

Le train de la réforme des lois sur la protection de la vie privée continue de rouler

11 JANVIER 2023 16 MIN DE LECTURE

Expertises Connexes

- [Respect de la vie privée et gestion de l'information](#)

Auteurs(trice): [Maryna Polataiko](#), [Colleen Morawetz](#), [Adam Kardash](#)

Au cours de l'année écoulée, c'est la réforme législative qui a continué retenir toute l'attention dans le domaine très dynamique de la protection de la vie privée au Canada. La première phase de la réforme du cadre législatif québécois en matière de protection des renseignements personnels est entrée en vigueur ainsi que les obligations de notification des atteintes à la sécurité et certaines autres nouvelles obligations auxquelles les sociétés doivent se conformer (entrées en vigueur en septembre 2022). En septembre 2023, la majorité des modifications apportées au cadre législatif du Québec entreront en vigueur, y compris un régime d'application de la loi assorti de sanctions financières potentiellement sévères.

Par ailleurs, en 2022, le gouvernement fédéral a réintroduit un nouveau cadre législatif en matière de protection de la vie privée dans le secteur privé. S'il est adopté, ce cadre exposera les sociétés canadiennes à de lourdes sanctions financières en cas d'atteinte à la vie privée, à un risque accru de litige et à des coûts de conformité considérables.

Il est plus important que jamais pour les sociétés qui font des affaires au Québec et ailleurs au Canada de bien comprendre et maîtriser leurs pratiques en matière de renseignements personnels et leurs obligations en ce qui concerne la protection de la vie privée. Les sociétés devront cerner et atténuer l'éventail croissant de risques liés à la vie privée et à la réputation et les risques juridiques associés à la collecte, à l'utilisation, à la communication et aux autres modes de traitement des renseignements personnels.

Parmi les autres nouveaux projets de loi fédéraux présentés au cours de l'année écoulée figurent des cadres législatifs régissant les systèmes d'intelligence artificielle et la cybersécurité des infrastructures essentielles. Quoi qu'il en soit, le train de la réforme législative n'a pas eu le même élan partout au Canada.

Québec : des parties du projet de loi 64 entrent en vigueur

La première vague de modifications apportées par le projet de loi 64 du Québec, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* [PDF], est entrée en vigueur le 22 septembre 2022. Bien que les nouvelles dispositions relatives aux sanctions n'entrent en vigueur qu'en 2023, les sociétés qui font des affaires au Québec sont maintenant assujetties à un certain nombre de nouvelles exigences.

En particulier, la personne ayant la « plus haute autorité » au sein d'une organisation est reconnue comme la personne responsable de la protection des renseignements personnels, à moins qu'elle ne délègue cette responsabilité par écrit à une autre personne au sein de l'organisation. De plus, l'organisation doit signaler à la Commission d'accès à l'information

(CAI) et aux personnes concernées les « incidents de confidentialité » présentant un risque de préjudice sérieux pour ces dernières. L'organisation doit également tenir un registre de tous les incidents de confidentialité.

Le projet de loi 64 modifie la Loi concernant le cadre juridique des technologies de l'information par l'introduction de l'obligation, pour les organisations qui procèdent à la vérification ou à la confirmation de l'identité de personnes, de divulguer à la CAI tout procédé permettant de saisir des caractéristiques biométriques. La création d'une banque de caractéristiques ou de mesures biométriques doit être divulguée à la CAI au plus tard 60 jours avant sa mise en service.

Enfin, une organisation peut désormais communiquer des renseignements personnels en l'absence de consentement, dans des conditions prescrites, notamment lorsque cela s'avère nécessaire aux fins de la conclusion d'une transaction commerciale ou lorsque le destinataire souhaite utiliser les renseignements à des fins d'étude, de recherche ou de production de statistiques.

À l'exception des dispositions relatives à la portabilité des données, le reste des modifications introduites par le projet de loi 64 entreront en vigueur en septembre 2023. Parmi celles-ci figurent les dispositions relatives aux sanctions. Les organisations qui enfreignent la Loi sur la protection des renseignements personnels dans le secteur privé sont passibles d'une amende pouvant atteindre 25 millions de dollars ou le montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé. Elles peuvent également être passibles de sanctions administratives pécuniaires pouvant atteindre 10 millions de dollars ou le montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé.

