Projet de loi C-8 : un nouveau cadre fédéral de cybersécurité pour les télécommunications et les cybersystèmes essentiels

21 septembre 2026

Auteurs

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Guillaume Laberge

Associé, Avocat

Ghiles Helli

Avocat

Le projet de loi C-8 a reçu la sanction royale le 15 juin 2026et mérite une attention particulière. Il marque un changement de rythme en cybersécurité : il donne à l'État fédéral des moyens pour intervenir rapidement lorsqu'une menace est identifiée. De plus, il impose pour certains acteurs, une logique de conformité avec des attentes plus élevées et des sanctions réelles en cas de manquement.

Le texte de loi s'articule autour de deux axes. D'une part, il muscle la *Loi sur les télécommunications* en habilitant le gouverneur en conseil et le ministre de l'Industrie à imposer des mesures concrètes par décret ou arrêté. D'autre part, il crée la *Loi sur la protection des cybersystèmes essentiels* (la « LPCSE »), visant des services et systèmes critiques.

Par ces modifications législatives, la cybersécurité sort du sous-sol : elle devient un enjeu de gouvernance et de conformité. Avec l'adoption de cette loi, les choix technologiques, la gestion des fournisseurs et la réponse aux incidents de cybersécurité devront être plus robustes, mieux encadrés et dûment documentés. Nous sommes d'avis que les organisations qui se préparent maintenant (gouvernance, preuves, plans d'intervention) seront plus agiles et plus crédibles auprès de leurs clients et partenaires.

Une distinction importante s'impose toutefois d'entrée de jeu : les modifications de la *Loi sur les télécommunications* prévues à la Partie 1 sont désormais en vigueur, tandis que l'entrée en vigueur

de la LPCSE prévue à la Partie 2 dépendra d'un ou de plusieurs décrets. À ce jour, l'annexe 2 de la LPCSE, qui doit identifier les catégories d'exploitants désignés et leur organisme réglementaire correspondant, demeure vide.

À retenir en un coup d'œil - Le projet de loi C-8 introduit :

(i) un pouvoir d'ordonnance en télécommunications (décrets/arrêtés);
(ii) un cadre de programme obligatoire pour certains cybersystèmes essentiels (LPCSE), sous réserve de son entrée en vigueur et des désignations à venir;
et (iii) une mise en application renforcée (renseignements, vérifications, SAP, infractions).

Partie 1 de la loi — Télécommunications : la sécurité devient un levier d'action

Le projet de loi C-8 inscrit explicitement la sécurité dans la politique canadienne de télécommunication en ajoutant l'objectif de « promouvoir la sécurité du système canadien de télécommunication ». Il fournit l'assise législative à des interventions désormais conçues pour être directes, rapides et exécutoires.

Un élément important de la loi, à la fois pour son application et pour circonscrire la nature des menaces visées, est la précision selon laquelle « l'ingérence, la manipulation, la perturbation ou la dégradation » en ce qui concerne un système de télécommunication s'entend notamment d'actes de nature technique qui entravent le fonctionnement de ce système, mais ne vise pas les effets « de l'expression licite d'opinions, de la persuasion ou du débat politique ». Le texte ménage ainsi expressément un espace pour la liberté d'expression et le débat public licite.

La Partie 1 de la loi comporte une mécanique d'application à deux niveaux : **les décrets** et **les arrêtés ministériels** (relevant du ministre de l'Industrie).

Le décret

Le gouverneur en conseil peut agir par décret s'il a des motifs raisonnables de croire que la mesure est nécessaire pour sécuriser le système face à une menace, et qu'elle est raisonnable eu égard à cette menace. Concrètement, le décret peut :

interdire aux fournisseurs de services de télécommunication (« FST ») d'utiliser, dans leurs réseaux/installations (ou en lien avec ceux-ci), les produits et services fournis par une personne précisée;
ordonner le retrait de produits fournis par une personne précisée.

