**Projet de loi C-26 – Q et R**

## 1. Les mesures de protection des renseignements personnels et d'établissement de rapports énoncées dans le projet de loi C-26 s'appliquent-elles à l'article 15.4?

**Protection des renseignements personnels**

- **Les mesures de protection des renseignements personnels prévues par le projet de loi C-26 s'appliquent à l'article 15.4, qui régit la collecte de renseignements pour soutenir les décrets ou les arrêtés rendus en vertu des articles 15.1 et 15.2.**

- **Pour illustrer l'utilisation de l'article 15.4, le ministre pourrait demander des détails techniques sur l'architecture d'un réseau ou sur les mesures prises par un exploitant pour mettre en œuvre un décret ou un arrêté.**
    - D'accord, il s'agit d'une bonne hypothèse. Cependant, en dépit des engagements pris par les représentants du gouvernement au CST, selon lesquels le type de renseignements qui seraient recueillis concerne essentiellement des « renseignements techniques », un amendement visant à restreindre la collecte de données spécifiquement aux « renseignements techniques[1] » a été explicitement rejeté par le Parlement. Comme l'a déclaré un représentant du CST au Parlement : « Toute restriction réduirait[2] également la collaboration du CST avec ses partenaires du Groupe des cinq ». Il est donc probable que les renseignements soient communiqués au gouvernement des États-Unis, entre autres. Comme l'a fait remarquer la commissaire à la protection de la vie privée du Canada : « Ces vastes[3] pouvoirs pourraient conduire à un échange de renseignements étendu et persistant à l'insu des personnes ou sans leur consentement ».

- **L'article 15.4 ne vise pas à recueillir des renseignements personnels et ne permet pas la surveillance; l'accent est mis sur les réseaux et non sur les consommateurs.**
    - Il s'agit peut-être de l'intention, mais la portée du texte législatif est beaucoup plus large : « Le ministre peut exiger de toute personne qu'elle fournisse, selon les modalités qu'il précise, à la personne qu'il désigne ou à lui-même les renseignements à l'égard desquels il a des motifs raisonnables de croire qu'ils sont pertinents 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 ». Cela inclut clairement les renseignements personnels.

    - Ce pouvoir n'est encadré que par une norme subjective, de sorte que bon nombre de ces décrets ou arrêtés (en vertu des articles 15.1 et 15.2) ne requièrent que l'avis du ministre selon lequel ceux-ci sont « nécessaire[s] […] pour sécuriser le système canadien de télécommunications ».

- **Il est limité par les objectifs politiques de la loi, qui comprennent la protection du système de télécommunications, mais pas les objectifs de sécurité générale comme l'application de la loi. Il est également limité par les diverses autres mesures de protection des renseignements personnels prévues par le projet de loi, notamment les définitions de renseignements personnels et de renseignements dépersonnalisés, l'interdiction de communiquer des renseignements confidentiels au niveau international ou dans le cadre d'affaires pénales, ainsi que les protections prévues par la *Loi sur la protection des renseignements personnels* et la *Charte* contre les perquisitions et saisies abusives.**
    - La question de la définition de renseignements personnels et de renseignements « dépersonnalisés », qui peuvent être considérés comme des « renseignements confidentiels » par un fournisseur, est une diversion. La véritable préoccupation, c'est la possibilité réelle que les renseignements personnels recueillis par le biais du projet de loi C-26 pour soutenir la prise de décrets ou d'arrêtés relatifs à la sécurité du secteur des télécommunications puissent servir de vecteur à la collecte de renseignements soutenant la collecte de renseignement étranger. De plus, le projet de loi C-26 permet au gouvernement fédéral de divulguer ces renseignements à presque n'importe qui, y compris à des gouvernements étrangers, comme les États-Unis[4].Étant donné que le Canada s'est engagé à

---

[1] Chambre des communes. Comité permanent de la sécurité publique et nationale. *Témoignages*, 44-1, n° 101 (8 avril 2024), à 1540 (Stephen Bolton). En tout état de cause, la Cour suprême du Canada a récemment reconnu que même les renseignements techniques peuvent être des renseignements personnels. *Voir R. c. Bykovets,* 2024 CSC 6.
[2] Chambre des communes. Comité permanent de la sécurité publique et nationale. *Témoignages,* 44-1, n° 101 (8 avril 2024), à 1540 (Stephen Bolton).
[3] Commissariat à la protection de la vie privée du Canada « Fiches des enjeux au sujet du projet de loi C-26 », (14 juin 2024), en ligne <https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/divulgation-proactive/cpvp-parl-bp/secu_20240212/fe_20240212/>.
[4] *Projet de loi C-26*, partie I, art. 15.7.

partager les renseignements étrangers par l'intermédiaire du Groupe des Cinq, il est plausible que ces renseignements soient susceptibles de circuler au-delà des institutions canadiennes[5].

