CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

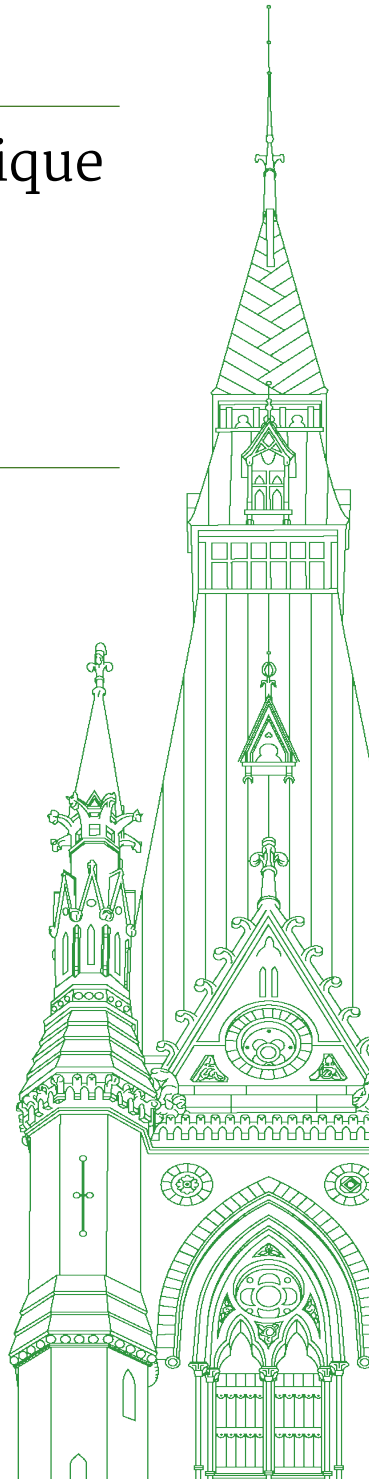
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 036

Le mardi 5 mai 2026



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le mardi 5 mai 2026

● (1555)

[*Français*]

Le président (L'hon. Jean-Yves Duclos (Québec-Centre, Lib.)): J'ouvre maintenant la séance.

Je remercie tout le monde d'être présent.

Tout d'abord, je suis désolé pour toutes les émotions que vous avez pu vivre au cours des dernières heures. Je pense au greffier en particulier. Il y a eu des changements d'horaire, des votes, des places assignées, des places non assignées, des places réassignées, et autres. Alors, je vous remercie tous de votre bienveillance et de votre indulgence.

Bienvenue à la réunion n° 36 du Comité permanent de la sécurité publique et nationale.

Nous nous réunissons aujourd'hui dans le cadre de l'étude du projet de loi C-22, Loi concernant l'accès légal.

Souhaitons d'abord la bienvenue aux témoins, qui sont tous de hauts fonctionnaires. Les ministres se joindront à nous dans environ une heure.

Nous accueillons Ramzi Nashef, directeur général, Service canadien du renseignement de sécurité; Kimberley Gibner, Normand Wong et Anne-Marie LeBel, du ministère de la Justice; Shannon Hiegel, Mike McGuire et Fenton Ho, du ministère de la Sécurité publique et de la Protection civile; et Richard Burchill, de la Gendarmerie royale du Canada.

Monsieur McGuire, nous allons commencer par vous, et vous avez la parole pour cinq minutes.

[*Traduction*]

Mike McGuire (directeur général, Politiques internationales et frontalières, ministère de la Sécurité publique et de la Protection civile): Merci, monsieur le président et mesdames et messieurs, de nous recevoir ici aujourd'hui.

Je m'appelle Mike McGuire. Je suis directeur général des politiques internationales et frontalières au ministère de la Sécurité publique du Canada. Je suis heureux de me retrouver ici avec des collègues, comme on vient de le mentionner, du ministère de la Justice, du ministère de la Sécurité publique, de la GRC et du SCRS pour répondre à des questions techniques concernant le projet de loi C-22, Loi concernant l'accès légal.

L'accès légal est un dossier connu qui a été étudié dans le passé par le Parlement, tout récemment par le Comité des parlementaires sur la sécurité nationale et le renseignement, qui a publié un rapport spécial, l'an dernier, réclamant une réforme législative de l'accès légal.

[*Français*]

Le projet de loi C-22 vise à combler des lacunes fondamentales et bien documentées dans le cadre canadien de l'accès légal. L'environnement en ligne a facilité, voire favorisé la communication, la coordination et la dissimulation des activités criminelles et de celles des acteurs menaçants. L'utilisation généralisée des appareils mobiles, des communications basées sur Internet, des plateformes de messagerie et d'autres technologies émergentes a fondamentalement transformé la manière dont les crimes et les menaces à la sécurité nationale sont planifiés et exécutés, ainsi que la façon dont les enquêtes en la matière sont menées.

En parallèle, les services de police canadiens et le SCRS font face à des défis croissants pour obtenir rapidement l'information essentielle aux enquêtes. Le projet de loi C-22 cherche à répondre à ces défis tout en maintenant des garanties solides, notamment le respect de la Charte canadienne des droits et libertés et la protection de la vie privée des Canadiennes et des Canadiens.

[*Traduction*]

Les dispositions dans le projet de loi C-22 sont regroupées sous deux thèmes principaux. D'abord, la partie 1 du projet de loi modernise les autorisations législatives du Canada afin d'aider la police et le SCRS à obtenir un accès légal et en temps opportun aux renseignements numériques nécessaires pour mener des enquêtes, chaque outil ayant été soigneusement conçu pour tenir compte du type d'information qui sera recueilli et du droit à la vie privée qu'il soulève.

Cela comprend la création d'un nouvel outil de confirmation de la fourniture de services, qui permettrait à la police de confirmer si un fournisseur de services de télécommunications offre ou a offert un service à un identifiant particulier, par exemple une adresse IP ou un numéro de téléphone particulier. La portée de cet outil a été délibérément limitée à une confirmation par oui ou non, et elle ne concerne que les fournisseurs de services de télécommunications.

La partie 1 créerait également une nouvelle ordonnance de communication des renseignements relatifs à la personne abonnée plus restreinte, comme son nom, son adresse et des renseignements de base au sujet des services offerts, et moderniserait les pouvoirs liés au mandat de perquisition afin de mieux refléter les recherches informatiques.

En outre, il établirait une nouvelle autorisation législative permettant aux autorités policières canadiennes de présenter une demande à un fournisseur de services électroniques étranger et renforçant la coopération internationale en matière criminelle concernant les données électroniques.

Ces mesures visent à faire en sorte que, lorsqu'ils sont autorisés par la loi, les enquêteurs puissent agir de manière opportune et efficace, en gardant à l'esprit que les retards peuvent entraîner des préjudices graves et continus pour les victimes dans des circonstances et des cas particuliers.

● (1600)

[*Français*]

La deuxième partie du projet de loi établit un cadre législatif clair et moderne afin de garantir que les fournisseurs de services électroniques ont les capacités techniques nécessaires pour répondre efficacement aux demandes d'accès légal, c'est-à-dire un accès déjà approuvé en vertu des lois en vigueur, telles que le Code criminel ou la Loi sur le Service canadien du renseignement de sécurité.

Le Canada est actuellement la seule démocratie occidentale à ne pas disposer d'un cadre juridique complet exigeant que les fournisseurs de services électroniques développent et maintiennent de telles capacités techniques. À l'exception d'un régime de licences désuet datant des années 1990, la collaboration dans ce domaine demeure largement volontaire et inégale.

La partie 2 du projet de loi C-22 établit des exigences minimales en matière de capacités techniques pour les fournisseurs principaux alignées sur les normes internationales, et elle confère au ministre de la Sécurité publique le pouvoir de prendre des arrêtés ministériels ciblés et souples lorsque des capacités précises sont nécessaires pour répondre à des besoins opérationnels.

[*Traduction*]

Les mesures de protection liées à ce nouveau cadre sont intégrées dans le projet de loi. Par exemple, les arrêtés ministériels seraient soumis à une approbation par le commissaire au renseignement et signalés de manière proactive à l'OSSNR. Les considérations en matière de vie privée et de cybersécurité sont explicitement incluses dans le projet de loi. Les obligations liées à la rétention des données sont restreintes, et des rapports publics annuels sont requis.

