CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

45e LÉGISLATURE, 1re SESSION

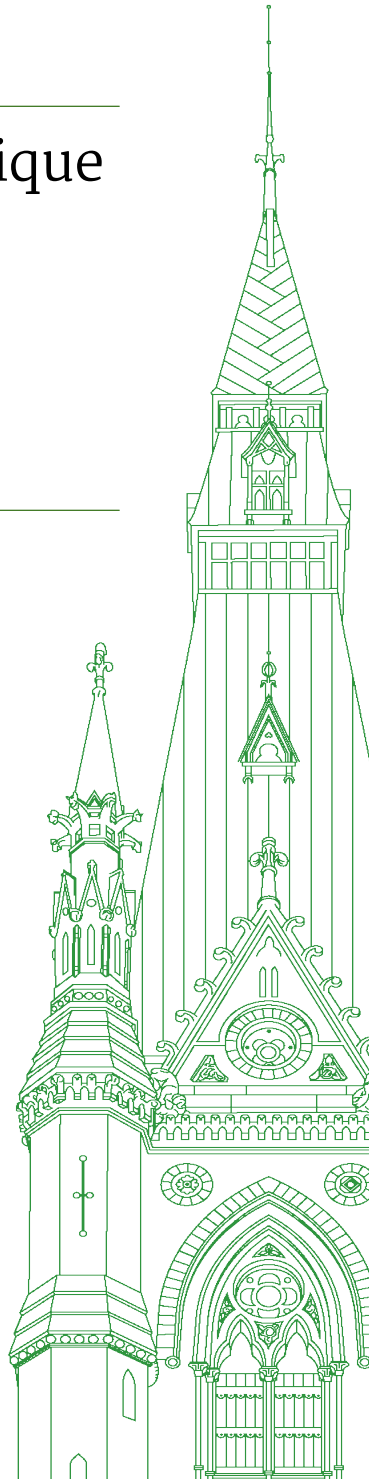
Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 009

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le mardi 28 octobre 2025



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le mardi 28 octobre 2025

● (1210)

[*Français*]

Le président (L'hon. Jean-Yves Duclos (Québec-Centre, Lib.)): Je souhaite à nouveau la bienvenue aux quatre mêmes hauts fonctionnaires, qui ont eu la gentillesse de rester des nôtres pour la deuxième heure. Nous accueillons aussi deux témoins de plus, à savoir Mme Bridget Walshe, dirigeante associée du Centre canadien pour la cybersécurité, et M. Daniel Couillard, directeur général des cyberpartenariats au Centre canadien pour la cybersécurité.

Madame Walshe, je comprends que vous êtes la seule à faire une présentation. Vous avez la parole pour cinq minutes.

Bridget Walshe (dirigeante associée, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci, monsieur le président.

[*Traduction*]

Bonjour, monsieur le président et mesdames et messieurs les membres du Comité. Je vous remercie de nous avoir invités aujourd'hui pour discuter 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.

Je m'appelle Bridget Walshe et je suis la dirigeante associée du Centre canadien pour la cybersécurité, que l'on appelle souvent le Centre pour la cybersécurité et qui fait partie du Centre de la sécurité des télécommunications Canada, ou CST. Je suis accompagnée de mon collègue Daniel Couillard, qui est le directeur général des Partenariats et de l'atténuation des risques.

[*Français*]

Le Centre canadien pour la cybersécurité est l'autorité technique du Canada en matière de cybersécurité. Nous dirigeons les interventions du gouvernement lors d'événements liés à la cybersécurité, et nous représentons une source unifiée de conseils spécialisés.

[*Traduction*]

Nous sommes heureux d'être ici aujourd'hui pour discuter du contexte des cybermenaces du Canada et de l'importance de la cybersécurité dans le cadre du projet de loi C-8.

J'aimerais commencer par une vérité toute simple: notre monde n'a jamais été aussi connecté. Pensons aux téléphones intelligents dans nos poches ou aux satellites qui orbitent au-dessus de nous. La technologie fait partie intégrante de nos vies. Elle alimente nos communications, nos économies, nos systèmes de santé, et même nos démocraties. Cette connectivité et cette dépendance sans précédent à la technologie nous exposent toutefois à ses vulnérabilités. Qu'il s'agisse des risques liés aux cybermenaces parrainées par des États, à l'exploitation des systèmes informatiques vieillissants ou à l'utilisation abusive de l'intelligence artificielle, cette interconnexion comporte un ensemble complexe de défis qui touchent tous les secteurs et toute la population canadienne.

[*Français*]

Aujourd'hui, les auteurs de menace peuvent contourner les méthodes traditionnelles d'espionnage et d'ingérence étrangère en déployant des activités malveillantes sophistiquées d'une portée inégalée, et ce, dans le confort de leur maison. En effet, à l'aide de plateformes de cybercriminalité comme service et de quelques commandes sur un clavier, n'importe qui possédant les capacités nécessaires peut mener rapidement des campagnes à grande échelle pour voler des données sensibles, perturber ou interrompre des services, ou influencer l'opinion publique.

[*Traduction*]

Comme nous le mentionnons dans notre Évaluation des cybermenaces nationales 2025-2026, nous nous préoccupons de plus en plus de la résilience durable de la cybercriminalité à l'échelle mondiale, puisque les adversaires perfectionnent leurs méthodes, adoptent de nouvelles technologies et collaborent entre eux dans le but d'élargir leur champ d'action. J'ai d'ailleurs apporté aujourd'hui un exemplaire du rapport d'évaluation des cybermenaces pour les membres du Comité.

Pour pouvoir faire face à l'environnement de menace en constante évolution, nous devons mettre en place des mesures bien réfléchies et axées sur l'avenir. Il est essentiel de renforcer les capacités de cyberdéfense du Canada, au même titre que de favoriser l'importante collaboration entre le gouvernement et l'industrie. En travaillant ensemble, nous pouvons viser à atténuer les menaces de façon proactive. Pour appuyer ces efforts, l'établissement d'un cadre exhaustif de signalement des incidents permettrait d'assurer la résilience et la réponse continues du Canada face aux cybermenaces de plus en plus sophistiquées.

[*Français*]

Le projet de loi C-8 s'appuie sur son prédécesseur, le projet de loi C-26, pour faire avancer l'approche pansociétale complète du Canada à l'égard de la cybersécurité.

[*Traduction*]

Même si le CST n'obtiendra pas de nouveaux pouvoirs, ce projet de loi fournira au gouvernement de nouveaux outils et pouvoirs pour améliorer les cyberdéfenses et protéger les infrastructures essentielles. Il établira un cadre réglementaire pour la cybersécurité de base des secteurs essentiels de l'industrie, ce qui facilitera l'échange d'information avec le Centre pour la cybersécurité et permettra aux organismes de réglementation de demander l'avis et les conseils du CST.

Le projet de loi C-8 souligne l'importance du signalement obligatoire des incidents en renforçant le rôle que joue le Centre pour la cybersécurité pour aider les organisations à résoudre les incidents et pour améliorer notre capacité collective à détecter les cybermenaces, à intervenir et à prévenir en mettant en commun l'information sur les cybermenaces.

● (1215)

[*Français*]

Le signalement des incidents nous aide à comprendre ce qui s'est produit, à communiquer les indicateurs de menace et à renforcer nos défenses. L'information que le Centre canadien pour la cybersécurité recevrait d'exploitants désignés, en vertu du projet de loi C-8, serait strictement de nature technique, puisqu'elle mettrait l'accent sur les indicateurs de compromission et les vulnérabilités exploitées.

[*Traduction*]

En terminant, permettez-moi de vous dire ceci. La cybersécurité est une responsabilité partagée. S'il y a une leçon que nous avons apprise en cybersécurité, c'est qu'aucune entité, qu'il s'agisse d'une agence, d'un gouvernement ou d'une entreprise, ne peut réussir seule.

[*Français*]

Le président: Merci beaucoup, madame Walshe.

Cela m'amène à passer la parole à M. Lloyd pour six minutes.

[*Traduction*]

Dane Lloyd (Parkland, PCC): Merci, monsieur le président.

Je remercie les témoins. Vous avez comparu pendant une heure devant nous juste avant ceci. C'était à huis clos. Nous avons posé de bonnes questions et nous avons obtenu des réponses. Par souci de transparence, je vais poser à nouveau des questions semblables et j'espère que nous pourrons obtenir les mêmes réponses.