- **En outre, l'article 15.4 s'inspire d'une disposition de la *Loi sur les télécommunications* (article 37) qui permet de recueillir des renseignements auprès des entités réglementées et qui existe depuis plus de trente ans pour les questions générales de télécommunications. Elle a toujours été utilisée pour recueillir des renseignements commerciaux.**
    - Il y a certainement une analogie avec l'article 37, mais la différence ici consiste à savoir avec qui ces renseignements peuvent être communiqués (projet de loi C-26, partie I, article 15.6) et la capacité d'organismes comme le CST à réaffecter ces renseignements à ses autres mandats, comme le renseignement étranger. En dépit des engagements pris par les représentants du gouvernement au CST, selon lesquels le type de renseignements recueillis concerne essentiellement des « renseignements techniques », un amendement visant à restreindre la collecte de données spécifiquement aux « renseignements techniques » a été rejeté par le Parlement[6]. Les efforts visant à confiner l'utilisation de l'information ont également été spécifiquement rejetés.

**<u>Établissement de rapports</u>**

- **En vertu de l'article 15.21, le ministre est tenu de présenter un rapport annuel. Ce rapport doit contenir certains renseignements précis, notamment le nombre d'injonctions prononcées, leur nature, une description de la conformité et une explication de la nécessité, du caractère raisonnable et de l'utilité des décrets ou des arrêtés.**
    - Cette évolution est quelque peu encourageante, mais des inquiétudes subsistent. Que se passe-t-il s'ils ne fournissent pas l'information? Quel est la sanction ou le mode de recours si l'institution gouvernementale refuse de coopérer? Exactement comme cela s'est produit dans le passé avec le CST qui a refusé de donner des renseignements à l'OSSNR et au CPSNR? En outre, cette obligation d'établissement de rapport annuel ne concerne que les décrets ou les arrêtés au titre des articles 15.1 et 15.2. Comment le public sera-t-il informé de la manière dont les pouvoirs de collecte de renseignements sont utilisés en vertu de l'article 15.4?

- **L'article 15.4 ne peut être utilisé que pour prendre, modifier ou révoquer un décret, un arrêté ou un règlement, et pour en vérifier la conformité.**
    - C'est vrai. Il s'agit toutefois d'un pouvoir très large avec des normes peu contraignantes et subjectives. Le ministre doit seulement avoir des « motifs raisonnables » de penser que les renseignements qu'il cherche à recueillir sont « pertinents » pour prendre, modifier ou révoquer les décrets ou les arrêtés (ce qu'il peut faire « [s]'il a des motifs raisonnables de croire que cela est nécessaire »).

    - Ce n'est pas seulement moi qui parle ici. Comme l'a noté la commissaire à la protection de la vie privée du Canada, ces pouvoirs « accorderai[en]t également à certains organismes réglementaires des pouvoirs de perquisition sans mandat[7] » dans le contexte d'une norme très subjective où le ministre doit seulement estimer que l'activité de collecte de renseignements pourrait être « pertinente » lors « de la prise, de la modification ou de la révocation » de l'un des décrets ou des arrêtés visant à sécuriser le système de télécommunications[8], pour les décrets ou les arrêtés qu'il peut prendre dans les cas qu'il estime « nécessaires […] pour sécuriser le système canadien de télécommunications[9] ».

    - De plus, une fois ces renseignements recueillis, le projet de loi C-26 n'empêche pas le CST de les réaffecter à d'autres mandats, comme le renseignement étranger, une préoccupation signalée par la commissaire à la protection de la vie privée du Canada[10].