En outre, les organisations seront tenues de créer un ensemble de politiques internes pour traiter le cycle de vie des renseignements personnels dont elles ont la garde et le contrôle. Elles devront aussi procéder à des évaluations des facteurs relatifs à la vie privée à l'égard de tout projet comportant l'acquisition, le développement ou la refonte d'un système d'information ou de prestation électronique de services nécessitant le traitement de renseignements personnels.

Le projet de loi 64 renforce les exigences en matière de consentement et crée de nouvelles exceptions au consentement pour le traitement des renseignements personnels. Les organisations devront passer en revue tous les modes de collecte, d'utilisation et de communication des renseignements personnels, améliorer leurs avis de consentement, mettre en place ou améliorer leurs propres pratiques de gestion du consentement et assurer autrement la légalité du traitement des renseignements personnels.

En vertu de la nouvelle exigence de « confidentialité par défaut », les organisations qui offrent au public un produit ou un service technologique disposant de paramètres de confidentialité doivent s'assurer que, par défaut, ces paramètres assurent le « plus haut niveau » de confidentialité. Enfin, les organisations qui recueillent des renseignements personnels auprès de personnes physiques en ayant recours à une technologie comprenant des fonctions permettant de les identifier, de les localiser ou d'effectuer un profilage de celles-ci doivent, au préalable, les informer du recours à une telle technologie et des moyens offerts pour activer les fonctions en question.

Une fois que les restrictions relatives à la localisation des données seront en vigueur, les organisations devront créer un inventaire de toutes les communications et de tous les transferts transfrontaliers, y compris les transferts de renseignements personnels vers d'autres provinces canadiennes. Les organisations seront tenues de procéder à une évaluation des facteurs relatifs à la vie privée avant toute communication de renseignements

personnels à l'extérieur du Québec afin de s'assurer que les renseignements personnels bénéficient d'une « protection adéquate » dans les autres territoires. Il sera interdit aux organisations de transférer ou de communiquer des renseignements personnels à l'extérieur de la province de Québec si ces renseignements ne bénéficient pas d'une « protection adéquate ». Cette protection sera déterminée au regard des « principes de protection des renseignements personnels généralement reconnus ».

Fédéral : introduction d'une réforme législative radicale

En juin 2022, le gouvernement du Canada a déposé le projet de loi C-27, la *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, qui crée un nouveau cadre législatif régissant les pratiques en matière de renseignements personnels dans le secteur privé. Le projet de loi est actuellement en deuxième lecture et, s'il est adopté, il établira trois nouvelles lois :

- La *Loi sur la protection de la vie privée des consommateurs* (la « LPVPC »), une loi touchant le secteur privé qui abrogera et remplacera le régime de protection des renseignements personnels de la *Loi sur la protection des renseignements personnels et les documents électroniques*.
- La *Loi sur le Tribunal de la protection des renseignements personnels et des données*, qui créera un tribunal administratif chargé d'examiner certaines décisions prises par le commissaire à la protection de la vie privée du Canada et d'imposer des sanctions en cas de contravention à la LPVPC.
- La *Loi sur l'intelligence artificielle et les données* (la « LIAD »), qui créera une approche fondée sur le risque pour réglementer les échanges et le commerce des systèmes d'IA.

La Loi sur la protection de la vie privée des consommateurs

Le régime de protection de la vie privée proposé dans le projet de loi C-27 est essentiellement semblable à l'ancien projet de loi C-11, qui est mort au feuillet en 2021, avant les élections fédérales. Une fois la LPVPC promulguée, toute entreprise qui l'enfreindra sera passible d'une amende pouvant atteindre 25 millions de dollars ou le montant correspondant à 5 % du chiffre d'affaires mondial de l'exercice précédent, si ce dernier montant est plus élevé. Elle pourrait également être passible d'une sanction administrative pécuniaire pouvant atteindre 10 millions de dollars ou le montant correspondant à 3 % du chiffre d'affaires mondial de l'exercice précédent, si ce dernier montant est plus élevé.

Parmi les autres caractéristiques clés de la LPVPC, telle qu'elle est actuellement projetée, figure l'obligation pour les entreprises de mettre en œuvre un programme de gestion de la protection des renseignements personnels. La LPVPC renforce également le consentement (en particulier le consentement explicite) à titre d'autorité principale permettant aux organisations de traiter les renseignements personnels. Toutefois, elle clarifie les « exceptions au consentement » pour la collecte, l'utilisation ou la communication de renseignements personnels et en crée de nouvelles. Ces exceptions s'appliquent à certaines « activités d'affaires » standard déterminées et à l'appui des « intérêts légitimes », sous réserve de certaines conditions.