Le projet de loi C-8 impose une contrainte de proportionnalité : la portée et la teneur doivent être nécessaires et raisonnables eu égard à la gravité de la menace. Le décret prime sur des décisions/arrêtés/autorisations incompatibles, y compris sous la *Loi sur la radiocommunication*. D'autre part, l'État n'assume pas le coût économique : aucune indemnité n'est payable pour les pertes financières attribuables au décret. Il s'agit, en quelque sorte, de l'artillerie lourde de la loi.

Le décret peut également comporter une interdiction de divulguer son existence ou tout ou partie de son contenu. Avant d'inclure une telle interdiction, le gouverneur en conseil doit notamment tenir compte de la mesure dans laquelle la divulgation pourrait compromettre l'objectif du décret, de la nécessité de cette interdiction compte tenu de la nature de la menace, de la possibilité d'en limiter la portée, de son effet sur la transparence et la responsabilisation du gouvernement du Canada, ainsi que des observations des FST touchés.

Avant de prendre le décret, le gouverneur en conseil doit aussi considérer l'effet de la mesure sur les activités des FST visés, ses répercussions financières, son effet sur la fourniture des services de télécommunication au Canada — y compris sur la confidentialité et la sécurité des télécommunications — ainsi que ses répercussions potentielles sur la protection de la vie privée des Canadiens.

L’arrêté

Le ministre de l’Industrie peut imposer, par arrêté, des mesures très opérationnelles lorsqu’elles sont nécessaires et raisonnables eu égard à la menace. L’arrêté peut notamment :

interdire l’utilisation de produits/services précis, ordonner des retraits, imposer des conditions d’utilisation et de fourniture de services;
encadrer des ententes de service ou y mettre fin;
exiger des processus d’examen des réseaux/installations et de projets d’approvisionnement;
imposer des plans de sécurité, des évaluations de vulnérabilités et des mesures d’atténuation;
imposer la mise en œuvre de normes;
exiger un système d’appoint;
interdire à des FST de fournir des services à une personne précisée;
ordonner la suspension, pour une période donnée, de la fourniture de services à une personne précisée;
interdire certaines mises à niveau;
ordonner aux FST de faire ou de s’abstenir de faire toute chose précisée, sous réserve des limites prévues par la loi.

Comme pour le décret, le ministre doit tenir compte des impacts opérationnels et financiers, de l’effet sur la fourniture des services, y compris sur la confidentialité et la sécurité des télécommunications, et des répercussions potentielles sur la vie privée des Canadiens. Le ministre ne peut ordonner ni l’interception d’une communication privée ou radiotéléphonique, ni le décodage d’une communication privée chiffrée. Enfin, l’arrêté est, lui aussi, assorti d’une règle d’absence d’indemnité.

La loi prévoit aussi une limite particulière : la suspension de la fourniture de services à un individu ne peut être ordonnée que si l’arrêté est nécessaire pour sécuriser le système canadien de télécommunication face à une menace de nature technique précisée dans l’arrêté.

Comme le décret, l’arrêté peut comporter une interdiction de divulgation. Avant d’inclure une telle interdiction, le ministre doit tenir compte de facteurs comparables, dont l’effet de la non-divulgation sur les principes de transparence et de responsabilisation du gouvernement du Canada.

Particularités sur la publication des décrets et des arrêtés

En principe, les décrets et arrêtés doivent être publiés dans la *Gazette du Canada* dans les 90 jours suivant leur prise, mais l’autorité peut ordonner l’absence de publication dans le texte même. De plus, l’inclusion par renvoi favorise l’intégration de documents techniques évolutifs. On peut donc s’attendre à l’adoption par un tel mécanisme de normes techniques internationales.

Collecte de renseignements par le ministre

Le projet de loi C-8 prévoit que le ministre peut exiger la communication de renseignements s’il a des motifs raisonnables de croire, d’une part, qu’il est raisonnable qu’ils soient fournis eu égard à la gravité de la menace et, d’autre part, qu’ils sont nécessaires. Toutefois un cadre de confidentialité est mis en place pour les informations transmises, notamment lorsqu’il s’agit de secrets industriels ou de renseignements financiers, commerciaux, scientifiques ou techniques. Les renseignements personnels et les renseignements dépersonnalisés sont aussi visés par des mesures de protection.

