PROJET DE LOI C-26 : UN NOUVEAU CHAPITRE DANS LA RÉGLEMENTATION CANADIENNE EN MATIÈRE DE CYBERSÉCURITÉ

Publié le 6 janvier, 2025

Catégories: Perspectives, Publications

[Note de la rédaction : avant l'adoption du projet de loi C-26, une erreur de rédaction a été identifiée et le projet de loi a été renvoyé à la Chambre des communes pour résoudre l'erreur. L'avancement du projet de loi a ensuite été suspendu lorsque le Parlement a été prorogé le 6 janvier 2025. Le présent bulletin a été révisé pour tenir compte de cette évolution.]

Une nouvelle ère s'ouvre en matière de cybersécurité pour les organismes sous réglementation fédérale. Mais il faudra attendre encore un peu pour qu'elle arrive.

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* (« **Projet de loi C-26** »), était prêt à être adopté par le Parlement au début du mois de décembre[1].

Comme l'a écrit la CBC, une erreur technique de rédaction a été décelée alors que le projet de loi était au Sénat, ce qui a entraîné son renvoi à la Chambre des communes pour un nouveau vote. L'erreur était de nature technique; la Chambre des communes et le Sénat ont tous deux approuvé le contenu réel du projet de loi. Par conséquent, il est encore possible que le Projet de loi C-26 soit adopté sous une forme proche de sa forme actuelle à une date ultérieure. On ne sait pas encore si ce sera à la reprise des travaux du Parlement le 24 mars ou après les élections fédérales.

Comme nous l'avons écrit lorsque le Projet de loi a été présenté pour la première fois, les principaux éléments du Projet de loi sont (1) la modification de la *Loi sur les télécommunications* et (2) l'édiction de la *Loi sur la protection des cybersystèmes essentiels* (« **LPCE** ») qui créerait une série de nouvelles exigences en matière de cybersécurité pour certaines organisations réglementées par le gouvernement fédéral. Nous les résumerons successivement.

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

Qui sera touché?

Les modifications apportées par le Projet de loi C-26 à la *Loi sur les télécommunications* donneraient au gouvernement fédéral le pouvoir d'interdire aux fournisseurs de services de télécommunications (« **FST** ») canadiens de faire appel à certains fournisseurs considérés comme « à haut risque ». Ces modifications permettraient au gouvernement fédéral de donner suite à son intention déclarée d'interdire à Huawei et à ZTE de participer au déploiement du réseau 5G et d'obliger les fournisseurs de services de télécommunications à cesser d'utiliser le matériel 4G de ces entreprises d'ici la fin de 2027.

Ces modifications toucheraient principalement les FST et les autres entreprises de la chaîne d'approvisionnement des services de télécommunications.

Quels seraient les effets de ces modifications?

Parmi les changements apportés par le Projet de loi C-26 à la *Loi sur les télécommunications*, un nouvel objectif serait ajouté à la politique canadienne de télécommunication : promouvoir la sécurité du système canadien de télécommunication.

Pour atteindre cet objectif, les modifications conféreraient au gouverneur en conseil et au ministre de l'Industrie le pouvoir (a) d'interdire aux FST d'utiliser les produits et les services fournis par toute personne qu'il précise; ou (b) leur ordonner de retirer de tout ou partie de leurs réseaux ou installations de télécommunication tous les produits fournis par toute personne qu'il précise[2]. Les modifications conféreraient également au ministre de l'Industrie le pouvoir de prendre divers autres types de décrets, s'il a des motifs raisonnables de croire que ces mesures sont nécessaires pour assurer la sécurité du système canadien de télécommunications[3].

En termes d'application, le Projet de loi C-26 établirait un cadre de sanctions administratives pécuniaires pour la *Loi sur les télécommunications* et prévoirait pour les organisations des amendes pouvant atteindre 10 millions de dollars pour une première violation et 15 millions de dollars en cas de récidive[4]. Les modifications offriraient également des lignes directrices pour les contrôles judiciaires de ces sanctions.

Il est important de noter qu'en dépit du fait que le Projet de loi accorderait au gouvernement des pouvoirs importants lui permettant d'intervenir dans les activités des FST pour des raisons de sécurité nationale, le texte prévoit expressément l'impossibilité d'obtenir une indemnité pour les pertes financières subies par suite de la prise d'un arrêté ou d'un décret.