La LPVPC comprend de nombreuses dispositions relatives au traitement licite des données « dépersonnalisées » et des données « anonymisées ». Les dispositions proposées précisent que les données anonymisées ne relèvent pas du champ d'application de la LPVPC. Le projet de loi crée également un statut spécial pour les renseignements personnels des mineurs.

Dans certaines circonstances – à savoir, lorsqu'il pourrait y avoir une « incidence importante » pour un individu –, la LPVPC donnerait à l'individu le droit de demander à l'organisation d'expliquer comment elle a utilisé le système décisionnel automatisé pour faire des prédictions, formuler des recommandations ou prendre des décisions et comment elle a obtenu les renseignements. En outre, l'individu pourrait demander à l'entreprise de retirer ses renseignements personnels et l'entreprise devrait y donner suite dans des circonstances particulières.

Enfin, la LPVPC comprend des dispositions accordant aux individus des droits de mobilité des données, leur permettant de diriger le transfert de leurs renseignements personnels d'une organisation à une autre.

La Loi sur l'intelligence artificielle et les données

En plus d'établir un nouveau régime de protection de la vie privée, le projet de loi C-27 édicterait la LIAD, la première loi au Canada réglementant la création et l'utilisation des systèmes d'intelligence artificielle. Si elle était adoptée, la LIAD créerait un important régime de sanctions en cas d'infraction, y compris des amendes pouvant atteindre 3 % des recettes globales ou 10 millions de dollars canadiens et, pour les infractions plus graves, des amendes pouvant atteindre 5 % des recettes globales ou 25 millions de dollars canadiens – ou l'emprisonnement, dans le cas d'un individu.

Parmi les éléments clés du régime proposé de réglementation des systèmes d'IA, mentionnons l'obligation, pour le responsable d'un système d'intelligence artificielle, d'évaluer si le système est un système à incidence élevée, terme qui sera défini par voie de règlement. Les organisations doivent publier une description et une explication de chaque système à incidence élevée et atténuer les risques de préjudice ou de résultats biaisés que pourrait entraîner l'utilisation du système.

En outre, la LIAD obligerait les organisations à produire des rapports et accorderait au ministre des pouvoirs lui permettant d'ordonner la production de documents, de mener une vérification, de publier des avertissements et d'ordonner la cessation de l'utilisation ou de la distribution d'un système à incidence élevée. La LIAD envisage en outre la nomination d'un commissaire à l'intelligence artificielle et aux données qui serait chargé d'appuyer le ministre dans l'exécution et le contrôle d'application de la loi.

Projet de loi C-26

En juin également, le gouvernement du Canada a présenté le projet de loi C-26, *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, pour sa première lecture au Parlement. Le projet de loi vise à créer de nouveaux pouvoirs permettant au gouvernement fédéral de réagir rapidement et avec souplesse aux menaces à la sécurité nationale qui touchent les réseaux d'infrastructures essentielles sous réglementation fédérale.

Le projet de loi C-26 promulguerait la *Loi sur la protection des cybersystèmes essentiels* (la « LPCE ») qui « prévoit un cadre de protection des cybersystèmes essentiels liés aux services et systèmes qui sont d'une importance critique pour la sécurité nationale ou la sécurité publique ». Surtout, la LPCE prévoit des sanctions administratives pécuniaires pouvant atteindre 15 000 000 \$ par infraction.

Plus précisément, la LPCE permettrait au Cabinet de désigner les services ou les systèmes qui sont d'une « importance critique » à l'aide d'une liste qui comprend actuellement les services

de télécommunication, les systèmes de pipelines et de lignes électriques interprovinciaux ou internationaux, les systèmes d'énergie nucléaire, les systèmes de transport relevant de la compétence législative du fédéral, les systèmes bancaires et les systèmes de compensation et de règlements. Les « exploitants désignés » à l'égard d'un service ou d'un système essentiel seraient tenus d'établir un programme de cybersécurité.

La LPCE imposerait également aux exploitants désignés l'obligation de signaler immédiatement les incidents de cybersécurité au Centre de la sécurité des télécommunications, ainsi qu'à l'un des nombreux organismes réglementaires compétents. Les exploitants désignés seraient également tenus de tenir des registres de cybersécurité.

