Projet de loi n°64 - Comment la modernisation des obligations en matière de protection des renseignements personnels affectera-t-elle votre entreprise?

Vanessa Deschênes[*] et Jean-François Normand[†]
ROBIC, S.E.N.C.R.L.
Avocats, agents de brevets et de marques de commerce

Le 12 juin dernier, l'Assemblée nationale déposait le Projet de Loi n°64 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« **Projet de loi** »). Cette réforme, visant notamment la *Loi sur la protection des renseignements personnels dans le secteur privé* (« **LPRPSP** »), souhaite instaurer un régime plus strict, notamment en réponse aux événements fortement médiatisés des dernières années (brèche de confidentialité) et afin d'emboîter le pas quant à la mise en place de standards plus élevés tel qu'instauré par le *Règlement général pour la protection des données* (« **RGPD** ») en Europe.

Rappelons que le Québec a été l'une des premières juridictions en Amérique du Nord à introduire une loi sur la protection des renseignements personnels (« **PRP** ») dans le secteur privé. Datant de 1994, et avec la progression fulgurante des nouvelles technologies et de l'engouement pour la donnée, une refonte majeure était non seulement attendue, mais de mise.

Afin de clarifier les applications pratiques qui devront être instaurées au sein de votre entreprise si le projet de loi devait être adopté tel quel, vous trouverez, dans ce bref article, les principales modifications proposées ainsi que leurs implications et impacts sur les activités commerciales des entreprises.

Notes préliminaires :

Nous constatons que plusieurs des dispositions reflètent les concepts introduits dans le RGPD ou ce que les commissaires à la vie privée, notamment au fédéral, avaient déjà émis comme lignes directrices, recommandations ou positions de principe. Ainsi, les entreprises ayant déjà implanté ces éléments dans leurs pratiques et procédures internes auront déjà une longueur d'avance, surtout si ces dernières ont déjà documenté de telles pratiques. En effet, nous notons un désir du Gouvernement de vouloir s'assurer que les entreprises prendront au sérieux les questions relatives

[*] Vanessa Deschênes est avocate chez ROBIC, S.E.N.C.R.L., un cabinet multidisciplinaire d'avocats et d'agents de brevets et de marques de commerce.
[†] Jean-François Normand est avocat chez ROBIC, S.E.N.C.R.L., un cabinet multidisciplinaire d'avocats et d'agents de brevets et de marques de commerce.

à la PRP en les obligeant, en quelque sorte, à documenter leur façon de faire afin de pouvoir en démontrer la conformité.

1. Obligation de nommer un responsable de la protection des renseignements personnels.

Le Projet de loi prévoit que les entreprises devront nommer un responsable qui devra s'assurer de la mise en œuvre de pratiques conformes avec la LPRPSP et de la relation avec les individus pour lesquels les informations ont été collectées. Malgré que cela puisse apparaître comme un changement majeur, une disposition très similaire est déjà présente dans la législation fédérale, soit la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** ») ainsi que dans le RGPD.

Qu'est-ce que cela implique pour votre entreprise? Chaque entreprise doit nommer un responsable de la PRP et fournir ses coordonnées aux individus pour lesquels des renseignements personnels sont collectés. Généralement, ces informations se retrouvent dans la politique de protection des renseignements personnels de l'entreprise.

Si votre entreprise est déjà assujettie à la LPRPDE et/ou au RGPD, cette obligation devrait déjà être en place au sein de votre organisation et ne nécessiterait donc pas de mesures additionnelles.