Cette partie ne crée pas de nouveaux pouvoirs pour les forces d'application de la loi ou le SCRS d'intercepter des communications ou d'obtenir des renseignements, pas plus qu'il ne permet l'accès direct du gouvernement aux systèmes des fournisseurs de services électroniques. Il interdit aussi explicitement la création de vulnérabilités systémiques, garantissant ainsi qu'un règlement ou un arrêté ministériel ne fragilise pas le chiffrement et ne crée pas de portes dérobées.

Enfin, la partie 2 établit des outils pour promouvoir la conformité, ce qui comprend les inspections et les sanctions administratives pécuniaires.

[*Français*]

Ensemble, ces mécanismes visent à garantir que les organismes canadiens d'application de la loi et du renseignement disposent des outils nécessaires pour faire leur travail important, tout en maintenant une reddition de comptes et une transparence solides.

Monsieur le président et membres du Comité, mes collègues et moi serions maintenant heureux de répondre à vos questions.

Le président: Merci, monsieur McGuire.

Je cède maintenant la parole à M. Caputo pour six minutes.

[*Traduction*]

Frank Caputo (Kamloops—Thompson—Nicola, PCC): Merci beaucoup, monsieur le président.

Merci à tous nos témoins. C'est formidable d'avoir autour de la table autant de personnes pour discuter d'un enjeu aussi complexe. Nous aurons l'occasion de mieux nous connaître au cours des deux prochaines semaines parlementaires.

Je ne sais jamais à qui adresser mes questions parce qu'il y a beaucoup d'experts ici. N'hésitez pas à me dire qui est la personne la mieux placée pour y répondre.

J'ai examiné les définitions. J'ai examiné les définitions de « vulnérabilité systémique », la manière dont elle englobe la définition des données chiffrées dans une certaine mesure, ainsi que la définition, à la partie 2, selon laquelle un fournisseur de services ne doit rien faire qui créerait une vulnérabilité systémique. Je vais poser une question très directe. Ce projet de loi couvrira-t-il les données chiffrées? Ensuite, est-ce bien l'intention? Je présume que la réponse sera oui. Ce projet de loi couvrira-t-il les données chiffrées? Y a-t-il quelqu'un qui pourrait m'aider à y voir clair?

Shannon Hiegel (directrice générale, Direction de la politique de sécurité nationale, ministère de la Sécurité publique et de la Protection civile): Merci beaucoup de poser la question. Je suis Shannon Hiegel, directrice générale de la Direction de la politique de sécurité nationale au ministère de la Sécurité publique.

Il s'avère que le projet de loi est neutre sur le plan du chiffrement. Nous voulons nous assurer que, lorsque le chiffrement est utilisé… Il y a différents moyens de l'utiliser et différents moyens pour les entreprises de l'employer. Par conséquent, nous ne voulons pas exclure la possibilité que certaines entreprises utilisent un chiffrement pour lequel des clés sont disponibles et où les données peuvent être déchiffrées de façon relativement simple.

Frank Caputo: D'accord, mais avec tout le respect que je vous dois, madame Hiegel, vous dites « des clés sont disponibles ». Or, tel que je le comprends, ce projet de loi exigerait justement qu'une clé soit disponible, n'est-ce pas?

Shannon Hiegel: Certaines entreprises emploient déjà un type de chiffrement pour lequel elles ont la clé. Nous ne demandons pas que des clés soient créées si une entreprise en a déjà une.

● (1605)

Frank Caputo: Nous ne parlons peut-être pas exactement de la même chose, parce que, d'après ma compréhension de la partie 2 — particulièrement l'article 5 proposé — il y est question d'un niveau de base auquel les fournisseurs doivent se conformer. Est-ce que je suis clair jusqu'ici?

Shannon Hiegel: Oui.

Frank Caputo: Si les fournisseurs doivent se conformer à ce niveau de base et qu'ils n'en sont pas encore là, comment se fait-il qu'ils n'aient pas à créer de clé pour atteindre le niveau de base que l'article 5 proposé exige d'eux? Voyez-vous ce que je veux dire?

Shannon Hiegel: Parlez-vous d'un fournisseur qui devrait atteindre un niveau alors qu'il n'a même pas ce chiffrement? C'est ce que je comprends de votre question.

Frank Caputo: Non, je voulais dire un cas où un service de chiffrement est offert. Ma question était de savoir si ce fournisseur de chiffrement…?

L'entreprise A fournit un service de chiffrement de bout en bout dans les messages. Dans le cadre du projet de loi, l'entreprise A devra-t-elle créer une sorte de mécanisme en fonction duquel les données pourront être interceptées et le gouvernement ou l'État — lorsque je dis « État », je pense que vous savez ce que je veux dire, les forces de l'ordre — pourra accéder à ces données chiffrées?

Est-ce clair?

Shannon Hiegel: Absolument.

Si une entreprise offre le chiffrement de bout en bout dans le cadre de ses services et de son modèle d'affaires, nous ne l'obligeons pas à déchiffrer ces communications.

Frank Caputo: D'accord. Ce n'est pas clair jusqu'ici. Lorsque j'ai lu le projet de loi, je me suis dit: « D'accord, c'est ce que cela signifie », mais nous avons aussi vu de la correspondance à ce sujet. Si le projet de loi ne vise pas les données chiffrées, je suggère que nous l'indiquions explicitement: « Il est entendu que cette partie ne s'applique pas aux données chiffrées », puis que nous ajoutions une définition.

Est-ce que cela aurait du sens de procéder ainsi?

Shannon Hiegel: Je pense que nous voulons faire preuve d'un peu de souplesse lorsqu'il s'agit de chiffrement. Je m'excuse si la première partie de ma réponse n'était pas claire, mais il existe différents types de chiffrement. Si on parle de chiffrement sans aucun qualificatif, cela signifie que, lorsque les entreprises possèdent des clés et peuvent déchiffrer les données aux fins d'une enquête lorsqu'un mandat et qu'une ordonnance de communication sont fournis, elles pourraient en fait toujours utiliser ces clés à cette fin.

Frank Caputo: Je parle en fait d'une entreprise dont la « sauce secrète » — si vous excusez mon expression vernaculaire — fournit un service de chiffrement. C'est ce qu'elle fait. L'entreprise A fournit un service selon lequel la communication du terminal un au terminal deux, ou du contact un au contact deux, sera chiffrée. C'est son modèle d'affaires.

Ma question est la suivante: le projet de loi C-22 exigera-t-il que cette entreprise puisse se brancher sur ce chiffrement et déchiffrer les données pour les forces de l'ordre?

Shannon Hiegel: Non. S'il n'y a pas de clés et qu'il n'existe aucun moyen de le décrypter, et que c'est son modèle d'affaires, alors on considérerait que cela constituerait une vulnérabilité systémique pour l'ensemble de son système, et il faudrait en discuter avec le gouvernement. Au bout du compte, nous ne l'obligerions pas à intégrer dans son système une vulnérabilité systémique.

Frank Caputo: C'est exactement ce que je cherchais, mais, d'après ma lecture du projet de loi — en passant par une définition, puis par la notion de vulnérabilité systémique —, ce n'était pas clair pour moi. Voici donc ma recommandation: en tant que fonctionnaires, je vous invite à vous pencher sur cette question, car, selon moi, il faudrait, premièrement, une définition des données chiffrées et, deuxièmement, une disposition qui énonce très clairement ce que vous venez de dire — à savoir que le déchiffrement de données chiffrées donne lieu à une vulnérabilité systémique — ou alors l'intégrer directement dans la définition de « vulnérabilité systémique ».

Je sais que c'est technique. J'espère que je suis clair.

Le président: C'est peut-être très clair, mais malheureusement, nous ne saurons pas ce qu'en pense Mme Hiegel, car nous devons céder la parole à Mme Acan pour six minutes, s'il vous plaît.

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

Monsieur McGuire et madame Hiegel, j'ai des questions plutôt techniques, alors je suppose que c'est vous qui allez y répondre.

Alors que nous examinons le paysage changeant de la sécurité publique et de la sécurité nationale, il est essentiel de comprendre clairement le rôle des métadonnées. On décrit souvent les métadonnées comme des données au sujet des données qui ne saisissent pas le contenu des communications, mais fournissent plutôt des renseignements contextuels comme le moment, le lieu, la durée, l'origine ou la destination d'interactions numériques.

Bien qu'elles soient différentes des données de contenu, les métadonnées peuvent, dans des circonstances précises, apporter un éclairage analytique et aider à recenser des tendances pertinentes pour les besoins opérationnels. Cela fait des métadonnées un outil opérationnel précieux pour les forces de l'ordre et les agences du renseignement, qui joue un rôle essentiel pour assurer la détection des menaces, l'évaluation des risques et l'efficacité des enquêtes, en particulier à une époque où, l'activité numérique est fortement intégrée dans notre vie quotidienne.

