BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

VERSION PRÉLIMINAIRE

NON RÉVISÉE

La version préliminaire du présent résumé législatif est mise à la disposition des parlementaires, de leur personnel parlementaire ainsi que du public afin qu'ils puissent accéder en temps opportun à de l'information, des recherches et une analyse qui faciliteront leur étude du projet de loi visé. La version officielle du résumé législatif, qui pourrait différer de la présente version non révisée, remplacera cette dernière sur le site Web du Parlement du Canada.

Résumé législatif

PROJET DE LOI C-8 : LOI CONCERNANT LA CYBERSÉCURITÉ, MODIFIANT LA LOI SUR LES TÉLÉCOMMUNICATIONS ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

45-1-C8-F

20 avril 2026

Révisée par Sabrina Charland

Cette publication s'inspire d'une publication antérieure de la Bibliothèque du Parlement rédigée par Jed Chong, Khamla Heminthavong et Holly Porteous.

Services de bibliothèque et de recherche

VERSION PRÉLIMINAIRE
NON RÉVISÉE

ATTRIBUTION

Le 20 avril 2026	Sabrina Charland
Le 28 août 2025	Sabrina Charland
Le 6 octobre 2022	Jed Chong, Khamla Heminthavong et Holly Porteous

À PROPOS DE CETTE PUBLICATION

Les résumés législatifs de la Bibliothèque du Parlement résument des projets de loi à l'étude au Parlement et en exposent le contexte de façon objective et impartiale. Ils sont préparés par les Services de bibliothèque et de recherche, qui effectuent des recherches pour les parlementaires, les comités du Sénat et de la Chambre des communes ainsi que les parlementaires, et leur fournissent de l'information et des analyses. Les résumés législatifs sont mis à jour au besoin pour tenir compte des amendements apportés aux projets de loi au cours du processus législatif.

Par souci de clarté, les propositions législatives du projet de loi décrit dans le présent résumé législatif sont énoncées comme si elles avaient déjà été adoptées ou étaient déjà en vigueur. Il convient cependant de souligner, qu'un projet de loi peut faire l'objet d'amendements au cours de son examen par le Sénat et la Chambre des communes, et qu'il est sans effet avant d'avoir été adopté par les deux Chambres du Parlement, d'avoir reçu la sanction royale et d'être entré en vigueur.

Dans ce résumé législatif de la Bibliothèque du Parlement, tout changement d'importance depuis la publication précédente est signalé en **caractères gras**.

© Bibliothèque du Parlement, Ottawa, Canada, 2026

Résumé législatif du projet de loi C-8
(Version préliminaire)

45-1-C8-F

This publication is also available in English.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

TABLE DES MATIÈRES

1 CONTEXTE* 1

1.1 Stratégie nationale de cybersécurité 1

1.2 Fondements législatifs et contextuels 2
1.2.1 Origines du projet de loi sur la cybersécurité 3
1.2.2 Relance du projet de loi sur la cybersécurité et modifications clés 3

2 DESCRIPTION ET ANALYSE 4

2.1 Partie 1 : Modifications à la Loi sur les télécommunications 4
2.1.1 Objectifs de la politique canadienne de télécommunication (art. 1 du projet de loi) 4
2.1.2 Nouveaux pouvoirs (art. 2 du projet de loi) 4
2.1.2.1 Pouvoir de prendre des décrets 6
2.1.2.2 Pouvoir de prendre des arrêtés 6
2.1.2.3 Pouvoir de prendre des règlements 7
2.1.2.4 Ordonnance de non-divulgation d'un décret ou d'un arrêté 8
2.1.2.5 Fourniture de renseignements 9
2.1.2.6 Contrôle judiciaire des nouveaux pouvoirs 10
2.1.3 Conformité du Conseil de la radiodiffusion et des télécommunications canadiennes (art. 3 du projet de loi) 11
2.1.4 Enquête et contrôle d'application (art. 4 à 6 du projet de loi) 11
2.1.5 Nouveau régime de sanctions administratives pécuniaires (art. 7 du projet de loi) 12
2.1.5.1 Violation et détermination de la pénalité financière 12
2.1.5.2 Procès-verbaux et leur contenu 13
2.1.5.3 Paiement, présentation d'observation ou transaction 13
2.1.5.4 Perpétration d'une violation par une personne morale 14
2.1.5.5 Conclusions des procédures et prescriptions 14
2.1.6 Dispositions communes aux régimes de sanctions administratives pécuniaires et d'infractions pénales (art. 8 à 10 du projet de loi) 15
2.1.6.1 Admissibilité en preuve 15
2.1.6.2 Infractions pénales 15

2.2 Partie 2 : Loi sur la protection des cybersystèmes essentiels (art. 11 du projet de loi) 16
2.2.1 Objectif 16
2.2.2 Liste des services et systèmes critiques et des exploitants désignés 16
2.2.3 Établissement et de maintien d'un programme de cybersécurité 17

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.2.4 Atténuation des risques associés à la chaîne d'approvisionnement et aux tiers 18
2.2.5 Signalement obligatoire des incidents de cybersécurité 19
2.2.6 Directives de cybersécurité secrètes 20
2.2.6.1 Contrôle judiciaire par la Cour fédérale des directives de cybersécurité secrètes 21
2.2.7 Interdictions et autorisations relatives à la communication de renseignements 22
2.2.8 Tenue de documents 23
2.2.9 Exécution et contrôle d'application de la Loi sur la protection des cybersystèmes essentiels 24
2.2.9.1 Immunité judiciaire en responsabilité civile 24
2.2.9.2 Pouvoirs des organismes réglementaires 24
2.2.9.3 Ordonnance de vérifications internes obligatoires 24
2.2.10 Demande de révision d'un ordre de conformité 25
2.2.11 Règlements 26
2.2.12 Infractions et peines 26
2.2.12.1 Moyens de défense 27
2.2.13 Maintien du secret professionnel 27
2.2.14 Rapport annuel 27

3 COMMENTAIRES 28

3.1 Incertitudes réglementaires et défis de mise en œuvre pour les exploitants désignés 28

3.2 Répercussions des nouveaux pouvoirs de surveillance : directives, arrêtés et décrets 29

3.3 Préoccupations en matière de renseignements personnels et confidentiels 30

3.4 Absence de soutien financier ou technique 31

3.5 Répercussions sur les relations contractuelles et l'industrie 32

VERSION PRÉLIMINAIRE
NON RÉVISÉE

RÉSUMÉ LÉGISLATIF DU PROJET DE LOI C-8 : LOI CONCERNANT LA CYBERSÉCURITÉ, MODIFIANT LA LOI SUR LES TÉLÉCOMMUNICATIONS ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

1 CONTEXTE*

Le projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois (également appelé : « Loi sur la cybersécurité »), a été déposé à la Chambre des communes par le ministre de la Sécurité publique et de la Protection civile le 18 juin 2025 [1]. Il a depuis été adopté par la Chambre des communes le 26 mars 2026 avec des amendements [2]. Le projet de loi est actuellement à l'étape de la deuxième lecture au Sénat.

Ayant comme objectif de renforcer la résilience des infrastructures essentielles au Canada face aux cybermenaces croissantes, le projet de loi C-8 établit un cadre réglementaire permettant de protéger les services et systèmes essentiels à la sécurité publique et nationale [3]. Le projet de loi C-8 reprend en grande partie le libellé du projet de loi C-26 [4], déposé en juin 2022 lors de la 44e législature. Les principales distinctions entre les deux projets de loi sont abordées dans la section Fondement législatif et contextuel du présent résumé législatif.

Ce cadre repose sur deux parties. La première partie modifie la *Loi sur les télécommunications* afin d'y intégrer la sécurité du système de télécommunications canadien comme objectif de politique publique, et confère au gouvernement fédéral des pouvoirs accrus pour ordonner aux fournisseurs de services de télécommunications (FST) de prendre des mesures contre les cybermenaces. La seconde édicte la Loi sur la protection des cybersystèmes essentiels (LPCE), qui impose de nouvelles obligations en matière de cybersécurité aux entités sous réglementation fédérale opérant dans les secteurs jugés essentiels à la sécurité publique et nationale – tels que les finances, l'énergie nucléaire et électrique, les télécommunications et le transport.

1.1 STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

Le 6 février 2025, le gouvernement du Canada a annoncé une nouvelle stratégie nationale de cybersécurité intitulée Sécuriser l'avenir numérique du Canada [5]. La stratégie souligne l'accélération et la complexification des cybermenaces,

VERSION PRÉLIMINAIRE
NON RÉVISÉE

lesquelles englobent un large éventail d'activités, notamment « les rançongiciels et la cyberfraude, et l'ingérence non sollicitée dans les réseaux et systèmes [6] » canadiens. D'après le gouvernement, il devient essentiel de renforcer la résilience des infrastructures numériques et de protéger les citoyens, les entreprises et les institutions publiques contre ces cybermenaces. Le projet de loi C-8 s'inscrit dans la mise en œuvre de cette stratégie fondée sur trois piliers interdépendants.

Le premier pilier vise à protéger les Canadiens et les entreprises canadiennes contre les cybermenaces en misant sur la collaboration et l'échange d'information à l'aide de partenariats pansociétaux. Le deuxième pilier cherche à « faire du Canada un chef de file mondial de l'industrie de la cybersécurité », notamment en soutenant l'innovation, en renforçant les capacités de la main-d'œuvre et en ciblant la recherche stratégique. Enfin, le troisième pilier consiste à « détecter et perturber les auteurs de cybermenaces », notamment en améliorant les capacités de lutte du gouvernement du Canada contre la cybercriminalité et en renforçant la résilience des systèmes essentiels [7].

Dans son message d'introduction à la nouvelle stratégie, le ministre de la Sécurité publique de l'époque, l'honorable David J. McGuinty, a indiqué que l'augmentation de cybermenaces « entraîne des répercussions réelles pour les Canadiens et Canadiennes et devient une menace majeure pour la sécurité nationale et l'économie du pays ». Il a souligné que le gouvernement fédéral continuerait

> [d']utiliser tous les outils disponibles afin de protéger les infrastructures essentielles du Canada, de mieux nous adapter aux cyberrisques et de mieux les combattre, de garantir la sécurité et l'intégrité des systèmes essentiels du Canada et de créer un mécanisme pour faire appliquer notre déclaration 2022 sur la sécurité des télécommunications [8].

Le projet de loi C-8 concrétise cet engagement en établissant un cadre législatif pour protéger les cybersystèmes essentiels, en renforçant les pouvoirs de surveillance et d'intervention du gouvernement fédéral, et en imposant des obligations précises aux exploitants de services essentiels afin de mieux prévenir, détecter et répondre aux cybermenaces qui pèsent sur la sécurité nationale.

1.2 FONDEMENTS LÉGISLATIFS ET CONTEXTUELS

Tel que mentionné, le projet de loi C-8 reprend en grande partie le libellé du projet de loi C-26. Bien que ce dernier soit parvenu à franchir toutes les étapes législatives, une erreur technique relevée au Sénat a entraîné son renvoi à la Chambre des communes, retardant ainsi son adoption avant de mourir au *Feuilleton* à la prorogation du Parlement en janvier 2025 [9].

VERSION PRÉLIMINAIRE
NON RÉVISÉE

1.2.1 Origines du projet de loi sur la cybersécurité

Tout comme le projet de loi C-8, le projet de loi C-26 comportait deux parties. La partie 1 – introduisant des modifications à la *Loi sur les télécommunications* – donne suite à l'annonce du gouvernement canadien, en mai 2022, de son intention d'interdire l'utilisation des produits et services de Huawei et de ZTE dans les systèmes de télécommunications, en particulier dans les réseaux sans fil 5G [10]. Cette décision s'inscrit dans une tendance observée chez des alliés du Canada – dont les États-Unis, le Royaume-Uni, l'Australie et le Japon – qui ont également exclu Huawei de leurs réseaux sans fil 5G pour des raisons de sécurité nationale [11].

La partie 2 – proposant la création de la LPCE – semble s'inspirer du modèle australien en reprenant plusieurs éléments de la *Security of Critical Infrastructure Act 2018* [12] et des modifications substantives apportées par la *Security Legislation Amendment (Critical Infrastructure) Act 2021* [13]. Ces réformes de 2021 ont permis au gouvernement fédéral australien d'élargir considérablement ses pouvoirs pour imposer des obligations de cybersécurité aux exploitants d'infrastructures essentielles et pour intervenir directement en cas d'incidents cybernétiques majeurs. De manière similaire, la LPCE canadienne imposerait aux exploitants désignés de secteurs critiques (télécommunications, énergie, transport et finance) des obligations, telles que la mise en place de programmes de cybersécurité, la déclaration obligatoire des incidents et la conformité à des décrets gouvernementaux en matière de cybersécurité.