2. Pouvoirs accrus de la CAI et sanctions

Le Projet de loi introduit de nouveaux pouvoirs à la CAI, lesquels sont demandés depuis de nombreuses années afin de réellement donner du mordant à législation. Ainsi, la CAI pourra dorénavant émettre des avis de non-conformité et imposer des sanctions administratives pécuniaires en cas de i) défaut d'informer les personnes concernées de l'objet du dossier, de l'utilisation qui sera faite des renseignements personnels, des catégories de personnes qui y auront accès, de l'endroit et de la durée de conservation de ses renseignements personnels ainsi que des droits d'accès ou de rectification ii) collecte ou d'utilisation de renseignements personnels en contravention avec les dispositions de la LPRPSP iii) non-déclaration d'un incident de confidentialité à la CAI ou aux personnes concernées iv) défaut d'informer la personne concernée qu'une décision fondée exclusivement sur un traitement automatisé a été prise à son sujet.

Les sanctions administratives peuvent atteindre 50 000$ pour une personne physique et 10 000 000$ pour une organisation ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé. Quant aux sanctions pénales, elles peuvent atteindre 50 000$ dans le cas d'une personne physique et 25 000 000 $ pour une organisation ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé. Avec l'introduction de ces pouvoirs accrus et de l'augmentation faramineuse des sanctions, les modifications proposées sont sans rappeler ce que prévoit le RGPD.

Qu'est-ce que cela implique pour votre entreprise? Le risque juridique du non-respect des règles entourant la PRP devra, si ce n'est déjà le cas, devenir une priorité pour l'organisation puisque les conséquences pécuniaires peuvent être considérables. Qui plus est, détenant maintenant des pouvoirs de contraindre les entreprises à changer leurs pratiques, les entreprises pourront se voir imposer des délais par la CAI. C'est ici que l'adage « vaut mieux prévenir que guérir » prend, à notre avis, tout son sens!

3. Obligation de mettre en place des politiques encadrant la PRP

Le Projet de loi impose à toutes les entreprises d'instaurer des politiques internes de gouvernance en matière de gestion des renseignements personnels. Cette obligation, similaire à celle prévue au RGPD, assure, en quelque sorte, la conformité des à la LPRPSP. À noter que la Commission d'accès à l'information (« **CAI** ») pourra exiger, en tout temps, une démonstration de conformité à la LPRPSP et ses règlements.

Qu'est-ce que cela implique pour votre entreprise? Chaque entreprise doit publier sur son site web ses politiques, approuvées au préalable par le responsable. Ces dernières doivent afficher les critères quant à la conservation et la destruction des renseignements personnels, prévoir les responsabilités et rôles des membres du personnel en plus d'expliquer le mécanisme de plainte. Ces informations peuvent aussi se trouver au sein de la politique de PRP.

Pour ce qui est du volet « démonstration de la conformité », cela signifie que les entreprises devront documenter leurs processus et procédures et mettre en place ce que nous appelons souvent dans l'industrie un *Programme de gestion de la conformité* ou *Programme de gestion de la vie privée*. À titre d'exemple, déjà en 2012, les commissaires à la vie privée de l'Alberta, de la Colombie-Britannique et du fédéral avaient émis un guide[‡] à cet égard. Ce guide constitue donc un point de départ pour les entreprises.

4. Obligation de procéder à des évaluations de facteurs relatifs à la vie privée

Les entreprises devront entreprendre une analyse des facteurs relatifs à la vie privée avant chaque prestation de service ou création de projets qui nécessitent soit la collecte, l'usage, la communication, la conservation ou la destruction de renseignements personnels. Bien qu'il

[‡] Commissariat à la protection de la vie privée du Canada (2012). Un programme de gestion de la protection de la vie privée : la clé de la responsabilité, Commissariat à la protection de la vie privée du Canada. Récupéré le 15 juin 2020 de https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/gl_acc_201204/

s'agisse d'un changement important, cette obligation est toutefois similaire à celle que l'on trouve dans le RGPD et était déjà une recommandation du Commissaire à la protection de la vie privée du Canada (« **CPVPC** »).

Qu'est-ce que cela implique pour votre entreprise? Tout nouveau système nécessitant l'utilisation de renseignements personnels doit faire l'objet de cette étape préliminaire. De plus, cette obligation prévoit aussi que les renseignements personnels doivent pouvoir être communiqués « dans un format technologique structuré et couramment utilisé ».

