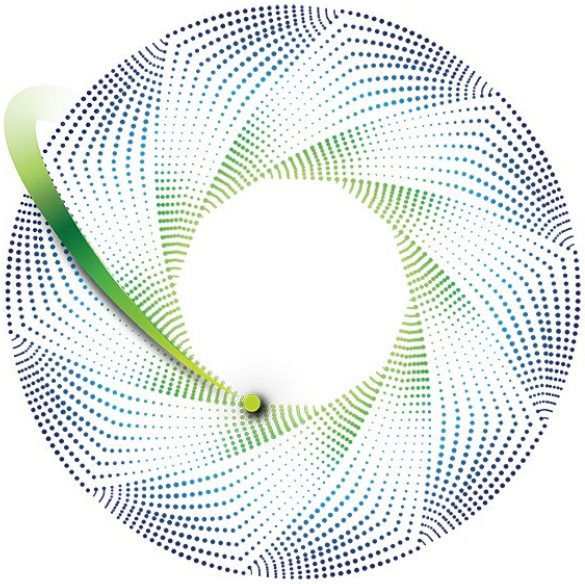
Deloitte.



Alerte canadienne – Fiscalité et Services juridiques

Nouvelles lois sur la cybersécurité et la protection de la vie privée

Nouveaux risques, nouvelles exigences en matière de conformité

Le 18 juillet 2022

Le gouvernement fédéral a récemment présenté non pas un, mais bien deux nouveaux projets de loi qui, s'ils sont adoptés, donneront lieu à une refonte du droit de la cybersécurité et de la protection de la vie privée au Canada. Bien qu'il s'agisse de développements intéressants pour les praticiens dans le domaine de la protection de la vie privée, la nouvelle législation crée une foule d'obligations (qui soulèvent d'importantes questions) pour les entreprises d'infrastructures essentielles, les sociétés qui recueillent, utilisent ou communiquent des renseignements personnels et les organisations du secteur privé qui développent et utilisent l'intelligence artificielle (IA).

Certains points essentiels à retenir

- Les projets de loi C-26 et C-27 créeraient des obligations importantes pour les entreprises relativement à la mise en œuvre de plans d'atténuation des risques associés aux incidents touchant la cybersécurité et la protection de la vie privée.
- Des exigences de signalement obligatoire des incidents de cybersécurité sont également incluses, ce qui créerait de nouvelles considérations liées à la sécurité nationale pour les entreprises d'infrastructures essentielles.

- Des millions de dollars en sanctions pécuniaires par jour pourraient être infligées en cas de violations continues[1].
- Les administrateurs et les dirigeants pourraient faire face à une responsabilité personnelle pour des violations ou des infractions en vertu des projets de loi C-26 et C-27 (mais ils pourraient faire valoir un moyen de défense fondé sur la diligence raisonnable).
- Les organismes de réglementation disposeraient de pouvoirs d'enquête étendus et renforcés.
- Les nouvelles règles concernant le développement et la mise en œuvre de l'IA dans le secteur privé seraient liées à la protection des données, à la limitation des résultats biaisés[2] et à des sanctions pécuniaires importantes en cas de contravention.
- Comme ces projets de loi viennent tout juste d'être déposés, les parties prenantes de l'industrie devraient avoir l'occasion de se prononcer au cours des étapes de l'étude en comité parlementaire.

Aperçu du projet de loi C-26

Le projet de loi C-26, la ***Loi sur la cybersécurité*** **(LCS)**, a été déposé le 14 juin 2022 afin de conférer au gouvernement fédéral de vastes pouvoirs sur les secteurs des infrastructures essentielles.

La partie 1 de la LCS modifierait la ***Loi sur les télécommunications*** afin d'habiliter le gouvernement fédéral à interdire la mise en œuvre d'un produit ou d'un service déterminé (ou ordonner de retirer un produit) considéré comme présentant un risque pour la sécurité nationale dans le secteur des télécommunications.

