BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

Résumé législatif

PROJET DE LOI C-26 : LOI CONCERNANT LA CYBERSÉCURITÉ, MODIFIANT LA LOI SUR LES TÉLÉCOMMUNICATIONS ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS

Publication nº 44-1-C26-F

Le 6 octobre 2022

Jed Chong, Khamla Heminthavong et Holly Porteous

Services d'information, d'éducation et de recherche parlementaires

ATTRIBUTION

Le 6 octobre 2022	Jed Chong	Division de l'économie, des ressources et des affaires internationales
	Khamla Heminthavong	Division de l'économie, des ressources et des affaires internationales
	Holly Porteous	Division de l'économie, des ressources et des affaires internationales

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 d'information, d'éducation et de recherche parlementaires, qui effectuent des recherches pour les parlementaires, les comités du Sénat et de la Chambre des communes et les associations 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 devant la Chambre des communes et le Sénat, 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**.

Résumé législatif du projet de loi C-26
(Résumé législatif)

Publication nº 44-1-C26-F

This publication is also available in English.

TABLE DES MATIÈRES

RÉSUMÉ LÉGISLATIF 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

1 CONTEXTE

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, a été déposé à la Chambre des communes par le ministre de la Sécurité publique le 14 juin 2022 [1].

Ce projet de loi modifie la *Loi sur les télécommunications*[2] et crée la Loi sur la protection des cybersystèmes essentiels (LPCE). Les modifications à la *Loi sur les télécommunications* autorisent le gouverneur en conseil et le ministre de l'Industrie à ordonner aux fournisseurs canadiens de services de télécommunications de prendre des mesures pour protéger le système de télécommunications canadien contre un éventail de menaces. Ces modifications font suite à l'annonce par le gouvernement de son intention d'utiliser ces pouvoirs pour interdire l'utilisation des produits et services de Huawei et de ZTE dans les systèmes de télécommunications du Canada, en particulier dans les réseaux sans fil 5G [3]. Les États-Unis, le Royaume-Uni, l'Australie et le Japon ont également banni Huawei de leurs réseaux 5G [4].

La LPCE établit un régime de conformité en matière de cybersécurité pour les infrastructures essentielles sous réglementation fédérale. Cette loi semble s'inspirer de la *Security of Critical Infrastructure Act 2018* de l'Australie [5], qui a été modifiée en vertu de la *Security Legislation Amendment (Critical Infrastructure) Act 2021* [6] afin, notamment, d'élargir considérablement les pouvoirs du gouvernement fédéral australien pour faire respecter les obligations en matière de cybersécurité s'appliquant aux infrastructures essentielles et intervenir dans les mesures prises par le secteur privé en cas d'incidents cybernétiques touchant ces mêmes infrastructures. Il convient également de souligner la *Cyber Incident Reporting for Critical Infrastructure Act of 2022* des États-Unis [7], qui exige que les exploitants d'infrastructures essentielles signalent les incidents cybernétiques à la Cybersecurity and Infrastructure Security Agency, et le règlement intitulé *The Network and Information Systems Regulations 2018* du Royaume-Uni [8], qui est dérivé de la directive de 2016 de l'Union européenne sur la sécurité des réseaux et des systèmes d'information [9]. L'objectif général de tous ces régimes est d'atteindre un niveau de sécurité commun et amélioré pour les cyberinfrastructures essentielles et de donner une idée plus claire de la situation aux autorités compétentes.

2 DESCRIPTION ET ANALYSE

2.1 PARTIE 1 : MODIFICATIONS À LA *LOI SUR LES TÉLÉCOMMUNICATIONS*

La partie 1 du projet de loi comprend 12 articles. Les principaux articles sont détaillés ci-dessous.

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

L'article 1 du projet de loi ajoute la promotion de la sécurité du système de télécommunications aux objectifs stratégiques énoncés à l'article 7 de la *Loi sur les télécommunications* (la *Loi*). Cet ajout permet au ministre de l'Industrie et 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*. La même considération est permise en vertu de la *Loi sur la radiocommunication* (qui régit l'attribution du spectre), qui incorpore les objectifs de la *Loi* par renvoi [10].

