CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

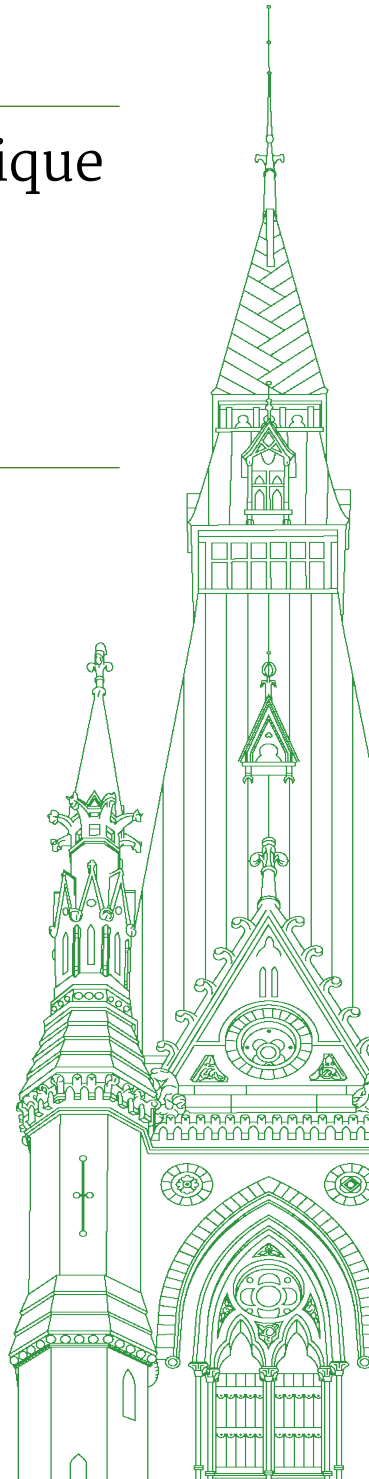
44e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 094

Le lundi 12 février 2024



Président : M. Heath MacDonald

Comité permanent de la sécurité publique et nationale

Le lundi 12 février 2024

● (1600)

[*Traduction*]

Le président (M. Heath MacDonald (Malpeque, Lib.)): La séance est ouverte.

Bienvenue à la 94e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

La réunion d'aujourd'hui se déroule en mode hybride, conformément au Règlement. Des membres sont présents dans la salle et d'autres sont à distance, à l'aide de l'application Zoom.

Je vais faire quelques remarques à l'intention des témoins et des membres du Comité.

Veuillez attendre que je vous donne la parole nommément avant de parler. Afin de prévenir les incidents dus à un effet Larsen, toujours perturbants, les participants sont invités à garder leurs oreillettes loin de tout microphone. Les incidents de rétroaction audio peuvent gravement blesser les interprètes et perturber nos délibérations.

Conformément à l'ordre de renvoi du lundi 27 mars 2023, le Comité reprend son étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et d'autres lois en conséquence.

Nous accueillons deux groupes de témoins aujourd'hui et je vais souhaiter la bienvenue à nos témoins du premier groupe.

Du Commissariat à la protection de la vie privée du Canada, nous accueillons, en personne, M. Philippe Dufresne, commissaire à la protection de la vie privée du Canada. Par vidéoconférence, du Bureau du surintendant des institutions financières, nous avons M. Tolga Yalkin, surintendant auxiliaire, Secteur des mesures de réglementation. De Citizen Lab, nous accueillons Mme Kate Robertson, associée de recherche principale à la Munk School of Global Affairs and Public Policy de l'Université de Toronto.

Bienvenue à tous.

Vous disposerez d'un maximum de cinq minutes pour vos déclarations liminaires, après quoi nous passerons aux questions.

J'invite maintenant M. Dufresne à faire une déclaration liminaire.

Je vous en prie, allez-y.

[*Français*]

M. Philippe Dufresne (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Merci, monsieur le président.

Mesdames et messieurs les membres du Comité, je suis heureux d'être ici pour vous assister dans le cadre de votre étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Au Canada et ailleurs, la cybersécurité est un domaine très important. Les services numériques offerts au moyen de cybersystèmes et de réseaux de télécommunications sont au cœur de notre façon de vivre, de travailler et d'interagir. De plus, ils ont une incidence sur une grande quantité de données et de renseignements personnels. C'est pourquoi il est essentiel de protéger la cyberinfrastructure du Canada contre d'éventuelles menaces.

[*Traduction*]

Parallèlement, nous devons veiller à ce que les efforts déployés pour sécuriser ces systèmes et réseaux protègent et respectent aussi le droit fondamental à la vie privée des Canadiennes et des Canadiens. Il ne s'agit pas d'un jeu à somme nulle: la vie privée et l'intérêt public sont non seulement compatibles, mais ils se renforcent mutuellement. J'appuie fortement les objectifs du projet de loi C-26 et j'estime qu'en tant que société, il est essentiel que nous disposions des outils et de la capacité nécessaires pour satisfaire à ces importants objectifs d'intérêt public.

Au cours de mon témoignage, je vous exposerai les moyens par lesquels je recommande que le projet de loi soit renforcé afin de protéger davantage le droit fondamental à la vie privée et de tenir compte des conséquences possibles sur la vie privée tout en atteignant les importants objectifs du projet de loi.

Selon le projet de loi C-26, toute personne ou entité désignée pourrait recueillir et analyser un large éventail de renseignements, dont des renseignements personnels de nature délicate détenus par des banques, des exploitants de télécommunications et des fournisseurs de services énergétiques. Le projet de loi permettrait aussi l'échange de ces renseignements avec des organisations, comme des organismes de renseignement, des gouvernements provinciaux et étrangers ainsi que des organisations établies par des États étrangers.

● (1605)

[*Français*]

Selon le projet de loi, tel qu'il est rédigé, ces pouvoirs sont larges. Afin d'assurer que les renseignements personnels sont protégés et que la vie privée est traitée comme un droit fondamental, je recommanderais au Comité d'envisager de resserrer les seuils qui encadrent l'exercice de ces pouvoirs et d'imposer des limites plus strictes à l'utilisation de ces pouvoirs. Pour ce faire, on pourrait exiger que toute collecte, utilisation et communication de renseignements personnels respecte les principes de nécessité et de proportionnalité. Il s'agit de principes de base du traitement des renseignements personnels qui sont reconnus à l'échelle internationale.

[*Traduction*]

Obliger les institutions gouvernementales à réaliser des évaluations des facteurs relatifs à la vie privée, les EFVP, et à consulter le Commissariat pour les nouveaux programmes et les nouvelles initiatives créés en vertu des pouvoirs conférés par le projet de loi C-26 permettrait aussi de renforcer la protection de la vie privée et la confiance de la population canadienne, tout en servant l'intérêt public. La réalisation d'une EFVP est actuellement une exigence prévue par la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor, mais elle n'est pas une obligation juridique contraignante sous le régime des lois sur la protection des renseignements personnels. L'EFVP constitue un outil important qui permet de cerner, d'analyser, de traiter et d'atténuer les problèmes relatifs à la protection de la vie privée avant de mettre en œuvre des initiatives, et ainsi permettre de réduire les préjudices involontaires à la vie privée lors du lancement de ces initiatives. C'est pourquoi j'ai recommandé que la réalisation d'une EFVP devienne une obligation juridique pour le gouvernement au titre de la Loi sur la protection des renseignements personnels.

Le projet de loi C-26 permettrait aussi au ministre de l'Innovation, des Sciences et de l'Industrie d'interdire la communication publique de certaines décisions et de certains décrets rendus sous le régime de la Loi proposée. Il importe que ce type de disposition relative à la confidentialité, qui a pour effet de réduire la possibilité d'un examen critique de la part du public concernant la mise en œuvre du projet de loi, notamment toute collecte, utilisation ou communication de renseignements personnels, soit accompagné de mesures appropriées de transparence. Il pourrait s'agir d'exiger du gouvernement qu'il rende compte régulièrement au Parlement ou au Commissariat du nombre, de la nature et de l'objet de tels décrets et décisions, en particulier lorsqu'ils portent sur des renseignements personnels de nature délicate. Cela donnerait l'assurance aux Canadiennes et aux Canadiens que leur vie privée est protégée à tout moment.

[*Français*]

Je recommanderais aussi que le projet de loi soit amendé afin d'inclure des mesures de responsabilité plus rigoureuses en vue d'assurer la protection des renseignements personnels qui sont communiqués à l'extérieur du Canada. Ces mesures pourraient comprendre, par exemple, des mécanismes de contrôle supplémentaires et des critères établis qui doivent être inclus dans les ententes sur les échanges de renseignements avec des gouvernements étrangers, comme des restrictions sur tout transfert ultérieur de renseignements personnels, des mesures de protection établies qui doivent être appliquées et des conséquences en cas de non-conformité.

Pour conclure, je dirai que, si le projet de loi C-26 est adopté, il sera important que le Commissariat dispose de la souplesse dont il aura besoin pour coordonner, le cas échéant, ses activités avec celles des autres organismes de réglementation et de surveillance qui participent aux interventions en cas d'incidents liés à la cybersécurité dans les cas où il pourrait y avoir une atteinte à la sécurité des renseignements personnels.

Sur ce, je serai heureux de répondre à vos questions.

[*Traduction*]

Le président: Merci, monsieur Dufresne.

Monsieur Yalkin, vous êtes le suivant.

M. Tolga Yalkin (surintendant auxiliaire, Secteur des mesures de réglementation, Bureau du surintendant des institutions financières): Merci beaucoup.

[*Français*]

Monsieur le président, mesdames et messieurs les membres du Comité, bonjour.

Compte tenu de son mandat, le Bureau du surintendant des institutions financières, ou BSIF, contribue au maintien de la confiance du public dans le système financier canadien par la réglementation et la surveillance d'environ 400 institutions financières fédérales. À ce titre, nous veillons à ce que les institutions financières conservent une bonne santé financière, évaluent continuellement les risques et les tendances du secteur, et se protègent contre les menaces à leur intégrité ou à leur sécurité, y compris les cybermenaces.

Il ne fait aucun doute que les institutions financières sont ciblées par des cyberattaques. C'est un fait bien noté dans le document intitulé « Regard annuel du BSIF sur le risque », qui est publié en ligne et dans lequel nous soulignons que le cyberrisque est l'un des principaux risques pour la stabilité financière du Canada.

[*Traduction*]

Cela dit, vous ne serez pas surpris d'apprendre que, depuis un certain temps et notre qualité d'organisme de réglementation, nous attendons des institutions financières qu'elles adoptent des pratiques de gestion des risques adaptées face aux cyberrisques. Plus précisément, nous avons pris soin de préciser, dans nos lignes directrices, ce que nous attendons des institutions financières en matière de gestion des risques technologiques et cybernétiques afin de prévenir les pannes et les atteintes à la protection des données, et pour améliorer la résilience globale en matière de technologie et de cybersécurité.

On s'attend également à ce que les institutions financières réagissent rapidement et efficacement aux incidents technologiques et de cybersécurité et, surtout, qu'elles nous informent de chaque événement perturbateur. Leurs déclarations d'incident nous aident vraiment à cerner les domaines dans lesquels les institutions — ou l'industrie en général — doivent prendre des mesures pour prévenir les problèmes.

Nous fournissons en outre des outils aux institutions financières. Notre autoévaluation de la cybersécurité, qui les aide à évaluer leur niveau actuel de préparation à la cybersécurité et à élaborer des pratiques efficaces en matière de cybersécurité, en est un excellent exemple. Il y a aussi notre cadre TCFR — soit le test de la cyberrésilience fondé sur le renseignement —, qui fournit des instructions aux institutions financières sur la façon de mettre en œuvre une approche sophistiquée connue sous le nom « méthode de l'équipe rouge ».

Ces efforts et d'autres sont quant à moi essentiels, car il est indéniable que les cyberattaques continueront d'augmenter en fréquence et en sophistication. De plus, il s'agit d'un environnement à risque qui, d'après notre expérience, évolue rapidement, et le fait de ne pas se protéger contre les risques peut avoir de graves conséquences. Une cyberattaque réussie peut porter atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes, avec pour conséquence une perte de confiance du public, des dommages à la réputation et des pertes financières.

● (1610)

[*Français*]

C'est pourquoi le BSIF est si focalisé sur la promotion d'une bonne gestion des cyberrisques et des risques technologiques au sens large dans l'ensemble des institutions financières fédérales dont il est responsable.

En tant qu'organisme fédéral responsable de la réglementation d'un secteur important, le BSIF est à la disposition du Comité et lui offre son soutien dans le cadre de son étude du projet de loi C-26. Nous voulons contribuer aux efforts visant à améliorer la résilience du système financier du Canada.

Je serai très heureux de répondre aux questions des membres du Comité.

Merci, monsieur le président.

[*Traduction*]

Le président: Merci.

J'invite maintenant Mme Robertson à faire sa déclaration liminaire.

Mme Kate Robertson (associée de recherche principale, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, à titre personnel): Merci, monsieur le président et distingués membres du Comité. Comme vous le savez, j'ai aussi comparu devant le Comité la semaine dernière au sujet de ce projet de loi.

Je suis chercheuse principale au Citizen Lab, qui fait partie de la Munk School of Global Affairs and Public Policy de l'Université de Toronto. J'ai soumis au Comité un mémoire corédigé avec une collègue, Lina Li, de la faculté de droit de McGill, qui s'appuie sur la recherche et l'analyse de mon ancien collègue du Citizen Lab, Christopher Parsons.

Aujourd'hui, je vais reprendre et compléter mes remarques de la semaine dernière.

Tout d'abord, plusieurs préoccupations ont été soulevées au cours de ces audiences au sujet du ciblage malveillant, par exemple, par rançongiciels visant des volets de l'économie qui ne relèvent pas de la responsabilité fédérale, comme les hôpitaux. Le besoin de protection dans d'autres domaines est important, mais le Comité peut aussi être conscient de la portée appropriée de sa responsabilité dans le cadre de son travail sur le projet de loi C-26.

