# Projet de loi C-26 : Nouvelle loi canadienne sur la cybersécurité des infrastructures essentielles

**20 juin 2022**

Une nouvelle loi sur la cybersécurité a été introduite par le gouvernement fédéral qui *imposera des obligations aux organisations agissant dans certains secteurs d'importance nationale. Ces obligations comprendront des programmes de* cybersécurité obligatoires et le signalement des incidents de cybersécurité, et seront assorties de sanctions administratives pécuniaires en cas de non-conformité.

## Aperçu

Le 14 juin, la Chambre des communes a déposé le projet de loi C-26, qui comprend la nouvelle Loi sur la protection des cybersystèmes essentiels (LPCE), ou en anglais, le *Critical Cyber Systems Protection Act* (CCSPA). La LPCE établit un vaste cadre réglementaire permettant au gouvernement fédéral de :

- définir et renforcer la cybersécurité de base pour les systèmes et services d'importance nationale critique;
- exiger de certaines organisations qu'elles élaborent et mettent en œuvre certains programmes de cybersécurité;
- veiller à ce que les incidents de cybersécurité ayant un impact sur les systèmes et services vitaux soient signalés;
- publier des directives relatives à la cybersécurité des systèmes;
- encourager la conformité par l'introduction de sanctions administratives pécuniaires.

Nous examinerons chacun d'entre eux plus en détails ci-dessous.

## Secteurs impactés

La LPCE imposera des obligations aux "exploitants désignés", c'est-à-dire aux personnes, sociétés de personnes ou organisations non dotées de la personnalité morale qui appartiennent à une catégorie d'exploitants figurant à l'annexe 2 de la Loi, catégories qui seront identifiées par décret. L'annexe 1 de la LPCE identifie les services et systèmes critiques qui seront à la base de ces désignations, lesquels pourront être ajustés ultérieurement :

- Services de télécommunication
- Systèmes de pipelines et de lignes électriques interprovinciaux ou internationaux
- Systèmes d'énergie nucléaire
- Systèmes de transport relevant de la compétence législative du Parlement;
- Systèmes bancaires
- Systèmes de compensations et de règlements

Chaque catégorie d'exploitants se verra attribuer un organisme réglementaire correspondant : soit le ministre de l'Industrie, le ministre des Transports, le surintendant des institutions financières, la Régie canadienne de l'Énergie, la Banque du Canada ou la Commission canadienne de sûreté nucléaire.

# Programme de cybersécurité

Les exploitants désignés seront tenus d'établir un programme de cybersécurité à l'égard des systèmes critiques qu'ils gèrent. Le programme de cybersécurité devra comprendre des mesures de sécurité raisonnables afin de :

- identifier et gérer les risques de cybersécurité, y compris les risques liés à la chaîne d'approvisionnement de l'opérateur et à l'utilisation de produits et services tiers ;
- protéger les systèmes critiques contre toute compromission;
- détecter les incidents de sécurité affectant les systèmes; et
- minimiser l'impact de tout incident de sécurité.

Les exploitants désignés auront l'obligation de prendre des mesures raisonnables pour atténuer les risques identifiés liés à leurs chaînes d'approvisionnement et à l'utilisation de produits et services tiers.[1]

**Dépôt du programme de cybersécurité** . Les exploitants désignés seront tenus de fournir leur programme de sécurité auprès de leur organisme réglementaire, de réexaminer annuellement leur programme et d'informer leur organisme de réglementation si des modifications ont été apportées à la suite de ce réexamen.[2]

**Changements importants** . Les exploitants désignés seront tenus de notifier à leur organisme réglementaire certains changements importants, notamment (i) tout changement important dans la propriété ou le contrôle de l'exploitant désigné, (ii) tout changement important dans la chaîne d'approvisionnement de l'exploitant désigné ou dans son utilisation de produits et services tiers, et (iii) toutes circonstances prévues par réglement.[3]

# Directives de cybersécurité

La LPCE prévoit que le gouverneur en conseil pourra, par décret, donner des directives enjoignant à un exploitant désigné de se conformer à toute mesure prévue dans la directive en vue de la protection d'un cybersystème essentiel. Ces instructions pourront exiger des exploitants désignés qu'ils prennent des mesures spécifiques en réponse aux cybermenaces émergentes et à d'autres développements. La LPCE autorise également le partage d'informations entre le gouvernement, les organismes

réglementaires et les services de police à toute fin liée à l'élaboration, à la modification ou à la révocation d'une instruction de cybersécurité concernant un exploitant désigné[4].