---

[5] Hogan, Stephanie, *CBC*, « What are the 'Five Eyes'? As Canada accuses India, what you need to know about the intelligence alliance » (21 sept. 2023), en ligne à l'adresse : <https://www.cbc.ca/news/canada/five-eyes-canada-india-1.6972210>.

[6] Chambre des communes, Comité permanent de la sécurité publique et nationale, *Témoignages*, 44-1, nº 101 (8 avril 2024), à 1540 (Stephen Bolton). En tout état de cause, la Cour suprême du Canada a récemment reconnu que même les renseignements techniques peuvent être des renseignements personnels. *Voir R. c. Bykovets*, 2024 CSC 6.

[7] Commissariat à la protection de la vie privée du Canada « Fiches des enjeux au sujet du projet de loi C-26 », (14 juin 2024), en ligne <https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/divulgation-proactive/cpvp-parl-bp/secu_20240212/fe_20240212/> (« Notamment, le projet de loi C-26 ne comporte pas de restrictions en ce qui a trait à la collecte de renseignements personnels. Il ne prévoit pas non plus de mesures de protection permettant de veiller à ce que les organismes réglementaires (ou leurs délégués) qui effectuent des perquisitions sans mandat le fassent de manière raisonnable »).

[8] *Projet de loi C-26*, partie 1, article 15-4.

[9] *Projet de loi C-26*, partie I, articles 15.1 et 15.2.

[10] Commissariat à la protection de la vie privée du Canada « Fiches des enjeux au sujet du projet de loi C-26 », (14 juin 2024), en ligne <https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/divulgation-proactive/cpvp-parl-bp/secu_20240212/fe_20240212/ (« Notamment, le projet de loi C-26 ne comporte pas de restrictions en ce qui a trait à la collecte de renseignements personnels. Il ne prévoit pas non plus de mesures de protection permettant de veiller à ce que les organismes réglementaires (ou leurs délégués) qui effectuent des perquisitions sans mandat le fassent de manière raisonnable »).

- **Alors que les articles 15.21 et 15.4 ne se font pas référence directement l'un à l'autre, ils sont liés par le fait qu'ils s'appliquent tous deux aux décrets et aux arrêtés rendus en vertu des articles 15.1 et 15.2.**
    - D'accord!

- **Le texte de l'article 15.21 a été proposé par le NPD qui s'est basé sur une proposition des groupes de défense des libertés civiles. Voir la discussion concernant le NDP-7 et le mémoire des parties prenantes connexe à la page 16.**
    - Il doit être maintenu. Je me demande simplement ce qui se passera quand ou si les institutions du gouvernement fédéral n'en tiendront pas compte. Consultez le plus récent rapport annuel de l'OSSNR et le nombre de fois où le CST a répondu que les renseignements demandés « restent classifiés et ne peuvent être publiés ».

**2. Le projet de loi C-26 permet-il au gouvernement d'accéder sans mandat à des renseignements privés, sans aucune limite quant à leur utilisation?**

- **Non. Le projet de loi C-26 n'est pas destiné à la collecte de renseignements privés, et des mesures de protection contre les abus sont prévues dans les deux parties du projet de loi ainsi que dans d'autres régimes de protection des renseignements personnels qui existent déjà dans le droit canadien.**
    - L'intention est trompeuse; nous devrions examiner ce que la loi permet. L'article 15.4 autorise clairement la collecte de renseignements privés et ne prévoit pas de garanties quant à leur réutilisation. Par conséquent, la réponse à cette question (« Le projet de loi C-26 permet-il au gouvernement d'accéder sans mandat à des renseignements privés, sans aucune limite quant à leur utilisation? ») est bien évidemment oui.

**Part 1: Modifications à la *Loi sur les télécommunications***

- **La portée de la première partie est limitée au système de télécommunications plutôt qu'à des questions plus générales d'application de la loi. Elle contient des dispositions explicites visant à protéger la confidentialité des renseignements, et le ministre n'est pas autorisé à ordonner à un fournisseur de services de télécommunications (FST) d'intercepter une communication privée.**
    - Le paragraphe 15.2(2) énonce clairement que le ministre peut ordonner à un FST d'utiliser « de[s] produits ou de[s] services, notamment ceux fournis par toute personne qu'il précise, notamment un fournisseur de services de télécommunication », de « [mettre] en œuvre des normes qu'il précise relativement à leurs réseaux ou installations de télécommunication ou à leurs services de télécommunication », ou de « faire toute chose qu'il précise, à l'exception d'une chose prévue ». Il s'agit de pouvoirs très, très vastes.
    - On peut également penser que l'article 15.4 constitue un moyen détourné d'intercepter des communications privées sous le prétexte d'un éventuel décret ou arrêté au titre de l'article 15.1 ou de l'article 15.2.