Je remercie les autres témoins qui ont mentionné les menaces actuelles qui pèsent sur la société canadienne. Cependant, ce n'est jamais une bonne idée de légiférer sous la peur. Il s'agit d'une question importante qui exige que tout amendement soit soumis à une diligence raisonnable et à une réflexion minutieuse pour définir ce qu'il convient d'inclure. Je suggère au Comité d'examiner attentivement ce qu'il se propose de faire. S'il était possible de prendre la bonne décision maintenant, on se trouverait à améliorer la sécurité, la sûreté, la protection des renseignements personnels et les droits garantis par la Charte pour tous les Canadiens pendant des décennies. Il est extrêmement important que les législateurs soient réfléchis et nuancés et qu'ils soient la personnification du genre d'amendements qu'ils proposent pour le projet de loi.

Deuxièmement, notre mémoire énonce la recommandation 12 — qui se décline en recommandations 12A à 12C — relative aux procédures de contrôle judiciaire en vertu du projet de loi C-26. Cela comprend la nomination d'avocats spéciaux dans les instances de contrôle judiciaire et la nécessité d'harmoniser le projet de loi C-26 avec les dispositions analogues de la Loi sur la preuve au Canada relativement à la preuve secrète. Ces modifications sont non seulement importantes, mais aussi équitables, simples et sensées.

Enfin, je veux aussi parler de notre recommandation voulant que les entités gouvernementales dotées de nouveaux pouvoirs de collecte et d'échange de renseignements soient tenues de limiter l'utilisation des données recueillies aux seules fins de cybersécurité et d'information.

La collecte ou l'utilisation de renseignements sur des Canadiens ou des personnes se trouvant au Canada — par des organismes de renseignement de sécurité nationale comme le Centre de la sécurité des télécommunications, le CST — est une question fondamentale d'intérêt public et constitutionnelle. La crainte que le CST réaffecte l'information qu'il reçoit aux termes du projet de loi C-26 à ses autres activités de renseignement n'a rien d'hypothétique. Dans de récents rapports, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, indique que le CST ne considère actuellement pas qu'il lui est interdit, en vertu de sa loi constitutive, de modifier la destination de l'information détenue sur les Canadiens dans le cadre de ses mandats.

Cependant, il y a quelques années à peine, dans le projet de loi C-59, le Parlement a établi un équilibre non négligeable en ce qui concerne la nécessité d'imposer des limites importantes, étant donné qu'il est interdit aux organismes de renseignement de diriger leurs activités vers des personnes se trouvant au Canada. Le projet de loi C-26 pourrait porter atteinte à cet important équilibre. À l'heure actuelle, le texte envisage de vastes pouvoirs de collecte et de partage de renseignements concernant des personnes au Canada, voire des pouvoirs secrets. Bien que l'énoncé concernant la Charte du ministère de la Justice au sujet de ce projet de loi fasse référence à l'utilisation possible par le gouvernement de renseignements uniquement techniques et non de renseignements personnels de nature délicate, il n'y a pas de mises en garde ni de mesures de protection pour le préciser dans la loi. Des précisions sont nécessaires.

Les fournisseurs de services de télécommunications, par exemple, sont véritablement les transporteurs des renseignements les plus privés que puisse posséder notre système juridique. Je suis d'accord avec les témoins de l'Autorité canadienne pour les enregistrements Internet, ou ACEI, et d'OpenMedia pour dire qu'il s'agit d'une question fondamentale de confiance du public. Le public ne devrait pas avoir à se demander si le projet de loi du gouvernement sur la cybersécurité ne serait pas en fait un projet de loi concernant l'espionnage, mais sous un nom différent.

Comme l'a souligné M. Hatfield la semaine dernière, l'OSSNR — l'Office de surveillance des activités en matière de sécurité nationale et de renseignement — a signalé un problème chronique dans l'examen de la légalité des activités du CST depuis sa création. Les législateurs devraient faire preuve d'une grande prudence quand ils se demandent si l'octroi de nouveaux pouvoirs supplémentaires est approprié ou nécessaire en vertu du projet de loi C-26, et quels mécanismes de contrôle judiciaire sont nécessaires et adaptés pour protéger la vie privée de tous les Canadiens.

Merci. Je serai heureuse de répondre à vos éventuelles questions.

● (1615)

Le président: Merci, madame Robertson.

Nous allons maintenant passer aux questions.

Nous allons commencer par M. Shipley qui a six minutes.

M. Doug Shipley (Barrie—Springwater—Oro-Medonte, PCC): Merci, monsieur le président.

Je remercie les témoins de leur présence.

Le projet de loi C-26 est une question très importante. Je vais demander un peu de temps à ce sujet. Je n'ai pas l'intention d'empiéter sur le temps de parole de qui que ce soit aujourd'hui, monsieur le président, mais j'aimerais présenter rapidement une motion qui a fait l'objet d'un avis, et j'espère revenir rapidement au projet de loi C-26. La motion est courte.

Je propose:

> Que le Comité reconnaisse que le vol d'autos est un problème pressant auquel sont confrontés les Canadiens et que, conformément à la motion convenue au sujet des vols d'autos le 23 octobre 2023, le Comité commence cette étude le lundi 26 février et y consacre les six réunions du lundi suivantes, tout en réservant ses réunions du jeudi à l'étude du projet de loi C-26. De plus, conformément à la motion convenue concernant les droits des victimes d'actes criminels, reclassement et le transfèrement des délinquants fédéraux le 23 octobre 2023, que le Comité prolonge sa réunion du jeudi 15 février d'une heure supplémentaire et que le ministre soit invité à comparaître pendant les trois heures complètes afin de discuter de toutes les questions liées à son mandat.

Monsieur le président, j'estime que cette description et cette motion justifient que l'on accorde la priorité à une question par ailleurs sérieuse. Je pense que nous sommes tous d'accord pour dire que le vol de voitures est un problème grave.

Nous avons indiqué qu'il fallait essayer d'obtenir un peu plus de temps avec le ministre, parce que celui-ci n'a fait aucun compte rendu au Comité depuis le 30 mai 2023. La dernière fois qu'un ministre est venu pour parler du budget des dépenses, c'était le 19 mai 2022. Le 23 octobre 2023, nous avons tous adopté une motion disant « que le Comité invite immédiatement le ministre de la Sécurité publique et les fonctionnaires du ministère à comparaître pendant deux heures pour discuter de son mandat ». J'espérais regrouper certaines de ces réunions et rentabiliser notre temps. Le ministre pourrait peut-être trouver le temps de nous parler des nombreuses questions urgentes qui se posent actuellement.

Sur ce, je rends la parole, monsieur le président.

● (1620)

Le président: Merci.

Observations?

Madame Michaud, à vous la parole.

[*Français*]

Mme Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Merci, monsieur le président.

J'aimerais parler de la motion, si vous me le permettez.

Cela faisait longtemps que nous avions eu l'occasion de parler d'une motion. Bref, je veux juste mentionner qu'il est tout à fait vrai que le ministre n'est pas encore venu témoigner sur son mandat en général, alors que cela devait être le cas en tout début d'année, et même en milieu d'année 2023, après sa nomination. Je serais donc d'accord sur cette partie de la motion.

Comme j'ai proposé cette étude sur les vols de voiture, je ne suis certainement pas opposée à ce que nous la devancions. Par contre, je veux préciser que ce n'est pas mon intention de retarder l'étude du projet de loi C-26 non plus. Faire les deux en même temps me paraît une proposition assez raisonnable.

Je ne sais pas s'il est prévu de voter sur cette motion aujourd'hui, mais je voterais en faveur de la motion.

[*Traduction*]

Le président: Merci.

Monsieur Julian, je vous en prie.

[*Français*]

M. Peter Julian (New Westminster—Burnaby, NPD): Merci beaucoup, monsieur le président.

J'aimerais souhaiter la bienvenue aux élèves de l'école secondaire de Saint-Hyacinthe. Je les remercie d'être avec nous aujourd'hui.

Je veux souligner que cette motion comporte plusieurs aspects, et je préfère toujours que nous ayons des discussions avec le comité directeur dans ces cas-là. D'abord, je suis tout à fait d'accord pour inviter le ministre, mais il me semble peu probable qu'il puisse changer son horaire de jeudi.

Bien que je trouve important de commencer le plus vite possible l'étude proposée par Mme Michaud, que nous appuyons tous, il y a le fait que nous accumulons du retard dans l'étude du projet de loi C-26. Depuis un mois, nous avons connu plusieurs perturbations à la fois dans les discussions et avec les témoins. À mon avis, nous devons améliorer le projet de loi C-26 sans tarder. Ensuite, nous pourrons procéder à l'étude des vols de voiture, que je trouve importante.

Je vais donc voter contre cette motion, mais je vais la soumettre au comité directeur. Je souhaite d'ailleurs que ce comité tienne une réunion le plus rapidement possible.

Cela étant dit, je trouve important d'établir l'horaire et d'inviter à nouveau le ministre. M. Shipley a raison de dire que le ministre n'est pas venu souvent, et il faut que cela change. Nous pourrons débattre des vols de voiture le plus rapidement possible une fois que nous aurons terminé les discussions sur le projet de loi C-26.

[*Traduction*]

Le président: Merci, monsieur Julian.

Madame O'Connell, s'il vous plaît.

Mme Jennifer O'Connell (Pickering—Uxbridge, Lib.): Merci, monsieur le président.

Je signale simplement que, n'était l'obstruction des conservateurs, nous en aurions fini avec le projet de loi C-26 et nous serions en train de nous occuper du problème des vols de voitures.

S'il s'agissait d'une question aussi grave, les conservateurs n'auraient pas présenté des motions en vertu de la Loi sur les mesures d'urgence — au moins six fois la même, le seul changement étant le nombre de séances — et ils seraient allés droit au but. Ce n'est qu'à la dernière séance que, pour la première fois, un député conservateur a posé aux témoins une question sur le projet de loi C-26. Si c'était un tel sujet de préoccupation, nous aurions déjà commencé à étudier la question des vols de voitures — ce sur quoi portait du reste la motion de Mme Michaud, motion qui faisait l'unanimité.

Il est d'une importance cruciale que nous achevions l'étude du projet de loi C-26 et que nous nous attaquions au problème des vols de voitures, et nous pouvons le faire. Il reste à présenter des amendements, par exemple, et à soumettre le projet de loi à l'étude article par article, mais nous pouvons entretemps nous saisir du problème des vols de voitures.

Je vais simplement confirmer que les ministres, le ministre LeBlanc et le ministre Champagne, doivent comparaître pour parler du projet de loi C-26 le 15 février, et que la présence du ministre LeBlanc est confirmée pour la semaine où nous siégerons en mars. Il sera là en vertu de son mandat, et le greffier en a reçu confirmation. Les deux comparutions sont prévues.

Je signale que le ministre était disponible plus tôt, mais que nous étions alors plongés dans une autre étude. Il a donc été décidé d'inviter d'autres témoins à comparaître avant. Je suis consciente de l'irritation suscitée par le choix de la date de comparution du ministre. Je me suis rétractée, mais sans ces obstructions constantes, le Comité n'en serait pas là.

Nous devons terminer l'étude du projet de loi C-26. Il ne nous reste que deux séances après celle-ci. Les ministres comparaîtront, après quoi il y aura une autre séance, je crois, et puis nous passerons à autre chose. Mais si les conservateurs s'entêtent à présenter des motions pour faire obstruction et s'ils ne tiennent pas à discuter du projet de loi C-26, nous ne pourrons pas nous attaquer à la question des vols de voitures. C'est une honte qu'ils se soient comportés de la sorte, car il s'agit d'un enjeu vraiment important.

J'espère vraiment que nous pourrons achever cette étude et passer au problème des vols de voitures, ce qui a toujours été notre plan. Nous serions déjà en train de l'étudier si les conservateurs n'avaient pas fait perdre son temps au Comité et gaspillé l'argent des contribuables en débattant de motions sur lesquelles ils ne voulaient même pas se prononcer.

● (1625)

Le président: Merci.

Oui, la comparution du ministre est prévue pour le jeudi 21 mars. Nous savons tous que notre calendrier de mars est amputé. Nous nous attendons à ce que le ministre soit là le 21.

Nous sommes saisis d'une motion. Voulez-vous un vote à main levée?

M. Doug Shipley: Un vote par appel nominal, monsieur le président.

Le président: D'accord.

(La motion est rejetée par 6 voix contre 5.)

Le président: Nous allons poursuivre.

Monsieur Gaheer, c'est votre tour de poser des questions.

M. Iqwinder Gaheer (Mississauga—Malton, Lib.): Merci, monsieur le président.

Je remercie les témoins d'avoir pris le temps de venir nous rencontrer.

Ma question s'adresse au commissaire à la protection de la vie privée, M. Dufresne.

Normalement, à quel moment le commissaire à la protection de la vie privée se prononce-t-il sur les projets de loi? Lorsqu'ils sont à l'étude en comité ou au stade de la réglementation?

M. Philippe Dufresne: Nous le faisons à tout moment qui convient. Idéalement, nous espérons être consultés avant la présentation du projet de loi, mais d'habitude, mon bureau et moi-même sommes convoqués par le comité pour faire une recommandation sur un projet de loi. Nous pouvons aussi intervenir au stade de la réglementation et des consultations avec le gouvernement.

M. Iqwinder Gaheer: Simple confirmation: le Commissariat participera-t-il aux consultations sur la réglementation?

M. Philippe Dufresne: Je l'espère. Nous sommes certainement prêts à le faire. Nous nous y attendons et nous demandons au gouvernement de nous faire participer.

M. Iqwinder Gaheer: Jusqu'à maintenant, au cours de l'étude du projet de loi C-26 au Comité, nous avons entendu beaucoup de réactions d'intervenants au sujet du droit à la vie privée et de l'échange de renseignements. Vous avez effleuré le sujet dans votre exposé liminaire. Comment peut-on calmer ces inquiétudes au moyen de la réglementation, surtout lorsqu'il s'agit de données qui vont à l'étranger? Avez-vous des idées?