J'ai remarqué qu'en vertu de la Loi sur le SCRS, pour prendre des mesures de réduction de la menace, vous devez obtenir un mandat de la Cour fédérale. En vertu de ce projet de loi, il n'est pas clair si le gouvernement aurait besoin d'un mandat pour prendre les mesures qu'il se donne le pouvoir de prendre. Pourquoi?

Andre Arbour (directeur général, Direction générale de la politique des télécommunications et d'Internet, ministère de l'Industrie): Les pouvoirs prévus dans le projet de loi C-8 visent à régir au quotidien la sécurité des infrastructures de base.

En télécommunications, il s'agit de l'infrastructure de réseau de Bell. Certains droits garantis par la Charte ou certaines considérations relatives à la vie privée ne s'appliquent pas dans ce contexte. De même, c'est toute la façon dont les fournisseurs de services de télécommunications sont réglementés actuellement. Par exemple, l'attribution des licences de spectre qui sont nécessaires pour exploiter leurs réseaux sans fil relève actuellement du ministre de l'Industrie, et il n'y a pas de surveillance judiciaire nécessaire.

Dane Lloyd: Nous avons parlé d'une personne en particulier pendant l'heure précédente, et vous m'avez dit qu'il s'agissait d'une entité juridique, et pas nécessairement d'une personne physique.

Il y a lieu de craindre que... Lorsqu'il est écrit dans la loi que le ministre a le pouvoir d'ordonner aux entreprises de télécommunications de cesser de fournir des services à une personne qu'il précise, il y a lieu de craindre qu'on parle ici de Canadiens, individuellement. Si vous croyez qu'un Canadien représente une menace pour le système de télécommunications, qu'il dégrade le système, le perturbe ou le manipule, pourquoi n'êtes-vous pas tenu d'obtenir un mandat dans ce cas?

Andre Arbour: Si je comprends bien la question, en ce qui concerne le pouvoir de retirer des services à une entité dans ce contexte, tout d'abord, ces pouvoirs sont motivés par la nécessité de protéger le système canadien de télécommunications. Dans ce contexte, les commentaires individuels des Canadiens ou leur trafic en ligne ne sont pas pertinents, dans les faits. Il faut plutôt penser à une attaque par déni de service distribué, par exemple, qui revient à inonder un réseau et, essentiellement, à empêcher son fonctionnement pour d'autres Canadiens.

Le recours à ce pouvoir doit être raisonnablement nécessaire pour atteindre l'objectif énoncé. Ce ne peut pas être une décision prise pour un rien. La gravité de la menace doit le justifier. Il s'agit de circonstances où le temps presse. On pense ici à des services dont la vie et la mort de Canadiens dépendent (de pouvoir appeler le 911 ou des choses de cette nature), alors il doit y avoir des considérations qui nécessitent de pouvoir agir rapidement.

Dane Lloyd: Pourquoi ce secret? Pourquoi y a-t-il des dispositions de confidentialité dans ce projet de loi?

● (1220)

Andre Arbour: De façon générale, les dispositions sur la confidentialité ne sont ni nécessaires ni applicables. Lorsqu'il s'agit de l'équipement utilisé par toutes les entreprises de télécommunications, dans 99,9 % des cas, nous procéderons à des consultations publiques encadrées par des règles, et nous voudrons que tout le monde connaisse les règles.

Il peut y avoir des circonstances particulières où, par exemple, un exploitant aurait une vulnérabilité dans son réseau telle que la divulgation de cette vulnérabilité inviterait essentiellement les pirates informatiques à inonder la zone pendant que l'exploitant essaie de régler le problème. Mais ce seraient des circonstances très particulières. C'est là qu'il pourrait être justifié d'exiger la confidentialité.

Ce pouvoir fera l'objet d'une surveillance. Il faut ainsi aviser l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) afin qu'ils soient au courant et qu'ils puissent s'assurer que ce pouvoir est utilisé de manière appropriée. Il y a également des rapports annuels au Parlement.

Même si...

Dane Lloyd: Y a-t-il une possibilité de contrôle judiciaire si quelqu'un estime que ce genre de décision porte atteinte à ses droits garantis par la Charte?

Andre Arbour: N'importe qui peut s'adresser aux tribunaux pour demander un contrôle judiciaire et...

Dane Lloyd: Mais si c'est secret, si on a ordonné aux gens de ne rien dire? Comment peuvent-ils s'adresser aux tribunaux?

Andre Arbour: Nous devons tout de même consulter les parties touchées. C'est ce que prévoit le projet de loi; c'est aussi une disposition fondamentale en droit administratif.

L'entité touchée doit toujours avoir la possibilité de faire valoir ses arguments sur la façon dont un décret pourrait la toucher, et elle peut s'adresser aux tribunaux. Il y a aussi, encore une fois, l'avis envoyé aux organismes d'examen et le rapport annuel au Parlement qui, même s'il ne décrit pas la nature détaillée du décret, doit tout de même décrire les activités visées, ainsi que leur nécessité.

Dane Lloyd: Y a-t-il une limite de temps pour toutes ces choses? Il est question de délais précis.

Andre Arbour: Nous avons 90 jours pour aviser l'OSSNR et le CPSNR, et un rapport est déposé au Parlement chaque année.

Dane Lloyd: Merci.

Le président: Merci, monsieur Lloyd, pour ces bonnes questions.

Je cède maintenant la parole à Mme Acan pour six minutes.

Sima Acan (Oakville-Ouest, Lib.): Merci, monsieur le président.

Je vous remercie d'être parmi nous aujourd'hui.

J'allais poser cette question à Mme Walshe, mais M. Arbour et M. MacSween peuvent y répondre aussi.

Les entreprises canadiennes ont recours à la délocalisation pour la fabrication de produits hors du Canada. La partie du projet de loi C-8 qui porte sur la protection des cybersystèmes essentiels impose une exigence fondamentale aux exploitants désignés qui gèrent des services essentiels comme les télécommunications, les banques et l'énergie afin d'atténuer les risques liés à la chaîne d'approvisionnement et aux tiers.

Si, jusqu'à présent, la fabrication est délocalisée, la responsabilité devrait toujours incomber à l'entreprise canadienne qui l'a demandée, et elle devrait bien vérifier le produit qu'elle reçoit avant de le déployer en production.

En quoi le fait d'obliger explicitement les entreprises canadiennes, les exploitants désignés, à établir et à maintenir des programmes de cybersécurité complets, qui comprennent des mesures visant à cerner et à gérer les risques associés à la chaîne d'approvisionnement des exploitants désignés et à l'utilisation de produits et de services de tiers, garantit-il le respect des normes de sécurité canadiennes élevées, quel que soit l'emplacement physique de la fabrication de produits ou de l'équipe de soutien?

Kelly-Anne Gibson (directrice, Division de la politique de cyberprotection, ministère de la Sécurité publique et de la Protection civile): Je pense que cela touche un aspect très important du projet de loi. Comme vous le dites, il incombe à l'exploitant désigné de s'assurer que les services ou les produits de tiers qu'il utilise respectent une norme raisonnable pour atténuer les risques.

Concrètement, l'exploitant désigné doit donc mettre en place un programme de cybersécurité. Il doit avoir un plan pour atténuer les risques, ce qui signifie qu'il doit avoir un plan pour évaluer les divers services et produits qu'il peut obtenir par contrat pour utiliser dans ses réseaux.

Le Centre pour la cybersécurité publie des conseils à ce sujet, et l'exploitant désigné peut utiliser ces conseils pour déterminer comment trouver les produits et services les plus susceptibles de préserver la sécurité et l'intégrité de ses réseaux.

L'un des éléments qui aideront l'écosystème de la cybersécurité dans son ensemble, c'est que cela signifie que les entreprises qui vendent leurs produits et leurs services à des infrastructures essentielles devront s'assurer que leurs produits sont sécurisés dès la conception, de sorte qu'elles ne pourront pas les commercialiser trop vite dans l'espoir d'en corriger les lacunes potentielles après coup.

● (1225)

Sima Acan: Merci.

Non seulement faut-il atténuer les risques en général, mais les acteurs et les entités étatiques étrangers provenant de pays à haut risque représentent une menace directe pour notre sécurité nationale.