- Des sanctions pécuniaires pourraient être imposées pour le non-respect d'un décret de sécurité pouvant aller jusqu'à 25 000 $ pour une contravention initiale dans le cas d'un particulier (et jusqu'à 50 000 $ pour une contravention subséquente), et 10 000 000 $ dans le cas d'une organisation (et jusqu'à 15 000 000 $ pour une contravention subséquente).
- La LCS donnerait également au gouvernement le pouvoir de garder confidentiels les arrêtés en matière de préparation et d'intervention (p. ex., pour limiter la divulgation des cybervulnérabilités d'une entreprise de télécommunications).

La partie 2 de la LCS édicterait la ***Loi sur la protection des cybersystèmes essentiels*** **(LPCE)**, qui confère au gouvernement un plus grand pouvoir sur les mesures de cybersécurité mises en œuvre par les exploitants d'infrastructures essentielles, ainsi qu'un pouvoir de contrôle accru en ce qui concerne les obligations en matière de préparation et de signalement. D'autres obligations s'ajouteraient, notamment :

- La LPCE exigerait que les exploitants de cybersystèmes essentiels de quatre secteurs – télécommunications, énergie, finances et transports – signalent immédiatement les incidents et les atteintes au Centre canadien pour la cybersécurité (qui fait partie du Centre de la sécurité des télécommunications).
- Les organismes de réglementation, y compris le Bureau du surintendant des institutions financières et la Banque du Canada, auraient des pouvoirs accrus,

[1] Il est compté une violation distincte pour chacun des jours au cours desquels se commet ou se continue la violation.

[2] *Résultat biaisé* s'entend de contenu généré, prédiction ou recommandation faite ou décision prise par un système d'intelligence artificielle qui défavorisent, directement ou indirectement et sans justification, un individu sur le fondement d'un ou plusieurs motifs de distinction illicite prévus à l'article 3 de la Loi canadienne sur les droits de la personne, ou de leur effet combiné.

Personnes-ressources :

Hélène Deschamps Marquis
Leader nationale de la pratique
Confidentialité des données, Cybersécurité et Droit numérique
Associée, Deloitte Legal Canada
Tél. : 514-393-8300

Matt Saunders
Avocat associé
Deloitte Legal Canada
Tél. : 902-425-2431

Chetan Phull
Avocat associé
Deloitte Legal Canada
Tél. : 416-874-3400

Liens connexes :

Services de fiscalité de Deloitte

Deloitte Legal Canada S.E.N.C.R.L./s.r.l.

notamment des pouvoirs d'entrée dans tout lieu, ainsi qu'un pouvoir de vérification complet à l'égard des systèmes de cybersécurité d'un exploitant (incluant les documents et les dossiers).

- De plus, la LPCE exigerait des exploitants qu'ils établissent des programmes de cybersécurité rigoureux capables de détecter les menaces graves et de protéger les systèmes essentiels et de tenir des registres de la façon dont ces systèmes ont été mis en œuvre pour atténuer les risques.
- Les administrateurs et les dirigeants d'organismes d'infrastructures essentielles pourraient également être tenus personnellement responsables si leur organisation enfreint la LPCE; les sanctions pécuniaires pour les particuliers pourraient aller jusqu'à 1 000 000 $ par jour; pour les organisations, des sanctions pécuniaires pouvant aller jusqu'à 15 000 000 $ par jour seraient possibles en cas de violations continues.
- La liste précise des entités concernées par la nouvelle loi est encore en cours d'élaboration. Cependant, le gouvernement fédéral a spécifiquement cité les grandes entreprises de télécommunications et les compagnies ferroviaires canadiennes comme exemples lors d'un point de presse tenu le 14 juin 2022.
- Le gouvernement fédéral recommandera également à ses homologues provinciaux, territoriaux et municipaux d'envisager la rédaction et la mise en œuvre de lois similaires.

Aperçu du projet de loi C-27

Le projet de loi C-27, la ***Loi sur la mise en œuvre de la Charte du numérique***, qui avait été déposé à l'origine en 2020, mais qui n'avait pas été adopté avant les élections fédérales de l'an dernier, a été déposé le 16 juin 2022. Ce projet de loi est divisé en trois parties traitant (1) des obligations relatives à la protection des données, (2) des appels administratifs et (3) des nouvelles règles en matière d'IA.