M. Philippe Dufresne: À propos des données qui vont à l'étranger et sont communiquées à d'autres institutions, je recommande de soumettre à des exigences précises les ententes d'échanges de renseignements de sorte que la raison d'être de cet échange, les dispositions sur la conservation des renseignements et les garanties qui s'y appliquent chez nos partenaires internationaux soient bien énoncées et strictes, et de prévoir un mécanisme de règlement des différends simplement pour assurer une plus grande rigueur et placer des garde-fous dans ces échanges d'information. Les notions de nécessité et de proportionnalité devraient également s'appliquer lorsqu'il s'agit de décider, au départ, s'il faut communiquer l'information.

● (1630)

M. Iqwinder Gaheer: Quel rôle le Commissariat joue-t-il actuellement ou comment ce rôle évoluerait-il en fonction du libellé actuel du projet de loi?

M. Philippe Dufresne: Pour l'heure, le texte ne prévoit aucun rôle pour lui. Son rôle est défini dans la Loi sur la protection des renseignements personnels. Le Commissariat a compétence sur le traitement de l'information par le gouvernement et par le secteur privé.

L'une de nos recommandations veut qu'il y ait davantage de mécanismes pour garantir la transparence afin que nous sachions ce qui se passe, que nous connaissions la nature des renseignements recueillis, communiqués et utilisés pour pouvoir exercer nos pouvoirs à cet égard.

Quant aux rapports, le projet de loi prévoit en des termes généraux que le ministre publie un rapport annuel. Nous recommandons que cette disposition soit plus précise et détaillée.

Nous pourrions également collaborer avec les organismes de réglementation en cas d'atteintes et d'incidents cybernétiques. Je recommande entre autres qu'on nous accorde la capacité de collaborer avec les organismes de réglementation et, au besoin, d'échanger des renseignements et de collaborer lorsque des cyberincidents touchent des renseignements personnels. Nous savons que c'est une grande préoccupation pour les Canadiens.

M. Iqwinder Gaheer: Vous en avez dit un mot dans votre exposé liminaire. Je voudrais y revenir une fois de plus. J'ai l'impression que vous souhaiteriez obtenir des compétences plus larges, à la lumière de ce qui est proposé dans le projet de loi. Sur quels autres éléments voudriez-vous exercer une surveillance?

M. Philippe Dufresne: Je ne propose pas que le projet de loi nous confie un rôle de surveillance, mais plutôt qu'on nous communique l'information voulue pour que nous puissions exercer le mandat qui est le nôtre en vertu de la Loi sur la protection des renseignements personnels dans les secteurs public et privé.

J'ai recommandé notamment que soient obligatoires les évaluations de l'impact sur les renseignements personnels et que je sois consulté à ce propos pour que le Commissariat puisse informer et conseiller les ministères, car lorsque ces questions sont abordées dès le départ, il est possible d'apporter des correctifs avant que ne surgissent des problèmes qui risquent de miner la confiance des Canadiens.

Ce n'est pas tant le fait que le Commissariat serait l'organisme de réglementation; dans bien des cas, il n'aurait pas ce rôle.

Prenons l'exemple de l'ancien projet de loi C-11, qui relève du CRTC. C'est lui qui a compétence, mais nous pouvons donner notre avis, et le projet de loi reconnaît que la protection de la vie privée est un facteur à prendre en compte.

M. Iqwinder Gaheer: Merci.

C'est toujours un plaisir de vous accueillir au Comité.

Le président: Merci, monsieur Gaheer.

C'est maintenant le tour de Mme Michaud.

Je vous en prie. Vous avez six minutes.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Je remercie les témoins d'être avec nous.

Monsieur Dufresne, dans votre allocution d'ouverture, vous avez parlé de vos craintes relativement à la protection de la vie privée. En fait, la majorité des témoins que nous recevons mentionnent avoir cette même crainte.

Vous faites une recommandation différente de celle de la plupart des autres témoins, soit qu'il faut consulter le Commissariat à la protection de la vie privée du Canada. Le mandat du Commissariat est le suivant: « Le Commissariat [...] veille au respect de la Loi sur la protection des renseignements personnels, laquelle porte sur les pratiques de traitement des renseignements personnels utilisées par les ministères et organismes fédéraux, et de la Loi sur la protection des renseignements personnels et les documents électroniques [...] »

Dans le cadre du projet de loi C-26, s'il devient une loi, vous proposez que le ministère de la Sécurité publique ou le ministre responsable vous consulte.

Dans le cas d'autres projets de loi, un ministère ou un ministre vous consulte-t-il parfois lorsqu'il est question de la protection de la vie privée? Si oui, pouvez-vous nous donner des exemples? Cela nous donnerait une idée de la façon dont cela fonctionnerait dans ce cas-ci.

M. Philippe Dufresne: D'accord.

Ce sur quoi nous nous penchons, ce sont les activités qui ont des répercussions sur la vie privée. Les questions de sécurité ne font pas partie de notre mandat si elles ne concernent pas la vie privée. On ne cherche pas à élargir notre mandat.

Selon une politique du Conseil du Trésor, les ministères devraient nous consulter lorsque des activités ou des projets pourraient avoir une incidence sur la vie privée des Canadiens. Ce n'est pas toujours fait. Il s'agit d'une politique, et non d'une obligation juridique. Nous recommandons que ce soit intégré dans la Loi sur la protection des renseignements personnels.

Dans certaines situations, nous avons travaillé avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, par exemple, pour examiner les pratiques des ministères et le transfert d'information en matière de vie privée. Il y avait alors une question de sécurité et une question de vie privée.

En collaboration avec mes collègues du Bureau de la concurrence du Canada et du Conseil de la radiodiffusion et des télécommunications canadiennes, ou CRTC, nous avons créé le Forum canadien de réglementation numérique après avoir constaté qu'il existait un chevauchement, ou une zone grise, dans beaucoup de domaines. En effet, certains aspects des activités peuvent toucher la concurrence, la vie privée et la radiodiffusion. Nous voulons donc coordonner nos activités pour qu'il n'y ait pas de contradictions.

Nous recommandons que, s'il existe une possibilité que la vie privée soit touchée, mon commissariat soit tenu au courant. Ce serait non seulement bénéfique de le faire, mais cela permettrait aussi de rassurer les Canadiens.

● (1635)

Mme Kristina Michaud: Cette partie de l'explication est extrêmement intéressante, particulièrement quand vous parlez de rassurer les gens.

Selon ce que je comprends, s'il s'agit seulement d'une recommandation, le ministère ou le ministre en question ne serait pas nécessairement obligé de vous consulter, alors que, si on inclut cette obligation dans la Loi, par suite d'un amendement au projet de loi, par exemple, cela contraindrait le ministre ou le ministère à vous consulter.

Ai-je bien compris?

M. Philippe Dufresne: C'est tout à fait exact. Si c'est dans la Loi, c'est une obligation juridique. À ce moment-là, les ministères doivent le faire.

Mme Kristina Michaud: Vous avez également parlé de mécanismes de contrôle supplémentaires. C'est une question assez importante, qui revient souvent. Certaines craintes ont été exprimées quant au fait de confier au ministre le pouvoir de prendre un décret ou un arrêté, parce qu'on n'a pas la moindre idée de ce que cela peut représenter.

On peut confier des pouvoirs aux ministres, mais on sait que la Chambre et les parlementaires n'ont pas nécessairement le contrôle sur tout ce qui est fait dans le cadre d'une réglementation. C'est vraiment du ressort du gouvernement.

Selon vous, comment pourrait-on mieux encadrer cela pour assurer la protection de la vie privée.

M. Philippe Dufresne: On peut le faire en incorporant des critères de nécessité et de proportionnalité, et c'est ce dernier aspect qui manque. Le critère de nécessité se trouve dans la Loi. Par exemple, certaines dispositions sont libellées de telle sorte que, si le ministre est d'avis qu'il est nécessaire d'agir, il en a le pouvoir. On parle aussi de pertinence sur certains plans.

La notion de proportionnalité est importante. On peut dire qu'on a besoin du critère de nécessité et qu'elle contribue à atteindre l'objectif. Pour ce qui est de la proportionnalité, il faut déterminer si on a vraiment vérifié s'il s'agit de la méthode la moins intrusive relativement à la vie privée des gens. C'est un peu semblable à l'analyse qu'on fait en vertu de la Charte, soit avoir cet équilibre.

Une telle démarche permettrait d'incorporer ces éléments de nécessité et de proportionnalité, qui sont vraiment cruciaux dans le domaine de la vie privée. C'est le cas à l'échelle internationale et pour certains pays, comme l'Australie, les États-Unis ou la Grande-Bretagne. Ces derniers ont certains éléments plus précis par rapport au fait de considérer la vie privée ou les autres options.

Nous ne voulons pas empêcher le ministre de faire son travail. Ce n'est absolument pas le cas. Comme je l'ai dit, j'appuie fortement les objectifs, mais il faudrait imposer l'obligation d'avoir cette réflexion, surtout quand la question touche la vie privée des gens.

Mme Kristina Michaud: Je vous remercie.

Avez-vous d'autres éléments dont vous aimeriez nous faire part, toujours dans le contexte de protection de la vie privée, et qui pourraient contribuer à rassurer les gens ou les entreprises et les organisations qui devront se conformer à cette loi, si elle est promulguée?

En fait, certains ont exprimé des préoccupations en disant que cela pourrait donner lieu à une charge de travail supplémentaire et à une bureaucratie accrue. Il y a aussi des craintes concernant l'échange d'information.

M. Philippe Dufresne: Je pense que les recommandations que j'ai faites dans mon allocution visent toutes à rassurer les Canadiens et les Canadiennes, ainsi que les petites ou moyennes entreprises, ou PME. Les institutions sont là pour les aider. On ne délègue pas entièrement le travail aux individus ou aux PME.

Prenons, par exemple, les évaluations des facteurs relatifs à la vie privée. Si la réflexion est obligatoire et que l'on consulte mon bureau à cet égard, cela permettra de rassurer les gens. Ils comprendront qu'il existe une fonction de contrôle, que le commissaire est au courant, qu'il peut faire des recommandations et que, au besoin, il peut formuler des plaintes ou faire des recommandations.

Il y a la question de la transparence, c'est-à-dire...

[*Traduction*]

Le président: Merci, madame Michaud. Votre temps de parole est écoulé.

Monsieur Julian, à vous.

[*Français*]

M. Peter Julian: Merci beaucoup, monsieur le président.

Merci, monsieur Dufresne, pour les services que vous avez rendus à la Chambre des communes à titre de légiste et de conseiller parlementaire, ainsi que pour le travail que vous faites maintenant dans votre rôle de commissaire à la protection de la vie privée du Canada.

Je remercie également tous les témoins de l'information dont ils viennent de nous faire part.

Monsieur le commissaire, j'aimerais vous poser deux questions.

Vous avez mentionné l'importance d'inclure dans le projet de loi C-26 une obligation pour les organisations gouvernementales de réaliser des évaluations des facteurs relatifs à la vie privée.

D'abord, des organismes gouvernementaux ou non gouvernementaux vous ont-ils déjà consulté? Ce projet de loi a tout de même été déposé en juin 2022, alors c'est certain qu'il y aura des répercussions.

Ensuite, une organisation quelconque vous a-t-elle consulté pour savoir comment faire ces évaluations et quelles seront les répercussions du projet de loi C-26?

● (1640)

M. Philippe Dufresne: Pour le moment, le projet de loi C-26 ne comprend aucune obligation de réaliser des évaluations. Cependant, il y a une obligation suivant la politique du Conseil du Trésor. Nous avons des consultations avec des ministères de façon régulière. J'ai un bureau de service-conseil auprès du gouvernement et des ministères, et ils reçoivent des avis à cet égard.

Parfois, ces évaluations sont faites tardivement, après que l'outil a été utilisé. D'ailleurs, j'ai récemment témoigné devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique à ce sujet.

Lorsque les Canadiens et les Canadiennes apprennent qu'on utilise un outil ou qu'on crée un programme sans évaluations préalables, cela peut miner leur confiance. C'est pourquoi ces évaluations devraient être faites dès le départ.

De plus, le fait que mon bureau est consulté devrait être connu. Ainsi, quand l'information devient publique, les gens savent que la consultation a été faite et qu'il y a eu des échanges et des avis.

C'est ce que je souhaiterais voir dans le cas du projet de loi C-26, entre autres choses, étant donné l'effet potentiel de ces pouvoirs.

M. Peter Julian: Merci beaucoup.

J'aimerais vous poser une dernière question.

Quelles sont les meilleures pratiques en matière de protection de la vie privée dans d'autres pays pour empêcher que des renseignements personnels soient communiqués à l'étranger?

M. Philippe Dufresne: En fait, des renseignements peuvent être communiqués à l'étranger, pourvu que cela se fasse en fonction d'ententes légitimes assorties de conditions. Par exemple, le modèle européen exige que les lois et les mécanismes soient équivalents à ce qui existe en Europe. Au Canada, la loi exige que ce soit équivalent à ce qui existe ici, l'échange de renseignements pouvant peut-être se faire sur une base contractuelle.

C'est pourquoi nous recommandons, avant d'échanger des données avec des organismes d'autres pays, d'inclure dans la Loi une obligation de préciser les pratiques de rétention, les critères de nécessité et de proportionnalité, ainsi que les mesures de sécurité. Nous ne voulons pas que ces données soient elles-mêmes la cible de cyberattaques.

M. Peter Julian: Merci beaucoup.

[*Traduction*]

Je m'adresse à vous, monsieur Yalkin.

Vous avez soulevé des enjeux importants pour le BSIF, le Bureau du surintendant des institutions financières. J'ai deux questions à vous poser.

Tout d'abord, avez-vous été consultés au sujet du projet de loi C-26? Le secteur bancaire a-t-il été consulté avant ou après la présentation du projet de loi?

Deuxièmement, combien de cyberattaques y a-t-il eu contre les institutions financières visées par le mandat du BSIF? Combien y a-t-il eu de cyberattaques en 2023? Ce nombre est-il à la hausse, à la baisse ou stable?