Cette approche reflète une tendance internationale visant à renforcer la résilience des infrastructures essentielles face aux menaces numériques. Par exemple, aux États-Unis, la *Cyber Incident Reporting for Critical Infrastructure Act of 2022* [14] oblige les exploitants d'infrastructures essentielles à signaler les incidents cybernétiques à la Cybersecurity and Infrastructure Security Agency. Au Royaume-Uni, l'obligation de signalement est prévue au règlement intitulé *The Network and Information Systems Regulations 2018* [15] qui découle de la directive européenne de 2016 sur la sécurité des réseaux et des systèmes d'information (directive NIS) [16]. L'objectif commun de ces régimes est d'assurer un niveau de sécurité accru et harmonisé pour la cybersécurité des infrastructures essentielles, tout en permettant aux autorités compétentes de mieux comprendre et gérer les risques cybernétiques.

1.2.2 Relance du projet de loi sur la cybersécurité et modifications clés

Bien que le projet de loi C-8 reprenne en grande partie le libellé du projet de loi C-26, il s'en distingue par plusieurs modifications notables. D'abord, il supprime les modifications corrélatives proposées à la *Loi sur la preuve au Canada*, lesquelles visaient à accorder à la Cour fédérale une compétence particulière sur certaines questions, notamment par rapport au contrôle judiciaire des décrets, arrêtés ministériels et règlements pris en vertu de la *Loi sur les télécommunications* et de la LPCE [17].

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Le projet de loi C-8 introduit également une plus grande transparence dans le processus de contrôle judiciaire en éliminant à l'article 15.9 de la *Loi sur les télécommunications* (art. 2 du projet de loi C-26) et l'article 145 de la LPCE (art. 12 du projet de loi C-26) la possibilité pour le gouvernement de présenter des observations confidentielles au tribunal ou de refuser la divulgation d'informations pour des raisons de sécurité nationale [18]. Par ailleurs, certaines imprécisions rédactionnelles logées dans le projet de loi C-26 ont été corrigées [19].

Lors de l'examen à la Chambre des communes, le projet de loi C-8 a fait l'objet de plusieurs amendements visant notamment à encadrer l'application des nouveaux pouvoirs, à prévoir un mécanisme d'examen parlementaire et à préciser les implications du régime proposé en matière de protection des renseignements personnels.

2 DESCRIPTION ET ANALYSE

2.1 PARTIE 1 : MODIFICATIONS À LA LOI SUR LES TÉLÉCOMMUNICATIONS

La partie 1 du projet de loi comprend 10 articles. Les dispositions principales sont détaillées ci-dessous.

2.1.1 Objectifs de la politique canadienne de télécommunication (art. 1 du projet de loi)

L'article 1 du projet de loi ajoute la promotion de la sécurité du système canadien de télécommunications à la liste d'objectifs stratégiques de la politique canadienne de télécommunication énoncée à l'article 7 de la *Loi sur les télécommunications*. L'ajout permet au ministre de l'Industrie ainsi qu'au Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) de tenir compte de cet objectif dans l'exercice de leurs pouvoirs respectifs en vertu de la *Loi sur les télécommunications*. La même considération est permise en vertu de la *Loi sur la radiocommunication* (la loi régissant l'attribution du spectre), qui incorpore les objectifs de la *Loi sur les télécommunications* par renvoi [20].

2.1.2 Nouveaux pouvoirs (art. 2 du projet de loi)

L'article 2 du projet de loi ajoute les articles **15.01** à 15.91 à la *Loi sur les télécommunications* pour établir un cadre juridique permettant au gouverneur en conseil et au ministre de l'Industrie de donner des ordres aux FST afin de protéger la sécurité du système canadien de télécommunication contre des menaces telles que l'ingérence, la manipulation, la perturbation ou la dégradation, notamment en leur imposant des obligations ou des interdictions spécifiques par décret (art. 15.1), par arrêté (art. 15.2) ou

VERSION PRÉLIMINAIRE
NON RÉVISÉE

par règlement (art. 15.8). Avant de prendre un décret ou un arrêté, le gouverneur en conseil ou le ministre, doit en outre tenir compte de certains facteurs communs visant à encadrer l'exercice de ces pouvoirs. Il est notamment prévu que la portée d'un décret ou d'un arrêté soit proportionnelle à la gravité de la menace à laquelle il répond (nouveaux par. 15.1(2) et 15.2(3) de la *Loi sur les télécommunications*). À cette fin, le gouverneur en conseil ou le ministre est tenu d'évaluer les répercussions de la mesure envisagée sur les activités et la situation financière des FST, sur la fourniture de services de télécommunication au Canada, y compris la confidentialité et la sécurité des télécommunications, ainsi que sur la protection de la vie privée des Canadiens. Ils peuvent aussi tenir compte d'autres éléments jugés pertinents (nouveaux par. 15.1(4) et 15.2(6) de la *Loi sur les télécommunications*).

Lors de l'examen du projet de loi C-8, la Chambre des communes a en outre ajouté l'article 15.01 afin de préciser l'interprétation de certaines notions clés associées aux nouveaux pouvoirs. Cet article circonscrit les concepts d'ingérence, de manipulation, de perturbation ou de dégradation à des actes de nature technique affectant le fonctionnement d'un système de télécommunication. Il exclut explicitement les effets découlant de l'expression licite d'opinions, de la persuasion ou du débat politique, répondant ainsi aux préoccupations relatives à une atteinte potentielle à la liberté d'expression garantie par la *Charte canadienne des droits et libertés* (la *Charte*)[21].

Un autre article ajouté à la suite de la considération par la Chambre des communes est l'article 15.211 qui impose au ministre de l'Industrie une obligation d'avis à l'égard des personnes directement visées par un décret ou par un arrêté. Lorsque le décret ou l'arrêté ne comporte pas de disposition interdisant la divulgation, le ministre doit, dans les sept jours suivant sa prise, communiquer à toute personne qui y est précisée un avis accompagné du texte de la mesure. Cette exigence contribue à assurer que les personnes touchées soient informées en temps utile des obligations ou interdictions qui leur sont imposées.

Les articles 15.21(1) à 15.21(3) obligent le ministre de l'Industrie à déposer chaque année un rapport au Parlement portant sur les décrets (par. 15.1(1)) et arrêtés (par. 15.2(1) et 15.2(2)) pris en vertu de ces dispositions. Ce rapport doit inclure leur nombre, leur nature, les fournisseurs concernés, leur niveau de conformité, ainsi qu'une justification de leur nécessité et de leur caractère raisonnable. De plus, l'article 15.81 exige que le ministre soumette au Parlement, dans les trois mois suivant la fin de l'exercice financier, un rapport annuel concernant les arrêtés visés aux articles 15.1 et 15.2 qui ont été pris au cours de cet exercice. **Un résumé de ce rapport doit également être accessible sur le site Web du ministère de l'Industrie dans les 10 jours après ce dépôt.** Ensemble, ces mesures additionnelles visent à

VERSION PRÉLIMINAIRE
NON RÉVISÉE

assurer la transparence et la reddition de comptes en obligeant le ministre à justifier l'usage de pouvoirs exceptionnels devant le Parlement, permettant ainsi un suivi de leur utilisation et de leur impact.

2.1.2.1 Pouvoir de prendre des décrets

Le nouvel article 15.1 de la *Loi sur les télécommunications* permet au gouverneur en conseil d'émettre par décret une interdiction aux FST d'utiliser les produits ou les services de certains fournisseurs s'il est d'avis que cela est nécessaire pour sécuriser le système canadien de télécommunication contre toute menace **et que cela est raisonnable par rapport à la gravité de la menace**. Ces mesures peuvent notamment consister à interdire aux FST d'utiliser les produits ou services d'un fournisseur donné ou à leur ordonner de retirer de leurs réseaux ou de leurs installations de télécommunication tous les produits fournis par celui-ci (par. 15.1(1) de la *Loi sur les télécommunications*).

Le paragraphe 15.1(7) de la *Loi sur les télécommunications* prévoit que les dispositions d'un décret ont préséance sur toute autre décision, d'arrêté ou d'autorisation qui serait en contradiction avec lui.

Le paragraphe 15.1(8) de la *Loi sur les télécommunications* précise que personne n'a droit à une indemnisation du gouvernement fédéral pour les pertes financières résultant de la prise d'un tel décret.

2.1.2.2 Pouvoir de prendre des arrêtés

Le nouvel article 15.2 de la *Loi sur les télécommunications* confère au ministre de l'Industrie le pouvoir de prendre, par arrêté, diverses mesures visant à sécuriser le système canadien de télécommunication lorsqu'il existe des motifs raisonnables de croire que ces mesures sont nécessaires pour protéger le système canadien des télécommunications contre toute menace **et qu'elles sont raisonnables eu égard à la gravité de la menace**. L'exercice de ce pouvoir est assujetti à une consultation préalable du ministre de la Sécurité publique et de la Protection civile ainsi que de toute autre personne qu'il estime importante.

En vertu du paragraphe 15.2(1), le ministre de l'Industrie peut notamment interdire à des FST de fournir des services à certaines personnes, ou leur ordonner d'en suspendre temporairement la fourniture, y compris à l'égard d'autres FST. **Une exception a toutefois été ajoutée au paragraphe 15.2(1.1), limitant la possibilité d'ordonner la suspension des services à un individu si une telle mesure est nécessaire pour contrer une menace de nature technique expressément précisée dans l'arrêté.**

VERSION PRÉLIMINAIRE
NON RÉVISÉE

En vertu du nouveau paragraphe 15.2(2) de la *Loi sur les télécommunications*, le ministre de l'Industrie peut, par arrêté :

- interdire aux FST d'utiliser dans tout ou partie de leurs réseaux ou installations de télécommunication, ou en lien avec ceux-ci, les produits ou les services qu'il précise;
- ordonner aux FST de retirer de tout ou partie de leurs réseaux ou installations les produits qu'il précise;
- imposer des conditions aux FST quant à leur utilisation de produits ou de services ou relativement à la fourniture de leurs services à toute personne;
- interdire aux FST de mettre à niveau des produits ou des services;
- exiger que les réseaux ou installations des FST, ainsi que les projets d'approvisionnement qui s'y rapportent, fassent l'objet de processus d'examen;
- exiger que les FST élaborent des plans de sécurité liés à leurs services, à leurs réseaux ou à leurs installations;
- exiger que les FST mènent des évaluations pour repérer toute vulnérabilité de leurs services, réseaux ou installations ou de leur plan de sécurité;
- exiger que les FST prennent des mesures visant à atténuer toute vulnérabilité relevée dans leur évaluation.

Lors de l'étude du projet de loi C-8, la Chambre des communes a renforcé l'encadrement de ces pouvoirs en clarifiant que le ministre ne peut ni ordonner le décodage d'une communication privée chiffrée (par. 15.2(2.1)), ni exiger l'interception de communications privées ou radiotéléphoniques au sens de l'article 183 du *Code criminel*[22] (par. 15.2(4))[23].

Le nouveau paragraphe 15.2(9) de la *Loi sur les télécommunications* précise qu'en cas d'incompatibilité, les dispositions d'un arrêté pris en vertu de la *Loi sur les télécommunications* ont priorité sur toute autre mesure incompatible, y compris les décisions du CRTC, et les arrêtés pris ou les autorisations ministérielles données en vertu de la *Loi sur les télécommunications* ou de la *Loi sur la radiocommunication*.

Tout comme c'est le cas pour le décret, personne n'a droit à une indemnisation du gouvernement fédéral pour les pertes financières découlant d'un arrêté en vertu du nouveau paragraphe 15.2(10) de la *Loi sur les télécommunications*.

2.1.2.3 Pouvoir de prendre des règlements

En vertu du nouveau paragraphe 15.8(1) de la *Loi sur les télécommunications*, le gouverneur en conseil peut prendre des règlements pour tout ce qui pourrait autrement être visé par un arrêté ministériel pris en vertu de l'article 15.2 de la même

VERSION PRÉLIMINAIRE
NON RÉVISÉE

loi. Un règlement peut également servir à désigner les personnes ou entités aptes à échanger et communiquer des renseignements visés par l'application des articles concernés de la *Loi sur les télécommunications*.