En quoi les pouvoirs d'urgence élargis accordés au gouverneur en conseil en vertu de la partie I de la Loi sur les télécommunications — plus précisément le pouvoir découlant du nouvel article 15.1 proposé d'« interdire aux fournisseurs de services de télécommunication d'utiliser tous les produits et les services fournis par toute personne qu'il précise » et d'ordonner leur retrait — fournissent-ils au gouvernement l'outil précis nécessaire pour protéger le système canadien de télécommunications contre l'ingérence, la manipulation, la perturbation ou la dégradation?

Andre Arbour: Il y a des produits et des services qui peuvent être sous le contrôle d'un adversaire hostile, soit parce que le producteur de ces produits et services est soumis à une surveillance extrajudiciaire, soit autrement, s'ils peuvent être utilisés pour infiltrer les infrastructures canadiennes.

Dans ce contexte, d'autant plus que les logiciels sont de plus en plus importants, il n'est peut-être pas possible d'atténuer les risques si l'on utilise ce produit ou ce service. Par conséquent, le pouvoir en question donne au gouvernement le droit d'en restreindre entièrement l'utilisation ou de le faire retirer du système canadien de télécommunications.

Sima Acan: Merci beaucoup.

Compte tenu du fait que les membres des équipes de soutien étrangères peuvent accéder à distance aux environnements en temps réel, il est essentiel qu'elles adhèrent à la même posture de sécurité obligatoire que les employés canadiens, afin d'assurer l'équité concurrentielle dans l'ensemble du secteur.

Étant donné que les exploitants désignés doivent intégrer des mesures dans leurs programmes de cybersécurité pour protéger les cybersystèmes essentiels contre toute atteinte, comment la mise en œuvre de normes de sécurité obligatoires et de mesures d'atténuation des risques répond-elle à la préoccupation selon laquelle les entreprises qui utilisent des chaînes d'approvisionnement internationales pourraient autrement obtenir un avantage économique injuste en évitant les coûts nationaux nécessaires en matière de cybersécurité?

Kelly-Anne Gibson: Si je comprends bien la question, vous demandez comment une entreprise gérerait l'aspect financier de l'obligation d'atténuer les risques et si cela la placerait en situation de désavantage concurrentiel. Est-ce bien cela?

Sima Acan: C'est exact.

Kelly-Anne Gibson: Le projet de loi lui-même n'aborde pas directement cette question. Cependant, nous avons voulu nous assurer, dans le contexte de ce projet de loi, de créer un environnement cybersécuritaire sans pour autant imposer de fardeau indu à l'industrie. Dans ce cas particulier, il est important d'avoir un environnement cybersécuritaire parce que le plus grand risque, c'est un incident. Un seul incident peut effacer des années de profits et, franchement, causer tellement de dommages que cela viendrait éclipser ce qu'il en aurait coûté pour essayer de protéger l'environnement dès le départ.

Le projet de loi n'aborde pas directement cette question, mais il vise à protéger l'économie canadienne et les entreprises elles-mêmes de cette façon, simplement parce que la menace et le coût d'un incident de cybersécurité sont tellement élevés, le cas échéant.

Sima Acan: Merci beaucoup.

[*Français*]

Le président: Je vous remercie beaucoup de cette belle intervention, madame Acan.

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Merci, monsieur le président.

Madame Walshe, avant vous, nous avons discuté avec Mme Gibson, qui nous a dit que le gouvernement, quand il a rédigé le projet de loi C-8, était très conscient qu'il y avait des chevauchements avec les cadres provinciaux en matière de cybersécurité…

Le président: Madame DeBellefeuille, je suis désolé de vous interrompre, mais il faut éviter de mentionner des informations qui ont été fournies à huis clos.

Claude DeBellefeuille: C'est vrai, excusez-moi.

Madame Walshe, le projet de loi C-8 va probablement empiéter sur certaines responsabilités des provinces et des territoires. Notre formation politique a constaté la même chose dans le cadre des ententes entre Hydro-Québec et les États-Unis, par exemple.

De votre côté, vous jouez un rôle central pour protéger l'information du gouvernement, et vous avez dit d'entrée de jeu dans votre présentation que le gouvernement ne pouvait pas lutter seul contre les cybermenaces. Ça prend une équipe qui inclut les entreprises, les provinces et les territoires.

Avec le projet de loi C-8, comment prévoyez-vous partager l'information avec vos partenaires provinciaux et territoriaux?

● (1230)

Bridget Walshe: Je vous remercie de cette question et je vais répondre en anglais.

[*Traduction*]

Nous avons des relations de travail très solides avec nos homologues de toutes les provinces et de tous les territoires. Ainsi, nous rencontrons régulièrement les responsables de la cybersécurité. Nous avons un groupe de travail qui se réunit en personne au moins une fois par année pour échanger sur les questions de cybersécurité, et en fait, nous avons discuté des projets de loi C-8 et C-26, son prédécesseur, avec nos homologues et nous les avons bien entendus dire que...

L'exemple d'Hydro-Québec est intéressant, parce qu'elle est assujettie à la réglementation du Québec et à la réglementation des États-Unis comme elle vend de l'énergie de l'autre côté de la frontière. Elle serait également assujettie à la réglementation découlant du projet de loi C-8. Nous avons vraiment une bonne relation avec elle, et nous voulons bien comprendre ses préoccupations par rapport à la nouvelle réglementation et aux mécanismes dont il est question ici.

De plus, nous collaborons constamment, au quotidien, pour contrer les cybermenaces. Nous travaillons en étroite collaboration avec tous les fournisseurs d'infrastructures essentielles, les provinces et les territoires pour échanger des renseignements sur les menaces.

Par exemple, si quelqu'un entend parler d'un cyberincident ayant une incidence sur les infrastructures essentielles du Canada, même sans exigence de signalement, actuellement, nous recevons des signalements volontaires. Nous prenons cette information, l'analysons, puis déterminons ce que nous pouvons communiquer à nos partenaires. Nous transmettons les renseignements pertinents à nos partenaires des infrastructures essentielles, des provinces et des territoires afin que tout le monde puisse les utiliser pour défendre ses propres réseaux.

Je peux peut-être demander à mon collègue, Dan Couillard, de vous donner un peu plus de détails sur nos interactions avec les provinces et les territoires.

[*Français*]

Daniel Couillard (directeur général, Cyberpartenariats, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Depuis la création du Centre canadien pour la cybersécurité, nous travaillons énormément sur nos relations avec les provinces et les territoires. Comme ma collègue l'a mentionné, des incidents nous sont rapportés présentement, et ce, depuis l'ouverture du Centre.

Durant l'exercice 2024-2025, plus de 1 400 incidents de cybersécurité ont été signalés au Centre. Dans tous ces cas, nous avons travaillé avec d'autres territoires. Nous nous sommes échangé de l'information. Il y a souvent eu des cas impliquant des entités réglementées de manière transfrontalière avec les États-Unis, le Canada, ou des provinces. Ce sont donc des situations que nous connaissons déjà et sur lesquelles nous nous penchons depuis plusieurs années.

Selon le projet de loi C-8, certains incidents devront être rapportés de manière obligatoire. Le principe de cette approche est que, plus on a d'information, plus on a la capacité d'identifier la menace et d'en faire part à l'entité ciblée, de même qu'aux autres entités du secteur. Ainsi, elles pourront prendre des mesures proactives pour se protéger, et protéger également les autres secteurs. On le sait, il y a une très grande interconnexion des secteurs d'infrastructure critique au Canada. De plus, il est très important de pouvoir réagir en temps opportun. Nous connaissons donc tout cet aspect, et le projet de loi C-8 nous permettra de recueillir et d'échanger toute cette riche information.

Claude DeBellefeuille: Dans le projet de loi C-8, on prévoit aussi des sanctions. Vu qu'il y a du chevauchement ou du dédoublement, je me demande si, par exemple, Hydro-Québec pouvait être soumise à une double sanction si elle contrevenait au projet de loi C-8.

[*Traduction*]

Kelly-Anne Gibson: Le projet de loi C-8 a été rédigé de manière à nous permettre de nous fier à l'organisme de réglementation existant pour les entités. La raison en est que ces organismes connaissent déjà bien leur affaire, donc ils savent déjà très bien comment se débrouiller dans un environnement réglementaire où il y a un autre organisme de réglementation provincial compétent; ils savent comment dénouer les conflits.

Je ne peux pas vous dire comment ils s'y prennent pour résoudre les conflits s'il y a des sanctions administratives qui se chevauchent, par exemple, ou quelque chose du genre. Cependant, je peux vous dire que nous nous fierions aux organismes de réglementation existants, qui ont l'habitude de composer avec les réglementations provinciales et fédérale dans ces secteurs pour assurer la conformité.