2.1.2 Pouvoirs de prendre des décrets et des arrêtés (art. 2)

L'article 2 ajoute les articles 15.1 à 15.9 à la *Loi* pour donner au gouvernement fédéral le pouvoir de prendre des décrets. En vertu du nouvel article 15.1, le gouverneur en conseil peut, par décret, interdire aux fournisseurs de services de télécommunication (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. Le gouverneur en conseil peut également ordonner aux FST de retirer de leurs réseaux ou installations de télécommunication tous les produits d'un fournisseur donné.

Le nouveau paragraphe 15.2(1) donne au ministre de l'Industrie le pouvoir de prendre plusieurs types d'arrêtés. Après avoir consulté le ministre de la Sécurité publique, le ministre de l'Industrie peut, par arrêté, interdire aux FST de fournir des services – ou leur ordonner de suspendre la fourniture de services, pendant la période précisée dans l'arrêté – à toute personne, notamment un autre FST.

En vertu du nouveau paragraphe 15.2(2), le ministre de l'Industrie peut ordonner aux FST « de faire ou de s'abstenir de faire toute chose » qui est nécessaire, à son avis, pour sécuriser le système canadien de télécommunication. Ce nouveau paragraphe contient une liste non exhaustive d'exemples illustrant comment le ministre peut utiliser ce pouvoir. Entre autres, le ministre de l'Industrie peut, par arrêté :

- interdire aux FST d'utiliser dans leurs réseaux ou installations les produits ou les services qu'il précise;
- ordonner aux FST de retirer 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 qu'il précise;
- interdire aux FST de mettre à niveau les produits ou les services qu'il précise;
- exiger que les réseaux ou installations des FST, ainsi que les projets d'approvisionnement qui s'y rapportent, fassent l'objet des processus d'examen qu'il précise;
- 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.

Le projet de loi précise également que personne n'a droit à une indemnisation du gouvernement fédéral pour les pertes financières découlant de ces arrêtés.

Le nouvel article 15.4 permet au ministre de l'Industrie d'ordonner à toute personne de fournir les renseignements nécessaires à l'application des dispositions de cette loi.

Bien que le projet de loi oblige le gouverneur en conseil ou le ministre de l'Industrie à publier ces décrets et arrêtés dans la *Gazette du Canada*, il leur permet également d'y inclure des dispositions qui interdisent la communication de leur existence ou d'une partie ou de la totalité de leur contenu. Le nouveau paragraphe 15.5(1) précise que ce pouvoir peut être utilisé pour interdire la communication de secrets industriels ou de données sensibles sur le plan économique.

La *Loi* contient actuellement des dispositions permettant l'échange de renseignements entre le CRTC et Innovation, Sciences et Développement économique Canada. Le nouvel article 15.6 élargit ces dispositions pour inclure d'autres ministres ou entités qui peuvent participer à la prise d'un décret ou aux activités d'enquête et d'application de la loi liées à un décret [11].

Le nouveau paragraphe 15.7(1) permet au ministre de l'Industrie de conclure un accord concernant la communication de renseignements non confidentiels (c.-à-d. ceux qui ne sont pas des secrets industriels ou des données sensibles sur le plan économique) recueillis en vertu de la *Loi* à l'administration d'une province ou d'un État étranger ou à une organisation internationale. Le ministre doit croire que ces renseignements pourraient être utiles pour sécuriser le système canadien de télécommunications ou un système de télécommunications étranger.

En vertu du nouveau paragraphe 15.8(1), le gouverneur en conseil peut prendre des règlements pour tout ce qui pourrait être visé par un arrêté ministériel.

Le nouvel article 15.9 comprend des dispositions en matière de contrôle judiciaire. Si un décret du gouverneur en conseil ou un arrêté du ministre de l'Industrie est contesté devant les tribunaux, le juge doit entendre à huis clos (en l'absence du public, du demandeur et de son avocat) les éléments de preuve ou autres renseignements du gouvernement fédéral qui pourraient porter atteinte aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui.

Le juge doit fournir au demandeur un résumé des éléments de preuve et autres renseignements dont il dispose et qui permet au demandeur d'être suffisamment informé de la thèse du gouvernement du Canada. Le résumé ne doit pas comporter d'élément dont la divulgation porterait atteinte, selon le juge, aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui.

2.1.3 Inspection et contrôle d'application (art. 3 à 5)

En vertu de l'article 3 du projet de loi, le CRTC doit tenir compte des décrets du gouverneur en conseil ou des arrêtés du ministre de l'Industrie dans l'exercice de ses pouvoirs et fonctions de réglementation en vertu de la *Loi*.