Les règlements pris en vertu du nouveau paragraphe 15.8(1) ont préséance sur toute décision, arrêté ou autorisation incompatible émanant du Conseil ou du ministre, y compris ceux pris en vertu de la *Loi sur la radiocommunication* (par. 15.8(2)).

2.1.2.4 Ordonnance de non-divulgation d'un décret ou d'un arrêté

Bien que le projet de loi impose au gouverneur en conseil ou au ministre de l'Industrie de publier les décrets et arrêtés dans la *Gazette du Canada* dans un délai de 90 jours suivant leur adoption (nouveaux par. 15.1(6) et 15.2(8) à la *Loi sur les télécommunications*), il leur accorde également la possibilité de maintenir ces ordonnances secrètes par l'inclusion d'une clause de non-divulgation, interdisant à toute personne visée de révéler l'existence ou le contenu, même partiel, du décret ou de l'arrêté concerné (par. 15.1(3) et 15.2(5) à la *Loi sur les télécommunications*).

Les nouveaux paragraphes 15.3(1) à 15.3(4) de la *Loi sur les télécommunications* précisent les conditions d'application des décrets et arrêtés pris en vertu des articles 15.1 et 15.2. Ils clarifient qu'une personne ne peut être sanctionnée pour avoir contrevenu à un décret ou un arrêté que s'il est établi qu'elle en avait été informée, ce que peut démontrer un certificat signé par le ministre.

Une modification adoptée par la Chambre des communes permet d'encadrer davantage l'exercice de ces pouvoirs. Les paragraphes 15.1(3.1) et 15.2(5.1) prévoient qu'avant d'imposer une interdiction de divulgation, le gouverneur en conseil ou le ministre de l'Industrie tiennent compte de plusieurs facteurs, notamment le risque que la divulgation compromette l'objectif du décret, la nécessité et la portée de l'interdiction au regard de la menace, les effets de la non-divulgation sur les principes de transparence et de responsabilisation du gouvernement, ainsi que toute observation formulée par les FST concernés.

Dans ce contexte et selon l'article 15.22, le ministre doit informer, dans les 90 jours, le Comité des parlementaires sur la sécurité nationale et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement de toute mesure comportant une clause de non-divulgation.

Ces dispositions jouent un rôle clé dans l'équilibre entre sécurité nationale et respect des droits fondamentaux. Elles permettent au gouvernement d'imposer la confidentialité autour de certaines mesures (par. 15.1(3) et 15.2(5)), tout en précisant qu'aucune sanction ne peut être imposée sans preuve que l'intéressé a préalablement été informé (par. 15.3(1) à 15.3(4)).

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.2.5 Fourniture de renseignements

Les articles 15.4 à 15.71 de la *Loi sur les télécommunications* visent à encadrer la collecte, la désignation, l'échange et la communication de renseignements pertinents pour l'élaboration ou la modification de mesures réglementaires (décrets, arrêtés, règlements) liées à la sécurité des télécommunications.

Le nouvel article 15.4 permet au ministre de l'Industrie d'ordonner à toute personne de fournir les renseignements dont il a des motifs de croire qu'ils sont, d'une part, raisonnables par rapport à la gravité de la menace, et d'autre part, nécessaires dans le cadre de la prise, de la modification ou de la révocation d'un décret visé à l'article 15.1, d'un arrêté visé à l'article 15.2 ou d'un règlement visé à l'alinéa 15.8(1)a) de la *Loi sur les télécommunications*, ou de la vérification du respect ou de la prévention du non-respect de l'un ou l'autre de ces textes.

Le nouveau paragraphe 15.5(1) encadre la confidentialité des renseignements fournis en vertu de l'article 15.4, en permettant à la personne qui les communique de désigner comme confidentiels certains éléments comme les renseignements financiers, commerciaux, scientifiques ou techniques, ainsi que des renseignements personnels ou des renseignements dépersonnalisés. **Afin de renforcer la protection de la vie privée, le paragraphe 15.5(2.1), ajouté lors de l'étude du projet de loi C-8 à la Chambre des Communes, prévoit que les renseignements personnels et les renseignements dépersonnalisés sont réputés être désignés comme confidentiels même en l'absence d'une désignation expresse à cet effet.**

Par ailleurs, des modifications apportées au paragraphe 15.5(2) pendant le processus de révision du projet de loi C-26 ont permis d'introduire des définitions précisant les notions de « renseignements personnels » et « dépersonnaliser », contribuant ainsi à renforcir la compréhension et l'application des protections en matière de renseignement personnel. **La communication de renseignements désignés ou réputés confidentiels est interdite, sous réserve de certaines exceptions prévues aux paragraphes 15.5(3) à 15.5(5), notamment lorsque la communication est légalement exigée ou jugée nécessaire par le ministre pour sécuriser le système canadien de télécommunication face à une menace grave.**

Les articles 15.6 à 15.71 de la *Loi sur les télécommunications* précisent les modalités encadrant l'échange de renseignement entre les ministères et organismes fédéraux responsables de la sécurité, tout en renforçant les garanties applicables à la protection des renseignements personnels et confidentiels. Bien que la *Loi sur les télécommunications* contienne déjà des dispositions permettant l'échange de renseignements entre le CRTC et Innovation, Sciences et Développement économique Canada, le nouvel article 15.6 élargit ce cadre pour inclure d'autres ministres et organismes de sécurité nationale.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

À cet égard, le nouveau paragraphe 15.6(1.1) encadre plus strictement la collecte et la communication des renseignements personnels et des renseignements dépersonnalisés visés à l'alinéa 15.5(1)d), en exigeant que leur portée et leur teneur soient raisonnables au regard de la menace en cause.

L'article 15.7 autorise le ministre de l'Industrie à communiquer, dans le cadre d'accord, d'entente ou d'arrangement conclus par écrit avec des partenaires provinciaux ou internationaux, des renseignements recueillis en vertu de la *Loi sur les télécommunications*, à l'exclusion de ceux désignés comme confidentiels. **Cette communication est subordonnée au fait que le ministre croit que ces renseignements pourraient être utiles pour sécuriser le système canadien de télécommunications ou un système étranger, et qu'ils soient assortis de garanties additionnelles, notamment l'obligation de prévoir leur retrait lorsqu'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été communiqués.**

Dans ce contexte, l'article 15.701, ajouté à la suite de l'étude du projet de loi C-8 en Chambre des communes, impose une obligation explicite de retrait des renseignements personnels et des renseignements dépersonnalisés recueillis ou obtenus dans le cadre de ces accords, lorsque ceux-ci ne sont plus nécessaires aux fins liées à l'exercice des pouvoirs conférés par les articles 15.1, 15.2 ou 15.8, ou conformément aux exigences applicables de la *Loi sur la protection des renseignements personnels* (LPRP)[24].

Enfin, l'article 15.71 confirme que ces dispositions doivent respecter la LPRP**, tandis que l'article 15.72 introduit une interdiction spécifique visant à protéger l'identité des personnes qui fournissent volontairement des renseignements au ministre en demandant que leur identité demeure confidentielle**. Ensemble, ces articles établissent un équilibre entre sécurité nationale et protection de la vie privée, en assurant un cadre légal pour la gestion de renseignements confidentiels.

2.1.2.6 Contrôle judiciaire des nouveaux pouvoirs

Les articles 15.9 et 15.91 de la *Loi sur les télécommunications* établissent les règles encadrant le contrôle judiciaire et les appels relatifs aux décrets, arrêtés ou règlements pris en vertu des nouveaux articles 15.1, 15.2 et l'alinéa 15.8(1)a) de la *Loi sur les télécommunications*.

L'article 15.9 précise que le juge saisi d'un tel contrôle doit exclure de sa décision tout élément de preuve que le ministre de l'Industrie retire ou qui est jugé non pertinent, et il doit en assurer la confidentialité. Cela vise à protéger les renseignements sensibles tout en permettant un examen judiciaire. L'article 15.91 étend ces mêmes règles aux appels de ces décisions, assurant ainsi une continuité dans la protection des renseignements tout au long du processus judiciaire.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.3 Conformité du Conseil de la radiodiffusion et des télécommunications canadiennes (art. 3 du projet de loi)

L'article 3 du projet de loi modifie l'article 47 de la *Loi sur les télécommunications* afin d'inclure les décrets du gouverneur en conseil ou les arrêtés du ministre de l'Industrie dans les considérations du CRTC lorsqu'il exerce ses pouvoirs et fonctions sous la *Loi sur les télécommunications*.

2.1.4 Enquête et contrôle d'application (art. 4 à 6 du projet de loi)

Les articles 4 à 6 du projet de loi modifient les articles 71 et 72 de la *Loi sur les télécommunications* afin de renforcir les pouvoirs du ministre de l'Industrie en matière d'inspection et de vérification du respect des nouvelles obligations.

L'article 4 du projet de loi modifie l'article 71 de la *Loi sur les télécommunications*, afin d'intégrer les nouveaux pouvoirs de prise de décret (art.15.1), d'arrêté (art. 15.2) et de règlement (al. 15.8(1)a)) au régime d'inspection et d'application existant. Ainsi, le nouveau libellé de l'article 71 permet au ministre de l'Industrie de désigner des inspecteurs pour vérifier la conformité ou empêcher le non-respect des décrets, arrêtés ou règlements pris en vertu des nouveaux pouvoirs en la matière prévus dans le projet de loi.

Enfin, les articles 5 et 6 du projet de loi modifient le paragraphe 72(3) et l'article 72.001 de la *Loi sur les télécommunications* afin de préciser les conséquences juridiques des manquements aux nouvelles obligations. En vertu du paragraphe 72(1) de la *Loi sur les télécommunications*, quiconque a subi une perte ou un dommage par suite d'un manquement aux dispositions de la *Loi sur les télécommunications* (ou à une décision ou un règlement pris au titre de celle-ci) peut poursuivre le contrevenant afin de recouvrer un montant égal à la perte ou au dommage. Le paragraphe 72(3) exclut les recours civils contre les entreprises qui respectent les décrets, arrêtés et règlements en matière de cybersécurité, les protégeant ainsi contre des poursuites contractuelles indues.

L'article 72.001, quant à lui, précise que les nouveaux pouvoirs de prise de décrets prévus à la *Loi sur les télécommunications* ne sont pas assujettis au régime général de « sanctions administratives pécuniaires » de cette dernière. Le projet de loi instaure plutôt un régime de sanctions administratives pécuniaires particulier pour les manquants à ces nouveaux pouvoirs. Ces dispositions traduisent une volonté du législateur de garantir la conformité tout en protégeant les fournisseurs de services contre les risques juridiques liés à l'application de mesures de sécurité nationale.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.5 Nouveau régime de sanctions administratives pécuniaires (art. 7 du projet de loi)

L'article 7 du projet de loi C-8 introduit un nouveau régime de sanctions administratives pécuniaires spécifiquement lié à la sécurité du système canadien de télécommunication par l'ajout des articles 72.131 à 72.1393 à la *Loi sur les télécommunications*.

2.1.5.1 Violation et détermination de la pénalité financière

Le nouvel article 72.131 de la *Loi sur les télécommunications* prévoit que toute contravention à un décret, un arrêté ou un règlement pris en vertu des articles 15.1, 15.2 ou de l'alinéa 15.8(1)a) de cette même loi constitue une violation passible d'une pénalité financière. Par exemple, le non-respect d'un décret exigeant la transmission de données sur les pratiques tarifaires d'un fournisseur ou la divulgation non autorisée de renseignements confidentiels à des tiers pourrait constituer une telle violation.

Le montant maximal de cette pénalité est fixé à 25 000$ pour tout individu commettant une première violation et de 50 000$ en cas de récidive. Dans les autres cas, comme pour les entreprises, ces sanctions pécuniaires peuvent s'élever jusqu'à 10 millions de dollars pour une première violation et jusqu'à 15 millions de dollars en cas de récidive (nouvel article 72.131 à la *Loi sur les télécommunications*). Ces montants visent à refléter la gravité des enjeux liés à la cybersécurité et la volonté du législateur de dissuader toute négligence ou non-conformité dans les secteurs critiques.

L'article 72.132 de la *Loi sur les télécommunications* introduit la notion de violation continue, précisant qu'une infraction qui se prolonge dans le temps constitue une violation distincte pour chaque jour où elle persiste. Cette disposition vise à dissuader les retards de conformité en augmentant sensiblement les sanctions administratives pécuniaires.