Le texte prévoit aussi l’échange de renseignements entre diverses autorités fédérales, ainsi qu’avec les provinces, des États étrangers ou certaines organisations internationales dans le cadre d’accords écrits. Lorsqu’il s’agit de renseignements personnels ou dépersonnalisés, leur portée et leur teneur

doivent être raisonnables eu égard à la gravité de la menace. La loi prévoit en outre leur retrait lorsqu'ils ne sont plus nécessaires.

Il faut aussi noter que les renseignements personnels et les renseignements dépersonnalisés sont réputés être des renseignements confidentiels pour l'application de la Partie 1, même s'ils n'ont pas été expressément désignés comme tels.

Partie 2 de la loi – *Loi sur la protection des cybersystèmes essentiels* (LPCSE) :

Une précision est essentielle : cette partie de la loi n'entrera en vigueur qu'à la date ou aux dates fixées par décret. En outre, l'assujettissement effectif dépendra de futures désignations, puisque l'annexe 2 est actuellement vide. Le cadre est donc adopté, mais son déclenchement opérationnel reste à venir.

Concepts clés : ce que la loi vise réellement

La LPCSE vise des cybersystèmes essentiels au sens strict du texte, c'est-à-dire des cybersystèmes 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. La définition de « cybersystème » est volontairement large. En pratique, la loi ne se limite donc pas à un « réseau » au sens classique : elle peut englober des plateformes, environnements infonuagiques, systèmes de contrôle, services numériques, et actifs techniques interconnectés, dès lors que leur compromission pourrait affecter un service ou système critique.

La version sanctionnée ajoute aussi une définition de la « vérification interne », soit un examen indépendant et objectif effectué conformément à des directives reconnues à l'échelle internationale sur les pratiques professionnelles en matière de vérification interne. Cela renforce l'idée que la conformité attendue dépasse la seule adoption de politiques internes et suppose, au besoin, des mécanismes structurés d'assurance.

Désignations : comment une organisation devient assujettie

L'exploitant « désigné » qui contrôle, exploite ou possède un cybersystème essentiel est tenu de se conformer aux dispositions de la LPCSE et de ses règlements concernant ce cybersystème. Sur quoi repose cette désignation?

D'abord, les « services critiques » et « systèmes critiques » sont ceux énumérés à l'Annexe 1, soit : 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. Par décret, on peut ajouter, modifier ou retrancher des éléments de cette annexe dans le champ de compétence visé par la loi.

Ensuite, la loi prévoit une annexe actuellement vide, qui permet d'établir des catégories d'exploitants et l'organisme correspondants à ces services ou systèmes critiques.

En pratique, l'assujettissement dépend à la fois du service/système critique visé (Annexe 1) et de la catégorie d'exploitant dans laquelle l'organisation est classée (Annexe 2).

Programme de cybersécurité : l'obligation structurante

Le cœur de la LPCSE est l'obligation de bâtir un programme de cybersécurité. Après sa désignation

par une modification de l'Annexe 2, un exploitant doit établir, dans les 90 jours, un programme relatif à ses cybersystèmes essentiels.

Ce programme doit inclure des mesures, conformément aux règlements, pour identifier et gérer les risques organisationnels (incluant la chaîne d'approvisionnement et l'utilisation de produits et services de tiers), protéger les cybersystèmes essentiels, détecter les incidents et minimiser leurs conséquences, ainsi que toute mesure prévue par règlement. Le programme n'est donc pas une simple politique : il doit couvrir l'ensemble du cycle de gestion du risque et se prêter à une lecture « de conformité ». Cela forcera les organismes et entreprises à réagir rapidement lors d'une telle désignation.

La loi impose aussi une mécanique de supervision : dès que le programme est établi, l'exploitant doit en aviser par écrit l'organisme réglementaire compétent.

La loi exige aussi la mise à jour périodique de tout tel programme. Enfin, des obligations de notification existent lorsque surviennent des changements structurants (propriété/contrôle, chaîne d'approvisionnement, utilisation de tiers, etc.).