L'article 4 du projet de loi intègre les nouveaux pouvoirs de prise de décrets et d'arrêtés prévus à l'article 2 dans le régime actuel d'inspection et d'application de la *Loi*, ce qui permet au ministre de l'Industrie de désigner des inspecteurs pour vérifier la conformité ou empêcher le non-respect des décrets et arrêtés pris en vertu des nouveaux pouvoirs en la matière prévus dans le projet de loi.

En vertu du paragraphe 72(1) de la *Loi*, quiconque a subi une perte ou un dommage par suite d'un manquement aux dispositions de la *Loi* (ou à une décision ou un règlement pris au titre de la *Loi*) peut poursuivre le contrevenant afin de recouvrer un montant égal à la perte ou au dommage. Le paragraphe 72(3) de la *Loi* prévoit des exceptions à ce régime de responsabilité civile. L'article 5 du projet de loi modifie le paragraphe 72(3) de la *Loi* afin que les nouveaux pouvoirs de prendre des décrets et arrêtés prévus dans le projet de loi fassent partie de cette exception.

2.1.4 Sanctions administratives pécuniaires (art. 6 et 7)

Selon la version actuelle des articles 72.001 et 72.01 de la *Loi,* toute personne qui enfreint l'une de ses dispositions ou l'un de ses règlements afférents, que ce soit en matière de télécommunications non sollicitées ou de non-respect d'une décision prise par le CRTC, par exemple, s'expose à des sanctions administratives pécuniaires. L'article 6 du projet de loi modifie l'article 72.001 pour préciser que les nouveaux pouvoirs de prise de décrets et d'arrêtés qui y sont prévus ne sont pas assujettis au régime général existant de sanctions administratives pécuniaires de la *Loi*. L'article 7 du projet de loi introduit un régime de sanctions administratives pécuniaires après

l'article 72.13, soit les nouveaux articles 72.131 à 72.1393, sanctions qui s'appliquent en cas de violation des nouveaux pouvoirs de prise de décrets ou d'arrêtés.

L'article 7 du projet de loi prévoit l'imposition de sanctions administratives pécuniaires à quiconque contreviendrait à une disposition, un décret, un arrêté ou un règlement (nouveaux art. 72.131 et 72.132). Il prévoit des pénalités pouvant aller jusqu'à 25 000 $ par jour pour toute personne commettant une première violation et de 50 000 $ par jour en cas de récidive. Dans d'autres cas, ces sanctions pécuniaires peuvent s'élever jusqu'à 10 millions de dollars par jour pour une première violation et jusqu'à 15 millions de dollars par jour en cas de récidive. L'article 7 dresse 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 la capacité de payer de ce dernier (nouveau par. 72.133(1)). D'après le nouveau paragraphe 72.133(2), bien que le projet de loi établisse un régime de sanctions administratives pécuniaires, la pénalité vise non pas à punir, mais à favoriser le respect des décrets, arrêtés et règlements.

2.1.4.1 Désignation des agents autorisés à dresser des procès-verbaux, contenu des procès-verbaux et présentation d'observation

L'article 7 du projet de loi prévoit une procédure en cas de violation du nouvel article 72.131. Ainsi, le ministre peut désigner les agents autorisés à dresser les procès-verbaux pour une violation (nouvel art. 72.134) et à faire signifier les procès-verbaux aux auteurs présumés d'une violation s'ils ont des motifs raisonnables de croire que ladite violation a été commise (nouveau par. 72.135(1)).

Tout procès-verbal doit mentionner le nom de l'intéressé et les faits reprochés, le montant de la pénalité à payer ainsi que les modalités de paiement. Il doit aussi mentionner la possibilité pour l'auteur présumé de la violation de payer la pénalité ou de présenter ses observations au ministre dans la période précisée (nouveau par. 72.135(2)).

Lorsque l'auteur présumé présente des observations au ministre, celui-ci doit décider, selon la prépondérance des probabilités, si l'auteur est responsable de la violation (nouveau par. 72.136(2)). Conformément au nouveau paragraphe 72.136(3), l'auteur présumé est réputé avoir commis les violations décrites dans le procès-verbal en cas d'omission de payer ou de présenter des observations à l'égard du procès-verbal de violation. Le ministre peut infliger les pénalités mentionnées dans le procès-verbal.