Le nouveau paragraphe 72.133(1) de la *Loi sur les télécommunications* énonce également une liste de critères dont le ministre de l'Industrie doit tenir compte pour établir le montant de la pénalité, tels que la nature et la portée de la violation, les antécédents de l'auteur et sa capacité de payer. D'après le nouveau paragraphe 72.133(2), bien que le projet de loi établisse un régime de sanctions administratives pécuniaires, la pénalité ne vise pas à punir, mais a pour but d'encourager la conformité en favorisant le respect des décrets, arrêtés et règlements.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.1.5.2 Procès-verbaux et leur contenu

Les nouveaux articles 72.134 et 72.135 de la *Loi sur les télécommunications* précisent les rôles du ministre de l'Industrie et des agents verbalisateurs[25] dans la mise en œuvre du nouveau régime de sanctions, en assurant à la fois l'efficacité administrative et le respect des droits procéduraux des personnes visées.

Notamment, le nouvel article 72.134 confère au ministre le pouvoir de désigner les agents autorisés à dresser des procès-verbaux pour une violation, ainsi que les personnes habilitées à conclure des transactions. Le ministre peut également établir un sommaire pour chaque violation, qui sera inclus dans les procès-verbaux.

Le nouvel article 72.135, quant à lui, encadre la procédure du procès-verbal. Il prévoit qu'un agent peut dresser un procès-verbal s'il a des motifs raisonnables de croire qu'une violation a été commise. Ce document, qui doit être signifié à la personne concernée, doit contenir le nom de l'intéressé, les faits reprochés, le montant de la pénalité, ainsi que les options offertes à la personne visée : soit payer la pénalité, soit présenter des observations au ministre dans un délai de 30 jours (ou un délai prolongé à la discrétion du ministre). Le texte précise également que l'absence de réponse dans le délai imparti équivaut à un aveu de responsabilité.

Pourvu qu'aucune observation n'ait été soumise, l'agent peut corriger ou annuler le procès-verbal, ce qui permet de rectifier rapidement toute erreur administrative sans recourir à une procédure formelle.

2.1.5.3 Paiement, présentation d'observation ou transaction

Les nouveaux articles 72.136 et 72.137 de la *Loi sur les télécommunications* établissent le processus de sanction administrative pécuniaire en précisant les rôles du ministre, des fonctionnaires désignés et des personnes à qui un avis d'infraction a été signifié, y compris les conséquences du paiement, du défaut de réponse, des décisions ministérielles et du fonctionnement des accords de conformité.

Le nouvel article 72.136 clarifie les conséquences du paiement ou de la présentation d'observations. Dans tous les cas, le paiement de la pénalité constitue un aveu de responsabilité et met fin à la procédure.

Cependant, si des observations sont présentées par le prétendu auteur d'une violation, le ministre doit alors déterminer, selon la prépondérance des probabilités, si la personne est responsable ou non de la violation après avoir examiné les observations. Il peut alors confirmer, réduire ou annuler la pénalité.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

L’omission de payer ou de présenter des observations dans le délai prévu constitue également un aveu de responsabilité et permet au ministre d’imposer la pénalité indiquée au procès-verbal. Une copie de cette décision est ensuite signifiée à l’intéressé, assurant ainsi la transparence et la clôture formelle du processus.

Le nouvel article 72.137 introduit la possibilité de conclure une transaction entre la personne désignée et le prétendu auteur de la violation. Cette transaction peut inclure des conditions jugées appropriées et prévoir une réduction partielle ou totale de la pénalité.

Une fois la transaction conclue, l’intéressé ne peut plus présenter d’observations, et la transaction est réputée constituer une déclaration de responsabilité. Si la transaction est exécutée, un avis est signifié et la procédure prend fin.

En cas d’inexécution de la transaction conclue, un avis est également signifié, obligeant l’intéressé à payer la pénalité initiale, moins toute somme déjà versée. Le paiement conforme à cet avis met également fin à la procédure. Ce mécanisme offre une voie alternative à la contestation formelle, tout en assurant l’efficacité et la finalité du processus administratif.

2.1.5.4 Perpétration d’une violation par une personne morale

En vertu du nouvel article 72.138 de la *Loi sur les télécommunications*, lorsqu’une personne morale est l’auteur présumé d’une violation, ses dirigeants, administrateurs ou mandataires sont tenus responsables de la violation qu’ils ont ordonnée ou autorisée, ou à laquelle ils ont consenti ou participé, peu importe si la personne morale fait ou non l’objet de procédures en violation.

2.1.5.5 Conclusions des procédures et prescriptions

Les nouveaux articles 72.139 à 72.1393 de la *Loi sur les télécommunications* complètent le régime de sanctions administratives pécuniaires par une série de dispositions relatives au recouvrement, à la prescription, à la transparence et à la réglementation.

L’article 72.139 établit que toute pénalité imposée, ainsi que les intérêts afférents, constitue une créance de Sa Majesté recouvrable devant la Cour fédérale ou tout autre tribunal compétent. Le recouvrement de cette créance se prescrit par cinq ans à compter de la date à laquelle elle devient exigible, et toute somme perçue est versée au receveur général. Le ministre de l’Industrie peut également émettre un certificat de non-paiement, qui, une fois enregistré à la Cour fédérale, a la même valeur qu’un jugement de cette cour. Cela permet au gouvernement de recouvrer efficacement les montants dus, tout en assurant une base juridique solide pour l’exécution des décisions.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Par ailleurs, l'article 72.1392 autorise le ministre à publier le nom des contrevenants, la nature des violations ou des transactions conclues, ainsi que les montants des pénalités. Cette disposition vise à renforcer la transparence et à dissuader les comportements non conformes.

Enfin, l'article 72.1393 habilite le gouverneur en conseil à adopter des règlements pour notamment : exclure certaines dispositions de l'application des sanctions (art. 72.131 de la *Loi sur les télécommunications*), établir des critères supplémentaires pour déterminer le montant des pénalités (art. 72.133(1)e) de la *Loi sur les télécommunications*), ou encore encadrer les modalités des transactions prévues à l'article 72.137. Ces pouvoirs réglementaires permettent d'adapter le régime aux réalités opérationnelles et d'assurer une mise en œuvre souple et efficace.

2.1.6 Dispositions communes aux régimes de sanctions administratives pécuniaires et d'infractions pénales (art. 8 à 10 du projet de loi)

La *Loi sur les télécommunications* s'appuie à la fois sur un régime de sanctions administratives pécuniaires (art. 72.14) et sur un régime d'infractions pénales (art. 73). Les articles 8 à 10 du projet de loi C-8 introduisent des modifications aux articles 72.14 et 73 de la *Loi sur les télécommunications* afin d'inclure les règles de preuve, élargir les responsabilités pénales et renforcir les outils judiciaires à la disposition du gouvernement pour assurer la conformité aux nouvelles obligations en matière de cybersécurité.

2.1.6.1 Admissibilité en preuve

L'article 9 du projet de loi modifie l'article 72.14 de la *Loi sur les télécommunications* afin de préciser que dans les procédures en violation, le procès-verbal ou la copie de la décision apparemment signifiée en application des dispositions mentionnées, est admissible en preuve sans qu'il soit nécessaire de prouver l'authenticité de la signature, ni de la qualité officielle du signataire.

2.1.6.2 Infractions pénales

Les modifications à l'article 73 de la *Loi sur les télécommunications* introduisent au régime d'infractions pénales les violations aux décrets, arrêtés et règlements pris en vertu des articles 15.1, 15.2 et 15.8(1)a) de cette même loi.

Le nouveau paragraphe 73(3.1) prévoit que toute personne physique reconnue coupable d'une telle infraction est passible d'une amende et d'un emprisonnement maximal de deux ans moins un jour, tandis qu'une personne morale est passible d'une amende seule.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Les nouveaux paragraphes 73(3.2) à 73(3.5) étendent la responsabilité pénale aux dirigeants, administrateurs ou mandataires ayant participé à l'infraction, et permettent de tenir une personne responsable des actes de ses employés ou mandataires. L'auteur présumé de la violation peut invoquer en défense, en vertu du nouveau paragraphe 73(3.4) de la *Loi sur les télécommunications*, qu'il a pris toutes les précautions voulues pour prévenir la perpétration de l'infraction.

Enfin, le paragraphe 73(7) est modifié pour permettre au tribunal compétent d'ordonner une injonction lorsqu'il est convaincu qu'une violation des dispositions liées à la cybersécurité est en cours ou est imminente. Cette injonction peut imposer à toute personne de cesser ou de s'abstenir de toute activité liée à l'infraction, offrant ainsi au ministre de l'Industrie un outil judiciaire pour prévenir les atteintes à la sécurité du système canadien de télécommunication.

2.2 PARTIE 2 : LOI SUR LA PROTECTION DES CYBERSYSTÈMES ESSENTIELS (ART. 11 DU PROJET DE LOI)

La LPCE est édictée par l'article 11 du projet de loi. Les principales dispositions de la LPCE sont détaillées ci-dessous.

2.2.1 Objectif

L'objectif de la LPCE est de protéger les cybersystèmes essentiels afin d'assurer la continuité et la sécurité des services et systèmes critiques au Canada (art. 5 de la LPCE). Ces services et systèmes sont considérés comme vitaux pour la sécurité nationale, la sécurité publique et le bon fonctionnement des infrastructures sous compétence fédérale.

Plus précisément, la LPCE vise à permettre aux autorités et aux exploitants de mieux identifier et gérer les risques liés à la cybersécurité, y compris ceux associés aux chaînes d'approvisionnement et à l'utilisation de produits ou services de tiers (al. 5(a)). Elle cherche également à prévenir toute compromission des cybersystèmes essentiels (al. 5(b)), à détecter rapidement les incidents de cybersécurité qui les affectent ou pourraient les affecter (al. 5(c)), et à minimiser les conséquences de tels incidents lorsqu'ils surviennent (al. 5(d)).

En somme, la LPCE établit un cadre législatif pour prévenir, détecter et répondre aux menaces cybernétiques qui pourraient compromettre les infrastructures critiques du pays.

2.2.2 Liste des services et systèmes critiques et des exploitants désignés

Respectivement, les articles 6 et 7 de la LPCE habilitent le gouverneur en conseil à ordonner, par décret, l'ajout ou la modification de « services critiques et systèmes

VERSION PRÉLIMINAIRE
NON RÉVISÉE

critiques » sous réglementation fédérale à l'annexe 1 de la LPCE et à ajouter ou modifier les exploitants désignés et les organismes réglementaires de ces services et systèmes critiques à l'annexe 2 de la LPCE.

L'annexe 1 énumère présentement six services et systèmes critiques : 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 et les systèmes de compensation et de règlements.

2.2.3 Établissement et de maintien d'un programme de cybersécurité

L'article 9 de la LPCE impose aux exploitants désignés de secteurs critiques de mettre en place un programme de cybersécurité dans les 90 jours qu'un décret est publiée en vertu de l'article 7 et que l'exploitant devient membre d'une catégorie figurant à l'annexe 2 de la LPCE.

Le paragraphe 9(1) de la LPCE précise ce que ce programme de cybersécurité devrait accomplir. Les résultats attendus comprennent les suivants :

- identifier et gérer les risques organisationnels pour la cybersécurité, notamment les risques associés à la chaîne d'approvisionnement et à l'utilisation de produits et services de tiers;
- protéger les cybersystèmes essentiels contre toute compromission;
- détecter les incidents de cybersécurité qui touchent ou pourraient toucher ses cybersystèmes essentiels;
- réduire au minimum les conséquences des incidents de cybersécurité qui touchent les cybersystèmes essentiels.

Il est à noter qu'un « cybersystème essentiel » est défini à l'article 2 comme un « 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 ». Un « incident de cybersécurité » est défini comme un « incident, notamment acte, omission ou situation, qui nuit ou peut nuire » soit à la continuité ou à la sécurité d'un service critique ou d'un système critique, soit à la confidentialité, à l'intégrité ou à la disponibilité d'un cybersystème essentiel.

Aux termes de l'alinéa 9(1)e), les exploitants désignés doivent « prendre toute mesure prévue par règlement », ce qui laisse entendre que le gouvernement fédéral publiera de façon continue des directives sur les programmes de cybersécurité pour les services et les systèmes critiques.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Le paragraphe 9(2) de la LPCE exige que les exploitants désignés avisent immédiatement et par écrit « l'organisme réglementaire compétent[26] » qu'ils ont établi un programme de cybersécurité.