M. Tolga Yalkin: Monsieur le président, le ministère de la Sécurité publique nous a consultés au sujet du projet de loi. Pour ce qui est des consultations avec d'autres intervenants, je lui laisse le soin de répondre à ces questions.

Si le projet de loi est adopté, nous souhaiterons évidemment collaborer avec le ministère de la Sécurité publique à l'élaboration du règlement. Nous nous attendons à ce que le secteur bancaire puisse participer.

Quant à la fréquence et à la gravité des cyberincidents, je peux vous donner quelques renseignements, car nous avons un protocole de signalement que les institutions financières sont censées suivre. Elles nous signalent dans les 24 heures tout incident de nature technologique ou cyberincident.

Nous avons constaté une augmentation du nombre des incidents. En 2022, je crois que nous avons eu 10 incidents qualifiés d'incidents de priorité 1, mais nous avons constaté une hausse importante du nombre de ces incidents en 2023. Il a presque triplé pour atteindre environ 28 en 2023. Essentiellement, de 2022 à 2023, nous avons eu un certain nombre d'incidents aux conséquences plus lourdes. Cela représente une évolution importante de notre point de vue, en tant qu'organisme qui applique des règles de prudence.

M. Peter Julian: Je vais passer à Mme Robertson, mais au préalable, comment définit-on les cyberattaques ou les cyberincidents de priorité 1? Il serait très utile que vous en informiez le Comité. Un de mes collègues voudra peut-être reprendre la question.

Madame Robertson, vous avez souligné dans votre document qu'il était important d'avoir un avocat spécial. Pourriez-vous nous expliquer un peu plus en quoi cela a de l'importance dans le projet de loi?

● (1645)

Mme Kate Robertson: Oui, bien sûr.

La nomination d'avocats spéciaux vise à rendre plus équitables les audiences à huis clos qui portent sur des preuves secrètes sans compromettre la capacité du Canada de protéger les renseignements de sécurité. Ces avocats protègent l'équité pour la partie qui est exclue de l'audience à huis clos, ainsi que le droit du public à la liberté d'expression, en veillant à ce que le secret dans les procédures judiciaires soit nécessairement justifié.

Les avocats spéciaux peuvent soit contester le degré de secret que le gouvernement souhaite à l'égard de la preuve, soit vérifier, avec une diligence raisonnable et par des arguments contradictoires, si la preuve que le gouvernement veut invoquer est suffisante, a le poids voulu et est pertinente. Les tribunaux ont depuis très longtemps recours aux avocats spéciaux pour protéger la transparence des tribunaux ainsi que l'équité des procédures.

Le président: Merci, madame Robertson.

Merci, monsieur Julian.

Nous passons maintenant au deuxième tour.

Monsieur Lloyd, vous avez cinq minutes.

M. Dane Lloyd (Sturgeon River—Parkland, PCC): Merci, monsieur le président.

Je vais poser directement mes questions, en commençant par Mme Robertson.

Nous discutons ici des renseignements personnels des Canadiens et de la communication d'information. Tout cela peut sembler un peu abstrait. Pouvez-vous nous donner des exemples hypothétiques? Quels sont les renseignements dont vous craignez qu'ils ne soient communiqués de façon inacceptable entre organismes?

Mme Kate Robertson: L'étendue des pouvoirs de collecte et de communication est telle que la liste des cas hypothétiques concernant les fournisseurs d'infrastructures essentielles et de services de télécommunications pourrait être très longue.

Voici tout de même un exemple hypothétique. Il est possible que le ministre puisse obliger les fournisseurs de services de télécommunication à fournir des renseignements sur les abonnés qui utilisent les réseaux de télécommunication de façon anonyme dans des circonstances qui ont fait l'objet des directives de la Cour suprême du Canada parce qu'il est important de protéger ce type de renseignement personnel. Le projet de loi ne semble prévoir aucune restriction empêchant que ces renseignements ne soient communiqués à d'autres organismes gouvernementaux qui y sont mentionnés et qu'ils puissent être utilisés pour d'autres éléments de leur mandat, par exemple pour aider des organismes fédéraux chargés de l'exécution de la loi.

M. Dane Lloyd: J'ai lu qu'en vertu de cette loi et de la révision législative, le ministre n'a même pas à faire connaître ces décrets. Ils peuvent être confidentiels. Habituellement, ils doivent être publiés dans la *Gazette du Canada*, où tout le monde peut les consulter. Cependant, le ministre peut ordonner qu'ils n'y soient pas publiés.

Êtes-vous en train de dire qu'il pourrait arriver que des citoyens canadiens soient visés par des décrets relatifs aux télécommunications prévoyant la communication de renseignements personnels sans qu'ils sachent ce qui se passe, sans qu'ils aient le moindre recours pour savoir ce qui leur arrive?

Mme Kate Robertson: Oui. C'est la conséquence du fait que rien, dans le projet de loi C-26, n'exige qu'on rende les décrets publics ni ne donne des avis.

Nous avons recommandé dans notre mémoire que les contraintes relatives au secret soient définies et strictement limitées à ce qui est absolument nécessaire. On trouve dans le projet de loi un libellé qui permet un amendement en ce sens, sans oublier l'obligation d'aviser les personnes en cause, ce qui est une fonction essentielle des mécanismes d'examen nécessaires pour pareil pouvoir de collecte et de communication de données.

M. Dane Lloyd: Même si la personne visée par le décret apprenait que ces renseignements sont exigés du fournisseur de services de télécommunications et estimait que c'est injuste et voulait traîner le gouvernement devant les tribunaux, le projet de loi permet au gouvernement de tenir ces audiences en secret et d'échapper à l'obligation de communiquer l'information à cette personne. Est-ce exact? Pouvez-vous nous expliquer plus en détail comment cela fonctionne?

Mme Kate Robertson: Oui. Si un particulier ou une institution veut contester les pouvoirs ou les décrets relatifs à la collecte de renseignements prévus par le projet de loi C-26, il existe un mécanisme de contrôle judiciaire. Il y a d'autres procédures de plainte qui sont disponibles en droit en dehors du projet de loi C-26.

En l'espèce, le secret de la preuve est envisagé. Le projet de loi contient un passage à ce sujet. À la différence du pouvoir apparemment illimité du ministre de garder les décrets secrets, il s'y trouve au moins un certain libellé au sujet du secret de la preuve. Néanmoins, nous avons recommandé de le rendre plus strict et de le faire mieux correspondre aux dispositions de la Loi sur la preuve au Canada, car il n'y a aucune raison de diluer cette exigence ou la capacité du tribunal de concilier l'intérêt public pour la divulgation et l'intérêt du gouvernement pour la préservation de la confidentialité. C'est essentiel, à notre avis, à la constitutionnalité du régime.

● (1650)

M. Dane Lloyd: Merci.

Il pourrait y avoir des circonstances très convaincantes et extraordinaires où le gouvernement devrait garder certains renseignements secrets, mais nous refusons que soit adoptée une loi qui donne des pouvoirs trop vastes dont on pourrait abuser, si bonnes soient les intentions de ceux qui adoptent le projet de loi.

Ma dernière question s'adresse au commissaire à la protection de la vie privée. Dans les 30 secondes qu'il me reste, je lui demande quel genre de renseignements personnels risquent d'être communiqués de façon inacceptable en vertu de ce projet de loi?

M. Philippe Dufresne: Ce sont les renseignements sur les comptes des abonnés, les données de communication, les visites sur les sites Web, les métadonnées, les données de localisation et les données financières qui ne sont peut-être pas ce qui est demandé au bout du compte, mais nous voulons nous assurer que le projet de loi n'autorise pas la communication de ces données.

Nous recommandons l'application de la notion de nécessité et de proportionnalité, qui apporterait de la rigueur: « Vous avez peut-être besoin de ces renseignements, mais il faut aussi voir s'il y a des moyens moins intrusifs d'atteindre l'objectif visé. »

Le président: Merci.

Merci, monsieur Lloyd.

Nous allons passer à M. Schiefke, qui est en ligne. Merci.

M. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Merci beaucoup, monsieur le président.

Moi aussi, je tiens à remercier les témoins d'être là.

J'ai des questions à poser à M. Yalkin, puis à Mme Robertson.

Je vais commencer par M. Yalkin. Quels nouveaux pouvoirs et responsabilités cette loi confère-t-elle au Bureau du surintendant des institutions financières?

M. Tolga Yalkin: Bien des choses dépendraient de la réglementation, mais le Comité n'est pas sans savoir qu'on attend un certain nombre de résultats du projet de loi concernant l'identification, la gestion, la prévention, la détection et la limitation des préjudices causés par les cyberattaques. Nous sommes déjà très actifs dans bon nombre de ces domaines, et nous disposons de nombreux leviers dans notre travail de surveillance pour essayer d'encourager les institutions financières à répondre à ces différentes attentes.

La différence, ici, c'est que si le projet de loi et la réglementation étaient adoptés, on aurait des attentes différentes qui auraient force de loi et la réglementation s'appliquerait, au lieu qu'on s'en remette à notre surveillance comme levier pour encourager de bonnes pratiques.

Quant aux détails concernant ces différents leviers, d'autres seraient sans doute mieux placés que moi pour en parler.

M. Peter Schiefke: Merci.

Vous avez parlé plus tôt des rapports qui vous ont été communiqués au sujet des cyberattaques. Ces renseignements vous ont-ils été communiqués volontairement ou était-il obligatoire de les transmettre?

M. Tolga Yalkin: Nous avons un protocole de signalement des incidents qui établit nos attentes à l'égard des institutions financières: quand et comment faut-il signaler les incidents. En un sens, on pourrait dire que la communication est volontaire, mais je vais vous donner un peu de contexte, si vous me le permettez.

M. Peter Schiefke: Je vous en prie.

M. Tolga Yalkin: En tant qu'organisme de réglementation qui applique des règles de prudence, nous avons la responsabilité générale de surveiller les institutions financières et de veiller à ce qu'elles adoptent de saines pratiques de gestion des risques. Au lieu de prendre des règlements qui ont force de loi, nous énonçons nos attentes et exerçons ensuite une surveillance.

Lorsque, par exemple, nous publions un protocole de signalement que nous avons mis en place, le plus souvent, les institutions financières s'y conforment, car si elles ne le font pas, nous pourrions considérer que cette négligence pourrait donner lieu à une surveillance soutenue de notre part.

M. Peter Schiefke: D'accord.

Le projet de loi prévoit des mécanismes de signalement obligatoire. Êtes-vous d'accord sur ces mécanismes? Pourquoi la déclaration obligatoire est-elle importante?

M. Tolga Yalkin: Ce que le projet de loi prévoit diffère quelque peu du dispositif en place pour les signalements. En vertu de notre protocole, les banques nous font rapport. Si un incident se produit, nous avons un mécanisme qui leur permet de nous le signaler dans les 24 heures.

Aux termes du projet de loi, les signalements seraient transmis à un centre de cybersécurité, de sorte qu'il y aurait essentiellement un double signalement. Il faudrait voir par exemple comment nous pouvons faciliter un signalement efficace et efficient, car nous avons un formulaire de déclaration et il y en aurait sans aucun doute un aussi dans ce régime particulier. C'est une question que nous pourrions régler avec les banques pour faire en sorte que les attentes en matière de rapports soient claires pour les deux entités du gouvernement.

M. Peter Schiefke: Merci, monsieur Yalkin.

Je vais maintenant m'adresser à Mme Robertson. Merci d'être parmi nous.

J'aimerais beaucoup en savoir plus sur les mécanismes de surveillance que vous souhaitez. Vous en avez parlé plus tôt en répondant à des questions. Pouvez-vous étoffer davantage et peut-être nous dire comment le projet de loi C-26 recoupe la Loi sur la protection des renseignements personnels?

Y a-t-il quelque chose qui vous semble faire problème? Comment le Comité peut-il atténuer les difficultés? Que pouvons-nous faire?

● (1655)

Mme Kate Robertson: Il y a un certain nombre de recommandations, dont celles que j'ai décrites à ma dernière comparution et au cours des délibérations d'aujourd'hui, en plus de celles que le commissaire Dufresne a évoquées.

Nous avons formulé des recommandations concernant la nécessité d'établir des limites de proportionnalité et de raisonnabilité comme cadre général pour guider le ministre et le gouvernement dans l'application du projet de loi, mais aussi les mécanismes de surveillance qui devraient protéger le droit à la vie privée et les autres intérêts en jeu dans ce type de loi.

Nous avons recommandé que la loi officialise le rôle des organismes de réglementation indépendants dans l'évaluation du critère de proportionnalité lorsqu'il s'agit d'examiner les décrets qui pourraient être pris en vertu de la loi.

Compte tenu de la nature vraiment vaste des types de droits à la vie privée qui sont en jeu dans les institutions en cause, y compris chez les fournisseurs de services de télécommunication, nous avons recommandé, en tenant compte des obligations constitutionnelles du gouvernement lorsqu'il légifère, que la surveillance judiciaire s'applique aux renseignements personnels, aux renseignements anonymisés dont on peut raisonnablement s'attendre qu'ils sont protégés. Cela ne se trouve pas en ce moment dans le projet de loi.

M. Peter Schiefke: Merci, monsieur le président, et merci à vous, madame Robertson et monsieur Yalkin.

Le président: Merci, madame Robertson.

Nous allons passer à Mme Michaud, qui aura deux minutes et demie, puis M. Julian sera le dernier à prendre la parole. Il aura aussi deux minutes et demie, mais je devrai l'interrompre assez fermement parce que nous arrivons à la fin de la période prévue.

Madame Michaud, à vous.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Madame Robertson, je vous souhaite la bienvenue au Comité.

Le mémoire que vous avez déposé au Comité contient plusieurs recommandations, et nous vous en remercions. C'est très utile pour nous.

Vous avez recommandé la création d'un mécanisme par lequel les petits fournisseurs de services de télécommunication, par exemple ceux comptant moins de 250 000 ou 500 000 abonnés ou clients et qui ont toujours été consciencieux dans leurs ententes de sécurité, peuvent demander au moins un allégement temporaire s'ils sont tenus d'entreprendre de nouvelles pratiques commerciales ou organisationnelles, de modifier celles-ci ou de cesser leurs pratiques commerciales ou organisationnelles en cours à la suite d'une demande, d'un décret ou d'un règlement du gouvernement.