2.1.4.2 Procédure en violation, perpétration d'une violation par une personne morale et prescription

En vertu du nouvel article 72.137, toute transaction qu'une personne désignée propose de conclure avec l'auteur présumé de la violation est assujettie aux conditions qu'elle estime appropriées, y compris une réduction partielle ou totale

du montant de la pénalité indiquée dans le procès-verbal. L'article mentionne également qu'une conclusion de la transaction signifie un aveu de responsabilité à l'égard de la violation, et l'intéressé ne peut, dans ce cas, présenter d'observations. Si la personne désignée estime que la transaction est exécutée, elle fait signifier à l'intéressé un avis à cet effet, ce qui met fin à la procédure. Dans le cas d'une transaction inexécutée, l'intéressé reçoit un avis de défaut lui expliquant qu'il est tenu d'honorer ses obligations de payer ce qui est mentionné dans le procès-verbal, selon les délais et modalités prescrits dans l'avis.

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 (nouvel art. 72.138).

Toute procédure en violation se prescrit par trois ans à compter de la date où le ministre a eu connaissance des éléments constitutifs de la violation (nouveau par. 72.1391(1)).

2.1.5 Dispositions communes aux régimes de sanctions administratives pécuniaires (art. 11)

Pour encourager la conformité, le projet de loi s'appuie à la fois sur un régime de sanctions administratives pécuniaires et sur un régime pénal. Tout comme pour le régime de sanctions administratives pécuniaires, les dispositions pénales prévues par le projet de loi peuvent entraîner la responsabilité personnelle des dirigeants, administrateurs ou mandataires qui ont ordonné ou autorisé une violation, ou qui y ont consenti ou participé (art. 11 du projet de loi).

2.1.5.1 Admissibilité en preuve et moyens de défense (art. 9)

S'il s'agit d'une personne morale, quiconque contrevient à un décret, à un arrêté ou à un règlement commet une infraction passible, sur déclaration de culpabilité par procédure sommaire, d'une amende imposée à la discrétion du tribunal. S'il s'agit d'une personne physique, l'infraction est punie par une peine d'emprisonnement maximale de deux ans moins un jour ou par une amende que le tribunal estime indiquée, ou les deux (nouveau par. 73(3.1)).

L'article 9 du projet de loi modifie l'article 72.14 de manière à 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 la qualité officielle du signataire.

Dans la plupart des cas, l'auteur présumé de la violation peut invoquer en défense, selon le nouveau paragraphe 73(3.4) du projet de loi, qu'il ne peut être tenu responsable d'une violation s'il démontre qu'il a pris toutes les précautions voulues pour prévenir sa perpétration.

2.1.6 Modification corrélative à la *Loi sur la preuve au Canada* (art. 12)

L'article 12 modifie l'annexe de la *Loi sur la preuve au Canada* (LPC)[12] pour ajouter qu'un juge de la Cour fédérale est une « entité désignée » pour l'application de l'article 15.9 de la *Loi sur les télécommunications.* En vertu de la LPC, une entité désignée mentionnée à l'annexe qui rend une décision ou une ordonnance qui entraînerait la divulgation de renseignements sensibles ou de renseignements potentiellement préjudiciables ne peut les divulguer ou les faire divulguer avant que le procureur général du Canada ait été avisé de ce fait et qu'il se soit écoulé un délai de dix jours postérieur à l'avis.

2.2 PARTIE 2 : LOI SUR LA PROTECTION DES CYBERSYSTÈMES ESSENTIELS (ART. 13)

L'article 13 du projet de loi édicte la Loi sur la protection des cybersystèmes essentiels (LPCE), dont les principales dispositions sont détaillées ci-dessous.

Les articles 6 et 7 de la LPCE habilitent, respectivement, le gouverneur en conseil à ordonner l'ajout de services critiques et de systèmes critiques sous réglementation fédérale à l'annexe 1 de la LPCE et à ajouter les exploitants désignés et les organismes réglementaires de ces services et systèmes critiques à l'annexe 2 de cette même loi.

L'annexe 1 désigne 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.