Cette cadence transforme la cybersécurité en obligation de gouvernance et de maintenance, pas en projet ponctuel.

Chaîne d'approvisionnement et tiers : de l'évaluation à l'atténuation

La LPCSE insiste explicitement sur la chaîne d'approvisionnement. Une fois les risques liés à la chaîne d'approvisionnement et aux tiers identifiés dans le programme (art. 9(1)a)), l'exploitant désigné est tenu de les atténuer (art. 15). Le verbe est important : il ne suffit pas de « constater » ou de « surveiller »; la loi impose une démarche active d'atténuation, qui devra être démontrable.

Le Centre de la sécurité des télécommunications (le « CST ») peut élaborer des lignes directrices sur l'atténuation des risques associés aux chaînes d'approvisionnement et à l'utilisation de produits et services de tiers, en s'appuyant sur des cadres internationalement reconnus. Le régulateur compétent peut aussi transmettre au CST des renseignements, y compris confidentiels, concernant le programme ou les mesures prises, afin que le CST fournisse avis, conseils et services selon son mandat.

Pour les organisations, cela annonce une convergence entre exigences réglementaires et attentes techniques : la gestion des fournisseurs, des accès, des mises à jour, des dépendances logicielles et des sous-traitants devient un volet « cœur » de la conformité.

Signalement des incidents : une obligation de vitesse et de coordination

La LPCSE crée une obligation de déclaration des incidents de cybersécurité au CST. Tout exploitant désigné doit déclarer, dans les délais réglementaires qui ne peuvent dépasser 72 heures, tout incident de cybersécurité concernant un de ses cybersystèmes essentiels. La définition d'« incident de cybersécurité » couvre un incident (acte, omission ou situation) qui nuit ou peut nuire à la continuité ou la sécurité d'un service/système critique, ou à la confidentialité, l'intégrité ou la disponibilité du cybersystème essentiel.

Après la déclaration au CST, l'exploitant doit, sans délai, aviser l'organisme réglementaire compétent et lui remettre une copie du rapport d'incident. Le texte précise que ces obligations n'ont

pas pour effet de diminuer les obligations issues de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Directives de cybersécurité : l'outil d'intervention obligatoire

La LPCSE prévoit un instrument particulièrement intrusif : les directives de cybersécurité. Par décret, on peut donner des directives enjoignant à un exploitant désigné (individuellement ou par catégorie) de se conformer à toute mesure prévue dans les directives afin de protéger un cybersystème essentiel, mais seulement s'il a des motifs raisonnables de croire que les directives sont nécessaires. Avant de prendre le décret, le gouvernement doit considérer les impacts opérationnels, la sécurité publique, la protection de la vie privée, les impacts financiers, ainsi que les impacts sur la fourniture des services/systèmes critiques. La portée et la teneur doivent être raisonnables eu égard à l'objectif de protection, et l'exploitant visé est tenu de s'y conformer.

La loi prévoit aussi deux limites explicites : le gouverneur en conseil ne peut ordonner ni le décodage d'une communication privée chiffrée, ni l'interception d'une communication privée ou radiotéléphonique.

Par ailleurs, un « garde-fou » lié à la connaissance est mis en place : un exploitant ne peut être reconnu coupable d'y avoir contrevenu sauf si la directive avait été portée à sa connaissance ou si des mesures raisonnables avaient été prises pour l'en informer. Mais il sera important pour un exploitant de ne pas ignorer les avis reçus, même si ceux-ci sont parfois d'apparence bénigne.

L'exploitant visé ne pourra pas communiquer l'existence ou le contenu d'une directive sauf dans la mesure nécessaire pour s'y conformer. Cette contrainte a un effet pratique important : elle impose une gestion du « besoin de savoir » (*need-to-know basis*) interne et vis-à-vis des fournisseurs, sous-traitants, assureurs et autres partenaires.