Pouvez-vous nous en dire un peu plus à cet égard? À quelques reprises, j'ai demandé aux différents intervenants que nous avons reçus si les PME avaient des inquiétudes pour ce qui est de se conformer à de telles exigences dans la loi. En effet, cela représente peut-être plus de bureaucratie et une charge supplémentaire de travail pour ces entreprises.

Cela dit, c'est un peu inquiétant de voir que le gouvernement pourrait les forcer à cesser complètement leurs pratiques commerciales. Cela fait peut-être partie des pouvoirs de prendre des décrets qu'ont le ministre de l'Innovation, des Sciences et de l'Industrie et les ministres visés par le projet de loi.

Je m'interroge sur l'étendue des pouvoirs du ministre. Je vous pose donc la question que j'ai posée à M. Dufresne tout à l'heure: comment pouvons-nous encadrer davantage ces pouvoirs?

[*Traduction*]

Mme Kate Robertson: Je vous remercie de la question. Veuillez m'excuser de répondre en anglais.

Nos recommandations ont un lien avec les répercussions du projet de loi sur les politiques d'intérêt public et les risques constitutionnels relatifs aux répercussions sur l'équité ou à la discrimination dans l'exercice du pouvoir de prendre des décrets. Quant à la nécessité de normes pour les fournisseurs de services de télécommunications, pour protéger la sécurité des Canadiens, elles sont absolument nécessaires et doivent s'appliquer également à toutes les plateformes. Il y a cependant des répercussions possibles pour les Canadiens de certaines régions, notamment dans les collectivités rurales ou autochtones, qui pourraient souffrir des répercussions négatives du fait que les petits fournisseurs secondaires ne sont pas en mesure de maintenir leur viabilité en mettant en place des mesures de sécurité.

Nous avons constaté que le CRTC a jugé récemment que la concurrence a diminué au Canada pendant plusieurs années successives. C'est particulièrement le cas au Québec et en Ontario, où les reculs ont été les plus importants. C'est donc là que nous avons cerné le besoin d'un juste équilibre.

Le président: Merci, madame Robertson et madame Michaud.

Monsieur Julian, vous avez la parole pour deux minutes et demie.

● (1700)

[*Français*]

M. Peter Julian: Merci, monsieur le président.

Monsieur Dufresne, tout à l'heure, j'ai posé une question sur les renseignements qui sont transmis à l'extérieur des frontières d'un pays.

En fait, je voulais savoir quel pays pourrait servir de modèle quant à la protection de la vie privée?

M. Philippe Dufresne: Il y a plusieurs modèles. J'hésiterais à en désigner un comme étant le meilleur.

Ce que je peux dire, c'est que le modèle européen, par exemple, présente les attentes importantes en matière de vie privée, soit les critères de nécessité, de proportionnalité et de transparence, et il accorde un rôle important aux organismes consacrés à la protection des renseignements personnels. De plus, dans ce modèle, on exige que les autres pays aient un régime adéquat. Il y a une évaluation de ces pays. D'ailleurs, le Canada vient récemment de recevoir le statut de pays assurant un niveau de protection adéquat. Ce modèle fait en sorte de forcer l'application rigoureuse de ces critères.

D'autres pays concluent des ententes ou signent des traités pour y arriver. Le Québec a adopté la Loi 25. Cette loi prévoit l'obligation d'effectuer une évaluation des facteurs relatifs à la vie privée lorsque des données sont communiquées à l'extérieur du Québec.

Ce sont tous des exemples de discipline et de rigueur. Il faut penser à la vie privée dès le début, dès que l'on conçoit une initiative, dès que l'on décide d'utiliser un outil.

M. Peter Julian: Merci beaucoup, monsieur Dufresne.

[*Traduction*]

Monsieur Yalkin, vous avez dit plus tôt qu'en 2022, il y a eu 10 cyberincidents de priorité 1. En 2023, ce nombre est passé à 30. Comment décririez-vous une cyberattaque de priorité 1? Quelle est la différence entre ce niveau de cyberattaque et les autres niveaux?

M. Tolga Yalkin: Les incidents de priorité 1 sont essentiellement des incidents ayant un grand impact et qui entraînent une interruption du service ou une fuite de données. Tout ce qui répond à cette définition constitue un incident de priorité 1 et nous est donc signalé.

M. Peter Julian: À l'heure actuelle, nous sommes témoins d'un incident de cette ampleur toutes les deux semaines ou moins. Êtes-vous préoccupé par l'augmentation de ce nombre d'incidents? Comme certains témoins l'ont dit, si nous ne mettons pas en place des protections, par exemple avec le projet de loi C-26, les institutions financières canadiennes pourraient être de plus en plus ciblées.

M. Tolga Yalkin: Nous sommes préoccupés par l'augmentation de ce nombre. Nous suivons la situation de très près et nous avons hâte de voir si la tendance se maintiendra. C'est un élément de risque pour les institutions financières. Nous l'avons décrit dans notre aperçu annuel des risques, publié sur notre site Web, et les cyberrisques et les cyberattaques sont au nombre de ces risques.

Le président: Merci. S'il y a de l'information que, à votre avis, M. Julian voudrait recevoir en réponse à sa question, veuillez la lui transmettre.

Je tiens à remercier tous les témoins. Nous vous sommes reconnaissants du temps précieux que vous nous avez accordé. C'est un sujet très important.

Nous allons suspendre la séance pendant environ cinq minutes, le temps que les prochains témoins s'installent.

Merci.

● (1700)

(Pause)

● (1705)

Le président: Je souhaite la bienvenue au deuxième groupe de témoins.

Nous accueillons en personne Eric Smith, vice-président principal, et Robert Ghiz, président et chef de la direction, de l'Association canadienne des télécommunications. Par vidéoconférence, nous accueillons Angelina Mason, avocate en chef et vice-présidente principale, Affaires juridiques et risque, et Charles Docherty, avocat en chef adjoint et vice-président, Affaires juridiques et risque, de l'Association des banquiers canadiens. Nous accueillons enfin Andrew Clement, professeur émérite, Faculté d'information, Université de Toronto, qui témoigne à titre personnel.

Vous avez un maximum de cinq minutes pour faire votre exposé liminaire, après quoi nous passerons aux questions.

Nous allons commencer par vous, monsieur Ghiz.

M. Robert Ghiz (président et chef de la direction, Association canadienne des télécommunications): Merci, monsieur le président.

Bonsoir. Je m'appelle donc Robert Ghiz. Je suis président et chef de la direction de l'Association canadienne des télécommunications, et je suis accompagné de notre vice-président principal, Eric Smith.

[*Français*]

L'Association canadienne des télécommunications a pour objectif de bâtir un avenir meilleur pour les Canadiens grâce à la connectivité. Notre association comprend des fournisseurs de services, des fabricants et d'autres organisations qui investissent dans les réseaux de télécommunications de classe mondiale du Canada.

Nous sommes heureux de pouvoir prendre la parole devant vous aujourd'hui pour vous présenter le point de vue de notre association sur le projet de loi C-26.

● (1710)

[*Traduction*]

La sécurité du système de télécommunications du Canada est fondamentale. Nos membres reconnaissent que leurs services sont essentiels au bien-être social et économique des Canadiens, ainsi qu'à leur sécurité. Par conséquent, ils investissent des ressources importantes pour protéger leurs systèmes et leurs infrastructures contre les cyberattaques et d'autres menaces.

En outre, nos membres participent activement aux activités du Comité consultatif canadien sur la sécurité des télécommunications, ou CCCST, qui facilite les échanges d'informations entre le secteur privé et le secteur public, ainsi qu'une collaboration stratégique sur les enjeux actuels et en évolution qui peuvent avoir une incidence sur les systèmes de télécommunications, y compris les menaces à la cybersécurité. Bon nombre de nos fournisseurs de services de télécommunications assurent la connectivité, mais offrent également des solutions de cybersécurité aux entreprises partout au pays, ce qui les aide à protéger leurs opérations contre les cyberattaques.

Autrement dit, notre industrie prend la sécurité au sérieux et s'engage à assurer celle du système canadien de télécommunications. À ce titre, nous adhérons à l'objectif du gouvernement du Canada qui est de protéger les infrastructures essentielles contre les cyberattaques et d'autres menaces.

Cependant, dans sa forme actuelle, le projet de loi C-26 soulève certaines préoccupations. Nous avons exprimé nos réserves et proposé des amendements au projet de loi dans un mémoire remis au comité permanent. Je vais mentionner quelques-unes de nos réserves qui ont toutes trait à la partie 1 du projet de loi C-26 et aux modifications proposées à la Loi sur les télécommunications.

Premièrement, le projet de loi confère au ministre un pouvoir étendu en ce qui a trait à l'émission d'ordonnances sans application des freins et des contrepoids appropriés. Compte tenu de la portée très vaste et de l'incidence potentielle de ce genre de pouvoir, il y aurait lieu de modifier la loi proposée pour en limiter l'exercice. Plus précisément, les ordonnances devraient non seulement être nécessaires selon le ministre, mais également être raisonnablement nécessaires, c'est-à-dire proportionnelles au préjudice potentiel du risque pour la sécurité et raisonnables dans les circonstances. Le projet de loi devrait également exiger que les ordonnances ne soient prises qu'après consultation d'experts désignés par le ministre pour s'assurer que leurs prescriptions sont proportionnelles au risque posé, qu'elles ont une incidence limitée sur la disponibilité des services et qu'elles sont réalisables sur les plans économique et opérationnel pour les fournisseurs de services concernés.

Deuxièmement, bien que les ordonnances rendues en vertu du projet de loi puissent faire l'objet d'un contrôle judiciaire, la loi prévoit qu'un juge peut fonder sa décision sur des éléments de preuve que le demandeur n'est pas autorisé à voir et qu'il ne peut donc pas contester. Ce processus ne prévoit aucun autre moyen de vérifier les éléments de preuve du gouvernement, notamment en ce qui concerne la nomination d'un avocat spécial ayant la cote de sécurité appropriée.

Troisièmement, le projet de loi C-26 ne prévoit pas de défense fondée sur la diligence raisonnable pour les violations présumées des ordonnances rendues en vertu des nouveaux articles proposés de la Loi sur les télécommunications, même si une défense de ce type peut être invoquée pour d'autres infractions à la Loi, ainsi que pour la violation d'ordonnances par d'autres acteurs en vertu d'autres dispositions du projet de loi C-26. L'absence de défense fondée sur la diligence raisonnable est encore plus frappante étant donné que le projet de loi vise à imposer des sanctions pécuniaires lourdes. Les fournisseurs de services de télécommunications devraient avoir le droit, comme le prévoit le projet de loi C-26, de se prévaloir d'une défense fondée sur la diligence raisonnable dans des circonstances appropriées et démontrer qu'ils ont pris toutes les précautions raisonnables dans les circonstances pour éviter la violation reprochée.

Enfin, la partie 1 du projet de loi C-26 devrait être modifiée pour préciser que l'indemnisation peut, à la discrétion du gouvernement, être accordée pour les dépenses, les pertes et les coûts découlant du respect d'une ordonnance.

[*Français*]

Nous vous remercions de nous avoir donné l'occasion d'exprimer notre point de vue sur cette importante question. Nous serons heureux de répondre à vos questions.

[*Traduction*]

Le président: Merci, monsieur Ghiz.

J'invite maintenant Mme Mason à faire sa déclaration préliminaire.

Mme Angelina Mason (avocate en chef et vice-présidente principale, Affaires juridiques et risque, Association des banquiers canadiens): Merci.

Bonsoir.

Je tiens à remercier le Comité de nous avoir invités à exposer notre point de vue au sujet de la partie 2 du projet de loi C-26, loi édictant la Loi sur la protection des cybersystèmes essentiels.

Je m'appelle Angelina Mason. Je suis l'avocate en chef de l'Association des banquiers canadiens, et vice-présidente principale, Affaires juridiques et Risques. Je suis accompagnée de mon collègue Charles Docherty, avocat en chef adjoint et vice-président, Affaires juridiques et Risques.

L'Association des banquiers canadiens, l'ABC, est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiennes et les Canadiens à atteindre leurs objectifs financiers.

Chefs de file de la cybersécurité, les banques au Canada investissent massivement dans la protection du système financier et des données personnelles de leurs clients contre les cybermenaces. Le secteur bancaire est hautement réglementé et doit répondre aux exigences strictes du Bureau du surintendant des institutions financières quant à la gestion des cyberrisques, des risques liés à la chaîne d'approvisionnement et aux tierces parties, ainsi qu'à l'obligation de signalement des incidents.

La sécurité des secteurs qui représentent les infrastructures essentielles du Canada doit être assurée afin de protéger la sécurité et le bien-être économique de la population. Dans sa prestation de services financiers aux Canadiennes et aux Canadiens, le secteur bancaire compte sur d'autres secteurs névralgiques qui représentent des infrastructures essentielles, comme les télécommunications et l'énergie. Nous avons encouragé le gouvernement à utiliser et à promouvoir des normes de cybersécurité sectorielles communes qui s'appliqueraient aux entités formant ces secteurs névralgiques et soutenons ses efforts à s'y prendre en vertu de la Loi. Également, conscients du fait que certaines infrastructures essentielles, comme l'énergie, relèvent de divers niveaux de gouvernement, nous avons recommandé au gouvernement fédéral de collaborer avec les provinces et les territoires à la définition d'un cadre de cybersécurité applicable à l'ensemble des secteurs des infrastructures essentielles.

Des normes de cybersécurité cohérentes et bien définies permettront une meilleure supervision et donneront l'assurance que les systèmes restent efficaces et bien protégés. La protection contre les menaces parrainées par des États et d'autres acteurs néfastes nécessite une démarche coordonnée entre le gouvernement et le secteur privé. Le gouvernement peut donc jouer un rôle central à cette fin, en rapprochant les partenaires qui représentent des infrastructures essentielles et les autres intervenants, et en mettant à profit tous les efforts en cours pour contrer les cybermenaces.