La partie 1 édicterait la ***Loi sur la protection de la vie privée des consommateurs*** **(LPVPC)**, soit la deuxième tentative du gouvernement fédéral d'adopter une nouvelle loi sur la protection de la vie privée dans le secteur privé visant à moderniser la collecte, l'utilisation et la communication de renseignements personnels dans un monde numérique en constante évolution. Les principaux éléments de la LPVPC comprennent notamment ce qui suit :

- Les organisations qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre d'activités commerciales seraient tenues de mettre en œuvre un programme officiel de gestion de la protection des renseignements personnels, avec des ressources désignées et des politiques transparentes dans un langage clair pour les consommateurs.
- Les organisations seraient également tenues d'évaluer le volume et la nature sensible des renseignements personnels qui relèvent d'elles, de s'assurer d'obtenir un consentement valide de la part des consommateurs et de mettre en œuvre de manière formelle des périodes de conservation et des contrôles d'accès lorsqu'il s'agit de protéger les renseignements personnels (p. ex., des étapes d'authentification raisonnables pour les employés).
- Le commissaire fédéral à la protection de la vie privée (CPVP) aurait également de nouveaux pouvoirs pour rendre des ordonnances, y compris la capacité de forcer une entreprise à cesser de recueillir des données ou d'utiliser des renseignements personnels.
- Le CPVP serait également en mesure de recommander une gamme de sanctions financières en cas de non-conformité, y compris des sanctions administratives

pécuniaires pour avoir omis de mettre en œuvre un programme de gestion de la protection des renseignements personnels, ne pas avoir mis en œuvre des mesures de sécurité ayant trait aux renseignements personnels sous le contrôle de l'organisation, etc. Des pénalités allant jusqu'à 3 % des recettes globales ou 10 000 000 $ (selon le montant le plus élevé) pourraient être recommandées pour ces types de contraventions.

- Des infractions plus graves, comme le fait de ne pas signaler sciemment une atteinte à la protection des données au CPVP, pourraient entraîner des pénalités allant jusqu'à 5 % des recettes globales ou 25 000 000 $, selon le montant le plus élevé. Cependant, des moyens de défense fondés sur la diligence raisonnable et les efforts raisonnables déployés pour atténuer le préjudice seraient disponibles.
- La LPVPC définirait tous les renseignements personnels d'un mineur comme étant des renseignements de nature sensible et exigerait que les entreprises de technologies, médias et télécommunications (TMT) qui recueillent, utilisent ou communiquent les renseignements personnels de mineurs créent des messages spécifiques et des avis de consentement à l'intention des jeunes consommateurs.
- D'autres obligations comprendraient la mise en place de processus pour traiter les demandes des consommateurs visant le retrait de leur consentement, le transfert de leurs renseignements personnels à une autre organisation et la suppression des renseignements personnels au dossier.
- Les organisations qui utilisent des outils décisionnels algorithmiques (c.-à-d. la technologie utilisée à la place de la prise de décision par un humain), qui pourraient avoir une « incidence importante » sur un individu, seraient également tenues d'avoir des processus en place pour répondre aux demandes d'information des consommateurs concernant ces systèmes (p. ex., les types de renseignements personnels utilisés, la provenance de ces renseignements et les principaux facteurs ayant mené à la décision).

La partie 2 édicterait la ***Loi sur le Tribunal de la protection des renseignements personnels et des données*** **(LTPRPD)** constituant un nouveau tribunal administratif (Tribunal) qui entendrait les appels à l'encontre des décisions du CPVP et qui pourrait infliger des sanctions pécuniaires administratives en fonction des recommandations du CPVP. D'autres éléments clés comprennent ce qui suit :

- Alors que le Tribunal recevrait les recommandations du CPVP, la LTPRPD permettrait au Tribunal d'y substituer sa propre décision.
- Il n'y aurait aucun droit d'appel d'une décision du Tribunal; toutefois, une partie pourrait demander un contrôle judiciaire devant la Cour fédérale.
- Le Tribunal serait composé de trois à six membres à temps plein ou à temps partiel, et au moins trois d'entre eux auraient de l'expérience dans le domaine du droit à l'information et à la protection des renseignements personnels.