- **De nombreux garde-fous législatifs et judiciaires existent pour empêcher l'accès sans mandat à des renseignements privés, et ils s'appliquent au projet de loi C-26. L'article 8 de la *Charte canadienne des droits et libertés* protège contre les perquisitions et les saisies abusives, et le paragraphe 184(1) du *Code criminel* rend illégale l'interception de communications privées.**
    - En effet, je soupçonne que les dispositions de la partie I feront un jour l'objet d'une contestation fondée sur la *Charte*.
    - L'article 184 interdit l'interception illégale; cela n'a pas d'importance si l'interception est légale.

**Part 2: *Loi sur la protection des cybersystèmes essentiels***

- **La partie 2 du projet de loi C-26 autorise le gouvernement à obtenir des renseignements de deux manières. L'article 17 impose aux exploitants désignés de signaler au Centre de la sécurité des télécommunications (CST) les incidents de cybersécurité dépassant un certain seuil. Le paragraphe 23(1) autorise la collecte et l'échange de renseignements par certaines entités gouvernementales en vue de prendre, de modifier ou de révoquer des instructions en matière de cybersécurité, si le gouverneur en conseil estime, sur la base de motifs raisonnables, qu'il est nécessaire de le faire pour protéger un cybersystème essentiel.**
    - L'article 17 est nécessaire.
    - Le paragraphe 23(1) concerne la collecte et l'échange de renseignements entre les parties gouvernementales. Cela ne représente pas vraiment un problème.

- **Les renseignements requis pour protéger ces cybersystèmes essentiels seraient liés au fonctionnement technique du cybersystème. Il est donc peu probable qu'il contienne des renseignements personnels.**

- Même les renseignements techniques peuvent être des renseignements personnels, comme l'a souligné l'honorable Simon Noel à propos de l'arrêt *Bykovets* de la Cour suprême. Toutefois, je ne suis pas particulièrement préoccupé par les pouvoirs de collecte de renseignements prévus dans la partie II. Les questions les plus importantes sont celles de la transparence (articles 24 et 25).

• **Si des renseignements personnels devaient être recueillis de manière fortuite, ils seraient traités dans le respect de la protection des renseignements personnels prévue par toutes les lois applicables, y compris la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et la *Loi sur la protection des renseignements personnels*.**

- Oui, mais je soupçonne que les dispositions anti-transparence et les éléments d'instances sécurisées de contrôle d'une décision administrative feront l'objet d'une contestation à part entière.

**• De plus, à la demande de plusieurs organismes de la société civile appelés à témoigner lors de l'étude du projet de loi C-26 par la Chambre, un amendement a été ajouté au paragraphe 20(5) pour préciser que le gouverneur en conseil n'est pas autorisé à ordonner à un exploitant désigné d'intercepter une communication privée.**

- • Il s'agit d'un bon amendement.

**3. Le projet de loi C-26 crée-t-il des lacunes en matière de protection des renseignements personnels qui poseront des problèmes au Canada dans l'UE?**

• **Non. Le projet de loi C-26 contient des garanties en matière de protection de la vie privée et serait soumis aux lois canadiennes existantes sur la protection des renseignements personnels que l'UE a récemment examinées.**