Corrigez-moi si j'ai tort ou si quoi que ce soit m'a échappé concernant les métadonnées, mais dans ce contexte, pourriez-vous s'il vous plaît clarifier la portée de l'information à laquelle les forces de l'ordre seraient autorisées à accéder en vertu du projet de loi, et confirmer précisément en quoi les métadonnées diffèrent du contenu des communications dans la pratique?

● (1610)

Shannon Hiegel: Je vais commencer, et si vous n'y voyez pas d'inconvénients, je vais céder la parole à mon collègue, M. Ho. Puis, si vous m'accordez quelques minutes, je demanderai à la GRC et peut-être au SCRS d'expliquer l'importance des métadonnées dans leurs opérations.

Comme vous le voyez dans le projet de loi tel qu'il est actuellement libellé, nous n'avons pas beaucoup précisé les éléments des métadonnées que nous prévoyons réglementer. C'est parce que nous devons prendre le temps d'évaluer cet aspect avec nos organismes d'enquête et discuter avec l'industrie de la capacité de conserver divers types, et pour combien de temps. En aucun cas, nous ne présumons… Lorsque nous remarquons que c'est pour une période maximale d'un an, nous nous attendons à ce que ce ne soit pas tous les points de métadonnées qui soient conservés aussi longtemps. C'est pourquoi il y a un délai prévu.

Nous avons examiné les comparaisons internationales sur ce plan et avons trouvé un juste milieu. L'Australie détient ses métadonnées pendant deux ans, et le Royaume-Uni, pendant environ un an. Il y a toujours des petits caractères, mais en général, c'est bien cela.

Dans le cadre de ce processus, nous nous attendons à préciser les types particuliers de métadonnées qui sont les plus importantes à des fins d'enquête, puis à y appliquer un délai dans le cadre du processus réglementaire. C'est à ce moment-là que nous présenterons une contestation fondée sur la Charte.

Monsieur Ho, souhaitez-vous ajouter quelque chose?

Fenton Ho (directeur, Politique du renseignement, ministère de la Sécurité publique et de la Protection civile): Merci.

Je pense que l'idée principale ici, c'est que nous associons les métadonnées à des capacités qui soutiendront les forces de l'ordre. C'est ainsi que nous générons et établissons réellement ce dont nous avons besoin. L'idée générale, comme Mme Hiegel l'a expliqué, c'est que nous travaillerons en très étroite collaboration avec les forces de l'ordre et avec le SCRS pour déterminer quels champs de données sont nécessaires et comment ils appuient les enquêtes, afin de pouvoir présenter un argument solide démontrant en quoi c'est proportionnel et pourquoi il est nécessaire de les garder.

Ramzi Nashef (directeur général, Service canadien du renseignement de sécurité): J'ai un bref point opérationnel.

Ce dont nous parlons ici, c'est d'une meilleure compréhension de la tendance des communications, essentiellement. Dans le cadre des règlements, nous étudierons les détails particuliers des types de métadonnées que nous allons saisir. De manière générale, de notre point de vue, nous le ferions afin d'établir des tendances de communication, de manière justifiée, qui serviront de base à une enquête. Il y a évidemment de nombreux autres éléments, mais c'est le genre de tendances que nous rechercherions de notre côté.

Sima Acan: Ma prochaine question s'adresse encore probablement à vous ou au SCRS.

Le projet de loi C-22 introduit un nouveau pouvoir, l'ordre de confirmer la fourniture de services. Cette modification de la Loi sur le SCRS vise à permettre aux autorités de continuer d'obtenir les renseignements nécessaires pour les appuyer dans des enquêtes complexes et avancées.

Comment ce processus de confirmation de fourniture de services par oui ou non introduit dans le projet de loi C-22 concilie-t-il les considérations en matière de vie privée et les besoins en matière d'enquête? De quelle façon le fait de limiter la divulgation à l'existence d'un service, plutôt qu'à l'identité d'un abonné, influence-t-il la nature et la portée des renseignements mis à la disposition des forces de l'ordre?

Richard Burchill (directeur général, Services d'enquête technique, Gendarmerie royale du Canada): L'ordre de confirmer la fourniture de services se situe vraiment en amont, au tout début de l'enquête, afin de nous permettre de recueillir les renseignements de base nécessaires pour pouvoir la poursuivre. Nous disposons de très peu d'informations, par exemple un numéro de téléphone ou une adresse IP. Cette simple confirmation par oui ou non d'un fournisseur de services de télécommunications nous confère la capacité de vérifier que cette personne est abonnée à cette entreprise. Nous pouvons alors commencer le travail d'enquête autour de cet élément afin d'obtenir des motifs suffisants pour présenter une ordonnance de communication visant à obtenir les renseignements sur l'abonné, à l'étape suivante. Nous devons tout de même établir ces motifs d'enquête afin de pouvoir présenter à un juge une ordonnance de communication visant à obtenir les renseignements sur l'abonné.

Même si les membres des forces de l'ordre et du service du renseignement disposent de divers moyens pour obtenir ces renseignements de manière traditionnelle, cet ordre de confirmer la fourniture de services codifie ce processus et permet la divulgation. Nous devons documenter un ordre de confirmer la fourniture de services. C'est versé dans notre dossier, divulgué devant les tribunaux et peut faire l'objet d'un interrogatoire. Nous disposons de motifs raisonnables pour soupçonner et demander la confirmation de la fourniture de services. Une fois celle-ci obtenue, nous devons encore établir la capacité d'enquête nécessaire autour d'une ordonnance de communication afin de pouvoir nous adresser à un juge.

● (1615)

Le président: Merci beaucoup.

[*Français*]

Madame DeBellefeuille, la parole est à vous pour six minutes.

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

Madame Hiegel, le ministre nous a dit qu'entre les projets de loi C-2 et C-22, il y avait eu des consultations avec certains groupes.

Est-ce que vous pouvez me confirmer que la présidente actuelle de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, Mme Deschamps, a été consultée au sujet du projet de loi C-22?

Mike McGuire: Je peux parler un peu des consultations.

Claude DeBellefeuille: Je veux juste que vous me répondiez par oui ou non. Savez-vous si Mme Deschamps a été consultée au sujet du projet de loi C-22?

Mike McGuire: Il y avait différents types de consultations. Il y avait des rencontres que le ministre a eues lui-même avec certaines personnes, et aussi des tables rondes.

Claude DeBellefeuille: À votre connaissance, Mme Deschamps a-t-elle été consultée? C'est assez simple comme question, monsieur McGuire.

Mike McGuire: À ma connaissance, elle ne faisait pas partie des tables rondes que nous avons organisées.

Claude DeBellefeuille: Donc, l'actuelle présidente de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement n'a pas été consultée au sujet du projet de loi C-22. On a choisi un ex-président pour la consultation. C'est ce que j'ai compris de mes lectures.

Mike McGuire: Pour les tables rondes que nous avons organisées, c'est le cas, mais il y avait d'autres consultations.

Claude DeBellefeuille: Ne trouvez-vous pas un peu particulier que la présidente actuelle n'ait pas été consultée pour un projet de loi sur l'accès légal?

Quand on voit ce qui se fait ailleurs, dans les autres pays auxquels se compare le Canada, et que les homologues de l'Office ont quand même un rôle important à jouer dans les lois sur l'accès légal, ne trouvez-vous pas ça un peu curieux?

Mike McGuire: Beaucoup d'informations ont contribué à l'analyse que nous avons faite. Il y a aussi eu différentes consultations et différentes lettres que nous avons reçues de parties prenantes. Donc, différentes méthodes ont été utilisées pour établir les différentes positions des parties prenantes.

Claude DeBellefeuille: Monsieur McGuire, c'est juste que ça m'étonne, parce que c'est un office important. Ça m'étonne qu'on n'ait pas consulté sa présidente.

Avez-vous consulté le commissaire à la protection de la vie privée?

Mike McGuire: Oui, absolument.

Claude DeBellefeuille: Alors, vous avez choisi de consulter le commissaire à la protection de la vie privée, mais pas la présidente de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. C'est ce que je comprends.

Mike McGuire: Nous avons consulté le commissaire à la protection de la vie privée.

Claude DeBellefeuille: Cependant, vous n'avez pas consulté la présidente de l'Office.

