Incidents de confidentialité (IC) (atteintes à la protection des données)

Modifications à la Loi sur la protection des renseignements personnels dans le secteur privé du Québec

Articles 3.5 à 3.8

Introduction

Le 22 septembre 2021, le Québec a adopté la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (2021, chapitre 25) (la « Loi ») qui met à jour les lois sur la protection des renseignements personnels dans le secteur public et dans le secteur privé. Les dispositions de la Loi entrent en vigueur sur une période de 3 ans.

Ce document a été créé par des sommités canadiennes en matière de protection des renseignements personnels, en collaboration avec des associations industrielles nationales et régionales. Nous pensons qu'il est important d'adopter une approche harmonisée des lois sur la protection des renseignements personnels dans toutes les juridictions canadiennes afin que les règles soient compréhensibles pour les particuliers et les entreprises. L'interprétation des lois sur la protection des renseignements personnels doit être pragmatique, raisonnable et axée sur les résultats pour les particuliers et la mise en œuvre pour les entreprises. Dans cet esprit, nous avons élaboré des conseils qui nous semblent appropriés pour interpréter les dispositions les plus complexes de la Loi.

Ce document peut être partagé et utilisé par les entreprises. Il ne s'agit pas d'un avis juridique, mais de recommandations, de pratiques exemplaires à l'intention des entités qui souhaitent se conformer à la Loi avant que le gouvernement ou la Commission d'accès à l'information (la « CAI ») ne fournisse des règlements ou des directives supplémentaires. Nous encourageons les entreprises à suivre les développements de la CAI et des autorités gouvernementales sur ces sujets et ceux liés à la Loi.

Incidents de confidentialité (IC)

La Loi exige que les entreprises notifient la CAI et les personnes concernées si un IC atteint un seuil de risque de préjudice sérieux. Les entreprises peuvent également informer les tiers qui pourraient réduire le risque de préjudice. Les entreprises sont tenues de prendre des mesures raisonnables pour atténuer l'impact des incidents, empêcher leur récurrence et tenir un registre des incidents.

Les dispositions relatives aux IC entrent en vigueur le **23 septembre 2022**.

Les exigences relatives aux IC de la Loi sont essentiellement similaires au régime d'atteinte aux mesures de sécurité de la LPRPDÉ et se reflètent dans les processus de nombreuses entreprises qui se conforment déjà à la LPRPDÉ. Il est donc opportun de s'appuyer sur la

LPRPDÉ, les règlements connexes et les directives du Commissariat à la protection de la vie privée (« CPVP ») pour interpréter la Loi.

a) Qu'est-ce qu'un IC ? (art. 3.6)

La définition d'un IC est presque identique au concept d'« atteintes aux mesures de sécurité » de la LPRPDÉ.

Un IC résulte de :

- L'accès non autorisé par la loi à des renseignements personnels ;
- L'utilisation non autorisée par la loi de renseignements personnels ;
- La communication non autorisée par la loi de renseignements personnels ;
- L'utilisation non autorisée de renseignements personnels ; ou
- La perte de renseignements personnels ou toute autre atteinte à la protection de tels renseignements.

b) Quand une entreprise doit-elle fournir un avis d'IC ? (art. 3.5 et 3.7)

Une entreprise doit fournir un avis d'IC « si l'incident présente un risque qu'un préjudice sérieux soit causé ». Il est logique que le risque soit réel avant d'aviser la CAI ou les personnes touchées, et nous nous attendons donc à ce que le seuil de notification de l'IC soit le même que le « risque réel de préjudice grave » de la LPRPDÉ, suivant les questions et les exemples fournis dans le formulaire de déclaration d'incident de sécurité existant de la CAI. Les décisions et les directives du CPVP sur le « risque réel de préjudice grave » fournissent donc des indications utiles sur le seuil de notification en vertu de la Loi.

Les facteurs permettant d'évaluer le risque de préjudice sérieux sont les suivants : la sensibilité des renseignements concernés, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables (art. 3.7). Ces facteurs sont semblables aux préjudices énumérés à l'article 10.1 (7) de la LPRPDÉ : lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles.

c) Qui est notifié par un IC ? (art. 3.5)

Si un IC atteint le seuil de gravité du risque de préjudice sérieux, un avis **doit** être donné à la CAI et à « toute personne dont un renseignement personnel sont concernés par l'incident », sauf si les notifications entravent une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

L'entreprise **peut** notifier toute autre personne ou organisme sans le consentement de la personne concernée afin de réduire le risque/le préjudice.

d) Forme, contenu et conditions de l'avis d'IC (art. 3.5)

La forme, le contenu et les conditions de la notification seront précisés dans les règlements. La CAI a déjà publié des directives sur la notification d'un IC, mais celles-ci seront probablement révisées suite à l'adoption de la Loi modificatrice.

En ce qui concerne la forme et le contenu des avis, il est raisonnable de s'appuyer sur :

- Pour la notification aux individus : l'article 3 du Règlement sur les atteintes aux mesures de sécurité et les directives de la CAI à la page 6, étape 4.
- Pour l'avis à la CAI : l'article 2 du Règlement sur les atteintes aux mesures de sécurité, les formulaires du CPVP et le formulaire de déclaration volontaire d'incident de sécurité actuellement disponible sur le site Web de la CAI.

En ce qui concerne le délai de notification :

- La Loi et la LPRPDÉ utilisent des normes similaires : « avec diligence » dans la Loi et « le plus tôt possible » dans la LPRPDÉ. Les directives du CPVP devraient être utiles pour déterminer les délais.
- Le délai prévu dans la Loi ne s'applique qu'à l'avis à la CAI. Il n'y a pas de délai pour l'avis aux personnes concernées ou à la personne ou l'organisme qui pourrait aider à réduire le risque de préjudice. La meilleure pratique consisterait à appliquer la même norme que la LPRPDÉ, soit « dès que possible », pour les avis aux personnes ou aux tiers qui peuvent contribuer à atténuer les risques de préjudice.

e) Obligation de mitiger les risques de préjudice (art. 3.5)

Si une organisation pense qu'un IC s'est produit, elle « doit prendre des mesures raisonnables pour réduire les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Les mesures raisonnables ne sont pas définies, cependant, les entreprises pourraient s'appuyer sur les paragraphes 11 et 12 des lignes directrices du CPVP et sur les conseils publiés par la CAI.

f) Registre des IC (art. 3.8)

De manière similaire à la LPRPDÉ, les entreprises sont tenues de tenir un registre des IC. Le contenu du registre peut être précisé dans les règlements. Il semble que **tous** les IC, et non seulement ceux qui atteignent le seuil de notification devront être inclus dans le registre.

Nous croyons qu'il est raisonnable de s'appuyer sur les lignes directrices du CPVP (voir la partie 3) pour déterminer ce qu'un registre devrait contenir pour chaque IC :

- La date ou la date estimée de l'atteinte ;
- La description générale des circonstances de l'atteinte ;
- La nature des renseignements visés par l'atteinte et les personnes touchées ;
- Le fait que l'atteinte ait été signalée ou non au CPVP/les personnes concernées ont été avisées ;
- Une explication relative à l'évaluation du risque de préjudice, p. ex. pourquoi il n'y a pas eu de notification.