En vertu de l'article 10 de la LPCE, un exploitant désigné possède 90 jours suivant sa désignation au titre de l'annexe 2 pour mettre son programme de cybersécurité à la disposition de l'organisme réglementaire. En vertu de l'annexe 2, chaque exploitant désigné appartient à une catégorie d'exploitants et chaque catégorie d'exploitants est associée à un organisme réglementaire particulier à qui il doit rendre des comptes.

L'article 11 de la LPCE prévoit la possibilité d'obtenir un délai supplémentaire aux 90 jours prescrit, sur demande écrite à l'organisme réglementaire, pour permettre à l'exploitant désigné de se conformer aux exigences du paragraphe 9(1) ou à l'article 10.

L'article 12 de la LPCE exige que les exploitants désignés mettent en œuvre non seulement leurs programmes de cybersécurité, mais aussi en assurent la mise à jour au fil du temps. La LPCE établit deux mécanismes pour veiller à ce que les programmes de cybersécurité demeurent à jour : les règlements et les examens des programmes.

L'article 13 de la LPCE prévoit que les exploitants désignés entreprennent un examen périodique de leur programme de cybersécurité au moins une fois par année, soit à la date prévue par règlement, soit à chaque anniversaire de son établissement. Cet examen doit être complété dans un délai de 60 jours, sauf disposition contraire, et peut entraîner des modifications au programme. L'exploitant doit informer l'organisme réglementaire des changements apportés ou non dans les 30 jours suivant cet examen.

Enfin, l'article 14 de la LPCE prévoit des obligations de notification en cas de changements importants dans la propriété, la chaîne d'approvisionnement ou toute autre circonstance prévue par règlement. Un avis de suivi doit être transmis dans les 90 jours pour indiquer si le programme a été modifié, avec possibilité de prolongation du délai.

2.2.4 Atténuation des risques associés à la chaîne d'approvisionnement et aux tiers

L'article 15 de la LPCE impose aux exploitants désignés l'obligation d'atténuer, dès leur identification, les risques liés à leur chaîne d'approvisionnement ainsi qu'à l'utilisation de produits ou de services fournis par des tiers. Cette obligation signifie que « [d]ès que » ces risques sont découverts, les exploitants désignés doivent prendre des mesures raisonnables, y compris celles qui peuvent être prescrites par règlement, pour les atténuer.

Ajouté par la Chambre des communes, l'article 15.1 de la LPCE confère au Centre de la sécurité des télécommunications (CST) le pouvoir d'élaborer, en

VERSION PRÉLIMINAIRE
NON RÉVISÉE

consultation avec les intervenants de l'industrie, des lignes directrices portant spécifiquement sur l'atténuation des risques liés aux chaînes d'approvisionnement et à l'utilisation de produits et services de tiers. Ces lignes directrices peuvent tenir compte de cadres internationalement reconnus, notamment ceux élaborés par l'Organisation internationale de normalisation en matière de cybersécurité dans les relations avec les fournisseurs. Bien que ces lignes directrices ne soient pas de nature réglementaire, elles visent à orienter l'application des obligations d'atténuation prévues à l'article 15 de la LPCE, notamment en favorisant l'adoption de pratiques conformes aux cadres reconnus en matière de cybersécurité.

L'organisme réglementaire est autorisé, en vertu de l'article 16 de la LPCE, à communiquer au CST tout renseignement, y compris des renseignements confidentiels concernant le programme de cybersécurité d'un exploitant désigné et les mesures d'atténuation des risques prévues à l'article 15 afin d'obtenir « des avis, des conseils et des services ».

L'article 2 de la LPCE définit les « renseignements confidentiels » comme des renseignements dont la divulgation pourrait compromettre la sécurité ou la compétitivité d'un exploitant désigné. Cette définition repose sur trois principes : premièrement, sont considérés comme confidentiels les renseignements portant sur « la vulnérabilité des cybersystèmes essentiels » ou sur les méthodes de protection utilisées, à condition qu'ils soient « traités comme étant confidentiels de façon constante par l'exploitant désigné. » Deuxièmement, un renseignement dont la divulgation pourrait vraisemblablement entraîner « des pertes ou profits financiers appréciables à un exploitant désigné ou de nuire à sa compétitivité » est considéré confidentiel. Troisièmement, une information est considérée confidentielle si « la divulgation risquerait vraisemblablement d'entraver des négociations, notamment contractuelles, menées par un exploitant désigné ».

2.2.5 Signalement obligatoire des incidents de cybersécurité

Les articles 17 à 19 de la LPCE établissent des obligations claires en matière de signalement des incidents de cybersécurité pour les exploitants désignés.

L'article 17 impose aux exploitants désignés de déclarer au CST tout incident de cybersécurité touchant ses cybersystèmes essentiels dans les délais réglementaires, lesquels ne peuvent excéder 72 heures. Ce délai a été prolongé lors de l'étude du projet de loi C-26 afin de permettre au CST d'exercer ses fonctions de surveillance, d'analyse et d'intervention en matière de cybersécurité, tout en permettant aux exploitants désignés d'agir efficacement dans le cas d'un incident grave[27].

VERSION PRÉLIMINAIRE
NON RÉVISÉE

En vertu de l'alinéa 18(b) de la Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST)[28], le CST a pour mandat de mener des opérations de cyberdéfense « afin d'aider à protéger l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral ».

Une fois l'incident déclaré au CST, l'article 18 prévoit que l'exploitant doit aviser « sans délai » l'organisme réglementaire compétent et lui transmettre une copie du rapport d'incident. Cette double notification assure une coordination entre l'autorité technique (le CST) et les autorités réglementaires sectorielles responsables, renforçant ainsi la capacité de réponse à l'échelle gouvernementale.

Le nouvel article 18.1 de la LPCE précise que les obligations de déclaration prévues aux articles 17 et 18 n'ont pas pour effet de porter atteinte aux dispositions de la *Loi sur la protection des renseignements personnels et les documents électroniques*[29]. Cette précision confirme que le régime de signalement obligatoire des incidents de cybersécurité doit être mis en œuvre dans le respect des règles générales applicables en matière de collecte, d'utilisation et de communication des renseignements personnels.

Finalement, l'article 19 de la LPCE permet à l'organisme réglementaire compétent de demander au CST une copie du rapport d'incident, en tout ou en partie, afin de vérifier le respect des obligations prévues par la LPCE ou ses règlements. Cette disposition facilite le partage d'information entre les entités gouvernementales, tout en assurant le suivi réglementaire des exploitants désignés.

Ensemble, ces articles établissent un cadre rigoureux de déclaration, de transparence et de collaboration interinstitutionnelle, essentiel pour protéger les cybersystèmes essentiels contre les menaces croissantes dans le domaine numérique tout en assurant le respect des exigences applicables en matière de protection des renseignements personnels.

2.2.6 Directives de cybersécurité secrètes

Les articles 20 à 23 de la LPCE autorisent le gouverneur en conseil à transmettre, par décrets, des « directives de cybersécurité » secrètes aux exploitants, à condition qu'il ait des motifs raisonnables de croire que ces mesures sont nécessaires à la protection d'un cybersystème essentiel. D'après l'article 20 de la LPCE, ces directives peuvent être modifiées ou révoquées et doivent tenir compte de plusieurs facteurs, notamment les répercussions sur les activités opérationnelles, la sécurité publique, **la protection de la vie privée des Canadiens,** les finances des exploitants et la continuité des services critiques. Les exploitants visés par une directive sont tenus de s'y conformer.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Le ministre de Sécurité publique et de la Protection civile doit informer le Comité des parlementaires sur la sécurité nationale et le renseignement ainsi que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, dans les 90 jours de la prise d'une directive, de la prise de cette dernière. Il est également précisé que ces directives ne peuvent autoriser l'interception de communications privées au sens du *Code criminel*. L'article 21 encadre le contenu des directives, qui doivent préciser à qui elles s'appliquent, les mesures à prendre, les modalités d'exécution et les délais.

Le caractère secret et rapide de ces directives est permis par le paragraphe 22(1) de la LPCE, qui exempte les directives de cybersécurité des articles 3, 5 et 11 de la *Loi sur les textes réglementaires* (LTR)[30]. L'article 3 de la LTR exige que les règlements proposés soient examinés en consultation avec le sous-ministre de la Justice afin de vérifier, entre autres, leur conformité avec la *Charte*. L'article 5 de la LTR exige que tous les règlements soient transmis dans les deux langues officielles au greffier du Conseil privé aux fins d'enregistrement, et l'article 11 exige que tous les règlements soient publiés dans la *Gazette du Canada* dans les 23 jours suivant leur enregistrement.

L'article 22 de la LPCE prévoit toutefois qu'un exploitant ne puisse être tenu responsable d'une infraction à une directive que s'il est démontré qu'il en avait connaissance ou que des mesures raisonnables avaient été prises pour l'en informer.

Pour sa part, l'article 23 de la LPCE autorise un échange de renseignements, y compris de renseignements confidentiels, entre plusieurs ministères et organismes fédéraux – y compris le CST, le Service canadien du renseignement de sécurité, les ministères de la Défense nationale et des Affaires étrangères – dans la mesure nécessaire à l'établissement, la modification ou la révocation d'une directive. Ces renseignements doivent être traités par toutes les entités comme étant confidentiels.

Enfin, en vertu des articles 24 et 25 de la LPCE, il est interdit aux exploitants désignés assujettis à une directive de cybersécurité de communiquer ou de permettre à d'autres de communiquer le contenu de ces directives ou l'existence même de celles-ci, sauf si ces communications sont nécessaires pour se conformer à la directive.

2.2.6.1 Contrôle judiciaire par la Cour fédérale des directives de cybersécurité secrètes

Les articles 145 et 146 de la LPCE établissent les règles particulières encadrant le contrôle judiciaire des directives de cybersécurité émises en vertu de l'article 20 de la LPCE.

L'article 145 de la LPCE prévoit que le contrôle judiciaire des directives de cybersécurité soit effectué par un juge de la Cour fédérale. Dans le cadre d'une requête en contrôle judiciaire d'une directive de cybersécurité, l'article 145(1) précise

VERSION PRÉLIMINAIRE
NON RÉVISÉE

que le juge ne peut fonder sa décision sur des éléments de preuve ou renseignements s'il juge qu'ils ne sont pas pertinents ou si le ministre choisit de les retirer. Dans ce cas, le juge doit en informer le ministre et s'assurer de la confidentialité des éléments de preuve ou renseignements retirés de l'instance. De plus, le juge est tenu de garantir la confidentialité des éléments de preuve ou renseignements retirés de l'instance. Cette règle vise à protéger les informations classifiées ou sensibles, tout en permettant au tribunal de statuer sur la légalité de la directive.

L'article 146 de la LPCE étend ces règles aux procédures d'appel d'une décision rendue dans le cadre d'un tel contrôle judiciaire, assurant ainsi une cohérence procédurale et une protection continue des renseignements confidentiels tout au long du processus judiciaire.

2.2.7 Interdictions et autorisations relatives à la communication de renseignements

Les articles 26 à 29 de la LPCE traitent de la communication et de l'utilisation des renseignements recueillis en vertu de la LPCE. Bien que la LPCE interdise de communiquer sciemment des renseignements confidentiels ou d'en permettre la communication, elle crée également une liste d'exceptions, y compris l'exception prévue à l'alinéa 26(1)f) concernant la communication en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*[31], qui permet la communication de renseignements entre 17 ministères et organismes fédéraux afin de protéger le Canada contre les « activités qui portent atteinte à la sécurité du Canada ».

Il convient de noter que l'alinéa 26(1)b) crée une exception à l'interdiction de communication lorsque « les renseignements sont accessibles au public ». À l'heure actuelle, l'article 2 de la Loi sur le CST fournit la définition la plus large de l'expression « information accessible au public » en droit canadien, en la définissant comme une « information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat[32] ».