● (1235)

[*Français*]

Le président: Merci, madame DeBellefeuille.

Monsieur Gill, la parole est à vous pour cinq minutes.

[*Traduction*]

Sukhman Gill (Abbotsford—Langley-Sud, PCC): Merci, monsieur le président, et merci aux témoins d'être ici aujourd'hui.

Mes questions portent sur la liberté de parole et d'expression.

La Canadian Constitution Foundation a exprimé des craintes au sujet des répercussions du projet de loi C-8 et de l'article 15.2 proposé sur les libertés civiles. Cet article donnerait au ministre le pouvoir de prendre les décisions nécessaires pour expulser quelqu'un d'Internet.

Quelles sont les mesures de protection qui existent pour empêcher le gouvernement d'utiliser la cybersécurité comme prétexte pour réduire des gens au silence?

Andre Arbour: Je comprends totalement l'importance de la question soulevée. Il y a des protections au départ, pendant l'utilisation du pouvoir et après coup. Par exemple, on précise que l'objectif stratégique de cette politique est de protéger le système canadien de télécommunications, de sorte que le discours d'une personne n'a aucune incidence sur la capacité de Bell Canada ou de Rogers de maintenir son réseau ni sur la fiabilité des services. Il n'y a aucun lien.

De plus, on précise que le recours à ce pouvoir doit être raisonnable, soit proportionnel à la gravité ou à la nature de la menace qu'on veut combattre. Il y a des critères établis par la Cour suprême depuis de nombreuses décennies, notamment dans l'arrêt Vavilov de 2019, qui précisent ce qu'on entend par « raisonnable ». Il y a aussi des exigences en matière de surveillance et de rapports, notamment à l'OSSNR, au CPSNR et, enfin, au Parlement.

Sukhman Gill: D'accord, je vous remercie.

Eh bien, il semble que si ce projet de loi est adopté dans sa forme actuelle, sans amendement, nous allons donner au ministre de l'Industrie de vastes pouvoirs, pratiquement sans freins et contrepoids. En théorie, le ministre pourrait se réveiller un matin, comme l'un de mes collègues l'a mentionné, ne pas être impressionné par une publication sur les médias sociaux, et aller même jusqu'à dire essentiellement qu'elle constitue une menace pour nos services de télécommunications. Sans mandat, sans procès, sans contrôle judiciaire automatique, le ministre pourrait obliger Rogers ou Telus à rassembler les données personnelles de ces gens.

Qu'avez-vous à dire à ce sujet?

Andre Arbour: Je tiens à souligner que des mécanismes permettent de limiter la portée de toute action en cas d'interruption des services. En outre, cette délimitation de la portée s'applique également en ce qui concerne les données personnelles. Je rappelle que les données personnelles et l'historique de navigation des Canadiens ne sont pas des éléments déterminants quant au maintien en service ou à la fiabilité de notre infrastructure de télécommunications.

Un autre amendement a été adopté au moment où le projet de loi C-26 était à l'étude. Pour plus de certitude, on a interdit explicitement l'utilisation du pouvoir de rendre des ordonnances pour intercepter des communications privées. Cela était déjà interdit, mais on souhaitait ajouter un niveau de clarté supplémentaire.

Sukhman Gill: Quelles mesures peuvent être mises en place pour veiller à ce que ce pouvoir ne soit pas utilisé à mauvais escient ou, pire encore, transformé en outil politique pour le gouvernement libéral contre des personnes ou des organisations avec lesquelles il n'est pas d'accord?

Andre Arbour: Je ne peux pas parler au nom du Comité, car ce que le Comité décidera de faire relève de sa prérogative. Je tiens à souligner que l'ensemble des pouvoirs qui ont été introduits avec le projet de loi et qui ont été adoptés lors de l'étude précédente du Comité ajoute une protection à partir de l'établissement de la portée. La loi actuelle prévoit déjà des interdictions relativement aux préoccupations qui ont été soulevées. Il y a également des exigences en matière de consultation qui permettent d'exercer une surveillance accrue et d'évaluer la manière dont ces pouvoirs sont utilisés. En outre, il y a des exigences en matière d'avis et de rapports, y compris pour l'utilisation confidentielle des pouvoirs dans des circonstances bien définies, qui permettent d'assurer la supervision requise.

● (1240)

Sukhman Gill: J'ai une dernière question.

De nombreux groupes de la société civile ont fait part de leurs inquiétudes au sujet des gouvernements fédéraux qui tentent de s'octroyer le pouvoir d'intrusion dans notre vie privée au nom de la sécurité. Ces organisations ont-elles été véritablement consultées avant l'élaboration de ce projet de loi?

Le président: Il vous reste environ 15 secondes.

Kelly-Anne Gibson: La réponse courte est oui. Nous avons reçu de nombreux mémoires d'organisations de défense des libertés civiles. Je peux vous garantir que mon équipe les a examinés très attentivement et les a sérieusement pris en considération. Ce fut la même chose pour les mémoires présentés au Comité au cours de la législature précédente. Nous les avons étudiés avec grand intérêt.

[*Français*]

Le président: Merci de vos questions, monsieur Gill.

Madame Dandurand, vous avez la parole pour cinq minutes.

Marianne Dandurand (Compton—Stanstead, Lib.): Merci beaucoup, monsieur le président.

Mesdames et messieurs les témoins, je vous remercie de nous donner des réponses très claires. C'est vraiment intéressant.

J'aimerais faire écho aux questions de mon collègue qui portaient sur le droit à la vie privée. Je ressens beaucoup d'inquiétude chez le simple citoyen. Pourriez-vous éclairer notre lanterne en nous disant à qui la loi concernant la cybersécurité s'appliquera, exactement?

[*Traduction*]

Kelly-Anne Gibson: Je peux vous répondre concernant la partie 2, puis mon collègue pourra vous dire ce qu'il en est de la partie 1.

La partie 2 ne s'appliquerait qu'aux exploitants désignés à l'annexe 2 de la Loi. Selon le libellé actuel, l'annexe 1 dresse la liste des services essentiels que nous devons protéger, après quoi, dans le cadre du processus de réglementation, nous désignerions des exploitants dans ces différents secteurs. Les obligations ne s'appliquent qu'aux exploitants désignés, c'est-à-dire les propriétaires et les exploitants d'infrastructures essentielles. Ce sont ces entreprises qui seraient visées.

[*Français*]

Andre Arbour: En résumé, pour ce qui est de la partie 1, la loi s'appliquera aux fournisseurs de services de télécommunications tels que Bell et Rogers.

La question portant sur le droit à la vie privée a été soulevée, parce qu'en général les réseaux de ces fournisseurs détiennent les données des consommateurs, des Canadiens et des entreprises. C'est pourquoi la portée des pouvoirs prévus par le projet de loi C-8 est limitée. De plus, on y apporte des précisions, comme l'interdiction d'intercepter des communications personnelles. Tout ceci sert à clarifier le fait que ces pouvoirs ne ciblent pas les données personnelles des Canadiens. Il s'agit plutôt de protéger les réseaux et les infrastructures essentielles.

Marianne Dandurand: D'après ce que je comprends, le projet de loi tel que rédigé ne touche en aucun cas aux données personnelles des gens. En ce sens, est-il nécessaire d'avoir plus de protection? Puisque la future loi ne touche pas actuellement aux données personnelles, peut-on garantir qu'elle n'y touchera pas dans le futur?

Andre Arbour: Les pouvoirs prévus visent vraiment les fournisseurs de service de télécommunications et leurs réseaux. Certains pouvoirs permettent de collecter les informations de ces fournisseurs. L'objectif est de comprendre quel équipement est utilisé par leurs réseaux. L'information personnelle des Canadiens n'est pas visée par ces mesures, dont le but est de protéger les réseaux en question.

Les pouvoirs de cette partie de la loi et leur portée sont directement liés au décret ou à l'arrêté. Certains contextes font appel à seulement un élément du projet de loi, mais on doit lire la partie dans son ensemble pour mieux comprendre les protections prévues.

● (1245)

Marianne Dandurand: Merci beaucoup, monsieur Arbour.

Madame Walshe, nous n'avons pas exploré l'impact des cybermenaces et des rançongiciels. Quel impact financier représentent les menaces subies par les Canadiens actuellement?

