26 JUIN 2025 • 7 MIN. DE LECTURE

Le gouvernement réintroduit un projet de loi sur la cybersécurité pour les secteurs fédéraux « critiques »

AUTEURS


Molly Reynolds


Julie Himo


Rosalie Jetté


Nic Wall


Mavra Choudhry

La semaine dernière, le gouvernement fédéral a présenté le projet de loi C-8, *Loi sur la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*. Le projet de loi C-8 est presque identique au projet de loi éponyme C-26 introduit lors de la dernière session parlementaire. Il introduit notamment la *Loi sur la protection des cybersystèmes essentiels* (LPCE) et certains amendements à la *Loi sur les télécommunications*.

Ce que vous devez savoir

- Selon la version de la LPCE proposée, les organisations qui exploitent des « systèmes critiques » ou fournissent des « services critiques » désignés dans les secteurs de la finance, des télécommunications, de l'énergie et de l'infrastructure devront établir et mettre en œuvre un programme de cybersécurité, atténuer les risques associés aux chaînes d'approvisionnement et aux tiers et signaler rapidement les incidents de cybersécurité.
- Les exploitants désignés doivent aviser l'organisme réglementaire compétent de tout changement important dans leur propriété ou leur contrôle ou dans leur chaîne d'approvisionnement.
- Les organismes de réglementation dans ces secteurs seront également dotés d'importants nouveaux pouvoirs et pourront notamment demander de l'information ou examiner un lieu afin de vérifier la conformité ou de prévenir la non-conformité et imposer des pénalités pouvant aller jusqu'à 15 millions de dollars pour la non-conformité avec les ordonnances et les règlements.
- Le projet de loi C-8 modifie également la *Loi sur les télécommunications* en accordant au ministre de l'Industrie le pouvoir d'interdire à un fournisseur de services de télécommunication d'utiliser des produits ou des services fournis par une personne précise ou de fournir des produits ou des services à une personne précise.
- Les entreprises soumises à ces exigences doivent s'assurer de bien les comprendre et de mettre en place des mesures pour s'y conformer et atténuer les risques connexes.

Portée de la LPCE

La LPCE proposée impose des obligations à certaines catégories d'organisations qui fournissent des services ou exploitent des systèmes qui sont « critiques » pour la sécurité nationale ou la sécurité publique. Les services et les systèmes qui sont actuellement désignés comme critiques sont :

- 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 Parlement
- les systèmes bancaires
- les systèmes de compensations et de règlements

La plupart des obligations prévues par la LPCE s'appliquent aux « exploitants désignés » de ces secteurs qui contrôlent ou exploitent un « cybersystème essentiel » ou en sont propriétaires. Même si la version actuelle du projet de loi ne précise pas les catégories d'exploitants désignés, elle définit un « cybersystème essentiel » comme étant « tout cybersystème dont la compromission, en ce qui touche la confidentialité, l'intégrité ou la disponibilité, pourrait menacer la continuité ou la sécurité d'un service critique ou d'un système critique ».

Obligations des exploitants désignés

En vertu de la LPCE, un exploitant désigné devra :

- établir un programme de cybersécurité relativement à ses cybersystèmes essentiels peu après qu'il devient un exploitant désigné;
- inclure dans son programme de cybersécurité des mesures raisonnables en vue de : protéger ses cybersystèmes essentiels contre toute compromission; (ii) détecter les cybermenaces et les incidents de cybersécurité, et (iii) réduire au minimum les conséquences des incidents de cybersécurité qui se produisent;
- repérer les risques associés à la chaîne d'approvisionnement et aux tiers et prendre des mesures raisonnables pour les atténuer;
- aviser l'organisme réglementaire compétent de tout changement important dans (i) leur propriété ou leur contrôle ou (ii) leur chaîne d'approvisionnement ou leur utilisation de produits et services de tiers;
- examiner régulièrement son programme de cybersécurité et y apporter des améliorations;
- déclarer tout incident de cybersécurité concernant l'un de ses cybersystèmes essentiels au Centre de la sécurité des télécommunications dans un délai qui sera déterminé par règlement (d'au plus de 72 heures), puis en aviser sans délai l'organisme réglementaire compétent;
- tenir des documents attestant sa conformité avec les obligations prévues par la LPCE.

Des exigences supplémentaires pourraient être imposées par règlement.