- C'est incorrect. Les articles 15.1, 15.2 et 15.2 de la partie I et l'article 20 de la partie II créent de nombreux types de pouvoirs qui ont normalement préoccupé les Européens. Vous n'avez qu'à regarder les affaires *Schrems*. Au cœur de ces décisions se trouvaient des préoccupations concernant les activités de surveillance américaines. L'article 702 de la *Foreign Intelligence Surveillance Act*, qui autorise effectivement le ciblage sans mandat de « personnes dont on peut raisonnablement penser qu'elles se trouvent en dehors des États-Unis afin d'obtenir du renseignement étranger [TRADUCTION] », est particulièrement préoccupant[11]. De même, le décret exécutif 12333, signé à l'origine par le président Ronald Reagan, a été considéré comme une large autorisation pour les forces de l'ordre et les agences de renseignement de s'engager dans des pratiques de collecte de données et de surveillance à grande échelle (il exige la coopération avec les demandes de collecte de renseignements de la CIA[12]). Dans l'affaire *Schrems II*, ces instruments ont fait l'objet d'un examen particulièrement minutieux, la CJUE ayant conclu que l'article 702 et le décret exécutif 12333 ne prévoyaient aucune restriction des pouvoirs conférés aux autorités de surveillance, y compris des droits d'action devant les tribunaux pour les personnes concernées[13]. Lorsque nous considérons toutes les façons dont le CST obtient de nouveaux pouvoirs par le biais de ces projets de loi afin d'étendre sa mission à la collecte de renseignements électromagnétiques (SIGINT) sur des étrangers, y compris des Européens, nous devrions absolument anticiper leurs préoccupations concernant l'absence de consentement, l'absence de recours et l'absence d'indépendance des organes de contrôle. Il s'agit là de tous les aspects du droit à la vie privée garanti par la Charte européenne (voir les articles 7, 8 et 47 de la *Charte des droits fondamentaux de l'Union européenne*).

• **Dans une évaluation réalisée le 15 janvier 2024, la Commission européenne a réaffirmé sa décision selon laquelle le cadre canadien de protection de la vie privée dans le secteur privé, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), offre un niveau adéquat de protection des données. Par conséquent, les renseignements personnels peuvent continuer à circuler librement entre les organismes des États membres de l'UE et ceux du Canada, sans que les organismes canadiens soient tenus d'adhérer à des garanties supplémentaires en matière de protection des données.**

- D'accord, mais considérez que les dernières représentations d'ISDE auprès de l'UE ont mis l'accent sur le rôle du commissaire au renseignement, un bureau entièrement omis dans cette loi[14]. Et les représentations d'ISDE datent de 2020.

• **La Commission européenne a également examiné en profondeur la loi canadienne sur la protection de la vie privée dans le secteur public, la *Loi sur la protection des renseignements personnels*, ainsi que les cadres relatifs à l'application de la loi, à la sécurité nationale et au**

---

[11] 50 U.S. Code § 1881a - FISA Amendments Act of 2008 (« Procedures for targeting certain persons outside United States other than United States persons »). Cette disposition a été régulièrement renouvelée. *Voir REAUTHORIZATION ACT OF 2012*, du 2 août 2012, p. 112 (2012) et *FISA Amendments Reauthorization Act of 2017,* du 9 janvier 2018, art. 139 (2017). « FISA Section 702 Reauthorized for 2 years », *Lawfare* (30 avril 2024), en ligne sur : <https://www.lawfaremedia.org/article/fisa-section-702- reauthorized-for-two-years>.

[12] *Executive Order 12333* du 4 décembre 1981, figurant à 46 FR 59941, 3 CFR, 1981 Comp., p. 200, sauf indication contraire, et affaire 311/18 *Data Protection Commissioner v Schrems, Facebook Ireland Ltd*, [2020] CEDH au paragraphe 63 [*Schrems II*].

[13] *Schrems II*, paragraphes 180-182.

[14] Se reporter à https://ised-isde.canada.ca/site/plans-rapports/fr/sixieme-rapport-detape-evolutions-matiere-legislation-protection-donnees-canada.

**renseignement. Elle a constaté que les autorités publiques au Canada sont soumises à des règles claires, précises et accessibles régissant l'accès et l'utilisation des données à caractère personnel pour des objectifs d'intérêt public.**

- Il s'agit d'une analyse historique basée sur la dernière soumission d'ISDE à l'UE (en 2020), la décision étant rendue en janvier 2024. Ce *prochain* examen posera un problème si le projet de loi C-26 est adopté.