Nouveautés

Le Projet de loi C-26 a été critiqué lors de sa présentation initiale parce qu'il donnait au gouvernement un pouvoir discrétionnaire illimité pour imposer des obligations aux FST. Au cours du processus législatif, on a ajouté diverses conditions pour garantir que les nouveaux pouvoirs du gouvernement soient exercés de

manière proportionnée. À titre d'exemple :

- Le ministre de l'Industrie ou le gouverneur en conseil ne pourrait prendre un arrêté ou un décret que (i) s'il a des motifs raisonnables de croire qu'une telle mesure est nécessaire; (ii) après une consultation appropriée[5]; (iii) après avoir dûment pris en considération divers facteurs (notamment les répercussions financières et opérationnelles sur le FST et les services de télécommunications en général)[6]; (iv) si cette mesure est raisonnable compte tenu de la gravité de la menace en question[7].
- Le ministre ne serait pas autorisé à ordonner à un FST d'intercepter des communications privées[8].
- Bien que les arrêtés ou décrets puissent être pris en secret (c'est-à-dire avec une obligation de non-divulgation imposée au FST)[9], le ministre doit dans ce cas en informer le Comité des parlementaires sur la sécurité nationale et le renseignement[10].
- Le ministre doit présenter un rapport annuel détaillant, entre autres, les arrêtés pris au cours de l'année écoulée[11].

PARTIE 2 : ÉDICTION DE LA LPCE

Qui sera touché?

La LPCE créerait de nouvelles obligations pour les **exploitants désignés** de **services ou de systèmes critiques**. L'annexe 1 du Projet de loi énumère les services critiques et les systèmes critiques qui, pour l'instant, seraient assujettis au nouveau cadre :

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

Les exploitants désignés qui seraient assujettis à la LPCE n'ont pas encore été indiqués. Toute entreprise exerçant des activités dans les secteurs susmentionnés pourrait être désignée à l'avenir; les administrateurs doivent être conscients des obligations potentielles en matière de cybersécurité en vertu de la LPCE.

Quels seront les effets de la LPCE?

La LPCE créerait de nouvelles obligations pour les exploitants désignés :

- établir un programme de cybersécurité conformément à la réglementation, aviser l'organisme réglementaire compétente et lui fournir une copie du programme dans les 90 jours suivant la date à

laquelle il devient membre de la catégorie[12];
- prendre des mesures pour atténuer les risques associés à la chaîne d'approvisionnement identifiés par le programme de cybersécurité[13];
- déclarer, dans les délais réglementaires, lesquels ne doivent pas dépasser soixante-douze heures, tout incident de cybersécurité concernant l'un de ses cybersystèmes essentiels au Centre de la sécurité des télécommunications, puis en aviser l'organisme réglementaire compétent[14];
- se conformer aux décrets en matière de cybersécurité imposés par le gouverneur en conseil[15]; tenir certains documents conformément à la réglementation[16].

La LPCE autoriserait également le gouverneur en conseil à donner des directives enjoignant à un exploitant désigné de se conformer à toute mesure pour protéger un cybersystème essentiel[17].

La LPCE autoriserait également l'échange de renseignements entre diverses entités gouvernementales à des fins d'orientation en matière de cybersécurité[18] et interdirait la divulgation non autorisée de renseignements confidentiels sensibles concernant un cybersystème essentiel[19].

Quant à l'application de la LPCE, elle conférerait à certains organismes réglementaires (dont le Bureau du surintendant des institutions financières [BSIF], le ministre de l'Industrie, la Banque du Canada, la Commission canadienne de sûreté nucléaire, la Régie de l'énergie du Canada et le ministre des Transports) le pouvoir de faire enquête, de prendre des arrêtés et d'infliger des pénalités aux contrevenants (jusqu'à 1 million de dollars pour une personne physique ou 15 millions de dollars pour toute autre entité)[20].

Nouveautés

Au cours du processus législatif, on a ajouté diverses conditions pour garantir que les nouveaux pouvoirs du gouvernement en vertu de la LPCE soient exercés de manière proportionnée. Nombre d'entre elles sont similaires à celles ajoutées en vertu de la Partie 1 du Projet de loi. À titre d'exemple :

- Les décrets du gouverneur en conseil ne pourraient être pris que (i) sur la base de motifs raisonnables de croire qu'un tel décret est nécessaire[21]; (ii) en tenant dûment compte de divers facteurs (notamment les répercussions financières et opérationnelles sur les exploitants désignés, les répercussions sur la sécurité publique et sur la prestation de services et de systèmes critiques)[22]; (iii) avec avis au Comité parlementaire sur la sécurité nationale et le renseignement et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement[23].
- Le gouverneur en conseil ne serait pas autorisé à ordonner à un exploitant désigné d'intercepter une communication privée[24].
- De nouvelles protections pour les renseignements confidentiels des exploitants désignés[25].