[*Traduction*]

Bridget Walshe: Merci beaucoup de la question.

[*Français*]

Je vais répondre en anglais.

[*Traduction*]

Pour plusieurs raisons, il est difficile de mesurer l'impact de la cybercriminalité sur les organisations canadiennes. Nous savons toutefois que les répercussions sont considérables.

D'un point de vue financier, nous savons que des organisations canadiennes versent à des groupes de cybercriminels des sommes qui totalisent des centaines de millions de dollars, mais tous ces paiements ne nous sont pas déclarés. L'information à notre disposition n'est pas suffisamment complète pour nous permettre de bien saisir la véritable ampleur de ce phénomène.

Nous n'ignorons pas également que le coût financier pour une organisation ne se limite pas aux montants versés aux cybercriminels. Il y a aussi la perte de productivité et le rétablissement à la suite de ces attaques qui coûtent très cher.

C'est une autre réalité qu'il est également difficile de bien cerner parce que cela fait partie des éléments qu'une entreprise privée peut divulguer dans le cadre de ses rapports publics ou qu'elle peut décider de garder confidentiels. Il est donc difficile de savoir exactement à quoi s'en tenir.

[*Français*]

Le président: Merci, madame Walshe. C'est tout le temps que nous avons pour cette intervention.

Madame DeBellefeuille, vous avez la parole pour deux minutes et demie.

Claude DeBellefeuille: Merci, monsieur le président.

Monsieur Arbour, je vous félicite pour vos réponses en français aux questions. Je suis toujours un peu déçue de voir que les hauts fonctionnaires ne maîtrisent pas les deux langues officielles. En tant que francophone, je dois dire que vous me faites vraiment plaisir en répondant en français aux questions, car c'est la preuve que vous maîtrisez la langue.

J'ai une petite question concernant les fournisseurs. Tantôt, vous avez parlé des gros fournisseurs comme Bell. Or, beaucoup de petits fournisseurs contribuent au déploiement d'Internet haute vitesse dans les petites communautés rurales. Par exemple, chez moi, il y a Targo et la coopérative CSUR.

Croyez-vous que ces petits fournisseurs sont capables de satisfaire aux exigences du projet de loi C-8? Ont-ils les moyens financiers de le faire? Est-il prévu de les accompagner?

Andre Arbour: Le ministère de l'Industrie est habitué à travailler avec les petits fournisseurs de services de télécommunications. Un de nos objectifs est de soutenir ce type d'exploitants pour promouvoir la concurrence au sein des secteurs et élargir les réseaux dans les zones rurales et éloignées. Il est important pour nous d'établir des règles qui correspondent aux compétences des fournisseurs de services de toutes tailles, même des petites entreprises.

Par exemple, lors de la mise aux enchères de portions du spectre, nous avons établi des règles spécifiques aux petits fournisseurs de services. C'est la même chose pour la mise en œuvre de ce projet de loi. Par exemple, dans nos concertations, nous prenons en considération le temps nécessaire pour atteindre l'objectif d'un règlement selon l'envergure du fournisseur. Les grands joueurs présentent un certain niveau de risque systématique par rapport à un petit fournisseur qui sert 500 consommateurs.

Le président: Merci. Je suis désolé, madame DeBellefeuille, mais c'est déjà terminé.

Monsieur Lloyd, vous avez la parole pour cinq minutes.

[*Traduction*]

Dane Lloyd: Merci.

Certains groupes, comme l'Association canadienne des libertés civiles, ont parlé des normes de cryptage. On craint que ce projet de loi n'accorde des pouvoirs sans précédent pour contourner le chiffrement.

Y a-t-il quelque chose de précis dans ce projet de loi qui traite des pouvoirs de déchiffrement?

● (1250)

Andre Arbour: Il n'y a pas de disposition particulière régissant le chiffrement. Cependant, la capacité de contourner le cryptage à des fins de surveillance outrepasse la portée des pouvoirs prévus dans ce projet de loi.

La capacité d'accéder à des renseignements personnels aux fins de l'application de la loi est certes un enjeu important. C'est un sujet très chaud. Nous avons notamment pu le constater avec le projet de loi C-2. On a choisi de laisser le déchiffrement hors de la portée du projet de loi, car il ne contribue pas à la protection de l'infrastructure des réseaux de télécommunications. Cela n'a rien à voir.

Dane Lloyd: Je vous remercie de cette précision.

Je pense que l'argument qui a été avancé... Je m'excuse auprès de ces organisations si j'ai mal présenté leur argument. Elles parlent du libellé selon lequel le ministre peut ordonner aux entreprises de télécommunications « de faire ou de s'abstenir de faire toute chose », en soutenant qu'il s'agit d'un pouvoir très vaste qui pourrait aller jusqu'à autoriser le contournement du cryptage.

Pouvez-vous nous expliquer pourquoi ce pouvoir a été formulé en ces termes? Je me suis même dit que c'était là une formulation plutôt intéressante, « de faire ou de s'abstenir de faire toute chose ». Cela me semble permettre une interprétation très large.

Andre Arbour: Le libellé vise à couvrir tout l'éventail de facteurs pouvant mettre en péril l'infrastructure de télécommunications. Par exemple, on pourrait ordonner à un fournisseur de services de ne pas utiliser un produit ou un service en particulier dans son réseau, ou encore de prendre des mesures concrètes pour protéger son réseau.

Un principe fondamental de l'interprétation des lois est qu'il faut examiner un projet de loi dans son ensemble. Ainsi, l'objectif stratégique établit d'emblée la portée générale. Il y a des exigences supplémentaires — par exemple, le pouvoir de rendre des ordonnances doit être raisonnable par rapport à la gravité de la menace. Toutes ces exigences s'appliquent pour encadrer la capacité d'agir du gouvernement.

Dane Lloyd: Merci.

Nous avons parlé des renseignements personnels. Vous avez dit que cela dépassait la portée du projet de loi. Nous en avons discuté. Cependant, le commissaire au renseignement a déclaré dans son témoignage que ce pouvoir du ministre de demander aux entreprises de télécommunications de faire ou de s'abstenir de faire quelque chose pourrait lui permettre d'exiger des fournisseurs de télécommunications qu'ils transmettent les renseignements personnels des Canadiens. Je crois que le commissaire à la protection de la vie privée a également soulevé cette préoccupation.

Pouvez-vous nous en dire plus sur ces préoccupations ou alors nous indiquer pour quelles raisons il n'y a pas vraiment lieu de s'inquiéter?

Andre Arbour: Le pouvoir de collecte de renseignements prévu à la partie 1 est calqué sur l'article 37 de la Loi sur les télécommunications, qui est en vigueur depuis des décennies sans avoir causé d'incident. Ce pouvoir est simplement reporté, car il doit être appliqué aux nouvelles autorités de protection du réseau de sécurité. Il s'inscrit toujours dans le cadre de ce qui peut être fait pour protéger le système de télécommunications canadien, et ne vise pas l'atteinte d'objectifs plus généraux en matière de sécurité ou d'application de la loi. On se limite encore aux pouvoirs de rendre des ordonnances et à la protection des systèmes de télécommunications canadiens. On ne peut pas exercer ce pouvoir pour mener une collecte généralisée de renseignements à l'aveuglette ou une enquête sur des renseignements personnels.

Dane Lloyd: Merci.

Enfin, comment détermine-t-on que la décision prise par le ministre, en vertu de ce pouvoir, est raisonnable? Qui détermine si ce que le ministre a fait est raisonnable?

Andre Arbour: Premièrement, il y a une consultation au sujet de la réglementation. Nous sommes tenus de tenir compte des points de vue alors exprimés. Il y a des exigences en matière d'avis et de transparence une fois la décision rendue. En outre, toutes les décisions du ministre peuvent être révisées par les tribunaux. Les fournisseurs de services de télécommunications n'hésitent pas à s'adresser aux tribunaux. Ils sont bien dotés en ressources et ils ont souvent recours à cette option.

● (1255)

[*Français*]

Le président: Merci, monsieur Lloyd.

Nous terminons par M. Ehsassi.

[*Traduction*]

L'hon. Ali Ehsassi: Merci, monsieur le président.

Je remercie les témoins de leurs réponses très complètes.

Le projet de loi oblige-t-il tous ces exploitants à désormais signaler chacune des atteintes dont ils peuvent être victimes?

