

Data Breaches: Worth Noticing?

Sommaire

Rapport rédigé par le Centre pour la défense de l'intérêt public

Ce rapport examine la notification des atteintes à la protection des données au Canada dans le secteur privé en général et, plus particulièrement, si le projet de loi fédéral sur la notification des atteintes à la protection des données (Projet de loi C-12, *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*) permet de protéger de façon adéquate les consommateurs canadiens.

Les « atteintes à la protection des données » constituent une perte, un accès non autorisé aux renseignements personnels de la personne ou une divulgation de ceux-ci par un organisme détenant ces données. Actuellement, seule la loi de l'Alberta exige que les atteintes à la protection des données dans le secteur privé soient déclarées. Sur le plan fédéral, les atteintes en question font actuellement l'objet de directives facultatives émanant du Commissaire à la protection de la vie privée du Canada.

Le rapport conclut que les exigences proposées pour la notification des atteintes à la protection des données dans le Projet de loi C-12 accordent un pouvoir discrétionnaire étendu aux organismes qui ont subi une atteinte à la protection des données, leur permettant ainsi, unilatéralement, de qualifier l'atteinte comme un acte qui ne porte pas préjudice aux consommateurs. Les organismes obtiennent ainsi l'avantage d'une décision échappant, en grande partie, au contrôle judiciaire face à un conflit d'intérêts manifeste et indéniable. Le résultat sera probablement une vaste sous-déclaration d'atteintes graves à la protection des données, ce qui menace de manière excessive le bien-être du consommateur.

Par conséquent, le Centre pour la défense de l'intérêt public appuie une loi sur les atteintes à la protection des données modifiée selon le « modèle albertain » au niveau fédéral.

Les modifications législatives ci-après figurent parmi les recommandations (modifications au Projet de loi C-12 ou ajouts, ou modifications à la législation provinciale) :

- 1. Les organismes doivent avoir l'obligation de déclarer toutes les atteintes à la protection des données au Commissaire à la protection de la vie privée visé, soit « dans les meilleurs délais » ou dans un délai assez bref, tel que 48 heures;**
- 2. Des amendes clairement définies doivent être imposées pour ne pas faire de déclaration au Commissaire à la protection de la vie privée;**

3. **Le Commissaire à la protection de la vie privée doit décider de la notification des consommateurs, basée sur un test évaluant le préjudice. Ce test doit être objectif et conforme à la norme indiquant un « risque réel d'un préjudice important »;**
4. **Le Commissaire à la protection de la vie privée devrait se voir attribuer le pouvoir d'ordonner à un organisme de déclarer une atteinte aux consommateurs. Les arrêtés pour aviser les consommateurs doivent être rendus publics tout comme le nom de l'organisme en question;**
5. **Le Commissaire à la protection de la vie privée doit disposer de pouvoirs adéquats en matière d'audit pour se pencher sur les pratiques visant la sécurité des données d'entreprises et, en particulier, pour examiner la préparation et la réaction d'une notification d'atteintes à la protection des données de l'organisme;**
6. **La pertinence et l'efficacité du régime lié aux atteintes à la protection des données doivent être évaluées séparément lors du prochain examen de la LPRPDE ou dans le cadre de la législation provinciale relative à la protection de la vie privée.**

En outre, il convient de tenir compte des recommandations suivantes indépendantes du cadre législatif sur la notification des atteintes :

7. **Le Commissaire à la protection de la vie privée doit créer une division consacrée aux atteintes à la protection des données, pourvue suffisamment en personnel, pour s'occuper uniquement des atteintes à la protection des données.**
8. **Le Commissaire à la protection de la vie privée doit organiser un « conseil consultatif sur les atteintes à la protection des données » afin d'apporter l'expertise actuelle en matière de sécurité des informations d'entreprises, une expertise en matière de protection du consommateur et une expertise en matière de réglementation gouvernementale pour que les questions relatives aux atteintes à la protection des données ne restent pas sans réponse.**
9. **Le Commissaire à la protection de la vie privée doit jouer un rôle de premier plan en informant les Canadiens sur la façon dont fonctionne la notification des atteintes et en mettant également en œuvre une page Web réservée et des ressources en ligne.**

Reconnaissance

Le Centre pour la défense de l'intérêt public a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Industrie Canada. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Industrie Canada ou du gouvernement du Canada.

Décembre 2011

Publié janvier 2012