Concrètement, cela signifie donc que des processus et procédures devront être mis en place au sein de l'organisation afin de s'assurer et pouvoir démontrer qu'une telle analyse a été effectuée et que le responsable nommé au sein de l'organisation afin d'assurer la PRP soit consulté dès le début du projet afin de pouvoir intervenir à tout moment pour suggérer des mesures de PRP. Cette obligation permet également l'introduction du concept de *privacy by design* et *privacy by default* que l'on retrouve dans le RGPD.

5. Modification aux exigences relatives au transfert transfrontalier de renseignements personnels

En se modulant, encore une fois, à la vision européenne, ainsi qu'aux lignes directrices du CPVPC, le législateur prévoit dorénavant que les entreprises devront effectuer, avant chaque communication de renseignements personnels à l'extérieur du Québec, une évaluation visant à déterminer si la protection de l'État recevant ceux-ci est considérée comme étant équivalente.

Fait intéressant, le Gouvernement produira une liste des États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de PRP applicables au Québec.

Qu'est-ce que cela implique pour votre entreprise? L'entreprise devra mettre en place un cadre d'évaluation et procéder à une telle analyse avant le transfert. Cette dernière devra tenir compte de la sensibilité des renseignements personnels, la finalité de leur utilisation, les mesures de protection en place et, particulièrement, le cadre juridique applicable à la juridiction visée. Dans cette évaluation, l'entreprise devra établir et démontrer l'équivalence afin de permettre le transfert des renseignements personnels, le tout via un contrat écrit.

À noter que les entreprises conformes au RGPD ou ayant déjà implanté les lignes directrices du CPVPC en matière de transfert transfrontalier devraient pouvoir se considérer conformes à ces nouvelles exigences. De plus, quant à l'exigence d'un contrat écrit, bien que cette dernière n'était pas dans la LPRPSP, la CAI avait déjà statué sur sa nécessité dans une décision rendue en 2000.[§]

[§] Deschesnes c. Groupe Jean Coutu, [2000] CAI 216.

6. Droits individuels rehaussés et ajouts de nouveaux droits

Le Projet de loi rehausse ou ajoute des droits accordés aux individus. À titre d'exemple, il est maintenant clairement énoncé qu'un individu a le droit d'être informé dans un langage simple et clair, quel que soit le moyen utilisé. De plus, lorsqu'un individu fait une demande à cet effet, une entreprise devra dorénavant informer celui-ci de la véritable source ayant recueilli les renseignements personnels, si ces derniers ont été collectés par une autre entreprise. S'inspirant d'une obligation européenne similaire, le législateur québécois souhaite ainsi donner à la personne concernée un moyen supplémentaire de comprendre qui a réellement procédé à la collecte de ses renseignements.

Les autres changements, que nous qualifierions de majeurs et fortement influencés par le RGPD, incluent la **portabilité des données**, dans un format technologique structuré et couramment utilisé, le **droit à l'oubli**, ainsi que le droit, et donc l'obligation pour l'entreprise, avant la collecte de renseignements personnels, d'informer les personnes de l'utilisation des technologies permettant l'identification, la localisation ou le **profilage** et également du fait qu'il est possible de désactiver ces options. Il en est de même quant au droit des individus d'être informé, au moment de la décision ou avant celle-ci, qu'ils font l'objet d'une **décision automatisée**.

Qu'est-ce que cela implique pour votre entreprise? Concrètement, les entreprises devraient mettre en place des mesures comme des inventaires de renseignements personnels, une cartographie du flux de données ou des mesures comme la création de « tag » ou de métadonnées afin de pouvoir répondre à ces exigences additionnelles. Sans de tels outils, il risque d'être ardu pour les entreprises de respecter ces nouvelles obligations.

De plus, les entreprises devront rehausser les mécanismes par lesquels ils informent les individus de leurs pratiques en matière de PRP. À notre avis, une simple mention enfouie dans une politique de confidentialité ne sera pas suffisante. À notre avis, le Projet de loi vise à rendre les entreprises davantage transparentes et proactives dans leur façon d'informer les individus.