Application de la LPCE

Le projet de loi C-8 accorde aux organismes de réglementation désignés des pouvoirs étendus pour faire appliquer les exigences de la LPCE. À l'heure actuelle, les autorités réglementaires désignées comprennent le Bureau du surintendant des institutions financières (BSIF), le ministre de l'Industrie, la Banque du Canada, la Commission canadienne de sûreté nucléaire, la Régie de l'énergie du Canada et le ministre des Transports. Ces organismes ont notamment les pouvoirs suivants :

- demander de l'information ou examiner un lieu afin de vérifier la conformité ou de prévenir la non-conformité;
- ordonner aux exploitants désignés de mener des vérifications internes et d'en communiquer les résultats;
- rendre des ordonnances de conformité et conclure des accords de conformité;
- imposer des pénalités pouvant aller jusqu'à 15 millions de dollars pour la non-conformité avec les ordonnances et les règlements.

Modifications à la *Loi sur les télécommunications*

Le projet de loi C-8 modifie également la *Loi sur les télécommunications* en accordant au ministre de l'Industrie le pouvoir d'interdire à un fournisseur de services de télécommunication d'utiliser des produits ou des services fournis par une personne précise ou de fournir des produits ou des services à une personne précise. Une ordonnance à cet effet ne pourrait être prise que s'il existe des motifs raisonnables de croire que cela est nécessaire pour sécuriser le système canadien de télécommunication face à toute menace. L'ordonnance doit par ailleurs être proportionnée à la gravité de la menace. Tout comme en vertu de la LPCE, les pénalités en cas de non-conformité pourraient atteindre 15 millions de dollars.

À retenir

Même si le projet de loi C-8 vient tout juste d'être déposé, les entreprises qui sont régies par la Loi sur les télécommunications et qui seront probablement assujetties à la LPCE devraient être proactifs sur trois plans en particulier.

D'abord, elles devraient réfléchir sur la façon dont elles protégeront les renseignements assujettis au secret professionnel de l'avocat, au privilège relatif au litige et à tout autre privilège juridique. Protéger ces renseignements en cas d'incident de cybersécurité peut présenter des défis, compte tenu des vastes pouvoirs de mise en application (notamment les pouvoirs de fouille et de saisie) accordés aux organismes de réglementation, des obligations de tenue de dossiers imposées aux exploitants désignés afin de prouver la conformité et de l'exigence d'aviser sans délai le Centre de la sécurité des télécommunications et l'organisme de réglementation compétent en cas d'incident de cybersécurité.

Ensuite, les entreprises devraient prévoir l'examen et la mise à jour de leurs plans d'intervention en cas d'incident et de leurs politiques en matière de cybersécurité, conformément aux réformes proposées dans le projet de loi C-8. Leurs examens actuels et à venir devraient être axés sur les risques associés à la chaîne d'approvisionnement ou aux tiers, y compris les risques posés par les fournisseurs de services essentiels (particulièrement les fournisseurs de services informatiques), les autres fournisseurs clés et les fabricants d'appareils ou de produits. Une fois qu'elles auront obtenu davantage d'information, les entreprises devraient aussi examiner dans quelle mesure leurs « cybersystèmes essentiels » peuvent être séparés des autres systèmes et déterminer si cela peut contribuer à simplifier la conformité.

En troisième lieu, les entreprises assujetties aux réformes du projet de loi C-8 devraient réfléchir à la façon dont ces nouvelles exigences pourraient ou devraient être reflétées dans le cadre de la conclusion d'ententes de service avec des tiers. De même, les fournisseurs de services devraient s'attendre à l'exigence de normes de cybersécurité plus

élevées par leurs clients réglementés, particulièrement si leurs services sont liés aux cybersystèmes essentiels.

Si vous souhaitez discuter ces enjeux et ces questions, veuillez contacter les auteurs.

Dernières nouvelles et publications

L'appel du petit-déjeuner : *Remington Development v. CPKC*

Nos experts de l'appel du petit-déjeuner retournent sur les bancs d'école pour démêler le nœud gordien des dommages-intérêts pour la perte du profit espéré.

Lire la suite

Manitoba introduces algorithmic pricing and public sector AI regulation

Bill 49 and Bill 59 shape how AI is used by private and public sector corporations.

Lire la suite

Ontario releases framework for its first-of-its-kind Defence Industrial Strategy

Framework for the Ontario Defence Industrial Strategy outlines a ten year plan to position the province as a trusted partner in domestic and allied defence supply chains.

Lire la suite