Je vais poser une question que j'ai posée plusieurs fois en Chambre à l'équipe du ministère de la Justice. Je ne suis pas juriste, et j'aimerais comprendre pourquoi vous avez choisi le seuil le plus bas pour l'obtention de l'information.

Pour moi, le fait d'avoir des motifs raisonnables de « soupçonner » quelque chose me semble être un seuil très, très bas pour obtenir de l'information. Par contre, le fait d'avoir des motifs raisonnables de « croire » quelque chose serait un seuil plus élevé. Je ne comprends pas pourquoi vous avez choisi ce seuil.

Est-ce que vous pourriez donner au Comité des exemples de ce que pourrait être un motif raisonnable de soupçonner quelque chose? J'ai de la difficulté à imaginer ce qui ne serait pas acceptable. Il me semble que tout motif de soupçonner quelque chose peut être raisonnable. Comprendre cette partie du projet de loi me préoccupe beaucoup. Est-ce qu'il vous est possible de nous donner des exemples concrets de ce qui pourrait être un motif raisonnable de soupçonner quelque chose?

Anne-Marie LeBel (avocate, Section de la politique en matière de droit pénal, ministère de la Justice): Je vous remercie de cette très bonne question.

Effectivement, nous pouvons vous donner des exemples pratiques et je vais peut-être me tourner vers mon collègue de la GRC pour m'aider.

Cependant, avant d'en arriver là, je peux vous expliquer pourquoi nous avons choisi ce seuil. C'est un seuil légal qui existe pour d'autres ordonnances de communication précises dans le Code criminel, qui visent des types particuliers et précis de données dont la nature, en matière de vie privée, est moins sensible que d'autres, notamment le contenu qui est obtenu avec une ordonnance générale de communication.

Claude DeBellefeuille: Est-ce que vous pourriez nous dire ce que ce serait un motif raisonnable de soupçonner quelque chose pour que je puisse bien voir la différence entre ce seuil et d'autres seuils et que je comprenne ce qu'il y a derrière votre intention?

Anne-Marie LeBel: Avant que mon collègue vous donne un exemple concret, j'ajouterais qu'un motif raisonnable de soupçonner quelque chose, ce n'est pas juste un soupçon. Il faut qu'il y ait des faits observables. Le policier doit avoir des notes par rapport à ces faits lorsqu'il en vient à la conclusion qu'il a des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise.

Dans nos deux outils, la condition, c'est qu'il y ait des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise, mais également que l'information demandée sera utile à l'enquête.

● (1620)

Claude DeBellefeuille: Merci, madame Lebel.

Moi, j'aurais besoin de ça. Je ne suis pas juriste, et j'aimerais mieux comprendre, si possible.

Avec le temps qui me reste, j'aimerais aussi comprendre autre chose. Dans la première partie du projet de loi, on dit que le terme « fournisseur de services de télécommunication » s'entend au sens du paragraphe 2(1) de la Loi sur les télécommunications, alors que dans la partie 2 du projet de loi, on parle de fournisseur de services électroniques et de fournisseur principal. Or, dans l'annexe, il n'y a pas de définition.

Là, je veux comprendre pourquoi donner ce pouvoir réglementaire très grand dans des définitions. Il y a des gens qui nous interpellent et qui se demandent s'ils vont être concernés. Est-ce que vous pouvez m'expliquer pourquoi il n'y a pas de définition, pourquoi on ne trouve rien dans l'annexe et pourquoi tout va être décidé par règlement?

Anne-Marie LeBel: Je pense que la question se rapporte davantage à la partie 2, donc à la nouvelle loi et à l'annexe. Je vais laisser ma collègue y répondre.

Shannon Hiegel: Oui, c'est une question pour moi.

Dans la partie 2, vous avez raison de dire qu'il y a juste une définition pour « fournisseur de services électroniques ».

C'est une définition très large. C'est important, parce que la technologie change rapidement.

Le président: Malheureusement, je vais devoir vous interrompre, parce que le temps est déjà écoulé et que je crois que la réponse va être un peu longue. On y reviendra peut-être plus tard.

Monsieur le député Lloyd, vous avez la parole pour cinq minutes.

[*Traduction*]

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

Merci aux témoins d'être ici aujourd'hui.

Je vais commencer par M. McGuire.

Une chose que je trouve contradictoire dans le projet de loi — vous pourrez peut-être expliquer en quoi ce n'est pas contradictoire —, c'est que vous exigez des fournisseurs de services électroniques et des entreprises de télécommunications qu'ils créent les systèmes permettant l'interception des communications au sein de leurs réseaux, or vous affirmez ensuite que rien dans le projet de loi ne vise à miner l'intégrité des réseaux de chiffrement. Cela me semble très contradictoire.

À la lumière du piratage de Salt Typhoon que nous avons vu aux États-Unis… On a découvert par la suite que ce sont précisément les vulnérabilités créées par les exigences du droit américain — qui imposaient l'existence de portes dérobées dans les mécanismes de chiffrement — qui ont permis aux pirates d'accéder à ces renseignements.

Pouvez-vous expliquer en quoi consiste cette apparente contradiction?

Mike McGuire: Je vais commencer rapidement, puis je céderai la parole à Mme Hiegel.

L'intention de la partie 2 est de s'assurer que les fournisseurs de services électroniques disposent des capacités techniques nécessaires pour répondre aux demandes d'accès légales autorisées pour les forces de l'ordre et le SCRS.

Madame Hiegel, voulez-vous ajouter quelque chose?

Shannon Hiegel: Je vais commencer, puis je céderai la parole à M. Ho.

Nous avons examiné une multitude d'autres pays qui ont mis en place ce type de législation et ont trouvé des moyens de travailler avec les entreprises afin d'extraire les renseignements pour qu'ils puissent être fournis aux enquêteurs en vue de leurs enquêtes particulières.

Je ne crois pas qu'il y ait nécessairement de contradiction entre les deux parties, car nous allons définir des objectifs. Nous, le gouvernement, n'allons pas dire aux entreprises — ou aux principaux fournisseurs, essentiellement — ce qu'elles doivent créer et comment elles doivent le faire…

Dane Lloyd: Je comprends ce que vous dites, soit que le gouvernement ne dicte pas comment les entreprises doivent le faire, mais il oblige les entreprises à le faire, et pour se conformer, elles doivent créer dans leur système des vulnérabilités qui peuvent être exploitées par les pirates. N'êtes-vous pas d'accord avec moi?

Shannon Hiegel: Je dirais que les entreprises apportent toutes sortes de changements au sein de leurs systèmes pour leurs propres besoins. Dans le cadre de ce projet de loi, nous nous attendons à trouver des moyens sûrs de maintenir leur cybersécurité, ce à quoi le Canada s'attend.

Le Canada, d'abord et avant tout, accorde la priorité à la cybersécurité…

Dane Lloyd: Je vais vous arrêter ici.

S'il faut choisir entre une entreprise qui se conforme à la loi et la création d'une vulnérabilité qui peut être exploitée par des pirates, quel est le but ou le résultat final envisagé par le gouvernement du Canada?

Shannon Hiegel: Je pense que l'attente est que, en consultation avec le gouvernement, nous trouverons des solutions à ce problème. C'est un problème qui a désespérément besoin d'une solution. Collaborer avec l'industrie afin de pouvoir fournir les renseignements aux enquêteurs pour qu'ils enquêtent sur un si grand nombre de crimes pour l'instant non résolus…

● (1625)

Dane Lloyd: Si vous ne pouvez pas trouver de solution, du moins à court terme, est-il acceptable pour le gouvernement que les entreprises de télécommunications soient forcées de créer des vulnérabilités systémiques afin de se conformer à la loi?

Shannon Hiegel: Nous travaillons déjà avec certains partenaires, alors je remettrais en question l'idée selon laquelle il n'y a pas moyen de mettre des solutions en place.

Dane Lloyd: La Chambre de commerce du Canada a déclaré que cette loi va forcer ses membres à créer des vulnérabilités dans leurs systèmes. C'est un intervenant de tout premier plan, qui regroupe de nombreux acteurs avec lesquels le gouvernement du Canada collabore.

C'est une grande préoccupation, alors j'aimerais que ce soit clair: si le seul moyen de se conformer à cette loi est de créer des vulnérabilités systémiques, le gouvernement pense-t-il toujours que les entreprises doivent se conformer à la loi?