7. Consentement d'un enfant de moins de 14 ans

De façon similaire au RGPD, le Projet de loi ajoute une restriction quant à l'obtention d'un consentement visant des enfants de moins de 14 ans. Pour être valable, un tel consentement doit être obtenu par le titulaire de l'autorité parentale.

Qu'est-ce que cela implique pour votre entreprise? Il est à noter que les enfants de plus de 14 ans peuvent donner leur consentement. Ce faisant, les entreprises doivent adopter des barèmes de sécurité plus stricts et prévoir un mécanisme leur permettant de recueillir le consentement des titulaires de l'autorité parent, lorsque requis.

8. Destruction ou anonymisation des renseignements personnels

Changement important par rapport au régime actuel, le Projet de loi oblige formellement les entreprises à détruire ou à anonymiser les renseignements personnels recueillis une fois les fins pour lesquelles ils ont été recueillis sont accomplies. Bien que cette exigence faisait déjà partie des bonnes pratiques à implanter au sein d'une entreprise, cet ajout dans la loi démontre clairement l'intention du législateur de mettre un frein aux pratiques de certaines entreprises de conserver les données « à vie ». En effectuant cette modification législative, il n'y a maintenant plus de doute quant aux pratiques à adopter.

Qu'est-ce que cela implique pour votre entreprise? Les entreprises devraient mettre en place des calendriers de conservations ainsi que des mesures de gestion du cycle de vie des données (*data management »)* afin d'être en mesure d'être notifié du sort à donner à un renseignement personnel une fois la fin pour laquelle il a été recueilli est accomplie, et ainsi respecter ses obligations.

9. Gestion des incidents de confidentialité

Comme c'est déjà le cas en Alberta et en vertu de la LPRPDE et du RGPD, le Projet de loi instaure un nouveau régime de notification en cas de fuite ou autre brèche de sécurité.

Qu'est-ce que cela implique pour votre entreprise? Concrètement, une entreprise assujettie à la LPRPDE devrait déjà avoir en place les mécanismes permettant de répondre à cette nouvelle exigence. En effet, les ajouts proposés concernant l'obligation d'aviser et de maintenir un registre ainsi que l'implication du responsable de la PRP sont très similaires à ce qui a été introduit en 2018 dans la loi fédérale.

Concrètement, si l'entreprise n'est pas déjà conforme à la LPRPDE, cela signifie qu'elle devra créer un registre des incidents ainsi que des procédures internes afin de non seulement traiter l'incident, mais également élaborer des critères afin de déterminer les cas où une notification devra être faite.

En février 2020, la ministre Lebel nous annonçait vouloir redonner au citoyen le contrôle de leurs données et que, pour se faire, le Gouvernement s'inspirerait des « meilleurs standards » au monde en matière de protection des données. Elle mentionnait notamment « On s'en va vers les modèles européens, et c'est ce qui est reconnu comme le plus avancé ». Force est de constater que le Projet de loi présenté est fortement inspiré du RGPD et permet dorénavant aux individus d'être mieux informés des pratiques en place au sein des entreprises et de mieux connaître de l'ampleur de l'utilisation qui est faite de ses données, point qui était, de l'avis de la ministre « le bât qui blesse ».

Vous voulez déjà analyser l'impact réel de ces changements au sein de votre organisation s'ils étaient adoptés tel quel? Notre secteur *Protection des données, vie privée et cybersécurité* est là pour vous!

Nos professionnels en protection des données, vie privée et cybersécurité

Vincent Bergeron
Avocat et agent de marques, associé

418 653-1813

Vanessa Deschênes

Avocate

418 781-0767

Jules Gaudin

Avocat

514 987-8892

Marcel Naud
Avocat et agent de marques

514 987-8039

Jean-François Normand

Avocat

418 780-0962