Nous reconnaissons l'importance de la Loi. Toutefois, nous devons agir sciemment. Certaines dispositions proposées dans la Loi doivent être mieux adaptées aux risques opérationnels et aux autres préoccupations connexes. Par exemple: pouvoir utiliser les exigences strictes actuelles dans certains secteurs, comme le secteur bancaire, en vue d'éviter la duplication et l'incohérence des exigences; prévoir des mesures de protection des renseignements confidentiels plus importantes; et modifier les seuils et l'intervalle de temps propres au signalement des incidents de cybersécurité.

De plus, des mesures de protection adéquates doivent être prévues dans le contexte de l'invocation des pouvoirs très étendus du gouvernement en vertu de la Loi. Conformément à d'autres textes législatifs, la Loi doit comprendre des dispositions d'exonération qui accordent aux exploitants désignés une immunité contre les poursuites civiles et pénales lorsque, de bonne foi, ils se conforment aux exigences de signalement prévues par la Loi et aux directives en matière de cybersécurité.

Au-delà de l'obligation de communiquer les renseignements, la Loi devrait favoriser la communication plus large et volontaire des incidents, des renseignements sur les cybermenaces et de l'expertise en matière de cybersécurité, avec le Centre de la sécurité des télécommunications, le CST, et entre les catégories d'exploitants désignés. Ce partage doit être assorti de dispositions d'exonération afin de ne pas créer de risques additionnels. Le partage efficace de ce type de renseignements est une composante essentielle de la cyberrésilience et doit être encouragé par la Loi.

Enfin, nous pensons qu'il est nécessaire de permettre au CST et au SCRS de communiquer les renseignements pertinents aux exploitants désignés de cybersystèmes essentiels au Canada dans l'objectif de les aider à prévenir et à atténuer l'impact des incidents de cybersécurité.

Nous communiquerons au Comité, par écrit, de plus amples détails sur nos recommandations. Nous tenons à collaborer avec le gouvernement et avec les autres secteurs pour veiller à ce que le Canada demeure sûr, solide et sécuritaire.

Nous sommes prêts à répondre à vos questions.

● (1715)

Le président: Merci, madame Mason.

Nous allons maintenant passer à M. Clement pour sa déclaration liminaire.

M. Andrew Clement (professeur émérite, Faculty of Information, University of Toronto, à titre personnel): Merci, monsieur le président et distingués membres du Comité.

Je m'appelle Andrew Clement, je suis informaticien et professeur émérite à la faculté d'information de l'Université de Toronto. J'y ai cofondé l'institut interdisciplinaire de l'identité, de la protection des renseignements personnels et de la sécurité.

Au cours de la dernière décennie, je me suis concentré sur les aspects de la protection de la vie privée, de la sécurité et de la surveillance des communications sur Internet. Je codirige, avec l'Autorité canadienne pour les enregistrements Internet, l'ACEI, un projet portant sur la mesure Internet en vue de faire progresser la cybersécurité, la résilience et la souveraineté du Canada. Ce projet est financé par le Programme de coopération en matière de cybersécurité de Sécurité publique Canada. Outre les honoraires annuels de 1 500 $, je ne reçois aucun financement de l'ACEI ou de Sécurité publique. Bien que j'appuie le mémoire que l'ACEI a présenté à votre comité, je m'exprime ici à titre personnel.

J'appuie résolument les recommandations formulées dans le mémoire de Citizen Lab et dans le mémoire conjoint de plusieurs organisations de la société civile. Ces deux mémoires s'inspirent largement de l'excellent rapport de Chris Parsons, intitulé *Cybersecurity Will Not Thrive in Darkness*.

Il est évident que le Canada a besoin d'un régime plus solide pour protéger ses infrastructures cybernétiques essentielles. Le projet de loi C-26 contribue à l'établissement d'un régime de cybersécurité valable. Cependant, il a besoin d'un amendement substantiel pour faire en sorte que les vastes pouvoirs secrets qu'il accorde au gouvernement ne l'emportent pas sur d'autres valeurs tout aussi essentielles, comme la protection de la vie privée, la liberté d'expression, la transparence judiciaire et la responsabilité gouvernementale.

Que ce soit bien ou pas, le Centre de la sécurité des télécommunications est le principal organisme gouvernemental chargé d'assurer la cybersécurité. Il fait face à une tâche vitale et remarquablement difficile. Heureusement, il semble bénéficier du travail d'experts dévoués. Évidemment, comme il puise ses origines dans le renseignement électromagnétique en temps de guerre, le CST baigne dans la culture du secret et a un appétit sans bornes pour la collecte de données. Cela se comprend pour certains volets de son mandat, mais comme il dispose désormais d'une capacité accrue, notamment en ce qui concerne la surveillance des communications nationales, le CST devrait se montrer beaucoup plus ouvert et rendre des comptes au public.

Des documents publiés par Snowden en 2013 — notamment au sujet de l'architecture conjointe des capteurs cybernétiques CASCADE du CST — indiquaient que l'organisme intégrait des capacités d'interception étendues à l'infrastructure Internet lui permettant d'intercepter une très grande partie des communications des Canadiens sur Internet.

Bien que le CST n'ait pas légalement le droit d'étendre ses activités aux particuliers canadiens, sa capacité à extraire massivement du contenu et des métadonnées, à faire de la surveillance de masse et de la « surveillance accessoire » de renseignements personnels, voire intimes, concernant chaque internaute canadien constitue un défi important en ce qui a trait au droit à la vie privée et à la gouvernance démocratique en général.

Voici ce que Ron Deibert, expert renommé en cybersécurité et directeur de Citizen Lab, a déclaré en 2015: « Il s'agit de fantastiques pouvoirs [de surveillance] qui ne devraient être accordés au gouvernement qu'avec une grande appréhension et moyennant un investissement d'envergure correspondante dans des systèmes de surveillance, d'examen et de reddition de comptes publics tout aussi puissants. »

La question fondamentale est de savoir si le gouvernement devrait sensibiliser les Canadiens à cette surveillance de masse et leur donner des garanties solides que cette collecte de masse est nécessaire, proportionnée et sécuritaire, ainsi que l'occasion de décider collectivement si de telles pratiques sont acceptables ou non.

Comme l'ont mentionné d'autres témoins, le projet de loi C-26 est surtout préoccupant parce qu'il ne limite pas l'utilisation que le CST fait des renseignements qu'il recueille en vertu des nouveaux pouvoirs considérables que lui confère le projet de loi C-26. Comme Kate Robertson l'a dit clairement plus tôt, selon les rapports de l'OSSNR, à moins qu'on ne le lui interdise explicitement, le CST se considérera autorisé à utiliser ces renseignements dans le cadre de ses mandats. Ce déficit de reddition de comptes doit être comblé avant d'accorder au CST de nouveaux pouvoirs en vertu du projet de loi C-26.

La vie privée est un droit fondamental de la personne. Il est essentiel que le projet de loi C-26 soit modifié de sorte qu'il précise que les renseignements personnels anonymisés doivent être traités sous le sceau de la confidentialité, et veille à ce que le gouvernement obtienne une ordonnance du tribunal avant d'en demander la divulgation. Le gouvernement ne doit pas être autorisé à appliquer ses nouveaux pouvoirs considérables pour porter atteinte à la vie privée, notamment comme conséquence d'un affaiblissement du chiffrement ou de la sécurité des communications. Les périodes de conservation des données doivent être précisées en regard de l'information recueillie.

● (1720)

Avant de terminer, j'aimerais parler brièvement d'une question qui est absente du projet de loi C-26, mais que votre comité a déjà jugée importante, à savoir la façon dont le gouvernement devrait gérer les vulnérabilités en matière de cybersécurité. Advenant que le projet de loi C-26 exige que les fournisseurs de services de télécommunications effectuent des évaluations pour cerner toute vulnérabilité de leurs services...

Le président: Monsieur Clement, pourriez-vous vous arrêter là, car votre temps est écoulé. Nous allons peut-être revenir sur cet aspect dans les questions qui vous seront posées.

Je vais maintenant donner la parole à M. Motz, pour six minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci beaucoup, monsieur le président.

Je remercie nos témoins, sur place et en ligne.

Ma première question s'adresse aux trois groupes.

Je suis ici depuis 2016 et, durant tout ce temps-là, j'ai sans cesse vu ce gouvernement tenter d'utiliser la loi pour se donner des pouvoirs excessifs et éviter d'avoir à rendre des comptes. Je pense notamment au projet de loi C-59, la soi-disant Loi de 2017 sur la sécurité nationale. De plus, pendant la pandémie de COVID-19, le gouvernement a tenté pendant plus de deux ans d'obtenir le pouvoir absolu de dépenser l'argent des contribuables sans avoir à rendre de comptes; il a tenté de contrôler ce que les Canadiens voient et disent sur Internet au moyen du projet de loi C-11 et du projet de loi C-18. Bien sûr, en 2022, il a aussi invoqué de manière exceptionnelle la Loi sur les mesures d'urgence que la Cour fédérale vient d'ailleurs tout juste de déclarer illégale et inconstitutionnelle, comme vous le savez. Le modus operandi du gouvernement et ses projets de loi ont de quoi préoccuper les Canadiens.

S'agissant des organismes que vous représentez et à la lumière des recherches du professeur Clement, est-ce que ce projet de loi, tel qu'il est libellé actuellement, ne vous incite pas à la réflexion, surtout quand on parle de légiférer des pouvoirs qui limitent les droits fondamentaux et la vie privée des Canadiens?

Madame Mason, je vais commencer par vous. Je suis heureux de vous revoir, après votre passage au comité chargé de la Loi sur les mesures d'urgence. Cette fois-ci, nous espérons pouvoir agir a priori plutôt que de devoir régler le problème après coup, comme nous avons essayé de le faire la première fois. Pouvez-vous répondre à cette question?

Je m'adresse à vous trois. Dans vos réponses, et en reprenant éventuellement ce que vous avez peut-être déjà suggéré, pourriez-vous nous indiquer comment le Comité devrait répondre aux préoccupations des Canadiens à l'égard de ces lacunes?

● (1725)

Mme Angelina Mason: Comme nous l'avons dit dans notre exposé préliminaire, nous avons effectivement besoin de mesures de sauvegarde appropriées. Il faudrait introduire la notion de proportionnalité. À l'heure actuelle, les pouvoirs relatifs aux directives en matière de cybersécurité sont tellement vastes que nous ne savons même pas exactement jusqu'où elles pourraient aller.

Nous estimons que le projet de loi doit absolument comporter des dispositions concernant des mesures de sauvegarde permettant de convaincre tous les participants que le gouvernement intervient dans des limites raisonnables.

M. Glen Motz: Monsieur Clement, allez-y.

M. Andrew Clement: En plus de la proportionnalité, dont il a été question à plusieurs reprises, il faudrait que le fonctionnement des agences de sécurité et les mesures prises soient beaucoup plus transparents. Il n'y a pas beaucoup de transparence en ce moment.

De nombreuses recommandations, particulièrement dans les rapports dont j'ai parlé tout à l'heure, visent à instaurer beaucoup plus de transparence pour que les Canadiens puissent être informés. Cela permettrait d'atteindre un bien meilleur équilibre. Le projet de loi C-26 actuel n'est pas équilibré à cet égard.

M. Glen Motz: Très bien.

Monsieur Ghiz, vous avez la parole.

M. Robert Ghiz: Merci.

Comme je l'ai dit dans mon exposé préliminaire, je crois que nous sommes tous d'accord pour dire que la prémisse de ce projet de loi est importante et que nous en avons besoin, mais que, en matière de transparence, de reddition de comptes et de droits judiciaires, il faudrait resserrer certaines dispositions. À mon avis, ce sont les principaux aspects à examiner.

Nous proposons des amendements précis dans notre mémoire. La démocratie parlementaire suppose notamment que le Comité ait la possibilité de proposer des amendements et, dans le meilleur des cas, de renvoyer un meilleur projet de loi à la Chambre.

M. Glen Motz: Merci à vous trois.

Nous avons beaucoup entendu les mots « trop vaste », « proportionné » et « raisonnable ».

Mme Robertson, du Citizen Lab, dans le groupe de témoins précédent, nous a dit qu'il faut absolument prendre la bonne décision dès maintenant. Je suis d'accord avec sa recommandation d'instaurer la mesure de contrôle judiciaire nécessaire.

Cela dit, comment les témoins des trois groupes envisageraient-ils le juste équilibre entre le contrôle judiciaire et la protection du droit à la vie privée? Comment trouver le juste équilibre entre la protection des infrastructures essentielles et, dans certaines circonstances, la possibilité de prendre des mesures rapides à l'égard de ce que le secteur bancaire appellerait une atteinte à l'infrastructure essentielle de nature prioritaire? Comment protéger cette infrastructure en même temps que la population et les renseignements personnels dans ce cas, quand l'intervention est justifiée?

Je vais commencer par M. Smith, suivi de M. Clement et de Mme Mason.

M. Eric Smith (vice-président principal, Association canadienne des télécommunications): Nous ne suggérons certainement pas de contrôle judiciaire de tous les aspects du processus décisionnel avant que la décision ne soit prise. Il faut effectivement un contrôle judiciaire pour les droits d'appel et pour le droit des personnes visées par un décret de contester le décret au motif de sa proportionnalité et de sa justification.

Quand il a comparu ici, le commissaire à la protection de la vie privée nous a parlé de consultation pour s'assurer que le droit à la vie privée était respecté. Le rôle de la magistrature varie selon l'aspect du projet de loi que l'on examine. Tout cela fait partie de ce dont parlent la plupart des témoins. Il doit y avoir des freins et contrepoids.

● (1730)

M. Glen Motz: Merci.

Monsieur Clement, allez-y.

M. Andrew Clement: On pourrait entre autres améliorer ce dont Kate Robertson a parlé, à savoir le rôle de l'OSSNR, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. On doit s'inquiéter du fait qu'il ait dit et répété qu'il ne pouvait pas confirmer que le CST fonctionnait légalement parce qu'il n'avait pas eu accès à l'information dont il avait besoin pour faire cette évaluation. C'est très préoccupant.