Un nouvel article 26.1 a été ajouté à la LPCE après examen à la Chambre des communes, qui précise que les dispositions de la LPCE n'ont pas pour effet de porter atteinte aux obligations imposées par la LPRP. Aux fins de la LPCE, les « renseignements personnels » s'entendent d'ailleurs au sens de l'article 3 de cette *Loi*, conformément à la définition prévue à l'article 2 de la LPCE. L'article 26.1 de la LPCE confirme donc que, malgré les exceptions prévues à l'article 26, la collecte, l'utilisation et la communication de renseignements personnels demeurent régies par le cadre législatif général applicable au secteur public fédéral.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

L'article 27 de la LPCE permet au ministre de la Sécurité publique, aux ministres responsables et aux organismes réglementaires de conclure par écrit des accords ou des ententes d'échange de renseignements avec le gouvernement d'une province ou d'un pays étranger ou avec une organisation internationale créée par les gouvernements de divers États. L'échange de renseignements en vertu de ces accords ou ententes doit avoir trait à la protection des cybersystèmes essentiels et, sauf pour l'exception prévue pour les gouvernements provinciaux en vertu du paragraphe 27(2), ne peut inclure des renseignements confidentiels.

L'article 29 de la LPCE confère à l'organisme réglementaire compétent le pouvoir d'exiger que toute personne, société de personnes ou organisation non dotée de la personnalité morale, lui fournisse les renseignements nécessaires pour vérifier le respect ou prévenir le non-respect des dispositions de la LPCE ou de ses règlements. Les renseignements doivent être fournis dans le délai et selon les modalités précisées dans la demande, ce qui permet une certaine souplesse administrative tout en assurant l'efficacité du processus de vérification.

L'article 29.1 est une nouvelle addition qui introduit l'obligation explicite d'éliminer les renseignements personnels recueillis ou obtenus sous le régime de la LPCE lorsqu'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés, ni aux fins de vérification ou de prévention du non-respect de la LPCE, et ce, conformément aux exigences applicables de la LPRP. Enfin, l'article 29.2 précise que la LPCE ne porte pas atteinte aux dispositions de la Loi sur le CST relatives à la protection des renseignements personnels, confirmant ainsi la coexistence et la complémentarité des régimes de protection applicables.

2.2.8 Tenue de documents

L'article 30 de la LPCE exige que les exploitants désignés conservent des documents sur des éléments clés de leurs programmes de cybersécurité respectifs, y compris les mesures prises pour atténuer les risques liés à la chaîne d'approvisionnement ou aux tiers; tout incident de cybersécurité déclaré; les mesures prises pour mettre en œuvre les directives de cybersécurité; et tout autre élément précisé par règlement.

Les dispositions du paragraphe 30(2) exigent que ces documents soient conservés au Canada, dans tout lieu et de la manière désignés par règlement. En l'absence de précision au règlement, les documents doivent être conservés dans l'établissement de l'exploitant désigné.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.2.9 Exécution et contrôle d'application de la Loi sur la protection des cybersystèmes essentiels

Pour faciliter la mise en œuvre de la LPCE et son respect, des limites sont prévues concernant les responsabilités juridiques des exécuteurs, de même que l'encadrement des pouvoirs des six organismes réglementaires chargés de surveiller le fonctionnement des services et des systèmes critique.

2.2.9.1 Immunité judiciaire en responsabilité civile

L'article 31 de la LPCE établit une immunité judiciaire pour les personnes qui exercent des fonctions en vertu de cette loi et leurs accompagnateurs. Cette disposition vise à protéger les agents de l'État et les personnes autorisées contre toute responsabilité civile lorsqu'ils agissent de bonne foi dans l'exercice de leurs attributions.

2.2.9.2 Pouvoirs des organismes réglementaires

Les articles 32 à 85 de la LPCE énoncent les pouvoirs respectifs de chacun des six organismes réglementaires chargés de surveiller le fonctionnement des services et des systèmes critiques.

Afin de vérifier la conformité ou de prévenir le non-respect de la LPCE et de ses règlements, chacun de ces six organismes réglementaires est autorisé à pénétrer dans tout lieu, autre qu'une maison d'habitation, sans consentement ni mandat (articles 32, 41, 50, 59, 68 et 78). La LPCE exige que l'organisme réglementaire obtienne un mandat d'un juge de paix pour entrer dans une maison d'habitation au moyen d'une demande *ex-parte* (articles 33, 42, 51, 60, 69 et 79).

À son entrée dans un lieu, un organisme réglementaire peut examiner, utiliser ou voir à ce que soit utilisé tout cybersystème, notamment pour en obtenir des renseignements. L'organisme réglementaire peut alors préparer ou faire préparer un document contenant ces renseignements. L'organisme réglementaire a également le pouvoir d'examiner les registres, rapports, données et autres documents se trouvant sur les lieux et de les reproduire, à l'aide du matériel de reproduction trouvé sur place, au besoin. Enfin, l'organisme réglementaire est autorisé à retirer du lieu tout document, registre ou cybersystème, en tout ou en partie, afin de l'examiner ou d'en faire des copies.

2.2.9.3 Ordonnance de vérifications internes obligatoires

En vertu des articles 34, 43, 52, 61, 70 et 80 de la LPCE et sous réserve des règlements, un organisme réglementaire peut ordonner par écrit à un exploitant désigné d'effectuer une vérification interne dans un délai prescrit pour déterminer sa

VERSION PRÉLIMINAIRE
NON RÉVISÉE

conformité à la LPCE et à ses règlements. Comme ces ordres sont exemptés de la LTR, ils ne sont pas publiés dans la *Gazette du Canada* et ne sont donc pas publics.

Les articles 35, 44, 53, 62, 71 et 81 de la LPCE exigent que l'exploitant désigné communique les conclusions de sa vérification à l'organisme réglementaire. Si l'exploitant désigné a conclu à sa non-conformité, son rapport à l'organisme réglementaire doit indiquer la nature de la non-conformité et les mesures qu'il prendra pour se conformer.

Si un organisme réglementaire a des motifs raisonnables de croire qu'un exploitant désigné contrevient ou contreviendra vraisemblablement à la LPCE ou à l'un de ses règlements, les articles 36, 45, 54, 63, 73 et 82 de la LPCE l'autorise à ordonner à l'exploitant désigné de cesser de faire toute chose en contravention de la disposition en cause (ou toute chose qui donnera vraisemblablement lieu à une contravention à la disposition) ou de la faire cesser, dans un délai donné. De même, l'organisme réglementaire peut ordonner à l'exploitant désigné de prendre des mesures pour atténuer les effets de la non-conformité. Encore une fois, en vertu des paragraphes 36(3), 45(3), 54(3), 63(3), 73(4) et 82(3), ces ordres ne seront pas rendus publics.

Les articles 37, 46, 55, 64, 74 et 83 de la LPCE énoncent explicitement la nature obligatoire d'un ordre de conformité et exigent qu'un exploitant désigné visé par un tel ordre avise immédiatement l'organisme réglementaire compétent une fois qu'il s'y est conformé.

2.2.10 Demande de révision d'un ordre de conformité

Un exploitant désigné assujetti à un ordre de conformité peut présenter une demande écrite à l'organisme réglementaire pour qu'il révise l'ordre (articles 38, 47, 56, 65, 84 et 75(2) à 75(4) de la LPCE). La demande de révision doit être présentée selon les modalités et dans les délais établis dans l'ordre de conformité, énoncer les motifs de la révision et fournir des preuves à l'appui de la révision. Toutefois, à moins que l'organisme réglementaire n'en décide autrement, l'ordre de conformité demeure en vigueur pendant la révision.

Une fois que l'organisme réglementaire a terminé sa révision de l'ordre de conformité, les articles 39, 48, 57, 66, 76 et 85 de la LPCE exigent qu'il confirme, modifie, révoque ou annule l'ordre, en donnant un avis motivé de la décision à l'exploitant désigné. Par ailleurs, si l'organisme réglementaire n'a pas pris de décision après avoir reçu une demande de révision dans les 90 jours ou après tout autre délai convenu entre l'organisme réglementaire et l'exploitant désigné, l'organisme réglementaire est réputé avoir confirmé l'ordre de conformité original.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

2.2.11 Règlements

L'article 135 de la LPCE confère au gouverneur en conseil le pouvoir de prendre des règlements pour assurer la mise en œuvre efficace de la LPCE.

Plus précisément, le paragraphe 135(1) énumère une série de domaines dans lesquels des règlements peuvent être adoptés. Cela inclut les programmes de cybersécurité, les vérifications internes, les modalités de signalement des incidents (notamment ceux visés à l'art. 17 de la LPCE), les délais pour les avis de changement (art. 14 de la LPCE), la gestion documentaire (art. 30 de la LPCE), ainsi que la classification des violations (mineure, grave, très grave) et les montants maximaux des pénalités applicables. Le gouverneur en conseil peut également définir des termes non précisés dans la loi et prendre toute autre mesure réglementaire prévue par celle-ci.

Le paragraphe 135(2) ajoute que, dans l'élaboration de ces règlements, le gouverneur en conseil peut chercher à assurer leur compatibilité avec les régimes de réglementation existants, notamment ceux des organismes provinciaux. Cette disposition reflète une volonté d'harmonisation intergouvernementale, essentielle dans un domaine comme la cybersécurité, où les infrastructures et les responsabilités peuvent être partagées entre plusieurs niveaux de gouvernement.

2.2.12 Infractions et peines

Les articles 136 à 146 de la LPCE établissent un régime complet d'infractions, de sanctions pénales et de procédures judiciaires visant à assurer le respect des obligations prévues par la LPCE.

L'article 136 prévoit que toute personne qui contrevient à une série d'obligations précises – telles que la transmission du programme de cybersécurité (art. 10 de la LPCE), la déclaration d'incidents (art. 17 de la LPCE), ou la tenue de documents (art. 30 de la LPCE) – commet une infraction punissable par procédure sommaire.

L'article 137 élargit cette portée en prévoyant que certaines infractions, comme le non-respect d'une directive de cybersécurité (par. 20(4) de la LPCE) ou la communication interdite d'une directive (art. 24 de la LPCE), peuvent être poursuivies soit par procédure sommaire, soit par mise en accusation, avec des peines allant jusqu'à cinq ans d'emprisonnement pour les personnes physiques, et des amendes illimitées fixées par le tribunal pour les personnes morales.

L'article 138 précise que les dirigeants ou administrateurs qui ont participé à la commission d'une infraction sont considérés comme coauteurs et peuvent être poursuivis même si l'exploitant désigné ne l'est pas. L'article 139 introduit la notion d'infraction continue, comptant une infraction distincte pour chaque jour où la

VERSION PRÉLIMINAIRE
NON RÉVISÉE

violation persiste, ce qui peut considérablement alourdir les sanctions. Enfin, l'article 140 fixe un délai de prescription de trois ans pour engager des poursuites.

2.2.12.1 Moyens de défense

Des moyens de défense sont également prévus. L'article 141 de la LPCE permet à un accusé de se disculper s'il peut démontrer avoir pris toutes les précautions voulues pour prévenir l'infraction. L'article 142 de la LPCE facilite la preuve en permettant d'établir une infraction par les actes d'un employé ou mandataire, même si cette personne n'est pas identifiée ou poursuivie.

Enfin, les articles 143 et 144 de la LPCE facilitent l'administration de la preuve en reconnaissant la valeur probante des documents certifiés et des inscriptions aux registres. Les articles 145 et 146 de la LPCE encadrent les règles de contrôle judiciaire des directives de cybersécurité, en assurant notamment la confidentialité des renseignements sensibles présentés au tribunal.

2.2.13 Maintien du secret professionnel

Enfin, le nouvel article 148 de la LPCE précise que la LPCE n'a pas pour effet de porter atteinte au secret professionnel de l'avocat ou du notaire. Cette disposition confirme que, malgré l'étendue des pouvoirs d'enquête, de communication de renseignements et de contrôle judiciaire prévus par la LPCE, les protections reconnues au secret professionnel demeurent pleinement applicables. Elle vise ainsi à préserver un principe fondamental de l'administration de la justice, y compris dans le cadre des procédures pénales, réglementaires ou judiciaires engagées en vertu de la LPCE.

2.2.14 Rapport annuel

L'article 147 de la LPCE ordonne au ministre de la Sécurité publique de préparer un rapport sur l'administration de la LPCE dans les trois mois suivant la fin de chaque année fiscale et de déposer ce rapport au Sénat et à la Chambre des communes dans les 15 premiers jours de séance suivant l'achèvement du rapport.

Le paragraphe 147(2) précise que le rapport doit inclure des renseignements détaillés sur les décrets pris en vertu du paragraphe 20(1) de la LPCE, notamment le nombre de directives émises et révoquées, le nombre d'exploitants visés, ainsi que des descriptions de leur niveau de conformité – partielle ou complète – aux directives reçues. Le rapport doit aussi expliquer la nécessité, la proportionnalité et l'utilité de ces directives.