Fenton Ho: Nous parlons de diverses capacités. Ce n'est pas une seule capacité universelle. De plus, ces capacités existent déjà en ce moment. Beaucoup des grandes entreprises de télécommunications, à cause du système de permis, ont déjà la capacité de répondre à certaines demandes des forces de l'ordre ou du SCRS, alors dans ce cas, le projet de loi établit essentiellement des règles du jeu efficaces par rapport à ce qui existe déjà.

Cependant, si vous envisagez une application particulière, une capacité particulière qui n'existe pas, si elle atteint une vulnérabilité systémique, la réponse serait non.

Dane Lloyd: Il me reste 45 secondes. Si je peux obtenir cela par écrit, veuillez me l'envoyer par écrit.

Dans les 45 secondes qu'il me reste… La secrétaire d'État (Lutte contre la criminalité) a affirmé que de nombreux intervenants décrivent cette mesure comme un premier pas essentiel et affirment qu'il faut élargir le projet de loi. Le ministère de la Sécurité publique planche-t-il sur des dispositions législatives de suivi pour élargir les pouvoirs conférés en vertu du projet de loi C-22 à l'heure actuelle?

Shannon Hiegel: Non, pas en ce moment.

Dane Lloyd: Pouvez-vous affirmer que le ministère a réalisé des études sur ce que pourraient être les prochaines étapes, si le projet de loi était adopté, concernant les dispositions législatives de suivi dans ce domaine?

Shannon Hiegel: Non, nous sommes très concentrés sur l'étape réglementaire qui suivrait, si nous réussissons à obtenir la sanction royale.

Dane Lloyd: Merci.

Le président: Merci beaucoup, monsieur Lloyd.

Monsieur Powlowski, vous avez cinq minutes, s'il vous plaît.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): J'ai une lettre sous les yeux, intitulée « Appel conjoint au retrait du projet de loi C-22 », qui est signée par, me semble-t-il, un certain nombre d'organisations passablement réputées, comme la British Columbia Civil Liberties Association, la Canadian Association of University Teachers, l'Association canadienne des libertés civiles et le Conseil canadien pour les réfugiés. Dans cette lettre, on mentionne « la portée énormément envahissante du projet de loi C-22 et les pouvoirs illimités sans précédent qu'il instaure... » Et la lettre se poursuit.

J'aimerais vous parler d'une disposition spécifique, mais permettez-moi de lire l'ensemble du paragraphe:

> Le projet de loi C-22 a apporté quelques modifications à la proposition du projet de loi C-22 concernant l'accès de grande envergure et sans mandat aux renseignements sensibles sur les abonnés. Le pouvoir d'exiger ceux-ci sans mandat ne peut maintenant être utilisé que pour demander aux fournisseurs de services de télécommunication si une personne fait partie de leur clientèle. En revanche, l'approche des données sur les abonnés demeure déficiente dans le projet de loi C-22 en faisant passer la norme de l'autorisation judiciaire pour un mandat de la « raison de croire » au seuil très inférieur de la « raison de soupçonner », malgré les décisions de la Cour suprême reconnaissant que d'importants droits à la vie privée sont en jeu dans cette forme d'accès aux données.

Si nous sommes préoccupés par la portée envahissante du projet de loi, et si nous sommes préoccupés — comme elles le sont — par la surveillance de masse de tous les Canadiens, j'aurais tendance à dire, moi aussi, que « les raisons de soupçonner » semblent être un seuil très peu élevé pour permettre l'accès à des données éventuellement personnelles. Quelqu'un veut-il répondre à cette accusation?

Kimberly Gibner (sous-ministre adjointe déléguée, Secteur des politiques, ministère de la Justice): Je vais répondre à cette question.

Je pense que mon collègue a abordé la question et a souligné qu'il existe toutes sortes de dispositions dans le Code criminel qui utilisent la norme des motifs raisonnables de soupçonner. Dans ce cas, les renseignements de l'abonné que l'on cherche sont essentiellement le nom et l'adresse. En ce qui concerne l'équilibre entre ce type de renseignement et les préoccupations liées à la protection de la vie privée, la norme des motifs raisonnables de soupçonner a été choisie comme la norme appropriée.

Pour revenir sur votre point concernant l'affaire Spencer, l'arrêt précisait qu'il était essentiel qu'une autorisation légale soit mise en place, donc, depuis 2014, la police demande une autorisation légale. C'est ce que fait le projet de loi C-22. Il fournit une autorisation légale.

Marcus Powlowski: Maintenant, en ce qui concerne les services chiffrés de bout en bout, comme Signal, où les fournisseurs ne possèdent jamais les données chiffrées ou les clés de déchiffrement, on ne s'attendrait pas à ce que ces fournisseurs réduisent le niveau de protection de leur chiffrement pour se conformer. N'est-ce pas?

● (1630)

Shannon Hiegel: Exact.

Marcus Powlowski: D'accord.

Enfin, vous avez parlé de la collecte des métadonnées. Quel genre de métadonnées? Si je suis sur Internet, et que je suis sensible à la situation de la population de Gaza et que je fais des recherches sur Gaza et que, par inadvertance, quelque chose apparaît à l'écran au sujet du Hamas, y a-t-il une raison pour que le gouvernement enquête davantage sur moi en raison de la possibilité que je puisse, en quelque sorte, faire des choses pour promouvoir une organisation terroriste? Quel genre de métadonnées cherchez-vous? La notion de métadonnées semble très large. Ce que je veux dire, c'est qu'il s'agit de tout ce que nous faisons. Si vous posiez la question à l'intelligence artificielle, elle trouverait probablement quelque chose sur Marcus Powlowski.

Shannon Hiegel: Il est compréhensible d'être préoccupé par cela. Ce que je voudrais faire, c'est de m'en remettre à mon collègue de la GRC qui, avec son équipe, m'aidera à définir les éléments très spécifiques des métadonnées exigées. Elles seront réglementées, mais mon collègue peut donner des exemples précis.

Richard Burchill: Je peux vous donner quatre exemples de rétention des métadonnées qui sont utiles pour les organismes d'application de la loi, dans le cadre d'une enquête. Les premières, ce sont les données de transmission sur Internet, qui comprennent les horodatages, les adresses IP et les identificateurs d'appareil. Comme vous le comprendrez, nous ne lançons pas une enquête immédiatement après qu'un incident survient. Si quelque chose arrive et qu'il y a une activité en ligne, un signalement doit être fait, et une enquête doit être ouverte. Si nous cherchons à obtenir des métadonnées, nous devons obtenir une autorisation judiciaire; des activités criminelles ont dû avoir lieu, et des victimes sont impliquées dès le départ. Quand nous en arrivons à l'étape où nous demandons les métadonnées, c'est pour tenter d'associer des personnes à des lieux. C'est là qu'interviennent les données de transmission sur Internet.

Les données de signalisation des tours cellulaires sont également utiles pour situer des personnes à un moment donné, quand une infraction a été commise ou qu'un appel a été passé, s'il s'agit d'un enlèvement ou de quelque chose du genre, où il faut trouver l'endroit où se trouve la personne qui conduisait un véhicule ou avait un téléphone à un moment donné.

Le président: Je m'excuse, mais je dois vous interrompre brusquement pour que nous puissions passer à Mme DeBellefeuille.

[*Français*]

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

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Madame Hiegel, le projet de loi C-22 donne quand même un rôle important au commissaire au renseignement. Est-ce que vous avez évalué la surcharge de travail que l'adoption de ce projet de loi pourrait lui occasionner?

Shannon Hiegel: Je vous remercie de la question.

[*Traduction*]

Je m'excuse. Je vais parler dans ma langue.

Nous avons rencontré le commissaire au renseignement lui-même et son équipe afin de discuter de ce rôle. Une fois le processus approuvé, il constituera le deuxième niveau d'autorisation. Il a parlé du fait que… Nous avons donné une idée de nos attentes et avons parlé du nombre d'arrêtés ministériels qu'il pourrait y avoir chaque année.

[*Français*]

Claude DeBellefeuille: [*Inaudible*] votre évaluation. Comment pensez-vous qu'il va être interpellé, avec l'adoption du projet de loi C-22? Comme vous le savez, il a déposé son rapport annuel, qui contient 14 décisions, un nombre record. Maintenant, je me demande s'il va y avoir beaucoup de décisions. Est-ce que vous évaluez le nombre de décisions pour le commissaire?