Il serait très utile d'ajouter au projet de loi une recommandation prévoyant cette transparence et permettant à l'OSSNR d'avoir accès à cette information.

M. Glen Motz: Madame Mason, pouvez-vous répondre rapidement? Nous avons presque terminé.

Mme Angelina Mason: Il prévoit des seuils à partir desquels des décrets pourraient même être envisagés.

Nous sommes très préoccupés, parce que les exploitants font tout ce qu'ils peuvent pour s'assurer de maîtriser la situation et de prendre les mesures nécessaires. À quel moment le gouvernement intervient-il? A-t-il accès à des informations que vous n'avez pas? Que vous demande-t-il de faire? Est-ce raisonnable?

À mon avis, il devrait y avoir des seuils, surtout quand ce sont les exploitants eux-mêmes qui doivent s'arranger pour gérer la situation.

M. Glen Motz: Merci.

Le président: Merci, monsieur Motz.

Monsieur McKinnon, vous avez la parole.

M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Merci, monsieur le président.

Je vais d'abord m'adresser aux représentants de l'Association canadienne des télécommunications.

On nous a beaucoup parlé du pouvoir du ministre de publier des décrets, ainsi que des préoccupations en matière de confidentialité. Je crois que ces préoccupations sont légitimes. J'aimerais quelques éclaircissements. Avez-vous une idée du genre de décret dont il pourrait s'agir? Pouvez-vous imaginer le genre de décret qui pourrait être publié, ou est-ce trop hypothétique?

M. Eric Smith: Il vaut mieux ne pas trop spéculer, mais, comme on le sait, le gouvernement a déjà, en 2022, publié un énoncé de politique concernant l'obligation de retirer l'équipement de certains fournisseurs de l'infrastructure, notamment chez des fournisseurs de télécommunications. C'est donc un exemple.

Le pouvoir de publier des décrets est très large, comme vous le savez: « faire ou s'abstenir de faire ». Il pourrait s'agir de couper le service à une organisation, un particulier, etc. Il pourrait s'agir d'exiger, non pas nécessairement de retirer de l'équipement de votre infrastructure, mais d'en ajouter, ou de se conformer à certaines normes. Il pourrait s'agir d'un affaiblissement de l'encodage ou de l'obligation d'intercepter des communications.

Le libellé actuel pourrait être interprété de façon très large.

M. Ron McKinnon: On s'inquiète aussi, me semble-t-il, du fait que la diffusion publique de ces décrets risquerait de révéler les vulnérabilités de diverses pratiques du secteur à des gens malveillants. Avez-vous des commentaires à ce sujet?

M. Eric Smith: Parlez-vous de la confidentialité du décret ou de la confidentialité des renseignements fournis?

M. Ron McKinnon: Si le décret était rendu public, il pourrait révéler des vulnérabilités à des gens malveillants.

M. Eric Smith: C'est une bonne question. Nous sommes effectivement sensibles à cet enjeu. Il y a, en effet, des circonstances où des raisons légitimes justifieraient que certaines parties d'un décret ou, dans certains cas, la totalité du décret devraient être gardées secrètes.

À notre avis, le secret devrait être l'exception plutôt que la règle. C'est là qu'il me semble approprié d'avoir... Toute décision ou exigence portant sur la confidentialité d'un décret devrait être évaluée. Cela devrait être confié à un juge pour que le gouvernement fournisse la preuve des raisons pour lesquelles le décret devrait rester confidentiel, afin qu'il soit possible de vérifier cette hypothèse.

M. Ron McKinnon: À cet égard, vous avez parlé de l'éventualité d'un conseiller spécial ou d'un défenseur, si on veut. Pourriez-vous nous décrire ce rôle et ces pouvoirs? Un organisme actuel du gouvernement pourrait-il assumer ce rôle?

M. Eric Smith: Il existe déjà des mécanismes dans le cadre de situations ou d'audiences judiciaires où des renseignements confidentiels ou secrets ne peuvent pas être rendus publics ou communiqués à l'intéressé. Un avocat spécial doté de la cote de sécurité nécessaire peut interroger le gouvernement, vérifier les preuves et vérifier les hypothèses avancées. Ce n'est pas une situation parfaite, mais cela fournit au moins un mécanisme par lequel les preuves du gouvernement peuvent être évaluées.

● (1735)

M. Ron McKinnon: Vous avez parlé de la nécessité de freins et de contrepoids. Vous avez parlé de la nécessité de rationaliser ces décrets. Pourriez-vous suggérer d'autres sortes de freins et contrepoids utiles en l'occurrence?

M. Eric Smith: Certainement. À l'heure actuelle, si le ministre estime qu'il est nécessaire de faire ou de ne pas faire quelque chose... Il me semble important d'exiger que le décret ne soit publié qu'après consultation des organismes d'experts prévus. Il pourrait s'agir d'une structure de données en C, par exemple. Il pourrait s'agir d'autres organismes de cybersécurité au sein du gouvernement. Il faut non seulement déterminer s'il y a menace à la sécurité, mais aussi si le décret est proportionné et équilibré.

Il faut dire que nos systèmes de communication sont très complexes. Il peut sembler facile d'exiger de retirer tel équipement ou de prendre telle mesure, mais il faut aussi s'assurer que les experts, y compris les cibles des décrets s'il y a lieu, peuvent informer le gouvernement des conséquences imprévues que cela pourrait avoir pour le système ou même pour la viabilité de certains petits fournisseurs à qui on demande de se conformer à ces décrets. C'est une exigence très importante qui devrait figurer dans la loi.

M. Ron McKinnon: Ces décrets pourraient exiger que différents fournisseurs ajoutent ou retirent de l'équipement ou modifient leur logiciel. Cela entraîne des coûts. Prévoyez-vous, dans votre mémoire, qu'ils soient indemnisés?

M. Eric Smith: Nous ne disons pas qu'ils devraient être indemnisés. Ce pourrait être une simple question de rédaction, mais la loi actuelle dit que les fournisseurs ne peuvent pas obtenir d'indemnité. C'est sujet à interprétation. Est-ce que cela signifie simplement qu'ils n'y ont pas droit légalement ou est-ce que cela signifie qu'ils ne peuvent pas être indemnisés?

À notre avis, le ministre ou le gouverneur en conseil devrait avoir le pouvoir discrétionnaire d'accorder une indemnisation au cas par cas, et les fournisseurs visés par ces décrets devraient pouvoir faire valoir leur point de vue sur la question de savoir s'ils devraient être indemnisés ou sur les raisons pour lesquelles ils devraient l'être.

Par exemple, aux États-Unis, le gouvernement a créé un fonds de plusieurs milliards de dollars pour aider une certaine catégorie de fournisseurs à retirer de l'équipement fourni par la Chine de leurs infrastructures.

M. Ron McKinnon: Ma dernière question porte sur le moyen de défense fondé sur la diligence raisonnable. Pourriez-vous expliquer?

M. Eric Smith: Certainement. C'est quelque chose qui nous laisse perplexes dans le projet de loi, parce que toutes les autres parties prenantes sont en mesure de montrer... En cas de présomption d'infraction, les intéressés pourraient faire valoir qu'ils ont fait tout ce qui était raisonnablement possible pour éviter de commettre cette infraction. Il pourrait arriver, par exemple, que le gouvernement exige que vous remplaciez tel équipement dans votre infrastructure par de l'équipement provenant d'ailleurs et que cet équipement ne soit même pas disponible sur le marché.

Pour une raison ou une autre, la loi dit que nous sommes les seules parties qui n'ont pas le droit de présenter cette défense.

Le président: Merci, monsieur Smith et monsieur McKinnon.

Madame Michaud, c'est à votre tour.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Je remercie les témoins d'être avec nous.

J'aimerais poser ma première question aux représentants de l'Association canadienne des télécommunications. Par la suite, je poserai sensiblement la même aux représentants de l'Association des banquiers canadiens.

À peu près tout le monde s'entend pour dire que le projet de loi C-26 est un pas dans la bonne direction et que c'est relativement une bonne nouvelle que le gouvernement désire s'attaquer à la question de la cybersécurité. Cependant, il y a des craintes assez généralisées quant à la protection des renseignements personnels et de la vie privée, ainsi qu'au large pouvoir que le gouvernement se donne en matière de réglementation, de décrets et d'arrêtés, notamment.

Madame, messieurs, vous représentez des fournisseurs de télécommunications et des organisations qui investissent dans les réseaux de télécommunications. On peut penser à Vidéotron, Rogers ou Bell, de très grandes organisations qui, j'imagine, investissent déjà pour se prémunir contre toute cyberattaque. Elles ont la main-d'œuvre nécessaire pour le faire.

Vous représentez peut-être aussi des organisations un peu moins grandes, qui ont un peu moins de clients. Cela pourrait représenter une charge de travail supplémentaire pour elles. On peut penser que certaines d'entre elles ont déjà subi des cyberattaques.

À l'heure actuelle, comment les entreprises que vous représentez se prémunissent-elles contre les cyberattaques? Qu'est-ce que le projet de loi C-26 va changer?

Le projet de loi, s'il n'est pas amendé, par exemple, pour encadrer davantage les pouvoirs que le gouvernement se donne, apparaît-il comme un fardeau ou comme un soulagement pour les organisations un peu plus petites, comme les petites ou moyennes entreprises?

Je sais que c'est une question assez large.

● (1740)

[*Traduction*]

M. Eric Smith: C'est une très bonne question.

J'ajoute que nos membres se sont déjà dotés de processus de cybersécurité très robustes et que, comme l'a dit M. Ghiz dans son exposé, ils collaborent déjà étroitement avec le gouvernement. Beaucoup des mesures susceptibles de découler du projet de loi C-26 sont déjà en vigueur dans le secteur. Le CCCST, c'est-à-dire le Comité consultatif canadien sur la sécurité et les communications, publie des pratiques exemplaires, des instructions, etc., destinées à tous les fournisseurs de services de télécommunications. Le projet de loi C-26 permettrait en fait au ministre d'ordonner des pratiques précises, par exemple de l'information.

Quant au fardeau réglementaire, je ne connais aucun secteur d'activité qui accueille favorablement un supplément de réglementation, puisque cela alourdit le fardeau. Je rappelle que nos membres ont déjà des pratiques solides, et je pense que le fardeau supplémentaire aurait trait surtout à des choses comme l'obligation redditionnelle. C'est là que la loi pourrait nécessiter des améliorations. On y dit qu'il faut « déclarer sans délai » un incident. Eh bien, « immédiatement », c'est tout de suite, et l'on n'aurait même pas assez d'information pour savoir s'il y a eu un incident. Certaines dispositions pourraient être améliorées.

J'espère que cela répond à votre question.

[*Français*]

Mme Kristina Michaud: Oui, c'est le cas, monsieur Smith. Merci beaucoup.

Je veux poser la même question aux représentants de l'Association des banquiers canadiens.

Selon le Bureau du surintendant des institutions financières, les banques sont de plus en plus la cible de cyberattaques. On l'a vu dans certains cas au cours des derniers mois. J'imagine que cela peut susciter une certaine crainte chez les clients quant à la protection de leurs données personnelles. Comme c'est le cas pour les entreprises de télécommunications, j'imagine que les banques ont déjà certains mécanismes en place et qu'elles font déjà, comme le disait M. Smith, ce que le projet de loi C-26 va leur demander.

Qu'est-ce que cela représente pour les banques? Est-ce un soulagement ou plutôt un fardeau?

Qu'est-ce qu'il faudrait encadrer davantage, selon vous?

[*Traduction*]

Mme Angelina Mason: J'entérine le point de vue exprimé par le Bureau du surintendant des institutions financières, à savoir que nous traitons la reddition des comptes comme une obligation.

J'aimerais clarifier deux ou trois choses. La première, c'est que les rapports transmis au BSIF concernent la technologie et la cybersécurité. S'il y a un incident technologique, même s'il n'est pas lié à la cybersécurité, ou si l'on pense que le système a été infiltré, cela fait l'objet d'un signalement, parce que le BSIF se soucie énormément de la résilience de nos systèmes, non seulement pour assurer la sécurité, mais aussi pour fournir nos services.

Ce genre de reddition des comptes vise à aider à circonscrire les sujets de préoccupation potentiels pour qu'ils soient communiqués et que les gens s'appuient sur des systèmes plus solides. Cela se fait actuellement en vase clos. Nous le faisons avec le BSIF.

L'objectif de ce projet de loi est précisément de circonscrire les secteurs critiques et d'exiger des principaux intervenants de ces secteurs, en raison de ce qu'ils représentent pour la sécurité de l'ensemble de notre écosystème, qu'ils rendent des comptes à un organisme central, de sorte qu'il soit possible non seulement de savoir ce qui se passe ici ou là, mais dans tout le secteur, et de déterminer s'il y a une préoccupation commune, s'il y a des leçons à tirer et si ce qui se passe est lié d'une façon ou d'une autre.

L'un des objectifs essentiels de ce projet de loi est d'améliorer l'information disponible pour aider à lutter contre les cybermenaces. C'est effectivement l'un des aspects positifs que nous y voyons, et c'est pourquoi nous vous invitons à aller encore plus loin et à permettre le partage volontaire à tous les niveaux de l'écosystème. C'est très positif. Il y a aussi que notre planification en matière de cybersécurité et celle des autres seraient désormais validées et centralisées et que l'on pourrait, de ce fait, tirer des leçons de l'expérience de différentes administrations.

Le président: Merci, madame Mason.

Monsieur Julian, vous avez la parole.

M. Peter Julian: Merci, monsieur le président.

Merci aux témoins de leur présence.

Je vais commencer par vous, monsieur Ghiz.

Combien de cyberattaques l'Association canadienne des télécommunications a-t-elle subies au cours de la dernière année? J'aimerais savoir si vous constatez une tendance à la hausse, à la stabilité ou à la baisse.