Le paragraphe 147(3) complète cette exigence en demandant que le rapport contienne des données sur les directives émises au cours de l'exercice précédent, le nombre

VERSION PRÉLIMINAIRE
NON RÉVISÉE

d'exploitants concernés, ainsi que tout autre renseignement jugé pertinent par le ministre, à condition que l'identité des exploitants ou des personnes ne soit pas révélée.

3 COMMENTAIRES

Depuis son dépôt, le projet de loi C-8 a suscité de nombreuses réactions de la part de parties prenantes. La partie ci-dessous présente une synthèse de l'analyse du projet de loi par les parties prenantes, notamment les points de vue de la communauté universitaire, de juristes et de groupes de défenses des droits et des experts spécialisés en cybersécurité et en droit public.

Un énoncé concernant la *Charte* à l'égard du projet de loi C-8 a été rendu public en septembre 2025[33]. Cet énoncé apporte un éclairage juridique sur certaines des préoccupations soulevées par les parties prenantes, en particulier celles touchant l'étendue des pouvoirs conférés à l'exécutif, la protection des renseignements personnels et les répercussions possibles sur les droits et libertés garantis par la *Charte*.

3.1 INCERTITUDES RÉGLEMENTAIRES ET DÉFIS DE MISE EN ŒUVRE POUR LES EXPLOITANTS DÉSIGNÉS

Des juristes ont qualifié les obligations en matière de cybersécurité que le projet de loi C-8 impose aux exploitants désignés de « rigoureuses et étendues[34] ». Ces obligations de conformité et de surveillance opérationnelle – telles l'élaboration de programmes de cybersécurité, la déclaration rapide des incidents, et la gestion des risques liés à la chaîne d'approvisionnement – sont perçues comme étant importantes, particulièrement pour les entreprises disposant de ressources financières ou de capacités techniques limitées[35].

D'autre part, de nombreux professionnels du droit en matière de respect à la vie privée et de cybersécurité ont identifié un manque de clarté dans le projet de loi C-8, notamment par rapport aux catégories d'« exploitants désignés » qui ne sont pas définies[36], ainsi qu'à la portée générale des nouvelles obligations qui seront définies ultérieurement par voie réglementaire[37]. Selon eux, cette absence de clarté législative, conjuguée au pouvoir conféré au gouvernement d'émettre des directives contraignantes – et potentiellement confidentielles – en matière de cybersécurité, est susceptible de nuire à la planification stratégique des exploitants concernés ainsi qu'à la mise en œuvre efficace de leurs mesures de conformité[38].

Cela dit, d'autres juristes ont accueilli favorablement l'inclusion, dans la version amendée du projet de loi C-8, d'une obligation statutaire de révision ministérielle dans les cinq ans suivant la sanction royale. Selon ces observateurs, ce mécanisme de

VERSION PRÉLIMINAIRE
NON RÉVISÉE

révision constitue une mesure importante de gouvernance législative, puisqu'il permet d'évaluer, à la lumière de l'expérience acquise, si le régime instauré atteint ses objectifs en matière de cybersécurité et s'il impose des contraintes proportionnées aux exploitants désignés [39].

3.2 RÉPERCUSSIONS DES NOUVEAUX POUVOIRS DE SURVEILLANCE : DIRECTIVES, ARRÊTÉS ET DÉCRETS

Plusieurs juristes ont exprimé des préoccupations quant à l'ampleur des pouvoirs que le projet de loi C-8 confère aux organismes de réglementation, notamment le pouvoir de mener des inspections, d'exiger des audits internes et d'imposer des pénalités pécuniaires sévères, tout en reconnaissant que le projet de loi est bien intentionné et comporte de nombreux éléments nécessaires [40].

Les préoccupations se sont accentuées à la suite de l'adoption du projet de loi en troisième lecture. Plusieurs juristes ont souligné le rejet en Chambre de certains amendements adoptés en comité parlementaire, lesquels visaient à assujettir certaines ordonnances gouvernementales à une autorisation judiciaire préalable [41]. Selon ces juristes, cette décision a eu pour effet de rétablir un pouvoir exécutif étendu, la surveillance étant désormais limitée à un contrôle judiciaire exercé *a posteriori* [42]. Cela mettrait en lumière des préoccupations persistantes soulevées par certains observateurs du point de vue que l'absence de contrôle judiciaire préalable n'a pas été entièrement corrigée depuis 2025, et ce, malgré l'introduction de certains mécanismes procéduraux.

Des préoccupations soulignent la norme subjective prévue au nouvel article 15.4 de la *Loi sur les télécommunications*. Selon Matt Malone, un universitaire de la Faculté de droit de l'Université d'Ottawa spécialisé en droit à la vie privée et en cybersécurité, cette disposition permet au ministre de l'Industrie d'« exiger de toute personne », « selon les modalités qu'il précise », la communication de renseignement qu'il juge pertinent à la prise d'un décret, d'un arrêté ou d'un règlement [43]. Cet expert a souligné le caractère subjectif de cette norme, qui repose sur l'appréciation discrétionnaire du ministre, sans encadrement explicite quant à la nature des renseignements exigés ni aux garanties entourant leur utilisation [44]. D'autres préoccupations concernent l'absence – tant dans le projet de loi C-8 que dans son prédécesseur, le projet de loi C-26 – de dispositions encadrant la réutilisation ou la communication subséquente des données, notamment par le CST [45].

Par ailleurs, ce même universitaire fait écho aux inquiétudes exprimées par le Citizen Lab lors de l'étude du projet de loi C-26, concernant les nouveaux pouvoirs de directives secrètes prévus à la LPCE [46]. Il faut rappeler que ces pouvoirs échappent aux exigences de transparence normalement imposées par la *Loi sur les textes réglementaires*, qui prévoit la publication et l'examen des règlements susceptibles

VERSION PRÉLIMINAIRE
NON RÉVISÉE

d'avoir une incidence sur les droits fondamentaux. Selon ces experts, cette exemption pourrait compromettre les attentes raisonnables des Canadiens en matière de protection de la vie privée, et restreindre le contrôle démocratique et judiciaire de ces pouvoirs.

Cela dit, de nombreux témoins entendus lors de l'étude du projet de loi C-8 par le Comité permanent de la sécurité publique et nationale de la Chambre des communes (le Comité) ont formulé des recommandations visant à renforcer l'encadrement des nouveaux pouvoirs.

Plusieurs ont souligné l'importance d'adopter une norme claire et uniforme exigeant que l'exercice de ces pouvoirs soit à la fois nécessaire pour atteindre les objectifs poursuivis et proportionnel aux avantages attendus[47]. À cet égard, l'intégration explicite des critères de nécessité et de proportionnalité à plusieurs endroits dans la version révisée du projet de loi C-8 répond directement à ces recommandations.

3.3 PRÉOCCUPATIONS EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

Des experts du droit dans le domaine de la gouvernance des données et de la cybersécurité ont soulevé des inquiétudes quant à la protection des renseignements personnels et confidentiels dans le cadre du projet de loi C-8[48]. D'après eux, la protection de ce type de renseignement en cas d'incident de cybersécurité peut présenter des défis face aux nouveaux pouvoirs de fouille et de saisie accordés aux organismes de réglementation, à l'obligation de tenue de dossiers des exploitants désignés, et à leur exigence d'aviser sans délai le CST et l'organisme de réglementation compétent en cas d'incident de cybersécurité[49].

Le Commissaire à la protection de la vie privée du Canada a appuyé l'objectif de renforcer la cybersécurité des infrastructures essentielles, tout en exprimant des réserves quant à l'ampleur des pouvoirs conférés aux gouvernements et organismes de réglementation[50]. Il a notamment relevé des enjeux liés au respect de l'article 8 de la *Charte*, en raison de pouvoirs susceptibles d'autoriser des fouilles, perquisitions et saisies sans garanties suffisantes ni mécanismes de surveillance indépendants. Bien qu'il ait reconnu certaines améliorations par rapport au projet de loi C-26, il a indiqué que des risques subsistaient, en particulier en ce qui concerne l'encadrement du partage des renseignements, y compris avec des partenaires étrangers.

Des préoccupations similaires ont été soulevées par M. Malone quant à la compatibilité de ces pouvoirs avec les normes européennes de protection des données personnelles, une divergence susceptible de fragiliser la confiance des partenaires européens et de compliquer la collaboration transfrontalière dans les secteurs visés[51].

VERSION PRÉLIMINAIRE
NON RÉVISÉE

Dans son énoncé concernant la *Charte*, le ministre de la Justice reconnaît que certaines dispositions du projet de loi sont susceptibles de porter atteinte aux droits protégés par la *Charte*, notamment le droit à la vie privée garanti aux article 7 (droit à la vie, la liberté et à la sécurité de sa personne) et article 8 (droit à la protection contre les fouilles, les perquisitions ou les saisies abusives par l'État). Toutefois, l'énoncé conclut que ces atteintes potentielles sont justifiables au regard de l'article 1, compte tenu des objectifs de sécurité nationale et de sécurité publique et des mécanismes législatifs visant à encadrer l'exercice de ces pouvoirs [52].

L'énoncé souligne notamment que les pouvoirs conférés par le projet de loi C-8 sont assortis de limites explicites visant à prévenir les abus, telles que l'interdiction d'intercepter des communications privées, l'obligation de prendre en compte les répercussions sur la vie privée et la disponibilité de mécanismes de contrôle parlementaire et judiciaire [53].

3.4 ABSENCE DE SOUTIEN FINANCIER OU TECHNIQUE

Un autre point soulevé est l'absence de mesures d'accompagnement, telles que des incitatifs financiers, des subventions ou des ressources techniques, pour aider les entreprises à se conformer aux nouvelles exigences.

Notamment, la partie 1 du projet de loi C-8 ne prévoit aucune indemnisation pour les pertes financières liées au respect des ordonnances par les FST, tout en imposant des pénalités pouvant atteindre 15 millions de dollars par jour en cas de non-conformité, ce qui représente, selon des professionnels du droit, un fardeau financier majeur pour le secteur privé [54]. Selon une associée principale du groupe Confidentialité et cybersécurité d'une firme de Toronto, cette lacune pourrait freiner l'adoption rapide et efficace des normes de cybersécurité, surtout dans un contexte où les menaces évoluent rapidement [55].

Ces préoccupations ont été reprises lors de l'étude du projet de loi C-8 par le Comité. À cette occasion, certains témoins ont recommandé la mise en place d'un crédit d'impôt à l'investissement en cybersécurité, afin d'encourager les entreprises canadiennes à renforcer leurs capacités internes et à se conformer plus efficacement aux nouvelles exigences réglementaires [56]. D'autres ont suggéré de prévoir un mécanisme d'indemnisation permettant le recouvrement de certains coûts imposés par des ordonnances gouvernementales, ainsi que l'établissement d'un processus sécurisé de divulgation de l'information, afin de réduire les risques opérationnels et financiers pour les entreprises concernées [57].

En outre, les exploitants des secteurs touchés par la partie 2 du projet de loi C-8 sont confrontés à d'importants défis en matière de conformité. L'une des principales

VERSION PRÉLIMINAIRE
NON RÉVISÉE

inquiétudes porte sur les coûts opérationnels élevés et le risque financier considérable qu'ils encourent sans compensation. Lors de l'étude de l'ancien projet de loi C-26, des experts de la société civile ont souligné des lacunes vis-à-vis les coûts associés aux réformes et la viabilité des petits fournisseurs de service au Canada[58].

Un avocat du groupe de Protection de la vie privée et des données d'une firme de Toronto indique que ces nouvelles mesures vont créer d'importants problèmes de conformité pour le secteur des télécommunications et des infrastructures fédérales essentielles au Canada. Ces derniers devront assurer une planification stratégique afin d'éviter des mesures d'application coûteuses et des perturbations opérationnelles[59].

3.5 RÉPERCUSSIONS SUR LES RELATIONS CONTRACTUELLES ET L'INDUSTRIE

Le projet de loi C-8 pourrait avoir des effets en cascade sur les relations contractuelles entre les entreprises réglementées et leurs fournisseurs. Par exemple, l'article 15 de la LPCE, érigé sous l'article 11 du projet de loi C-8, exige des exploitants désignés « de prendre des mesures pour atténuer les risques associés à la chaîne d'approvisionnement identifiés par le programme de cybersécurité[60] ». Selon des experts, tels un universitaire et des professionnels du droit, ce sont des exigences accrues en matière de cybersécurité comme celle-ci qui pourraient se traduire par des obligations contractuelles plus strictes et éventuellement désavantager les petits fournisseurs ou ceux situés à l'étranger[61].