[*Traduction*]

Shannon Hiegel: Son rôle est précisément lié au processus d'approbation des arrêtés ministériels. Il examinera l'ensemble des renseignements fournis au ministre, au moment où le ministre prendra sa décision au sujet d'un arrêté ministériel, ce qui est une demande très précise visant à mettre en place certaines capacités pour une entreprise qui ne serait pas considérée comme un fournisseur principal.

[*Français*]

Claude DeBellefeuille: Ça veut donc dire que c'est exceptionnel. Ce ne sera pas courant. Il n'y aura pas de nombreuses décisions. Le commissaire au renseignement ne sera pas surchargé.

[*Traduction*]

Shannon Hiegel: Non, et il a confirmé ce point. Nous lui avons donné les chiffres préliminaires concernant le nombre d'arrêtés ministériels qui lui seraient transmis, et il était convaincu de pouvoir les gérer.

[*Français*]

Claude DeBellefeuille: D'accord.

Je sais que le budget de son bureau n'a pas été augmenté pour qu'il puisse remplir ses obligations découlant du projet de loi C-22, alors je me demandais quelle charge de travail cela allait représenter.

Vous n'aurez peut-être pas le temps de me répondre, mais pourquoi n'avez-vous pas inscrit, dans la partie 2, une définition claire de « fournisseur principal »?

● (1635)

[*Traduction*]

Shannon Hiegel: En ce qui concerne le fournisseur principal, nous avons une définition. Ce que nous prévoyons de faire, c'est passer par le processus réglementaire, dans le cadre duquel il y aura des classifications ou des catégories…

[*Français*]

Claude DeBellefeuille: Il n'y en a pas dans le projet de loi, madame Hiegel. On s'en remet à la voie réglementaire.

[*Traduction*]

Shannon Hiegel: Oui, il y en aura dans la réglementation.

[*Français*]

Le président: Malheureusement, je dois vous interrompre, je suis désolé.

Monsieur Caputo, vous avez la parole pour cinq minutes.

[*Traduction*]

Frank Caputo: Merci beaucoup.

La présence des fonctionnaires a été utile. Je tiens d'abord à dire que j'ai l'impression qu'il nous faudrait passer trois heures avec vous. Je ne dis pas cela pour plaisanter. C'est un projet de loi très technique. Nous ne pouvons pas traiter ce projet de loi à la hâte. J'ai une liste d'environ huit questions à vous poser.

Je vérifie actuellement la jurisprudence à la suite de l'argument que Mme DeBellefeuille a soulevé plus tôt concernant le seuil des « motifs raisonnables de soupçonner » par rapport aux « motifs raisonnables de croire ». Je ne me suis pas penché sur les motifs raisonnables de soupçonner depuis de nombreuses années. En ce qui concerne les motifs raisonnables de croire, je connais bien l'arrêt Storrey selon lequel une personne doit objectivement croire que ce qu'elle fait est raisonnable, et que cela doit être objectivement raisonnable.

Cela ne veut probablement rien dire pour de nombreuses personnes, mais ce sont des questions difficiles à comprendre. Puisque nous essayons de comprendre la question, je trouve qu'une seule heure avec vous avant l'étude article par article est insuffisante. Pour être très franc, je pense que nous avons besoin que vous restiez avec nous beaucoup plus longtemps. Je vous laisse y réfléchir, ainsi que le président et mes collègues libéraux, parce que nous avons de nombreuses questions, et je sais que je viens déjà d'utiliser une minute de mon temps.

C'est une question importante concernant l'obligation des fournisseurs de services électroniques de conserver les données pendant un an. S'agit-il, de fait, d'une saisie qui est contraire à l'article 8? Je crois comprendre qu'un mandat de recherche est nécessaire, et cela porterait sur l'aspect lié à la recherche. Normalement, il y a la recherche, ensuite la saisie. L'obligation de conserver des données constitue-t-elle en soi une saisie?

Shannon Hiegel: Je dirais simplement que nous n'avons pas considéré que l'obligation imposée à une entreprise de conserver des données équivalait à une saisie, dans le cadre d'une enquête, parce qu'aucune ordonnance de communication ni aucun mandat de recherche n'a été approuvé par un juge. Ce serait mon évaluation simple de la situation.

Avez-vous des idées à ce sujet?

Richard Burchill: Comme vous l'avez dit, une autorisation judiciaire est nécessaire pour avoir accès à ces données. Les délais de… Certaines entreprises conservent déjà ces métadonnées. Il n'existe pas d'application uniforme de cette pratique parmi les fournisseurs de télécommunications, alors que les organismes de sécurité et d'application de la loi recherchent cette uniformité. Quand on examine l'accès à ces données, la question des délais est importante parce que, si les données sont conservées pendant trois jours, mais qu'une semaine s'est déjà écoulée depuis le début d'une enquête pour enlèvement, ces données auront disparu, que l'on ait obtenu ou non une autorisation judiciaire, alors que certaines entreprises y donneraient rapidement accès.

Frank Caputo: Je comprends cela. Je vais vous expliquer mon point de vue à ce sujet. Dans ce cas, l'État ou le gouvernement impose une mesure, et cette mesure concerne les renseignements pour lesquels il existe une attente raisonnable en matière de protection de la vie privée. C'est pourquoi on a besoin d'un mandat. Dès le moment où l'on dit à un fournisseur A qu'il doit conserver ces données, il y a une attente raisonnable en matière de protection de la vie privée concernant les données qui doivent être conservées. Est-ce que jusque-là, tout le monde me suit? D'accord.

Est-ce que cela ne met pas en jeu l'article 8? Je me trompe peut-être, mais on m'a posé la question, et c'est donc un aspect que j'essaye d'examiner.

Shannon Hiegel: J'aimerais avoir une petite précision; quand vous parlez de l'article 8, voulez-vous parler de la partie 2 du projet de loi?

Frank Caputo: Oui.

Shannon Hiegel: Monsieur Ho, voulez-vous intervenir?

Fenton Ho: Évidemment, nous avons discuté des énoncés concernant la Charte et de questions relatives à cela. Une partie de l'analyse de ce point portera sur la façon dont nous limiterons notre utilisation des métadonnées. Dans ce cas, nous ne cherchons clairement pas… La durée maximale est d'un an. Nous ne disons pas qu'il s'agit d'une conservation généralisée. Dans le processus d'élaboration du règlement, nous devrions prouver que c'est nécessairement proportionnel à la durée. À ce moment-là, nous pourrons établir quelles obligations découlent de la Charte.

Frank Caputo: Pour aller dans ce sens, la période d'un an sert en quelque sorte de point de référence. Dites-vous…? Nous pourrions en parler pendant les 15 prochaines minutes — encore une fois, c'est une question très importante —, et il ne me reste que 33 secondes. Ce que vous dites, c'est qu'un an, c'est la période maximale. Ce n'est pas la période minimale. Ce n'est pas simplement une date limite absolue. Il ne s'agit que d'un an. Évidemment, toute date est arbitraire. Qu'est-ce qu'un an? Pourquoi ce n'est pas 9 ou 15 mois, ou encore 2 ans?

Pouvez-vous aider le Comité à comprendre pourquoi a-t-on choisi une période d'un an?

● (1640)

Shannon Hiegel: Comme je l'ai dit plus tôt, nous avons fait de nombreuses comparaisons avec d'autres pays, dans le cadre de notre analyse. Une période d'un an correspondait en fait assez souvent à la moyenne. Comme je l'ai dit, l'Australie se situe dans la tranche supérieure avec une période de deux ans.

Nous voulons également nous assurer qu'il est clair qu'il faut encore définir ce que nous prévoyons de conserver, dans le contexte des métadonnées. On s'attend à ce qu'il existe un certain niveau de justification. Peut-être que les métadonnées liées à mes communications avec M. Ho sont très importantes, parce que maintenant je sais qui parlait à qui, ce serait donc conservé pendant un an, tandis que quelque chose…

Le président: Je m'excuse de vous interrompre, madame Hiegel.

Nous devons passer à M. Housefather, pour cinq minutes, s'il vous plaît.

[*Français*]

Anthony Housefather (Mont-Royal, Lib.): Merci, monsieur le président.

[*Traduction*]

C'est toujours fascinant d'écouter mon collègue, M. Caputo.

D'abord, j'aimerais commencer par vous remercier d'être ici.

Évidemment, je soutiens tout à fait le projet de loi. Comme je l'ai dit à la Chambre, je crois que nous avons besoin d'un régime d'accès moderne. Je pense qu'il faut s'occuper des arrêts Bykovets et Spencer, et adopter un projet de loi approprié qui nous permet de traiter ces choses.