Le fait d'être considéré comme un « exploitant désigné » d'un service ou d'un système critique en vertu de l'annexe 2 crée toute une série d'obligations, la plus importante étant l'établissement d'un programme de cybersécurité dans les 90 jours suivant la date à laquelle l'exploitant désigné devient membre d'une catégorie d'exploitants visée à l'annexe 2.

2.2.1 Exploitants désignés tenus d'établir et de maintenir un programme de cybersécurité

Le paragraphe 9(1) de la LPCE énonce les résultats attendus de ce programme de cybersécurité; ils comprennent :

- l'identification et la gestion des risques liés à la cybersécurité pour l'organisation, notamment les risques associés à la chaîne d'approvisionnement et à l'utilisation de produits et services de tiers;
- la protection des cybersystèmes essentiels contre toute compromission;
- la détection des incidents de cybersécurité qui touchent ou qui pourraient toucher les cybersystèmes essentiels;
- la réduction au minimum des conséquences des incidents de cybersécurité qui touchent les cybersystèmes essentiels.

L'article 2 de la LPCE définit un « cybersystème essentiel » 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 ». Le même article définit un « incident de cybersécurité » comme un « incident, notamment [un] acte, [une] omission ou [une] situation, qui nuit ou peut nuire » à la continuité, à la sécurité, 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. Cette interprétation est renforcée par l'article 12 de la LPCE, qui ordonne aux exploitants désignés d'assurer la mise à jour de leur programme de cybersécurité au fil du temps.

L'article 10 de la LPCE exige que les exploitants désignés avisent immédiatement « l'organisme réglementaire compétent [13] » qu'ils ont établi un programme de cybersécurité et le mettent à la disposition de l'organisme réglementaire dans les 90 jours suivant la désignation au titre de l'annexe 2. En vertu de cette même annexe, 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.

Toutefois, l'article 11 permet à l'organisme réglementaire de prolonger le délai de 90 jours une ou plusieurs fois pour permettre à un exploitant désigné de se conformer à l'exigence d'établir un programme de cybersécurité ou à celle de le mettre à la disposition de l'organisme réglementaire de la manière prescrite, ou aux deux.

L'article 12 de la LPCE exige que les exploitants désignés non seulement mettent en œuvre leurs programmes de cybersécurité, mais aussi qu'ils 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. Alors que l'alinéa 9(1)e) exige que les exploitants désignés respectent les règlements, l'article 13 prévoit que les exploitants désignés doivent entreprendre un examen de leur programme de cybersécurité au moins une fois par année et le terminer dans un délai de 60 jours, à moins qu'un autre délai ne soit prévu par règlement.

L'exploitant désigné doit donner suite aux conclusions de l'examen et modifier son programme de cybersécurité au besoin. Sauf indication contraire de la part de l'organisme réglementaire, les exploitants désignés sont tenus, en vertu du paragraphe 13(3), d'informer l'organisme réglementaire des changements apportés à leur programme à la suite de l'examen du programme, et ce, dans les 30 jours suivant la fin de cet examen.

Les organismes réglementaires doivent être tenus au courant des autres changements qui pourraient avoir une incidence sur la situation d'un exploitant désigné en matière de cybersécurité. L'article 14 de la LPCE ordonne aux exploitants désignés d'informer leur organisme réglementaire dans les 90 jours de tout changement important touchant :

- la propriété ou le contrôle d'un service ou système critique;
- leur chaîne d'approvisionnement ou leur utilisation de produits et services de tiers;
- toutes les circonstances prévues par règlement.

Encore une fois, l'organisme réglementaire a le pouvoir discrétionnaire de prolonger une ou plusieurs fois ce délai de 90 jours.

L'article 15 de la LPCE exige que les risques liés à la chaîne d'approvisionnement et à la cybersécurité des tiers soient traités de toute urgence. « Dès 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. L'organisme réglementaire est autorisé, en vertu de l'article 16, à communiquer au Centre de la sécurité des télécommunications (CST) tout renseignement, y compris des renseignements confidentiels [14], 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 ».

2.2.2 Signalement obligatoire des incidents de cybersécurité

La LPCE impose aux exploitants désignés des exigences obligatoires – peut-être même automatisées [15] – en matière de signalement des incidents de cybersécurité. L'article 17 oblige les exploitants désignés à signaler « sans délai » au CST tout incident de cybersécurité mettant en cause leurs cybersystèmes essentiels afin que le CST puisse « exercer ses attributions ». En vertu de l'alinéa 18b) de la *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) [16], 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 ».