Renseignements : confidentialité, échanges et retrait des renseignements personnels

La LPCSE met en place un régime complet d'échange de renseignements, notamment pour soutenir l'établissement et l'évolution des directives. Pour les fins liées à l'établissement, la modification ou la révocation d'une directive, certaines autorités peuvent recueillir et communiquer des renseignements, y compris confidentiels, entre elles. La loi encadre aussi la communication et l'utilisation des renseignements confidentiels et prévoit des exceptions, notamment lorsque la communication est légalement exigée ou nécessaire à la protection des services / systèmes / cybersystèmes essentiels.

Une conformité « prouvable »

La LPCSE impose une tenue de documents couvrant la mise en œuvre du programme, les incidents déclarés, les mesures d'atténuation relatives aux tiers, l'exécution des directives et toute autre question prévue par règlement. Ces documents doivent être conservés au Canada, selon les modalités prévues par règlement ou, à défaut, par l'organisme réglementaire compétent. Cette exigence est centrale : elle transforme la conformité en obligation de preuve.

Le régime prévoit des pouvoirs étendus de vérification et d'exécution, exercés selon le secteur par différentes autorités (surintendant, ministre de l'Industrie via inspecteurs, Banque du Canada, Commission canadienne de sûreté nucléaire, Régie canadienne de l'énergie, ministre des Transports). Les dispositions d'accès aux lieux, d'examen de cybersystèmes, de reproduction et de

saisie temporaire de documents/systèmes sont détaillées dans la LPCSE. Des mécanismes d'ordres de vérification interne et d'ordres de conformité existent selon les autorités. La loi interdit l'entrave et les renseignements faux ou trompeurs, ce qui renforce l'importance de la qualité des informations remises.

La version sanctionnée ajoute aussi une protection expresse : la LPCSE n'a pas pour effet de porter atteinte au secret professionnel de l'avocat ou du notaire.

Attentions aux sanctions!

Il y a lieu de noter que des sanctions administratives substantielles sont prévues dans la loi, de même que des infractions pénales (y inclus l'emprisonnement).

Les dirigeants et administrateurs peuvent être considérés comme coauteurs d'une violation ou d'une infraction, selon le cas. Les violations continues peuvent être comptées jour par jour. Pour la Partie 2 de la loi, les sanctions administratives peuvent atteindre 500 000 $ pour un individu, et 15 000 000 $ dans les autres cas.

Certaines contraventions constituent en outre des infractions pénales punissables, dans certains cas, soit par procédure sommaire, soit par mise en accusation. Selon la nature du manquement et s'il s'agit d'un particulier, l'emprisonnement peut être possible.

Comment nous pouvons vous accompagner dans la mise en œuvre du projet de loi C-8

Nous pouvons notamment vous assister à l'égard des éléments suivants :

Positionnement réglementaire

Cartographier votre exposition (télécoms, services/systèmes critiques; désignation actuelle ou anticipée) et établir une feuille de route réaliste, priorisée par risques.

Réponse aux mesures imposées

Accompagner la réception, l'analyse et l'exécution de décrets, arrêtés ou directives.

Conformité

Bâtir ou consolider la gouvernance, la tenue de documents et les processus internes (demandes de renseignements, vérifications/inspections, traçabilité des décisions).

Tiers et approvisionnement

revoir et négocier les contrats et exigences de sécurité (notification d'incident, coopération, audit, sous-traitance, correctifs, retrait/substitution) et documenter les mesures d'atténuation.

Incidents et application

Accompagner la réponse aux incidents (qualification, notifications, préservation des preuves) et gérer le risque de SAP et d'exposition pénale, y compris pour les dirigeants et administrateurs.

Conclusion

En pratique, les organisations potentiellement visées ont intérêt à se préparer dès maintenant, même si la Partie 2 de la loi n'est pas encore en vigueur. La portée concrète du régime dépendra de l'entrée en vigueur de la LPCSE, de l'adoption des règlements d'application et de l'ajout, à l'annexe 2, des catégories d'exploitants visés et de leur organisme réglementaire correspondant. D'ici là, les organisations qui structurent dès maintenant leur gouvernance, leur documentation et leur gestion des tiers seront mieux placées pour s'adapter rapidement lorsque les obligations sectorielles seront précisées.