La LPCE accorde des pouvoirs aux organismes réglementaires désignés, y compris le Bureau du surintendant des institutions financières, le ministre de l'Industrie, la Banque du Canada, la Commission canadienne de sûreté nucléaire, la Régie canadienne de l'énergie et le ministre des Transports, pour veiller à ce que les exploitants désignés se conforment à la LPCE. Ces pouvoirs comprennent le pouvoir d'entrer dans tout lieu et le pouvoir d'ordonner des vérifications internes, ainsi que le pouvoir de donner des ordres de conformité et de conclure des transactions.

Le projet de loi C-26 modifierait également la *Loi sur les télécommunications*, par la création d'un nouveau pouvoir exécutif permettant d'ordonner aux fournisseurs de services de télécommunication de faire ou de s'abstenir de faire tout ce qui est nécessaire pour sécuriser le système canadien de télécommunication. Les règlements et les ordonnances connexes seraient appuyés par un régime de sanctions administratives pécuniaires prévoyant des amendes pouvant atteindre 15 millions de dollars en cas d'infraction.

Autres provinces : une lente évolution

Bien que l'on s'attende généralement à ce que d'autres provinces suivent l'exemple du Québec et réforment (ou créent) leurs propres lois sur la protection de la vie privée dans le secteur privé, l'évolution est beaucoup plus lente qu'au Québec ou au fédéral. Voici un aperçu de l'évolution de la réforme législative en Colombie-Britannique, en Alberta et en Ontario.

Colombie-Britannique

En février 2020, l'Assemblée législative de la Colombie-Britannique a formé un comité spécial chargé d'examiner la loi provinciale intitulée *Personal Information Protection Act*. Les [recommandations](#) [PDF ; en anglais seulement] du comité spécial comprennent la création de pouvoirs d'application renforcés pour l'organisme de réglementation, comme le pouvoir d'imposer des sanctions. Il est également recommandé de créer des exigences en matière de notification des atteintes à la sécurité et des droits de portabilité des données, ainsi que d'établir de nouvelles catégories de données, à savoir les données protégées par un pseudonyme et les renseignements sensibles. Les recommandations envisagent en outre la création de régimes particuliers de protection de la vie privée des employés et des renseignements personnels sur la santé.

À l'heure actuelle, le gouvernement de la Colombie-Britannique n'a pas encore présenté de projet de loi visant à mettre en œuvre l'une ou l'autre des réformes proposées.

Alberta

Le ministère des Services de l'Alberta a sollicité des commentaires sur la réforme législative touchant la protection de la vie privée au cours de l'été 2021 et a organisé des groupes de discussion ciblés à l'automne de la même année. Cependant, la province n'a pas encore présenté de projet de loi réformant la loi intitulée *Personal Information Protection Act* [PDF].

Ontario

Le gouvernement de l'Ontario a lancé une consultation concernant l'ébauche d'une loi détaillée sur la protection de la vie privée dans le secteur privé en 2020 et a publié un livre blanc sur le sujet en 2021. Cependant, la réforme législative n'a aucunement progressé depuis les élections provinciales de juin 2022.

En outre, le gouvernement de l'Ontario a introduit une nouvelle exigence de transparence en avril 2022 par la modification de sa *Loi sur les normes d'emploi*, qui oblige désormais les entreprises établies en Ontario comptant plus de 25 employés à mettre en œuvre une politique en ce qui a trait à la surveillance électronique des employés. Le commissaire à l'information et à la protection de la vie privée de l'Ontario a déclaré que bien que ces modifications représentent une première étape intéressante pour aider les Ontariens et les Ontariennes à comprendre les pratiques de leurs employeurs, la surveillance électronique en milieu de travail devrait être régie par une loi provinciale détaillée sur la protection de la vie privée dans le secteur privé. De plus amples informations sur les politiques de surveillance électronique sont disponibles dans notre article sur le travail et l'emploi.

Ce qui nous attend en 2023

L'année prochaine, le paysage canadien de la protection de la vie privée, tant sur la scène fédérale que provinciale, devrait continuer d'évoluer de façon importante. Compte tenu des coûts de conformité importants et des lourdes amendes auxquelles les entreprises peuvent s'exposer (de manière imminente au Québec), nous les encourageons toutes à agir de manière proactive et à se préparer à la mise en œuvre des modifications adoptées ou projetées.