Aux termes des articles 17 et 18, les exploitants désignés sont tenus de signaler un incident de cybersécurité au CST avant d'en aviser leur organisme réglementaire. L'alinéa 18b) de la LPCE prévoit en outre que les exploitants désignés fournissent des rapports sur les incidents de cybersécurité seulement « à la demande » de leur organisme réglementaire. Encore une fois, le délai et la priorité prévus pour la transmission de renseignements sur les incidents au CST suggèrent fortement que l'objectif consiste à donner au CST une idée plus claire de la situation à l'échelle nationale qui lui permettrait de défendre des systèmes et des services critiques si on le lui demandait.

Même si les organismes réglementaires ont accès aux rapports sur les incidents de cybersécurité en vertu de l'alinéa 18b), l'article 19 oblige le CST à fournir, sur demande, une copie ou une partie du rapport d'incident à l'organisme réglementaire approprié aux fins de la vérification du respect ou de la prévention du non-respect de tout règlement.

L'inclusion dans la LPCE d'un moyen supplémentaire permettant aux organismes réglementaires d'obtenir des renseignements sur les incidents de cybersécurité laisse entendre qu'il est plus probable que le CST apprenne qu'un incident de cybersécurité est survenu dans le cadre de ses propres activités autorisées et de ses partenariats internationaux d'échange de renseignements, plutôt que par des signalements venant d'un ou de plusieurs exploitants désignés. Certains de ces rapports provenant du CST pourraient également contenir des renseignements étrangers ou des renseignements opérationnels spéciaux (c.-à-d. au sujet des sources et des méthodes) qui ne peuvent pas être communiqués à d'autres parties.

2.2.3 Directives de cybersécurité

Les articles 20 à 23 de la LPCE autorisent le gouverneur en conseil à transmettre des décrets secrets appelés « directives de cybersécurité » aux exploitants désignés. Ce caractère secret est permis par le paragraphe 22(1), qui exempte les directives de cybersécurité des articles 3, 5 et 11 de la *Loi sur les textes réglementaires*

(LTR)[17]. L'article 3 de la LTR exige que les projets de règlement soient examinés en consultation avec le sous-ministre de la Justice pour vérifier, entre autres, leur conformité à la *Charte canadienne des droits et libertés*[18]. 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 de cette loi exige que tous les règlements soient publiés dans la *Gazette du Canada* dans les 23 jours suivant leur enregistrement.

En vertu des articles 24 et 25 de la LPCE, il est interdit aux exploitants désignés qui sont assujettis à des directives 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 aux directives.

2.2.4 Contrôle de la Cour fédérale

L'article 145 de la LPCE prévoit le contrôle des directives de cybersécurité par la Cour fédérale. Toutefois, le ministre de la Sécurité publique peut demander que de telles procédures soient tenues à huis clos et que le demandeur et son avocat reçoivent un résumé de la preuve plutôt qu'une divulgation complète de la thèse du gouvernement. Si le juge accepte l'argument du gouvernement selon lequel la divulgation de renseignements ou d'éléments de preuve dans le cadre du contrôle pourrait porter atteinte aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité d'autrui, la LPCE exige que le juge protège la confidentialité de ces renseignements ou de ces éléments de preuve. Il convient également de noter que l'alinéa 145(1)e) précise que la décision du juge peut être fondée sur des éléments de preuve qui n'ont pas été fournis au demandeur.

2.2.5 Interdictions et autorisations relatives à la communication de renseignements

Les articles 26 à 29 traitent de la communication et de l'utilisation des renseignements recueillis en vertu de la LPCE. Bien que la LPCE interdise de sciemment communiquer des renseignements confidentiels ou d'en permettre la communication, elle crée également une liste d'exceptions, y compris celle 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*[19], 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 ».

L'alinéa 26(1)b) de la LPCE 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 donne la définition la plus large de l'expression « information accessible au public » en droit canadien, 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 disponible au public sur demande, par abonnement ou achat[20] ».

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 arrangements sur l'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 arrangements doit avoir trait à la protection des cybersystèmes essentiels et, sauf l'exception prévue pour les gouvernements provinciaux en vertu du paragraphe 27(2), ne peut inclure des renseignements confidentiels.