## Signalement des incidents de cybersécurité

L'un des principaux objectifs de la LPCE est de préserver la continuité des services et systèmes vitaux en veillant à ce que les systèmes ne soient pas compromis et, dans la mesure où ils le sont, à ce que la compromission soit détectée et son impact minimisé[5]. En conséquence, la LPCE exigera des exploitants désignés qu'ils "signalent immédiatement un incident de cybersécurité concernant leurs systèmes essentiels", conformément au règlement. L'exploitant désigné devra signaler l'incident immédiatement à son organisme réglementaire, et le déclarer au Centre de la sécurité des télécommunications[6]. Sur demande de l'organisme réglementaire, l'exploitant devra lui remettre une copie du rapport d'incident.

Un "incident de cybersécurité" est défini comme étant tout incident qui nuit ou peut nuire à (a) la continuité ou la sécurité d'un service ou d'un système critique, ou (b) la confidentialité, l'intégrité ou la disponibilité du cybersystème essentiel[7].

Pour ceux qui sont familiers avec la déclaration des atteintes à la vie privée en vertu notamment de *la Loi sur la protection des renseignements personnels et les documents* électroniques (LPRPDE), le signalement des cyberincidents en vertu de la LPCE sera très différent. Le signalement sera basé sur l'interférence avec les systèmes ou services essentiels, et non sur les informations contenues dans les systèmes ou les dossiers. Le signalement sera également requis en fonction du simple potentiel d'interférence, une question de risque et de probabilité qui sera laissée à l'interprétation des régulateurs et des tribunaux.

## Registre des incidents et autres documents

Les exploitants désignés seront tenus de conserver un registre sur les incidents de cybersécurité ainsi que plusieurs autres informations, incluant :

- toute mesure prise pour mettre en œuvre le programme de cybersécurité de l'opérateur désigné ;
- tout incident de cybersécurité que l'exploitant désigné a signalé en vertu de l'article 17 ;
- toute mesure prise par l'exploitant désigné en vertu de l'article 15 pour atténuer les risques liés à la chaîne d'approvisionnement ou aux tiers ;
- toute mesure prise par l'exploitant désigné pour mettre en œuvre une directive en matière de cybersécurité ; et
- toute autre question prescrite par règlement.

Les exploitants désignés seront tenus de conserver ces informations au Canada, à un endroit prescrit par règlement ou, si aucun endroit n'est prescrit, dans leur établissement. Ils devront également tenir les documents de la manière et pour la période indiquée par l'organisme réglementaire compétent, à moins qu'une autre manière ou période ne soit prescrite par règlement.

## Sanctions administratives pécunières

La LPCE permettra à chaque organisme réglementaire d'émettre des sanctions administratives pécuniaires, dont les montants maximaux seront fixés par règlement et pourront atteindre 15 millions de dollars. De telles sanctions pourront être émises pour toute violation de la LPCE, y compris l'omission de signaler un incident de cybersécurité et le non-respect d'une directive de cybersécurité.

Les organismes réglementaires auront également le pouvoir d'engager des procédures réglementaires conduisant à des amendes et éventuellement à des peines d'emprisonnement en cas de non-respect des dispositions de la LPCE.

## Conclusion

La LPCE constitue une évolution majeure de la législation canadienne en matière de cybersécurité. Les organisations qui fournissent et exploitent des services et systèmes essentiels auxquels s'appliquera la LPCE ont peut-être déjà des programmes de cybersécurité bien établis, mais si la LPCE est adoptée, elles seront confrontées à de nouvelles exigences ainsi qu'à des obligations de dépôt de leur programme de cybersécurité et de signalement des incidents. Les obligations de dépôt et de signalement sont en soi les éléments clés de la nouvelle loi, et s'alignent sur le type de politique gouvernementale que beaucoup considèrent comme essentiel pour lutter contre la cybercriminalité.

Pour plus d'informations sur la LPCE ou toute autre aide liée à la gouvernance et à la réponse en matière de cybersécurité, veuillez contacter un membre de notre équipe de cybersécurité.

## Notes de bas de page

[1] LPCE, Article 15.

[2] LPCE, Article 10.

[3] LPCE, Article 14(1).

[4] LPCE, Article 23.

[5] LPCE, Article 5.

[6] LPCE, Article 18.

[7] LPCE, Article 2.

**Par**

Shane Morganstein, Daniel J. Michaluk

**Services**

Cybersécurité, respect de la vie privée et protection des renseignements personnels

---

## BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

**blg.com**

## Bureaux BLG


**Calgary**

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

**Ottawa**

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

**Vancouver**

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

**Montréal**

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

**Toronto**

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749