Conclusion et points à retenir

Étant donné que les partis politiques canadiens soutiennent généralement le contenu réel du Projet de loi C-26, il est probable qu'il sera adopté sous une forme proche de sa forme actuelle. Cela pourrait se produire lors de la reprise des travaux du Parlement à la fin du mois de mars, ou lors de la prochaine session parlementaire. Pour l'instant, nous ne pouvons pas en être sûrs.

L'adoption du Projet de loi C-26 marquerait un changement important dans le paysage de la cybersécurité au Canada, en ajoutant de nouveaux pouvoirs et de nouvelles obligations autour de deux grands piliers. Tout d'abord, grâce aux modifications apportées à la *Loi sur les télécommunications*, le gouvernement obtient le pouvoir d'intervenir dans les infrastructures de télécommunications pour des raisons de sécurité nationale, notamment en pouvant interdire les fournisseurs à haut risque et d'exiger le retrait d'équipements, avec toutefois de nouvelles garanties pour assurer l'exercice proportionné de ces pouvoirs.

Ensuite, grâce à la LPCE, les exploitants désignés œuvrant dans des secteurs critiques comme les services bancaires, les télécommunications et les transports seront confrontés à de nouvelles exigences en matière de programmes de cybersécurité et d'obligations de signalement des incidents, assorties d'importantes sanctions en cas de non-respect de celles-ci.

Pour les entreprises exerçant des activités dans les secteurs concernés, les répercussions sont considérables et nécessitent une attention particulière. Les organisations doivent commencer à se préparer à la conformité en révisant leurs programmes de cybersécurité, leurs procédures de réponse aux incidents et leurs relations d'affaires relatives à la chaîne d'approvisionnement. Bien que le Projet de loi C-26 prévoie d'importants mécanismes de contrôle de l'autorité gouvernementale et de protection des renseignements confidentiels, la possibilité de sanctions financières importantes (jusqu'à 15 millions de dollars) et l'absence d'indemnisation pour les pertes résultant de décrets gouvernementaux mettent en évidence la nécessité d'une gestion proactive des risques. Dans l'attente de l'adoption et de la mise en œuvre officielle du Projet de loi, les organisations concernées seraient bien avisées de commencer à élaborer leur stratégie en matière de conformité et de réfléchir à la manière dont ces nouvelles exigences s'intégreront dans leurs cadres existants de gestion de la sécurité et des risques.

[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*, texte intégral disponible ici. [Projet de loi C-26]
[2] *Loi sur les télécommunications*, articles 15.1 (1) et 15.2 (1), tels que modifiés par le Projet de loi C-26.
[3] *Loi sur les télécommunications*, article 15.2 (2), tel que modifié par le Projet de loi C-26.
[4] *Loi sur les télécommunications*, article 72.131, tel que modifié par le Projet de loi C-26.
[5] *Loi sur les télécommunications*, articles 15.1 (1) et 15.2 (1) et (2), tels que modifiés par le Projet de loi C-26.

[6] *Loi sur les télécommunications*, articles 15.1 (2.1) et 15.2 (3.1), tels que modifiés par le Projet de loi C-26.
[7] *Loi sur les télécommunications*, articles 15.1 (1.1) et 15.2 (2.1), tels que modifiés par le Projet de loi C-26.
[8] *Loi sur les télécommunications*, article 15.2 (2.2), tel que modifié par le Projet de loi C-26.
[9] *Loi sur les télécommunications*, articles 15.1 (2) et 15.2 (3), tels que modifiés par le Projet de loi C-26.
[10] *Loi sur les télécommunications*, article 15.22, tel que modifié par le Projet de loi C-26.
[11] *Loi sur les télécommunications*, article 15.21, tel que modifié par le Projet de loi C-26.
[12] *Loi sur la protection des cybersystèmes essentiels*, article 9 (1), tel qu'édicté par le Projet de loi C-26. [LPCE]
[13] LPCE, article 15.
[14] LPCE, articles 17 à 19.
[15] LPCE, article 20.
[16] LPCE, article 30.
[17] LPCE, article 20.
[18] LPCE, article 23.
[19] LPCE, article 26.
[20] LPCE, article 32 à 85; 88 à 134.
[21] LPCE, article 20.
[22] LPCE, article 20 (2.1).
[23] LPCE, article 20 (4).
[24] LPCE, article 20 (5).
[25] LPCE, article 23 (2); 26 (3) et 28 (2).

par Robbie Grant

Mise en garde