À cet égard, d'autres professionnels du droit estiment que « les fournisseurs de services devraient s'attendre à l'exigence de normes de cybersécurité plus élevées par leurs clients réglementées, particulièrement si leurs services sont liés aux cybersystèmes essentiels[62] ».

NOTES

* Le présent résumé législatif s'appuie en partie sur le résumé législatif préparé par la Bibliothèque du Parlement concernant 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 (44e législature, 1re session).

1. Projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, 45e législature, 1re session.
2. Après son adoption en deuxième lecture à la Chambre des communes le 3 octobre 2025, le projet de loi C-8 a été renvoyé au Comité permanent de la sécurité publique et nationale de la Chambre des communes (SECU), qui en a effectué l'étude article par article. À l'issue de cet examen, SECU a présenté à la Chambre un rapport avec des amendements le 11 mars 2026.
3. Sécurité publique Canada, *Stratégie nationale de cybersécurité du Canada : Sécuriser l'avenir numérique du Canada*, janvier 2025.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

4. Projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois, 44e législature, 1re session.

5. Sécurité publique Canada, *Stratégie nationale de cybersécurité du Canada : Sécuriser l'avenir numérique du Canada*, janvier 2025.

6. *Ibid*., p. 30.

7. *Ibid*.

8. *Ibid*., p. 3.

9. Catharine Tunney, « Senators amend error in cybersecurity bill that could have cancelled half of it », *CBC News*, 6 décembre 2024; cité dans Robbie Grant, *Projet de loi C-26 : un nouveau chapitre dans la réglementation canadienne en matière de cybersécurité*, McMillan S.E.N.C.R.L., s.r.l., 24 décembre 2024.

10. Le réseau sans fil 5G est la cinquième génération de technologie de communication cellulaire, permettant un plus grand nombre d'appareils utilisateurs, ainsi que des communications plus rapides et de plus grandes vitesses. Voir Centre de recherches sur les communications Canada, *Qu'est-ce que le 5G?* Voir aussi Innovation, Sciences et Développement économique Canada (ISDE), *Déclaration du ministre Champagne sur la sécurité des télécommunications*, 19 mai 2022; et ISDE, *Énoncé de politique – Sécuriser le système de télécommunications au Canada*, déclaration.

11. Sarah Lemelin-Bellerose, « La technologie 5G : Possibilités, défis et risques », *Notes de la Colline*, Bibliothèque du Parlement, 13 février 2020; et Royaume-Uni, Department for Digital, Culture, Media & Sport, National Cyber Security Centre et le très honorable Oliver Dowden, *Huawei to be removed from UK 5G networks by 2027*, communiqué, 14 juillet 2020.

12. Australie, *Security of Critical Infrastructure Act 2018* (nº 29, 2018).

13. Australie, *Security Legislation Amendment (Critical Infrastructure) Act 2021* (nº 124, 2021).

14. États-Unis, *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law 117-103, 117e Congrès, 136 Stat. 49, Division Y in *Consolidated Appropriations Act, 2022*, H.R.2471.

15. Royaume-Uni, *The Network and Information Systems Regulations 2018*, 2018 nº 506.

16. Union européenne, EUR-Lex, *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, dans *Journal officiel*, nº L 194.

17. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025; et Hélène Deschamps Marquis *et al*., *Le projet de loi C-8 relance la réforme canadienne en cybersécurité – Ce que doivent savoir les secteurs d'infrastructures critiques*, Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG), 28 juillet 2025.

18. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025.

19. *Ibid*.

20. Sécurité publique Canada, *Aperçu des modifications proposées à la* Loi sur les télécommunications, document d'information.

21. *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.).

22. *Code criminel*, L.R.C. 1985, ch. C-46.

23. Aux fins de cette disposition, une communication privée s'entend notamment d'une communication faite dans des circonstances où son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers, y compris une communication radiotéléphonique protégée contre la réception en clair. Le terme « intercepter » vise, entre autres, le fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de son contenu.

24. *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

25. Bien que le terme « agent verbalisateur » ne soit pas défini dans le projet de loi, le nouvel art. 72.134 de la *Loi sur les télécommunications* précise que le ministre peut désigner les agents autorisés à dresser des procès-verbaux pour une violation ou à conclure une transaction. Ce type d'agent est ensuite référé en tant qu'« agent verbalisateur » au nouvel art. 72.135 abordant la procédure entourant un procès-verbal.

26. Selon le secteur économique de l'exploitant désigné, l'organisme réglementaire peut être le ministre de l'Industrie, le ministre des Transports, le surintendant des institutions financières, la Banque du Canada, la Régie canadienne de l'énergie ou la Commission canadienne de sûreté nucléaire.

27. Dans la première version du projet de loi C-26, l'art. 17 de la Loi sur la protection des cybersystèmes essentiels prévoyait incomber à tout exploitant désigné de déclarer « sans délai » tout incident de cybersécurité concernant ses cybersystèmes essentiels au Centre de la sécurité des télécommunications.

28. *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76.

29. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.

30. *Loi sur les textes réglementaires*, L.R.C. 1985, ch. S-22.

31. *Loi sur la communication d'information ayant trait à la sécurité du Canada*, L.C. 2015, ch. 20, art. 2.

32. Pour une analyse des définitions juridiques existantes de « l'information accessible au public » dans le droit canadien de la protection de la vie privée, voir Holly Porteous, « L'importance grandissante du renseignement de sources ouvertes pour la sécurité nationale », *Notes de la Colline*, Bibliothèque du Parlement, 17 février 2022.

33. Ministère de la Justice du Canada, *Énoncé concernant la Charte pour le projet de loi C-8 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, 23 septembre 2025.

34. Hélène Deschamps Marquis *et al*., *Le projet de loi C-8 relance la réforme canadienne en cybersécurité – Ce que doivent savoir les secteurs d'infrastructures critiques*, BLG, 28 juillet 2025.

35. *Ibid*.; et Robbie Grant, *De retour sous un nouveau nom : le projet de loi C-8 relance la loi exhaustive concernant la cybersécurité*, McMillan S.E.N.C.R.L., s.r.l., 3 juillet 2025.

36. Molly Reynolds *et al*., *Le gouvernement réintroduit un projet de loi sur la cybersécurité pour les secteurs fédéraux "critiques"*, Société d'avocats Torys S.E.N.C.R.L., 26 juin 2025.

37. Hélène Deschamps Marquis *et al*., *Le projet de loi C-8 relance la réforme canadienne en cybersécurité – Ce que doivent savoir les secteurs d'infrastructures critiques*, BLG, 28 juillet 2025.

38. *Ibid*.

39. Leslie Milton *et al*., *Bill C-8 Passes House of Commons Following Substantive Amendments and Speaker's Ruling*, Technology, Media, and Telecommunications Bulletin, Fasken Martineau Dumoulin LLP, 14 avril 2026.

40. Hélène Deschamps Marquis *et al*., *Le projet de loi C-8 relance la réforme canadienne en cybersécurité – Ce que doivent savoir les secteurs d'infrastructures critiques*, BLG, 28 juillet 2025; Molly Reynolds *et al*., *Le gouvernement réintroduit un projet de loi sur la cybersécurité pour les secteurs fédéraux "critiques"*, Société d'avocats Torys S.E.N.C.R.L., 26 juin 2025; Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025; et Matt Malone, « Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows? », *Balsillie Papers*, vol. 7, nº 4, 23 juillet 2025.

41. Chambre des communes, *Débats*, 25 mars 2026, 1605 (L'hon. Francis Scarpaleggia).

42. Leslie Milton *et al*., *Bill C-8 Passes House of Commons Following Substantive Amendments and Speaker's Ruling*, Technology, Media, and Telecommunications Bulletin, Fasken Martineau Dumoulin LLP, 14 avril 2026.

43. Matt Malone, « Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows? », *Balsillie Papers*, vol. 7, nº 4, 23 juillet 2025.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

44. Anaïs Bussières McNicoll et Noa Mendelsohn Aviv, Association canadienne des libertés civiles, *Mémoire présenté au Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants au sujet du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, 13 novembre 2024. Voir aussi la soumission de Matt Malone au Comité permanent de la Sécurité nationale, défense et anciens combattants du Sénat, suite à son témoignage pendant l'étude du projet de loi C-26.

45. Soumission de Matt Malone au Comité permanent de la Sécurité nationale, défense et anciens combattants du Sénat, suite à son témoignage pendant l'étude du projet de loi C-26.

46. *Ibid*.; citant Kate Robertson, *Mémoire au Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants : Étude du projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto, au paragraphe 35.

47. SECU, *Témoignages*, réunion 10, 30 octobre 2025, 1140 (Philippe Dufresne, commissaire, Commissariat à la protection de la vie privée du Canada); SECU, *Témoignages*, réunion 10, 30 octobre 2025, 1235 (Luc Lefebvre, président et cofondateur, Crypto Québec); SECU, *Témoignages*, réunion 10, 30 octobre 2025, 1240 (Sharon Polsky, présidente, Conseil du Canada de l'accès à la vie privée); et SECU, *Témoignages*, réunion 18, 4 décembre 2025, 1115 (Matthew Hatfield, directeur exécutif, OpenMedia).

48. Molly Reynolds *et al*., *Le gouvernement réintroduit un projet de loi sur la cybersécurité pour les secteurs fédéraux "critiques"*, Société d'avocats Torys S.E.N.C.R.L., 26 juin 2025.

49. *Ibid*.

50. Commissariat à la protection de la vie privée du Canada, « Fiches des enjeux au sujet du projet de loi C-26, » *Comparution devant le Comité permanent de la sécurité publique et nationale du 12 février 2024,* 12 février 2024; et SECU, *Témoignages*, réunion 10, 30 octobre 2025, 1140 (M. Dufresne).

51. Matt Malone, « Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows? », *Balsillie Papers*, vol. 7, nº 4, 23 juillet 2025.

52. Ministère de la Justice du Canada, *Énoncé concernant la Charte pour le projet de loi C-8 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, 23 septembre 2025.

53. *Ibid*.

54. Hélène Deschamps Marquis *et al*., *Le projet de loi C-8 relance la réforme canadienne en cybersécurité – Ce que doivent savoir les secteurs d'infrastructures critiques*, BLG, 28 juillet 2025; et Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025.

55. Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025.

56. SECU, *Témoignages*, réunion 10, 30 octobre 2025, 1230 (Aaron Shull, directeur général et avocat général, Centre pour l'innovation dans la gouvernance internationale); et Aaron Shull, Centre pour l'innovation dans la gouvernance internationale, *Mémoire soumis au Comité permanent de la sécurité public et nationale de la Chambre des communes par le Centre pour l'innovation dans la gouvernance internationale*, 8 décembre 2025.

57. Aaron Shull, Centre pour l'innovation dans la gouvernance internationale, *Mémoire soumis au Comité permanent de la sécurité public et nationale de la Chambre des communes par le Centre pour l'innovation dans la gouvernance internationale*, 8 décembre 2025; et Association canadienne des télécommunications, *Projet de loi C-8 – Loi concernant la cybersécurité, modifiant la loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, mémoire soumis au Comité permanent de la sécurité public et nationale de la Chambre des communes, 12 novembre 2025.

58. Kate Robertson, *Mémoire au Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants : Étude du projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, Citizen Lab.

59. Robbie Grant, *De retour sous un nouveau nom : le projet de loi C-8 relance la loi exhaustive concernant la cybersécurité*, McMillan S.E.N.C.R.L., s.r.l., 3 juillet 2025.

VERSION PRÉLIMINAIRE
NON RÉVISÉE

60. *Ibid*.; et Jaime Cardy, *From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation*, Dentons Data, 8 juillet 2025.

61. Matt Malone, « Will Canada's Bill C-8 Impact the Future of EU–Canada Cross-border Data Flows? », *Balsillie Papers*, vol. 7, nº 4, 23 juillet 2025; et Robbie Grant, *De retour sous un nouveau nom : le projet de loi C-8 relance la loi exhaustive concernant la cybersécurité*, McMillan S.E.N.C.R.L., s.r.l., 3 juillet 2025.

62. Molly Reynolds *et al*., *Le gouvernement réintroduit un projet de loi sur la cybersécurité pour les secteurs fédéraux "critiques"*, Société d'avocats Torys S.E.N.C.R.L., 26 juin 2025.