Colin MacSween (directeur général, Direction générale de la cybersécurité nationale, ministère de la Sécurité publique et de la Protection civile): L'exigence de signalement obligatoire est énoncée à la partie 2 du projet de loi. La réponse à votre question est non. L'intention est que la loi établisse l'exigence de signalement obligatoire, puis que le règlement définisse exactement la forme que cela prendra.

Comme je l'indiquais précédemment, nous avons eu des discussions avec nos homologues du Groupe des cinq concernant leurs régimes obligatoires. Ceux-ci sont assortis d'un seuil à compter duquel un incident doit absolument être signalé. Nos collègues du Centre canadien pour la cybersécurité ne sont certainement pas intéressés à recevoir de l'information sur chaque cyberincident qui peut se produire. Il s'agit dans bien des cas d'événements du quotidien dont nous saisissons bien la nature. Nous sommes davantage intéressés à savoir de quoi il en retourne lorsque survient un incident d'une certaine importance. C'est le genre de situations qui devraient être signalées au Centre canadien pour la cybersécurité.

L'hon. Ali Ehsassi: Merci.

Il y a dans ce projet de loi une section sur les sanctions administratives pécuniaires. Avons-nous déjà une idée du montant maximal que ces sanctions pourraient atteindre?

Kelly-Anne Gibson: Oui. C'est précisé dans le projet de loi. Je suis désolée, mais je ne me souviens pas des chiffres exacts. Je peux vous dire que, comme il s'agit d'un cadre intersectoriel et que les différentes industries ont des seuils différents, le maximum est élevé, mais le montant précis sera établi dans une fourchette correspondant à ce qui se fait généralement dans l'industrie visée.

L'hon. Ali Ehsassi: Merci beaucoup.

J'ai une dernière question, si vous me le permettez. Selon l'information que vous nous avez fournie, les incidents liés à la cybersécurité coûtent 5 milliards de dollars par année à l'économie canadienne, alors que chaque fuite de données entraîne des coûts de 7 millions de dollars pour l'entreprise touchée. Pourriez-vous nous dire en gros pourquoi ces atteintes coûtent si cher aux entreprises? S'agit-il d'indemnisations offertes aux clients parce que leurs données personnelles ont été exposées? Pourquoi ces sommes sont-elles si élevées?

Kelly-Anne Gibson: Il y a différents facteurs à considérer.

En cas de cyberincident, vos données peuvent être compromises. Il faut donc, d'abord et avant tout, déterminer ce qui a pu être exposé. Cela peut être extrêmement coûteux, car il faut faire appel à des experts pour comprendre ce qui se passe exactement sur son réseau. Qu'est-ce qui a été compromis et qu'est-ce qui a pu être exfiltré?

Ensuite, il faut commencer à mettre en place des mesures correctives, et pas seulement d'un point de vue technique. Vous devez également voir quelles sont vos responsabilités par rapport à la réglementation en place. Respectez-vous encore les règles? Il y a des lois sur la protection de la vie privée qui vont entrer en jeu, comme la LPRPDE, la Loi sur la protection des renseignements personnels et ce genre de choses. Il y a des notifications à émettre. Des avocats et des conseillers en atteinte à la vie privée interviennent. Les coûts s'accumulent.

L'autre élément, un peu plus intangible, est simplement le coût lié à la réputation. Souvent, ces incidents finissent par être rendus publics, et vous commencez à perdre des clients. C'est ainsi que les coûts peuvent se multiplier très rapidement.

Bridget Walshe: J'aimerais ajouter quelque chose.

D'un point de vue technique, il y a effectivement d'énormes sommes à débourser, comme ma collègue l'a souligné, pour remédier à la situation dans l'immédiat, mais aussi des coûts faramineux liés au rétablissement et aux pertes de revenus qu'une entreprise peut subir pendant ce rétablissement. Nous savons donc qu'il y a un coût énorme à assumer, non seulement immédiatement après l'incident, mais aussi pour reconstruire la technologie afin de pouvoir la remettre en service.

Le président: Merci beaucoup.

[*Français*]

Chers témoins, je tiens à vous remercier tous les six de vous être déplacés. Nous vous sommes reconnaissants non seulement de votre présence, mais aussi de votre préparation à cette importante rencontre. Nous vous souhaitons une très bonne journée.

J'invite les membres du Comité à rester quelques instants, le temps de terminer cette réunion.

Monsieur Ramsay, vous avez la parole.

[*Traduction*]

Jacques Ramsay: J'aimerais proposer deux motions.

La première porte sur le projet de loi C-12:

> Que, en relation avec l'étude du projet de loi C-12:
>
> le Comité invite les membres à soumettre leur liste de témoins au greffier du Comité au plus tard le 29 octobre 2025 à 17 heures;

C'est demain.

> le Comité prévoit quatre réunions pour entendre les témoins; qu'il invite le ministre de la Sécurité publique à comparaître, ainsi que les fonctionnaires concernés;
>
> le Comité procède à l'étude article par article du projet de loi après la fin des témoignages des témoins lors de la quatrième séance, et que le Comité ne s'ajourne pas avant que l'étude article par article soit terminée.

C'est donc ma première motion.

● (1300)

[*Français*]

Le président: Merci, monsieur Ramsay.

Monsieur Caputo, vous avez la parole.

[*Traduction*]

Frank Caputo (Kamloops—Thompson—Nicola, PCC): Merci, monsieur le président, et merci à vous, monsieur Ramsay.

Comme il y a beaucoup d'éléments à considérer, je vais essayer de résumer tout cela, parce que je pense que nous avons un consensus. Je veux juste m'assurer que nous n'oublions rien.

En ce qui concerne la motion sur le projet de loi C-12 qui vient d'être lue, je ne suis pas certain si mon collègue a parlé d'un minimum de quatre réunions. C'est l'impression que j'ai eue.

S'agissait-il d'un minimum de quatre réunions?

Jacques Ramsay: Il s'agissait de quatre réunions.

Frank Caputo: D'accord. J'avais cru comprendre qu'il devait y avoir au moins quatre réunions.

Une chose qu'il convient de noter — et nous pouvons nous entendre ou convenir d'un accord à ce sujet —, c'est que nous ne passerions pas immédiatement à l'étude article par article. Par exemple, si les témoins terminent leur comparution à 13 heures, nous ne procéderons pas à l'étude article par article à compter de 13 h 5. Nous consacrerions deux heures par réunion à l'étude article par article.

Je pense que ce sont les deux principaux points à tirer au clair

M. Ramsay parle de quatre réunions. J'avais cru comprendre que nous nous étions entendus pour tenir un minimum de quatre réunions, alors je voudrais bien obtenir des éclaircissements à ce sujet.

Je crois qu'il va aussi traiter du projet de loi C-8, alors pendant que j'ai la parole...

Le président: Monsieur Caputo, pourriez-vous réserver vos commentaires jusqu'à ce que la motion concernant le projet de loi C-8 soit proposée?

[*Français*]

Madame DeBellefeuille, vous avez la parole.

Claude DeBellefeuille: Monsieur le président, j'aimerais proposer un amendement à cette motion, si c'est possible. Je vais lire le texte tel que modifié par les trois changements que je propose:

> Que, en relation avec l'étude du projet de loi C-12:
>
> Que le Comité invite les membres à soumettre leur liste de témoins au greffier du Comité au plus tard le 3 novembre 2025 à 16 heures;
>
> Que le Comité prévoie un minimum de quatre réunions pour entendre les témoins; qu'il invite le ministre de la Sécurité publique à comparaître, ainsi que les fonctionnaires concernés;
>
> Et que le Comité procède à l'étude article par article du projet de loi à une séance définie par le Comité suivant la dernière séance de témoins, et que le Comité consacre le nombre de séances nécessaire à l'étude article par article jusqu'à ce qu'elle soit terminée.

Nous trouvions que la date du 29 octobre était précipitée pour fournir la liste des témoins. Donc, en disant « au plus tard le 3 novembre », ça laisse une certaine latitude au greffier pour contacter les témoins et préparer la réunion de travail.

Je suis d'accord avec mon collègue conservateur qu'un minimum de quatre séances serait beaucoup plus judicieux. Par contre, je ne suis pas du tout d'accord sur l'idée d'enfiler l'étude article par article du projet de loi après l'audition des témoins, lors de la quatrième réunion, et ce, jusqu'à ce que ce soit terminé. Je pense qu'il est plus sage de commencer l'étude article par article du projet de loi après avoir terminé d'écouter les témoins, à une réunion ultérieure.