La partie 3 édicterait la ***Loi sur l'intelligence artificielle et les données***, qui vise à réglementer les échanges et le commerce internationaux et interprovinciaux en matière de systèmes d'IA. Plus particulièrement :

- La nouvelle loi créerait plusieurs infractions et violations liées à l'IA, y compris l'utilisation inappropriée de renseignements personnels, le déploiement imprudent de l'IA susceptible de causer un préjudice grave aux individus ou des dommages importants aux biens, et le déploiement de l'IA en vue de commettre une fraude.

- Les pénalités seraient les suivantes : jusqu'à 25 000 000 $ ou 5 % des recettes globales pour les organisations, et une amende discrétionnaire ou une peine d'emprisonnement pouvant aller jusqu'à cinq ans pour les particuliers.
- La question de savoir si une IA donnée est un « système à incidence élevée » sera importante. Les futurs règlements en fourniront la définition. D'ici là, les organisations peuvent se tourner vers la Loi sur l'IA[3] de l'Union européenne aux fins d'orientations (si l'on se fie à la pratique législative antérieure au Canada; par exemple, le législateur a déjà utilisé les quatre groupes de classification des risques liés à l'IA de la Loi sur l'IA de l'Union européenne dans la Directive sur la prise de décision automatisée[4] du Conseil du Trésor).

Comment Deloitte peut-il vous aider?

Au fur et à mesure que l'impact de ces propositions législatives se fait connaître, l'équipe nationale de Deloitte Legal en matière de confidentialité des données et de cybersécurité est heureuse d'aider les organisations à se préparer et à réagir à ces changements anticipés (et substantiels) dans le contexte fédéral canadien de la cybersécurité et de la protection de la vie privée.

[3] https://eur-lex.europa.eu/legal-content/fr/TXT/HTML/?uri=CELEX:52021PC0206&from=fr

[4] Cette Directive énonce les exigences auxquelles doivent satisfaire les institutions fédérales pour assurer l'utilisation responsable et éthique des systèmes décisionnels automatisés, y compris ceux qui utilisent l'IA. (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32592)

Deloitte.

Deloitte S.E.N.C.R.L/s.r.l.
La Tour Deloitte
1190, avenue des Canadiens-de-
Montréal, bureau 500
Montréal, Québec H3B 0M7
Canada

Deloitte assure la vérification et l'assurance, les services-conseils, les services-conseils financiers, les services-conseils en matière de risques, les services fiscaux, et des services connexes aux clients publics et privés de plusieurs secteurs d'activité. Deloitte dessert quatre des cinq entreprises Fortune Global 500® par l'entremise d'un réseau mondial d'entreprises membres dans plus de 150 pays et territoires qui offrent des capacités, des connaissances et des services de calibre mondial pour relever les défis commerciaux les plus complexes des clients. Deloitte s.r.l., société à responsabilité limitée de l'Ontario, est la société canadienne membre du Deloitte Touche Tohmatsu Limited. Deloitte fait référence à une ou plusieurs sociétés du Deloitte Touche Tohmatsu Limited, une société privée du Royaume-Uni limitée par garantie, et à son réseau d'entreprises membres, chacune étant une entité juridique distincte et indépendante. Veuillez consulter le site www.deloitte.com/about pour obtenir une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres.

Notre objectif global a une incidence importante. Chez Deloitte Canada, cela se traduit par un meilleur avenir en accélérant et en élargissant l'accès aux connaissances. Nous croyons que nous pouvons atteindre cet objectif en mettant en pratique nos valeurs communes afin de mener la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour obtenir un effet mesurable.

Pour en savoir plus sur Deloitte, environ 330.000 professionnels, dont plus de 11.000 font partie de l'entreprise canadienne, veuillez communiquer avec nous sur LinkedIn, Twitter, Instagram ou Facebook.