**4. Le projet de loi C-26 autorise-t-il les procédures à huis clos sans mesures de protection?**

- **Non. Bien que le projet de loi C-26 autorise les procédures à huis clos dans les affaires impliquant des renseignements sensibles, plusieurs mesures de protection sont prévues pour assurer le respect des procédures et l'équité. Par exemple, seul un juge, et non le gouvernement, peut décider de ne pas divulguer certains renseignements pour éviter de nuire aux relations internationales, à la défense nationale, à la sécurité nationale ou à la sécurité des personnes.**
    - Les instances sécurisées de contrôle d'une décision administrative remplacent le droit à la représentation par un « conseiller juridique spécial ». On ne voit même pas *comment* une personne concernée par un décret au titre de l'article 20 de la partie II pourrait en connaître l'existence, compte tenu des articles 24 et 25, et encore moins comment elle pourrait la contester de manière appropriée.

- **Il est important de noter que si le projet de loi C-26 reçoit la sanction royale, les articles concernés seront remplacés par le projet de loi C-70, qui définit les procédures générales pour les instances sécurisées de contrôle d'une décision administrative. Les protections prévues par le projet de loi C-70 vont encore plus loin que celles prévues par le projet de loi C-26, en permettant notamment la désignation d'un conseiller juridique spécial chargé de protéger les intérêts d'un demandeur. Des cadres similaires pour les procédures sécurisées existent dans des pays tels que les États-Unis, le Royaume-Uni et l'Australie.**

    - • Je suis curieux de voir comment et quand l'instance sécurisée de contrôle d'une décision administrative sera contestée. Ces mécanismes n'ont pas été testés.

**5. En vertu du projet de loi C-26, des personnes peuvent-elles être arrêtées si les entreprises pour lesquelles elles travaillent sont victimes d'un cyberincident?**

**Partie 1 : Modifications à la *Loi sur les télécommunications***

- **Les employés des entreprises de télécommunications ne peuvent pas être arrêtés en vertu du projet de loi C-26 simplement parce qu'un cyberincident s'est produit.**

- **En revanche, les personnes peuvent être inculpées si elles contreviennent à certains décrets, arrêtés ou règlements pris en vertu des articles 15.1 ou 15.2 ou de l'alinéa 15.8(1)a), ce qui signifie qu'elles ont refusé d'agir alors qu'on leur avait ordonné de le faire.**

- **Les personnes ne seront pas condamnées si elles démontrent qu'elles ont fait preuve de toute la diligence requise pour éviter que l'infraction ne se produise.**

- **Dans la plupart des cas, la Couronne se concentrera sur la direction si l'on pense que des fonctionnaires de haut niveau ont ordonné qu'un décret du gouvernement ne soit pas rendu.**

**Partie 2 : *Loi sur la protection des cybersystèmes essentiels***

- **Les employés des exploitants désignés ne peuvent pas être arrêtés en vertu du projet de loi C-26 simplement parce qu'un cyberincident s'est produit.**

- **La partie 2 du projet de loi C-26 vise à garantir que les exploitants désignés prennent des mesures pour prévenir les cyberincidents et se préparent à atténuer les effets des cyberincidents qui se produisent et à s'en remettre. Elle ne rend les exploitants désignés responsables que des actions qui sont sous leur contrôle.**

- **Les personnes en infraction avec la Loi pour des actions telles que la communication de renseignements confidentiels ou l'absence de mise en œuvre d'une directive sur la cybersécurité seront soumises à des sanctions.**

- **Comme pour la partie 1 de la Loi, les exploitants désignés et les particuliers peuvent invoquer une défense fondée sur la diligence raisonnable.**

## 6. Quelles sont les sanctions applicables en vertu de lois similaires dans d'autres pays du Groupe des cinq?

**États-Unis**

- **Les États-Unis ont entamé des consultations sur la Cybersecurity Incident Reporting for Critical Infrastructure Act. Les sanctions en cas de non-respect de la loi comprennent des amendes importantes et des peines d'emprisonnement pouvant aller jusqu'à cinq ans.**

- **La Commission fédérale des communications dispose d'une large autorité pour infliger des amendes aux entreprises de télécommunications qui ne mettent pas en œuvre des mesures de cybersécurité suffisantes. Parmi les exemples notables, citons l'amende de 350 millions de dollars américains (485 millions de dollars canadiens) infligée à T-Mobile en août 2021.**

**Royaume-Uni**

- **La Telecommunications (Security) Act 2021 du Royaume-Uni est largement similaire au projet de loi C-26.**