Le président: Très bien.

[*Traduction*]

Trois choses ont été dites: premièrement, un minimum de quatre réunions; deuxièmement, des listes de témoins d'ici le 3 novembre; et troisièmement, une entente implicite suivant laquelle nous suspendrions, et non ajournerions, nos travaux après la quatrième réunion, ce qui signifie que la prochaine réunion serait une continuation de la précédente qui n'aurait pas été ajournée. Ce sont les trois éléments que nous avons retenus.

Y a-t-il unanimité à ce sujet?

Nous vous écoutons, madame DeBellefeuille.

[*Français*]

Claude DeBellefeuille: Vous avez résumé l'esprit de mon amendement. C'est ce que je comprends, monsieur le président.

Le président: C'est ce que j'ai fait, oui.

Claude DeBellefeuille: D'accord.

Je veux que nous nous comprenions bien. Nous ne voulons pas que, lors de la quatrième réunion — dans l'éventualité où il y en aura quatre —, s'il reste encore quelques minutes après l'écoute des témoins, nous poursuivions avec l'étude article par article du projet de loi jusqu'à tard le soir. Est-ce bien ce que vous avez compris de mon amendement?

Je veux rappeler que c'est le Comité permanent de la citoyenneté et de l'immigration, ou CIMM, qui va étudier la partie du projet de loi portant sur les modifications apportées à la Loi sur l'immigration et la protection des réfugiés, et qui va entendre des témoignages. Comme il reviendra à notre comité de faire l'étude article par article du projet de loi, il m'apparaît important que les analystes puissent nous faire un résumé de ce qui aura été entendu au comité CIMM puisque nous devrons prendre connaissance de ses recommandations. En conséquence, il me semble qu'il faudrait un minimum de quatre réunions.

● (1305)

Le président: D'accord.

Le greffier aimerait fournir quelques précisions.

Le greffier du Comité (Andrew Wilson): J'ai parlé au greffier du comité CIMM, qui m'a dit que son comité soumettrait ses recommandations au président de notre comité une fois que son comité aura terminé d'entendre les témoignages. Ces recommandations seront alors distribuées aux membres de notre comité dès réception.

Le président: Très bien.

[*Traduction*]

Y a-t-il consensus, voire unanimité, sur ces trois modifications à la motion proposée? Premièrement, il y a le minimum de quatre réunions. Deuxièmement, il y a la date du 3 novembre pour soumettre une liste de témoins. Troisièmement, il est entendu que la quatrième réunion sera suivie d'autres séances pour l'étude article par article, et que cette quatrième réunion ne pourra pas être prolongée jusqu'à très tard dans la journée.

[*Français*]

Il me semble que c'est le consensus qui se dégage.

Madame Dandurand, la parole est à vous.

Marianne Dandurand: Les deux derniers changements proposés me vont. Par contre, je pense que nous devrions nous en tenir à quatre réunions, sans mentionner « un minimum de ». Nous ne donnerons pas notre consentement à cette proposition d'« un minimum de » quatre réunions.

Le président: D'accord. Je crois qu'il y a eu, à ce sujet, des discussions préalables entre les bureaux des leaders et qu'un accord préalable a été conclu. Nous ne pouvons pas refaire ces discussions une fois qu'une telle entente a été obtenue. Il faut éviter de tourner en rond.

[*Traduction*]

J'aimerais rappeler à tout le monde qu'il est préférable que ces discussions aient lieu en dehors d'une réunion comme celle-ci. Je crois comprendre que cette motion a fait l'objet d'un accord avant d'être déposée par M. Ramsay, alors nous ne devrions peut-être pas perdre de temps à réexaminer tout cela.

Monsieur Lloyd, vous avez la parole.

Dane Lloyd: Merci.

Je pense qu'il y a peut-être eu un malentendu. Je n'ai aucun problème avec le 3 novembre et le consensus implicite. Pour apaiser vos préoccupations, je souscris à l'idée des quatre réunions et je ne proposerai pas que nous en tenions au moins quatre. Si les événements nous obligent à tenir une cinquième réunion, nous pourrons en discuter le moment venu, mais je pense que quatre réunions suffiraient pour la motion actuelle.

Le président: Merci, monsieur Lloyd.

Maintenant, qu'en est-il de la date? Le 3 novembre vous apparaît-il raisonnable? D'accord.

Madame DeBellefeuille.

[*Français*]

Claude DeBellefeuille: Monsieur le président, quand vous avez fait le résumé des trois changements que j'ai proposés dans mon amendement — je pense que nous discutons amicalement de cet amendement —, vous l'avez fait en anglais. Je voudrais seulement m'assurer que j'ai bien compris.

Pour ce qui est de substituer aux mots « 29 octobre », les mots « 3 novembre », ça va. Si tout le monde s'entend pour tenir quatre réunions au lieu d'un minimum de quatre réunions, ça ne me pose pas de problème non plus.

Cependant, pour ce qui est de mon dernier changement, j'aimerais comprendre une chose. Il se peut que nous ayons besoin d'une ou deux réunions pour l'étude article par article. Vous comprenez bien que, après les témoignages, nous commencerions l'étude article par article et qu'on ne peut pas dire combien de réunions ça va nous prendre.

Le président: Je comprends, mais nous allons devoir être disciplinés, parce que nous avons beaucoup d'autres travaux à effectuer par la suite. Plusieurs d'entre vous attendent de mener ou de terminer d'autres études. Nous sommes donc conscients du fait que le temps dont disposent tous les députés est limité.

[*Traduction*]

Nous devons avoir des attentes raisonnables, car le temps est notre ressource la plus rare.

Monsieur Caputo, vous avez la parole.

Frank Caputo: Merci.

Je suis désolé. J'étais en communication tout au long de l'intervention de Mme DeBellefeuille.

Je crois comprendre que l'on a convenu de tenir quatre réunions. Je parle seulement des conservateurs et des libéraux. Cela s'est passé au-dessus de mon niveau.

J'espère que notre comité saura faire preuve de la souplesse nécessaire pour tenir compte des préoccupations de Mme DeBellefeuille. Si nous avons besoin d'une autre réunion, j'ose espérer que nous envisagerons cette possibilité pour apaiser ses inquiétudes. Nous débattons en fait pour savoir si ce sera quatre ou un minimum de quatre. Si l'on opte pour quatre séances, il est entendu que si d'autres réunions se révèlent nécessaires, nous réexaminerons la question. Est-ce que cela vous convient?

● (1310)

Le président: Je pense qu'il y a effectivement un certain consensus. Est-ce que tout le monde est d'accord?

Madame Dandurand.

[*Français*]

Marianne Dandurand: Je voudrais m'assurer d'une chose, monsieur le président.

Je pense avoir mal compris le dernier changement proposé par l'amendement de ma collègue. Selon ma compréhension, une seule réunion aurait lieu pour l'étude article par article et nous la poursuivrions jusqu'à ce qu'elle soit terminée. Une seule réunion serait tenue, sans ajournement.

Claude DeBellefeuille: Ce serait un sous-amendement.

Le président: D'accord.

Dans ce cas, une réunion s'ajouterait après la quatrième réunion sur le projet de loi C-8, mais, durant cette réunion, il faudrait terminer l'étude article par article du projet de loi. Ai-je bien compris?

Jacques Ramsay: Il s'agit du projet de loi C-12, monsieur le président.

Le président: Je me suis trompé. Nous parlons effectivement du projet de loi C-12. Sinon, ai-je bien compris?

Marianne Dandurand: Monsieur le président, il ne s'agit pas d'un sous-amendement. C'est exactement comme cela que la motion de M. Ramsay a été écrite. Une seule réunion serait tenue après les quatre réunions, laquelle serait ajournée seulement après la fin de l'étude article par article.

Le président: D'accord.

Je résume de manière plus informelle. Si la motion de M. Ramsay est acceptée, avec des amendements très précis, quatre réunions seront tenues pour examiner le projet de loi C-12. Après la quatrième réunion, une autre réunion suivra immédiatement et portera sur l'étude article par article du projet de loi C-12. Celle-ci durera aussi longtemps qu'il le faudra pour passer en revue les articles.

De plus, la liste des témoins serait soumise d'ici le 3 novembre prochain.