● (1745)

M. Robert Ghiz: Contrairement à l'agent des finances qui a témoigné tout à l'heure, nous ne sommes pas un organisme de réglementation et nous n'avons pas accès aux renseignements personnels de nos membres. Malheureusement, je n'ai pas l'information que vous demandez.

M. Peter Julian: Mais on en parle sûrement au sein de l'association, non?

M. Robert Ghiz: Non, nous n'avons pas accès à l'information relative aux affaires privées et personnelles.

M. Peter Julian: Je vais donc vous poser la question autrement. Si vous partagiez des pratiques exemplaires, vous constateriez sûrement que les types de cyberattaques pourraient être semblables dans tout votre secteur. Y aurait-il un échange de renseignements qui aiderait d'autres entreprises, par exemple, à se doter de mesures de protection contre les cyberattaques?

M. Robert Ghiz: Elles le font entre elles et avec le gouvernement par l'entremise du CCCST. Cela ne passe pas par notre entremise.

M. Peter Julian: Je vois.

Dans quelle mesure votre association a-t-elle été consultée au sujet de la rédaction du projet de loi C-26?

M. Robert Ghiz: Nous n'avons pas été consultés. Nous collaborons avec nos membres pour trouver des pratiques exemplaires, et il est possible qu'ils aient été consultés, mais nous n'en avons pas été informés non plus. Notre association n'a pas été consultée. Nous avons participé au mémoire présenté au Comité.

M. Peter Julian: D'accord. Merci beaucoup.

Madame Mason, j'aimerais vous poser la même question. Dans quelle mesure l'Association des banquiers canadiens a-t-elle été consultée au sujet de la rédaction du projet de loi C-26?

Mme Angelina Mason: Nous n'avons pas participé à la rédaction préliminaire. Depuis un certain temps déjà, nous préconisons des normes communes pour l'ensemble du secteur. Nous avons pu faire part de nos réflexions une fois que la première ébauche a été publiée, dans le cadre de rencontres avec des représentants de Sécurité publique auprès de qui nous avons fait valoir un certain nombre des recommandations que nous présentons aujourd'hui au Comité.

M. Peter Julian: Très bien.

Le BSIF — vous avez peut-être entendu le témoignage de son représentant tout à l'heure — a parlé d'une mesure... En 2022, il y a eu 10 cyberattaques de nature prioritaire. En 2023, ce nombre a triplé pour passer à 30. Constatez-vous la même tendance parmi les membres de l'Association des banquiers canadiens? Le nombre de cyberattaques contre les membres de votre association augmente-t-il?

Je vais vous poser une question très semblable à celle que j'ai posée à M. Ghiz. Dans quelle mesure partagez-vous des pratiques exemplaires? Dans quelle mesure vos membres communiquent-ils entre eux pour s'assurer de prévenir ce qui pourrait être des types de cyberattaques semblables?

Mme Angelina Mason: Nous partageons effectivement des pratiques exemplaires. Je ne crois pas que nous puissions vous fournir de chiffres précis.

Dans le cas du BSIF, cela s'applique à tous les établissements financiers sous réglementation fédérale. Je ne sais donc pas lesquels de ces établissements font partie de notre association. Mais je crois que les attaques sont signalées pour en informer tout le réseau et permettre de les contrer comme il convient.

M. Peter Julian: Merci.

J'aimerais entendre M. Clement.

Vous avez, en même temps qu'un certain nombre d'organisations importantes — dont l'Association canadienne des libertés civiles, la Ligue des droits et libertés, le Conseil national des musulmans canadiens, OpenMedia, le Conseil canadien de la protection des renseignements personnels et de l'accès à l'information — réclamé une série d'amendements, sous la forme de 16 recommandations qui contribueraient, pour reprendre les termes de la séance d'information, à « restreindre les pouvoirs ministériels », à « protéger les renseignements personnels et commerciaux confidentiels », à « maximiser la transparence », à « permettre aux conseillers spéciaux de protéger l'intérêt public », et à « accroître la responsabilisation du Centre de la sécurité des télécommunications ». Ce sont des recommandations très utiles que vous et la coalition nous avez présentées.

Quelles sont les recommandations les plus importantes, celles dont nous devrions absolument tenir compte quand nous proposerons des amendements au projet de loi C-26?

M. Andrew Clement: Il y a là beaucoup de recommandations. Nous venons de parler de certaines d'entre elles, mais je dirais que la première serait celle qui vise à limiter la portée des décrets ministériels — laquelle, à ce stade, est relativement illimitée, sauf par nécessité générale. D'autres réclament des mesures de transparence, de reddition des comptes, etc. Tous ces éléments sont très importants.

Comme je le disais tout à l'heure, il faut instaurer un bien meilleur équilibre entre ce qu'exige la sécurité et les autres intérêts en jeu.

Je vais m'arrêter ici, mais je pourrais vous fournir des priorités plus précises, si vous le souhaitez.

● (1750)

M. Peter Julian: Merci.

Vous dites donc que le projet de loi C-26 soulève des difficultés majeures auxquelles il faut trouver des solutions, qu'il doit être considérablement amélioré et que nous devrions envisager un certain nombre d'amendements pour qu'il fasse ce qu'il est censé faire, mais aussi pour assurer la protection de l'information et la transparence. C'est bien cela?

M. Andrew Clement: Oui, tout à fait.

Le président: Merci, monsieur Julian et monsieur Clement. Votre temps de parole est écoulé.

Passons à la série suivante...

M. Peter Julian: Monsieur le président, je suis désolé, mais il est 18 heures. Je dois partir et je ne consens pas à poursuivre la réunion.

Le président: Cette horloge est bien rapide. Il est, en fait, 17 h 51.

Monsieur Julian, laissez-moi finir. Je vais proposer deux minutes et demie chacun. Monsieur Julian, vous avez la dernière question, et, si vous voulez y renoncer, c'est parfait; nous pourrons terminer un peu plus rapidement. Mais il nous reste deux minutes et demie chacun.

Monsieur Kurek, vous avez la parole.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup. Je suis heureux d'avoir l'occasion de discuter de cet important sujet.

Monsieur Clement, si je me souviens bien, vous avez parlé de « pouvoirs incroyables ». Il est certain que le potentiel de contrôle, faute de mesures de protection suffisantes, est effectivement incroyable — ou, serais-je tenté de dire, « effrayant ».

Estimez-vous que, dans sa forme actuelle, le projet de loi prévoit des mesures de protection de la vie privée, des données et des droits des Canadiens?

M. Andrew Clement: Je ne crois pas que ces droits soient protégés par le texte actuel. C'est un projet de loi très unilatéral à cet égard. Il accorde trop de latitude et de pouvoirs aux organismes gouvernementaux sans la transparence et la reddition de comptes nécessaires.

M. Damien Kurek: Merci beaucoup. Je comprends.

Je vais m'adresser à nos témoins des télécommunications et des banques, deux secteurs à peu près aussi populaires que les politiciens.

Certains estiment que c'est une voie à sens unique en matière de reddition des comptes et du point de vue des mécanismes de communication des données au gouvernement. On ne sait pas très bien à quoi serviront ces données, qu'il s'agisse de renseignements exclusifs ou d'autres.

Dans la minute qu'il me reste — vous avez environ 20 secondes chacun — pourriez-vous expliquer en quoi les mécanismes redditionnels actuels sont à sens unique? Estimez-vous qu'il y a un problème à régler?

Je vais commencer par les témoins dans la salle.

M. Robert Ghiz: Eh bien, effectivement, et c'est un double coup dur, sur le plan politique et sur le plan des télécommunications.

À cet égard, je suis d'accord avec une bonne partie de ce qui a déjà été dit, à savoir que ce projet de loi est bien intentionné, mais qu'il doit être amélioré, et qu'il le sera grâce à des mesures favorisant ouverture et transparence et grâce à des freins et contrepoids valables.

M. Damien Kurek: Merci beaucoup.

Il reste environ 20 secondes à notre dernier témoin, s'il peut répondre.

Mme Angelina Mason: Avec plaisir.

Je pense que ce texte est très interventionniste et qu'on devrait mettre davantage l'accent sur l'échange d'information dans l'intérêt des participants au système.

Le président: Merci, monsieur Kurek.

Madame Michaud, vous avez deux minutes et demie. Je vous en prie.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

J'en profiterais pour...

[*Traduction*]

Le président: Madame Michaud, je me suis trompé. Veuillez m'excuser. Je vous reviens sous peu.

C'est au tour de Mme O'Connell. J'avais oublié qu'elle était ici.

Mme Jennifer O'Connell: Merci, monsieur le président. J'ai été trop silencieuse. Et vous m'avez oubliée.

Merci aux témoins.

Mme Michaud a posé une question semblable à celle que je voulais poser.

Madame Mason, vous y avez fait allusion. Je soupçonne que les banques auront déjà une longueur d'avance sur ce que propose ce projet de loi, et je vais donc adresser ma question à nos témoins des télécommunications.

L'enjeu de la vie privée et de sa protection est très réel, et nous voulons absolument instaurer un bon équilibre, mais, par ailleurs, on pourrait faire valoir que, si l'on ne s'occupe pas correctement de l'infrastructure essentielle, comme l'infrastructure des télécommunications, les gens malveillants susceptibles d'avoir accès à ces renseignements ne se soucieront pas de la protection de la vie privée des Canadiens.

Les entreprises de télécommunications et les banques — dont Mme Mason a aussi parlé, je crois — détiennent beaucoup de données sur les Canadiens, dont des données de localisation, des numéros de cartes de crédit et beaucoup de renseignements personnels. Si vos systèmes ne sont pas protégés des fluctuations constantes de la cybersécurité — n'oublions pas qu'elle évolue constamment — et que vous n'êtes pas en mesure de réagir à ces changements et de travailler avec le gouvernement, ne pensez-vous pas que les renseignements personnels des Canadiens seraient beaucoup plus exposés à des gens malveillants désireux d'y accéder et de les vendre ou de les diffuser pour des raisons infâmes? La protection de la vie privée des Canadiens ne serait-elle pas mieux servie par une solide infrastructure de cybersécurité?

● (1755)

M. Eric Smith: Oui. Je pense également que notre secteur fait du très bon travail à cet égard. C'est une fonction essentielle dont nos membres s'acquittent. Comme vous l'avez dit, les gens malveillants raffinent constamment leurs techniques. Nous devons constamment modifier nos procédures et notre technologie.

Mme Jennifer O'Connell: Merci.

Vous avez également posé des questions sur l'évolution des structures physiques auxquelles certains de vos membres pourraient avoir accès ounon. Là encore, je dirais que, s'il y a des tendances préoccupantes à l'échelle mondiale — et elles ne sont peut-être même pas encore visibles au Canada — et qu'il est possible de sécuriser notre infrastructure essentielle, la collaboration avec le gouvernement... je rappelle qu'il ne s'agit pas seulement du fonctionnement des télécommunications. Vous avez une grande responsabilité, à laquelle le gouvernement a contribué. Vous devez cela aux Canadiens. Si nous sommes préoccupés par les tendances, il vous revient d'instaurer ces changements pour protéger les données des Canadiens.

Le président: Merci, madame O'Connell.

Madame Michaud, c'est à vous.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

J'aimerais poser une question assez simple, la même que celle que j'ai posée à d'autres intervenants pendant d'autres rencontres.

Le projet de loi C-26 prévoit des sanctions pécuniaires assez lourdes pour les organisations qui ne se conformeraient pas aux décisions ou aux demandes qu'imposerait le gouvernement. Nous ne savons pas quelles seraient ces demandes parce que le pouvoir prévu est assez large.

J'ai demandé aux intervenants s'il était exagéré d'imposer ces sanctions. Certains disaient que, au lieu d'imposer des sanctions, il faudrait plutôt mettre en place des incitatifs pour inciter les organisations à se conformer aux demandes du gouvernement. D'autres disaient qu'il fallait conserver les sanctions, mais qu'ils mettraient quand même en place des incitatifs pour les organisations.

Messieurs Smith ou Ghiz, que pensez-vous de ces sanctions visant des entreprises comme celles que vous représentez dans votre association?

[*Traduction*]

M. Eric Smith: Merci de la question.

Les incitatifs sont toujours une bonne chose. Certaines organisations plus petites doivent assumer un plus grand fardeau pour introduire de nouvelles mesures. Je crois que nous avons déjà beaucoup d'incitatifs. La réputation de nos membres repose sur la protection de la vie privée, de la sécurité, etc.

Notre préoccupation concernant les pénalités est qu'elles sont très importantes et cumulatives. De plus, comme je l'ai dit, il se trouve que nous sommes le seul secteur à ne pas avoir droit à une défense fondée sur la diligence raisonnable. Autrement dit, il pourrait arriver qu'une organisation fasse tout ce qu'il est raisonnablement possible de faire pour se conformer, mais que, pour une raison ou une autre, la situation échappe à son contrôle et qu'elle ne le puisse pas, et que, malgré tout, elle soit assujettie à d'énormes sanctions pécuniaires et même à des sanctions pénales.

[*Français*]

Mme Kristina Michaud: Merci, monsieur Smith.

S'il reste du temps, j'invite les autres intervenants à répondre à la question s'ils le veulent.

[*Traduction*]

Mme Angelina Mason: Certainement. Je me ferai un plaisir de vous répondre.

Nous sommes un secteur très motivé et très respectueux de la loi, et nous n'avons pas vraiment besoin d'incitatifs. Il est vrai que des incitatifs pourraient aider de petites et moyennes entreprises à se conformer à la loi, mais ce n'est pas le cas des grandes entreprises et des parties visées par ce projet de loi.

Le président: Merci, madame Michaud.

Nous sommes dans les temps.

Je remercie les témoins d'aujourd'hui.

Avant de demander la levée de la séance, je tiens à vous informer que notre dernière réunion sur le projet de loi C-26 aura lieu jeudi. Nous envisageons de recevoir les amendements et de les préparer pour l'étude article par article à notre retour, c'est-à-dire d'ici mercredi midi la semaine prochaine. Il y a une certaine marge de manœuvre, et nous aurons donc probablement d'autres discussions à ce sujet jeudi. Voilà les grandes lignes du travail à venir.

La séance est levée.