2.2.6 Documents à tenir, généralement hors site

L'article 30 de la LPCE exige que les exploitants désignés tiennent des documents sur 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 toute question précisée par règlement.

Bien que la LPCE ne donne pas d'instructions explicites à ce sujet, des mesures sont probablement nécessaires pour protéger ces documents contre leur communication non autorisée. Le paragraphe 30(2) appuie cette interprétation, puisqu'il exige que les exploitants désignés conservent leurs documents au Canada, dans tout lieu et de la manière désignés par règlement. En l'absence de règlements, les documents doivent être conservés dans l'établissement de l'exploitant désigné.

2.2.7 Pouvoirs des organismes réglementaires

Les articles 32 à 85 de la LPCE énoncent les pouvoirs de chacun des six organismes réglementaires chargés de surveiller le fonctionnement des services et des systèmes critiques. Aux fins de la vérification de la conformité ou de la prévention du non-respect de la LPCE et de ses règlements, chacun de ces six organismes réglementaires est autorisé à entrer dans tout lieu – autre qu'une maison d'habitation – sans consentement ni mandat (art. 32, 41, 50, 59, 68 et 78). Les paragraphes 33(2), 42(2), 51(2), 60(2), 69(2) et 79(2) exigent 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*.

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. Il 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.

2.2.8 Vérifications internes obligatoires par les organismes réglementaires

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 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 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 décrire 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, il peut, selon les articles 36, 45, 54, 63, 73 et 82, 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 sont pas rendus publics.

Les articles 37, 46, 55, 64, 74 et 83 de la LPCE exigent explicitement qu'un exploitant désigné visé par un tel ordre s'y conforme et avise immédiatement l'organisme réglementaire compétent une fois qu'il l'a fait.

2.2.9 Demande de révision d'un ordre de conformité

En vertu de la LPCE, un exploitant désigné assujetti à un ordre de conformité peut présenter une demande écrite à l'organisme réglementaire pour qu'il révise l'ordre (art. 38, 47, 56, 65 et 84, et par. 75(2) à 75(4)). La demande de révision doit être présentée dans les délais et selon les modalités établis dans l'ordre de conformité, énoncer les motifs de la révision et fournir des preuves à l'appui de celle-ci. 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 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 dans les 90 jours après avoir reçu une demande de révision 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.

L'article 146 de la LPCE ordonne au ministre de la Sécurité publique de préparer un rapport au sujet de l'application de la LPCE dans les trois mois suivant la fin de chaque exercice et de déposer ce rapport au Sénat et à la Chambre des communes dans les 15 jours de séance suivant l'achèvement du rapport.

2.2.10 Modification corrélative à la *Loi sur la preuve au Canada* (art. 14)

Tout comme l'article 12, l'article 14 modifie l'annexe de la *Loi sur la preuve au Canada* pour ajouter qu'un juge de la Cour fédérale est une « entité désignée » aux fins de l'application de l'article 145 de la LPCE.

2.2.11 Modification corrélative à la *Loi sur le Bureau du surintendant des institutions financières* (art. 15 et 16)

L'article 15 du projet de loi modifie le paragraphe 23(1) de la *Loi sur le Bureau du surintendant des institutions financières*[21] pour exiger que, avant le 31 décembre de chaque année, le surintendant détermine le montant total des dépenses engagées pendant l'exercice précédent dans le cadre de l'application de la LPCE.

L'article 16 du projet de loi ajoute la LPCE à l'annexe de la *Loi sur le Bureau du surintendant des institutions financières.* Le surintendant doit étudier toutes les questions liées à l'application des lois mentionnées à l'annexe et en faire rapport au ministre des Finances.

2.2.12 Modification corrélative à la *Loi sur la sûreté et la réglementation nucléaires* (art. 17)

L'article 17 modifie la *Loi sur la sûreté et la réglementation nucléaires*[22] pour permettre à la Commission canadienne de sûreté nucléaire d'imposer les droits réglementaires pour les services, renseignements ou produits qu'elle fournit sous le régime de toute autre loi fédérale, ainsi que de rembourser ces droits dans certaines circonstances. Cet article autorise la Commission à dépenser les revenus provenant des droits exigés au cours de l'exercice pendant lequel les revenus sont perçus ou au cours du suivant.