J'avais également deux ou trois questions, si cela vous convient, en ce qui concerne les interactions des vulnérabilités systémiques dans ce projet de loi, dans les paragraphes proposés 5(5) et 7(5) du projet de loi, par rapport aux articles 12 et 13 proposés. Essentiellement, d'après ce que je comprends des paragraphes 5(5) et 7(5) proposés du projet de loi, un fournisseur n'est pas tenu de se conformer, si cela créait une vulnérabilité systémique. Je crois que j'ai bien compris ce point. Cependant, l'article 12 proposé indique ceci: « Le fournisseur de services électroniques visé par l'arrêté pris en vertu du paragraphe 7(1) est tenu de s'y conformer. » Ensuite, l'article 13 proposé précise que les arrêtés l'emportent sur tout règlement pris.

Personnellement, je ne comprends pas vraiment l'interaction ici, où l'on dit, d'un côté, qu'une personne n'est pas tenue de se conformer si cela crée une vulnérabilité systémique, mais que, d'un autre côté, s'il y a un arrêté, elle est tenue de s'y conformer, puisque l'arrêté l'emporte sur le règlement.

Pouvez-vous m'expliquer ce point pour que je comprenne le fonctionnement des paragraphes 5(5) et 7(5)?

Shannon Hiegel: Bien sûr. Je vais commencer, et je vais ensuite me tourner vers mon expert, M. Ho.

Il faut voir cela comme un continuum, le point de départ étant que vous êtes un fournisseur principal — que ce soit par voie réglementaire ou au moyen d'un arrêt ministériel —, vous devez vous y conformer. Il y a ensuite l'exception. Si, dans le cadre du processus que nous menons avec vous pour déterminer comment obtenir ces renseignements à partir de vos réseaux, on a déterminé qu'il y a une vulnérabilité systémique, l'entreprise a alors le droit de refuser et de dire, « non, nous ne pouvons pas vous donner les renseignements dont vous avez besoin, parce qu'il y a une vulnérabilité systémique ».

Anthony Housefather: Si nous voulons dire cela, pourquoi est-ce que le projet de loi lui-même ne…? Actuellement, nous sommes d'accord pour dire que l'arrêté prime, et qu'ils doivent s'y conformer. N'est-ce pas?

Shannon Hiegel: Oui. C'est la base.

Anthony Housefather: Si l'entreprise estime que cela créerait une vulnérabilité systémique, dans quelles circonstances l'entreprise peut-elle alors — à moins qu'elle arrive à convaincre le ministre ou les représentants du ministre — s'opposer et dire, « non, cela créerait une vulnérabilité systémique »? Comment se fait-il que le projet de loi, dans sa forme actuelle, ne prévoie pas que l'on doive se conformer à l'arrêté, sauf dans la mesure où l'entreprise estime que, en déployant des efforts commerciaux raisonnables, elle ne peut pas faire cela sans créer une vulnérabilité systémique, ou quelque chose du genre?

Si l'entreprise estime que c'est le cas, mais que le cabinet du ministre n'accepte pas cet argument, qu'arrive-t-il à l'entreprise?

Shannon Hiegel: Dans le contexte d'un arrêté ministériel en particulier… Je resterai loin de ceux qui sont…

Anthony Housefather: Je pose uniquement la question en ce qui concerne l'arrêté ministériel.

Shannon Hiegel: D'accord. On s'attend à ce que la Sécurité publique se charge d'effectuer l'analyse que le ministre envisage. Par conséquent, nous recueillons les renseignements transmis par l'organisme opérationnel qui a signalé le problème ou la menace qu'il y a dans le système de l'entreprise. Nous sommes en fait tenus de consulter l'entreprise particulière et de répondre à un certain nombre d'exigences prévues dans le projet de loi. Étant donné que l'entreprise collabore avec nous dans le cadre de ce processus, elle peut donner ses points de vue.

Une fois que nous arrivons à la dernière étape, si le ministre approuve alors le processus, le commissaire au renseignement a connaissance de tous les renseignements que le ministre avait, et si lui aussi est d'accord pour que le processus aille de l'avant, l'entreprise a le droit de demander un contrôle judiciaire.

● (1645)

Anthony Housefather: À quel moment? On dit à ce moment-là à l'entreprise que le ministre et le commissaire ont dit qu'elle doit aller de l'avant, malgré sa déclaration. Ils passeraient ensuite par un contrôle judiciaire.

Que se passe-t-il avant que ce contrôle soit instruit? Êtes-vous en train de dire qu'il y aurait un sursis à l'exécution de l'arrêté?

Shannon Hiegel: Oui.

Monsieur Ho, voulez-vous ajouter quelque chose?

Fenton Ho: Non, je n'ai rien à ajouter.

Anthony Housefather: Je comprends.

Le président: Malheureusement, il n'y a plus de temps.

Merci, monsieur Housefather, de cette intervention.

C'est maintenant au tour de M. Caputo, pour cinq minutes, s'il vous plaît.

Frank Caputo: Merci.

J'aimerais revenir sur la période de conservation d'un an. Si j'ai bien compris… Les métadonnées sont, de manière générale, ce dont nous parlons ici, ou quoi que ce soit qui est prévu à l'article 5 proposé. Disons qu'il s'agit de données que l'on doit conserver. D'après ce que j'ai compris de ce qui a été dit plus tôt, c'est qu'une année est la période maximale, et que l'on a choisi la période d'une année parce que c'est, en quelque sorte, une norme internationale. Il n'y a rien de magique à propos de la période d'un an. Je comprends cela. Tous les chiffres sont arbitraires. Cependant, ce ne sont pas toutes les données qui seront conservées pendant un an. Ai-je bien compris ce point?

Shannon Hiegel: Oui, c'est vrai.

Frank Caputo: Qui décide du type de métadonnées qui seront conservées et de la durée de leur conservation? Disons que ce type de données, une adresse IP ou peu importe, doit uniquement être conservé pendant six mois. Qui décide de cela?

Shannon Hiegel: Cela serait décidé au moyen d'un processus réglementaire, pour lequel nous élaborons une analyse en collaboration avec les organismes afin de déterminer ce qui est le plus utile, pour ce qui est des processus d'enquête, ainsi qu'avec les entreprises. Quand nous menons le processus réglementaire, nous devons tenir compte d'éléments comme le coût pour l'industrie de la mise en œuvre de nouvelles réglementations. Elle participerait assurément. Comme l'a mentionné M. Burchill, parfois, les entreprises ont déjà ces données en leur possession, et cela n'entraîne pour elles aucun coût supplémentaire. Dans d'autres cas, les coûts pourraient être importants. Il faut prendre le temps d'effectuer cette analyse et de revenir avec un plan réfléchi.

Frank Caputo: À première vue, j'ai un problème avec ce point, parce que l'on doit uniquement tenir compte des coûts; on ne doit pas prendre une décision fondée sur les coûts. Il s'agit d'un facteur dont il faut tenir compte.

L'autre facteur, c'est que l'un des principaux aspects de la discussion concernant ce projet de loi porte sur les éléments qui relèvent de la réglementation. Essentiellement, 90 % du projet de loi pourraient être mis en œuvre au moyen de règlements, d'arrêtés ministériels et de mécanismes semblables. Ne faudrait-il pas préciser davantage les choses dans le projet de loi afin d'assurer une plus grande certitude? Si vous êtes un petit fournisseur de services électroniques qui essaye de mettre en œuvre la partie 2, ne seriez-vous pas préoccupé en ce moment en vous disant, « oh mon Dieu, combien cela va-t-il me coûter pour me conformer? » Il n'y a aucune certitude quant à ce à quoi ils devront se conformer.

Shannon Hiegel: Permettez-moi de répondre directement à la dernière partie de votre question. On s'attend à ce que les fournisseurs principaux passent également par un processus, dans lequel nous examinons des facteurs comme leur taille et le nombre de clients qu'ils servent. Il est peu probable que nous réglementions des propriétaires et des exploitants de petites entreprises, dans le cadre de la partie relative aux fournisseurs principaux de ce projet de loi.

Frank Caputo: Encore une fois, je vais revenir sur mon point précédent. Cela relève de la réglementation et de la décision de quelqu'un d'autre, qui tiendra compte notamment de la taille et des coûts. Au bout du compte, simplement parce que c'est envisagé, cela ne signifie pas que le fournisseur principal n'aura pas à exécuter ce que l'arrêt ministériel prévoit. Est-ce logique?

