonscrire et déclarer les violations, par exemple pour se conformer aux lois de l'Alberta et celles d'autres pays. Si ce n'est fait, il est maintenant temps d'y voir. Le règlement prévoit un report de la date d'entrée en vigueur après la publication de la version définitive du règlement, afin d'accorder suffisamment de temps aux entreprises pour adapter leurs politiques et procédures pour observer la nouvelle loi.