2.2.13 Modification corrélative à la *Loi sur le Tribunal d'appel des transports du Canada* (art. 18)

L'article 18 modifie la *Loi sur le Tribunal d'appel des transports du Canada*[23] afin d'accorder à ce tribunal la compétence pour entendre des requêtes en révision et des appels portant sur les sanctions administratives pécuniaires prévues aux articles 127 à 133 de la LPCE.

2.2.14 Entrée en vigueur (art. 19)

En vertu de l'article 19, cette partie du projet de loi entre en vigueur à la date ou aux dates fixées par décret.

NOTES

1. 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. Il convient de noter que ce résumé législatif fait référence au « ministre de la Sécurité publique » plutôt qu'au « ministre de la Sécurité publique et de la Protection civile » afin de tenir compte de la pratique actuelle plutôt que du libellé de la loi de 2005 qui a créé ce ministère – la *Loi sur le ministère de la Sécurité publique et de la Protection civile* – qui demeure inchangée. Voir *Loi sur le ministère de la Sécurité publique et de la Protection civile*, L.C. 2005, ch. 10.
2. *Loi sur les télécommunications*, L.C. 1993, ch. 38.
3. 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*.
4. 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 hon. Oliver Dowden, *Huawei to be removed from UK 5G networks by 2027*, communiqué, 14 juillet 2020.
5. Australie, *Security of Critical Infrastructure Act 2018*, loi nº 29.
6. Australie, *Security Legislation Amendment (Critical Infrastructure) Act 2021*, loi nº 124.
7. États-Unis, *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law 117-103, 117th Congress, 136 Stat. 49, Division Y dans *Consolidated Appropriations Act, 2022*, H.R.2471, art. 101.
8. Royaume-Uni, *The Network and Information Systems Regulations 2018*, 2018 nº 506.
9. 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*, *Journal officiel* nº L194.
10. Sécurité publique Canada, *Aperçu des modifications proposées à la* Loi sur les télécommunications, document d'information.
11. *Ibid*.
12. *Loi sur la preuve au Canada*, L.R.C. 1985, ch. C-5.
13. 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.

14. L'art. 2 de la Loi sur la protection des cybersystèmes essentiels définit les renseignements confidentiels comme des renseignements :

> a) qui portent sur la vulnérabilité des cybersystèmes essentiels de l'exploitant désigné ou sur les méthodes employées pour leur protection et qui sont traités comme étant confidentiels de façon constante par l'exploitant désigné;
>
> b) dont la divulgation risquerait vraisemblablement de causer des pertes ou profits financiers appréciables à un exploitant désigné ou de nuire à sa compétitivité;
>
> c) dont la divulgation risquerait vraisemblablement d'entraver des négociations, notamment contractuelles, menées par un exploitant désigné.

15. Les outils automatisés de gestion de l'information et des événements de sécurité (GIES) existent depuis des décennies. Néanmoins, il est possible que certains exploitants désignés ne les utilisent pas ou que les outils de GIES qu'ils utilisent ne soient pas en mesure de fournir en temps opportun des renseignements précis sur les incidents au Centre de la sécurité des télécommunications (CST). Il convient donc de noter que la *Security of Critical Infrastructure Act 2018* de l'Australie habilite son secrétaire du ministère des Affaires intérieures à exiger qu'un exploitant d'infrastructure critique installe et tienne à jour un logiciel d'information sur les systèmes qui recueille et enregistre l'information sur les systèmes devant être transmise à l'Australian Signals Directorate (ASD, ou équivalent australien du CST). Voir Australie, *Security of Critical Infrastructure Act 2018*, loi nº 29.

Des intervenants ont indiqué que cette disposition était celle qui soulevait le plus de préoccupations lorsqu'elle a été proposée pour la première fois en 2020. Voir Parlement de l'Australie, Leah Ferris et Bernie Lai, *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*, Bills Digest nº 55, 2021-2022, Bibliothèque du Parlement, 28 mars 2022, p. 3.

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

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

18. *Charte canadienne des droits et libertés*, partie 1 de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.).

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

20. 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.

21. *Loi sur le Bureau du surintendant des institutions financières*, L.R.C. 1985, ch. 18 (3e suppl.), partie I.

22. *Loi sur la sûreté et la réglementation nucléaires*, L.C. 1997, ch. 9.

23. *Loi sur le Tribunal d'appel des transports du Canada*, L.C. 2001, ch. 29.