- **Elle oblige les fournisseurs de services de télécommunications à mettre en place des mesures pour détecter les cybermenaces et défendre leurs réseaux contre celles-ci. Des mesures doivent être prises rapidement après une atteinte à la sécurité afin de limiter les dégâts, d'y remédier et de les atténuer. Si un fournisseur ne respecte pas ses obligations en matière de sécurité, il peut se voir infliger une amende pouvant aller jusqu'à dix pour cent de son chiffre d'affaires. Dans le contexte canadien, cela représenterait une amende de 2,5 milliards de dollars canadiens pour Bell et de 1,9 milliard de dollars canadiens pour Rogers.**

**Australie**

- **En vertu de la Security of Critical Infrastructure Act de l'Australie, une entité responsable d'un système d'importance nationale est passible d'une amende maximale de 3,13 millions de dollars australiens si elle ne dispose pas d'un plan d'intervention en cas d'incidents liés à la cybersécurité.**

**Union européenne**

- **En vertu de la directive NIS-2 de l'Union européenne, qui entrera en vigueur en janvier 2025, les amendes pour défaut de mise en œuvre d'un plan de sécurité sont fixées à 2 % du chiffre d'affaires annuel mondial ou à 10 millions d'euros, le montant le plus élevé étant retenu. Dans le contexte canadien, cela permettrait d'infliger des amendes de 500 millions de dollars canadiens à Bell et de 386 millions de dollars canadiens à Rogers.**
    - Ce sont des modèles que nous devrions suivre. L'approche du plafonnement en fonction de la taille serait beaucoup plus efficace pour le respect de la loi.

- **Des mesures punitives peuvent également être prises à l'encontre des dirigeants, y compris le retrait forcé du poste au sein du conseil d'administration.**
    - Cela vaut la peine de retenir ce fait lorsque l'on pense à Solar Winds.

- **Le Règlement général sur la protection des données (RGPD) de l'UE a également été utilisé pour infliger des amendes à des organismes dont les pratiques en matière de cybersécurité étaient laxistes. Meta/Facebook s'est vu infliger une amende de 1,3 milliard de dollars américains en 2023, et Amazon une amende de 877 millions de dollars américains en 2021.**

## 7. Le Canada dispose-t-il d'autres lois qui prévoient des amendes similaires à celles prévues par le projet de loi C-26?

- **Les amendes prévues par le projet de loi C-26 sont comparables à celles prévues par d'autres lois nationales et internationales.**

- **Comme indiqué plus haut, des régimes comparables dans d'autres pays prévoient des sanctions de plusieurs centaines de millions de dollars.**

- **Au Canada, la *Loi sur la concurrence* prévoit des sanctions pouvant aller jusqu'à trois fois le chiffre d'affaires annuel global et 14 ans d'emprisonnement. La *Loi sur la protection de la vie privée des consommateurs* (LPVPC) qui serait créée par le projet de loi C-27 prévoit des amendes pouvant aller jusqu'à 25 millions de dollars ou 5 % du chiffre d'affaires mondial.**

- **Sans la possibilité d'infliger des sanctions maximales à des entreprises dont le chiffre d'affaires annuel s'élève à des dizaines de milliards de dollars, il existe un risque important que certaines entreprises ne prennent pas le respect des règles au sérieux.**

**8. Pourquoi la Chambre a-t-elle supprimé un amendement déposé en comité qui visait à limiter la durée de conservation des renseignements?**

- **Le Comité de la sécurité publique de la Chambre des communes a d'abord amendé la partie 2 du projet de loi C-26 de manière à ce que les renseignements échangés entre les entités gouvernementales en vertu de l'article 23 ne puissent être conservés « que pendant la durée nécessaire à la prise du décret visé à l'article 20, à sa modification ou à sa révocation, ou à la vérification du respect ou à la prévention du non-respect du décret ».**

- **Cet amendement a ensuite été supprimé par la Chambre à l'étape du rapport.**

- **Cette obligation de détruire les renseignements immédiatement après leur utilisation aurait pu créer un conflit avec l'article 6 de la *Loi sur la protection des renseignements personnels*, qui exige la conservation des renseignements personnels pendant une certaine période après leur utilisation « pour permettre à l'individu qu'ils concernent d'exercer son droit d'accès à ces renseignements ».**