Claude DeBellefeuille: Je m'y oppose, car le changement que j'ai proposé voulait éviter ça. Je pense que ce comité est assez rigoureux. Nous n'avons pas du tout l'intention de faire traîner l'étude du projet de loi C-12, mais je ne veux pas non plus que nous nous limitions à une seule réunion pour l'étude article par article, réunion qui durera peut-être deux, trois, quatre ou cinq heures. C'est l'esprit du changement que j'ai proposé.

Nous n'avons pas de comité directeur et c'est pour ça que nous tenons toujours une réunion du Comité au complet pour organiser nos travaux. Toutefois, je commence très sincèrement à me questionner sur cette façon de faire, parce que nous avions presque conclu une entente, mais le temps s'écoule, il est 13 h 15 et ça fait trois réunions que nous finissons de cette façon. Si les conservateurs et les libéraux s'entendent, qu'ils demandent le vote et je m'y opposerai. Je ne veux pas restreindre l'étude article par article et je ne veux pas faire cette étude pendant trois, quatre, cinq, six, sept ou dix heures. Je vais collaborer et je sais que nous travaillerons rigoureusement. Tant mieux si nous y arrivons dans un temps plus court, mais je ne veux pas qu'une motion nous restreigne.

Je ne sais pas comment vous allez vous débrouiller, monsieur le président, mais j'ai présenté un amendement. Si on le rejette, on peut en présenter un autre et voter. Ensuite, nous déciderons de la suite de nos travaux.

Le président: Monsieur Caputo, vous avez la parole.

[*Traduction*]

Frank Caputo: Merci, monsieur le président.

Je partage le sentiment de Mme DeBellefeuille. Nous entendons tous le son de cloche de nos partis respectifs. Je pensais que nous avions un accord de principe, et je ne crois pas que nous soyons si loin d'un consensus relativement à toutes ces questions.

Habituellement, cependant, cette question serait renvoyée au sous-comité dont les membres pourraient en discuter à huis clos, pour ainsi dire, en arrivant tous très bien préparés pour en débattre. Je ne suis pas certain... Ce serait moi, Mme DeBellefeuille, M. Ramsay et le président. Je crois que c'est nous quatre qui formons le sous-comité. Je ne sais pas si nous pouvons faire quelque chose de ce genre très rapidement, car j'ai l'impression que nous nous retrouvons dans une impasse.

Le président: Oui, il y a beaucoup de travail à faire à l'extérieur de cette salle et en dehors des cadres du sous-comité. D'après ce que j'ai compris — et je n'ai évidemment pas été informé de tout —, il y avait une entente, comme M. Caputo l'a dit plus tôt, à un échelon plus élevé, ce qui était la bonne chose à faire, parce que d'autres considérations auraient dû être prises en compte dans ces échanges. Les partis se sont entendus pour appuyer cette motion.

Cependant, il y a une ouverture pour changer la date, qui passerait au 3 novembre. À part cela, je crois comprendre qu'une entente a été conclue.

Monsieur Ramsay.

● (1315)

Jacques Ramsay: D'après l'information que je reçois, nous avons une entente selon laquelle si les choses se compliquent et si l'étude article par article devient trop difficile, nous pourrons toujours suspendre la séance et reprendre plus tard.

[*Français*]

Je ne sais pas si cette possibilité va plaire à Mme DeBellefeuille, mais nous pouvons ajourner la réunion. Ce n'est pas ce que nous voulons. Nous voulons avancer rapidement, mais si ce n'était pas le cas, nous serions évidemment raisonnables. Nous sommes d'accord sur le fait de ne pas commencer l'étude article par article à la quatrième réunion, mais plutôt à la cinquième réunion.

Le président: Très bien, alors c'est ce que je propose de faire. Nous allons voir comment ça se passe, mais si l'horaire ne nous permet pas de traiter l'étude article par article en une seule réunion, nous discuterons de la façon d'aménager l'horaire.

[*Traduction*]

Je demande le consentement pour l'amendement, qui consiste à remplacer « 29 octobre » par « 3 novembre ».

(L'amendement est adopté.)

(La motion modifiée est adoptée. [*Voir le Procès-verbal*])

Le président: Très bien.

Cela nous amène à la deuxième motion à laquelle vous avez fait allusion, monsieur Ramsay.

[*Français*]

Claude DeBellefeuille: Monsieur le président, j'aimerais intervenir.

Le président: Madame DeBellefeuille, la parole est à vous.

Claude DeBellefeuille: Excusez-moi, mais je donne rarement mon consentement quand je ne comprends pas.

Avez-vous disposé de mon amendement?

Le président: Oui, votre changement à propos du 3 novembre a été pris en compte.

Claude DeBellefeuille: Mon amendement proposait le « 3 novembre » et « quatre réunions », et aussi le changement qui est proposé dans le dernier paragraphe de mon amendement. Avez-vous disposé de mon amendement?

Le président: Écoutez, nous pouvons aussi voter sur votre… En fait, pour essayer…

Claude DeBellefeuille: Ça ne me dérange pas. On peut s'arranger, monsieur le président. L'idée, c'est qu'il faut que ce soit clair pour tout le monde, surtout pour le greffier. À la fin de la réunion, nous nous sommes entendus sur quoi au juste? Je crois qu'il y a consensus sur la date du 3 novembre.

Le président: Tout à fait.

Claude DeBellefeuille: Avons-nous aussi gardé la proposition de tenir « un minimum de quatre réunions »?

Jacques Ramsay: Non.

Claude DeBellefeuille: Avons-nous gardé la proposition de ne tenir que quatre réunions?

Le président: Oui, c'est exact.

Claude DeBellefeuille: D'accord. C'est parfait.

Jacques Ramsay: Il y a une possibilité que nous puissions négocier l'ajout d'une cinquième réunion.

Claude DeBellefeuille: Nous sommes en train de disposer de l'amendement que j'ai proposé, monsieur Ramsay, et nous ne pouvons pas le modifier, n'est-ce pas? Je suis d'accord sur le fait de tenir « quatre réunions » et de modifier mon amendement en supprimant « un minimum de », comme je l'avais indiqué.

Quant au dernier changement proposé par mon amendement, il propose de modifier le texte de la motion pour que l'étude article par article commence à la cinquième réunion, sans en limiter le nombre de réunions. Cette proposition est-elle retenue?

Le président: C'est ce qui a été retenu.

Claude DeBellefeuille: C'est parfait.

Le président: Sur le plan procédural, nous aurions dû effectivement voter sur votre amendement, en débattre, proposer un autre amendement…

Claude DeBellefeuille: Oui, mais en ce moment, nous sommes en train de nous entendre à l'amiable.

Le président: … ou un sous-amendement à la suite de votre amendement. Cela aurait peut-être été plus complet, mais plus compliqué aussi sur le plan procédural.

Nous nous sommes entendus sur la modification à la motion de M. Ramsay qui remplace la date du « 29 octobre » par le « 3 novembre ». Nous avons convenu de maintenir la proposition de tenir « quatre réunions », tout en tenant compte du souhait de M. Caputo que le Comité demeure ouvert à l'ajout de réunions en fonction des témoins qui comparaîtront devant le Comité. Il est également proposé de tenir une réunion deux ou quatre jours après la quatrième réunion pour procéder à l'étude article par article. Nous verrons alors comment les choses se passeront et le Comité décidera s'il veut prévoir d'autres réunions pour cette étude article par article.

Claude DeBellefeuille: Parfait. Merci beaucoup, monsieur le président.

Le président: Merci.

Monsieur Ramsay, vous avez la parole.

Jacques Ramsay: Je propose d'étudier le projet de loi C-8 lors de notre prochaine réunion, si vous êtes d'accord.

Le président: D'accord, si tel est votre souhait.

Madame DeBellefeuille, vous voulez intervenir. Vous avez la parole.

Claude DeBellefeuille: Le greffier peut-il nous faire parvenir le libellé de la motion sur lequel nous nous sommes entendus pour éviter de la confusion à la prochaine rencontre?

Le président: Oui.

Le greffier: Le texte de la motion paraîtra dans le Procès-verbal de la réunion.

Claude DeBellefeuille: D'accord. Merci.

Le greffier: Je viens tout juste de faire circuler le texte de la motion relative au projet de loi C-8 dont M. Ramsay donne avis en vue de la prochaine réunion.

Claude DeBellefeuille: Parfait. Merci beaucoup.

Le président: Très bien.

Merci beaucoup, tout le monde, et bon après-midi.