Shannon Hiegel: Je comprends ce que vous dites. L'une des raisons pour lesquelles le projet de loi est plus détaillé que d'autres auxquels vous pensez peut-être tient au fait qu'il est axé sur la technologie. L'utilisation de termes qui pourraient être désuets dans quelques années rendrait l'ensemble du projet de loi inutile.

● (1650)

Frank Caputo: Je comprends cela. Je sais que certaines choses doivent relever de la réglementation. Selon moi, un projet de loi comme celui-ci doit être aussi normatif que possible, lorsque c'est possible, parce que de très nombreux éléments relèvent de la réglementation.

Par exemple, chaque arrêté ministériel, selon ce que je constate dans l'article 7 proposé dans la partie 2, doit être approuvé par le commissaire au renseignement. Est-ce exact?

Shannon Hiegel: Oui.

Frank Caputo: Pourquoi pas un juge de la Cour fédérale? Je comprends. Ils sont tous deux supposés être indépendants. J'imagine que le commissaire au renseignement est supposé être indépendant; je ne comprends pas pourquoi. Ils sont tous les deux nommés par le gouvernement. Ils sont supposés tous les deux avoir des connaissances parfaites. Ils sont supposés tous les deux avoir toutes les connaissances nécessaires. Cependant, un juge de la Cour fédérale ne dépend pas du gouvernement. Il n'est pas « embauché ». Son mandat n'est pas renouvelé ou quoi que ce soit du genre. Il peut siéger jusqu'à l'âge de 75 ans.

Pourquoi un juge de la Cour fédérale ne joue-t-il pas le rôle de gardien, plutôt que le commissaire au renseignement, alors qu'il y a, au moins, une perception raisonnable de lien avec le gouvernement?

Shannon Hiegel: Avant de laisser M. Ho répondre à la question, je tiens à dire que, dans le cadre du processus d'arrêté ministériel, c'est le ministère de la Sécurité publique qui effectue l'analyse. Nous avons l'approbation du ministre. Le commissaire au renseignement, qui est indépendant, l'approuve également. Nous avons un organisme de surveillance quasi judiciaire, et il peut ensuite y avoir un contrôle judiciaire. Littéralement, du côté judiciaire, c'est la seule entité que nous avons laissée de côté.

Fenton Ho: J'ajouterais que, à la fin de tout cela, nous avons l'OSSNR.

Je pense que le commissaire au renseignement s'y connaît bien parce qu'il a l'habitude de faire ce genre de travail, liée par exemple aux autorisations ministérielles pour le Centre de la sécurité des télécommunications et le cadre de justification du SCRS. Il s'y connaît bien dans ces dossiers précis. Il a les connaissances nécessaires, donc il peut vraiment bien s'acquitter de cette fonction.

Le président: Merci.

Excusez-moi, monsieur Caputo, vous avez dépassé le temps qui vous était alloué.

Je vais maintenant suspendre la séance puisque, comme vous avez pu le constater, le ministre vient d'entrer.

Merci aux fonctionnaires. Bon nombre d'entre vous resteront parmi nous.

[*Français*]

Nous allons reprendre la séance dans quelques minutes. La séance est suspendue.

● (1650)

(Pause)

● (1655)

Le président: Nous reprenons la séance. Merci à tout le monde d'être de retour.

Je souhaite la bienvenue aux deux ministres et aux fonctionnaires qui les accompagnent, en commençant par le ministre Gary Anandasangaree, député et ministre de la Sécurité publique. Je souhaite aussi la bienvenue au ministre Sean Fraser, député et ministre de la Justice.

Vous êtes tous les deux les bienvenus, chers ministres. Nous allons commencer par une allocution de la part du ministre de la Sécurité publique, et ensuite ce sera celle du ministre de la Justice.

Monsieur Anandasangaree, la parole est à vous.

L'hon. Gary Anandasangaree (ministre de la Sécurité publique): Merci, monsieur le président.

[*Traduction*]

J'aimerais commencer par reconnaître que nous nous réunissons sur le territoire traditionnel non cédé du peuple algonquin anishinabe.

[*Français*]

Je vous remercie de l'invitation à comparaître aujourd'hui pour parler du projet de loi C-22.

[*Traduction*]

J'aimerais aussi saluer mon collègue, l'honorable Sean Fraser, avec qui je travaille sur ce projet de loi depuis un certain temps, et j'aimerais aussi saluer les fonctionnaires qui sont ici pour nous soutenir.

En tant que ministre de la Sécurité publique, ma priorité principale est de m'assurer que tous les Canadiens sont en sécurité. Depuis ma nomination, j'ai discuté avec des organismes d'application de la loi de tous les échelons — les services de police municipaux et la GRC — ainsi qu'avec des groupes de victimes, comme le Centre canadien de protection de l'enfance. Ils m'ont tous dit clairement que le Canada a besoin d'outils modernes pour lutter contre une vaste gamme d'activités illicites rendues plus faciles dans l'environnement numérique mondial.

La technologie a radicalement changé la nature de la criminalité et des menaces à l'échelle mondiale. Les criminels exploitent continuellement l'espace numérique dont nous nous servons tous pour commettre des infractions de tout genre. Cela inclut l'extorsion, l'exploitation d'enfants, le vol d'automobiles, le terrorisme et la traite de personnes. De plus, on se sert de cet environnement pour faciliter l'ingérence étrangère et l'extrémisme violent.

Nos lois n'ont tout simplement pas évolué au même rythme que notre monde axé sur le numérique. Cela a créé un écart important entre la criminalité et les menaces d'aujourd'hui et ce que peuvent faire adéquatement nos lois actuelles.

[*Français*]

Nous avons un devoir envers les Canadiens de nous attaquer à ces nouvelles menaces.

[*Traduction*]

C'est l'objectif du projet de loi C-22.

J'aimerais profiter de l'occasion pour souligner que le projet de loi C-22 ne vise pas à réglementer Internet ni à surveiller Internet. Il ne demande pas non plus aux fournisseurs de services Internet de devenir des agents du gouvernement, comme l'ont laissé entendre certains débats à la Chambre.

Comme l'ont confirmé nos fonctionnaires, le projet de loi C-22 est neutre en matière de chiffrement. Il vise simplement à combler les écarts relevés dans notre cadre juridique qui nous empêchent d'accéder rapidement à de l'information et à des renseignements essentiels pour mener une enquête. Il fournira à nos agents les outils dont ils ont besoin pour préserver la sécurité des Canadiens au XXI^{e} siècle, tout en garantissant que nous continuons de respecter les droits des Canadiens à la vie privée, établis dans la Charte.

● (1700)

[*Français*]

Nous avons écouté les préoccupations des intervenants et d'autres parlementaires après le dépôt du projet de loi C-2.

[*Traduction*]

Des dispositifs de protection importants sont prévus dans la partie 1 du projet de loi C-22, comme limiter la portée de l'ordre de confirmer la fourniture de services aux fournisseurs de services de télécommunications; une définition plus stricte de ce que sont les renseignements relatifs à la personne abonnée; et une surveillance judiciaire solide. La police devra toujours obtenir l'approbation de la Cour pour demander des renseignements personnels, comme les noms, les adresses et les numéros de téléphone.

Dans la partie 2 du projet de loi, nous nous assurons que les fournisseurs de services électroniques puissent répondre aux demandes d'accès légal. Je veux que ce soit clair: cette partie ne permet pas aux organismes d'application de la loi et au SCRS d'intercepter des communications ou d'obtenir de l'information. Elle vise à assurer que les fournisseurs de services électroniques peuvent se conformer aux ordres juridiques existants, prévus dans le Code criminel et la Loi sur le Service canadien du renseignement de sécurité. Les éléments clés comprennent un nouveau cadre de conformité qui exigera que les fournisseurs principaux aient la capacité technique nécessaire pour se conformer aux autorisations légales au moment d'obtenir de l'information, comme des mandats et des ordonnances de communication.

Elle conférerait aussi au ministre de la Sécurité publique de nouveaux pouvoirs liés aux arrêtés ministériels. Le ministre pourrait, mais avec l'approbation du commissaire au renseignement, ordonner à un fournisseur de services électroniques de se doter de capacités techniques précises, par exemple, pour composer avec les nouvelles technologies en développement, qui ne sont pas prévues dans la réglementation.

Enfin, elle ajoute un outil d'application de la réglementation, comme des sanctions administratives pécuniaires pour tout fournisseur qui ne se conforme pas.

Encore une fois, j'aimerais souligner les dispositifs de protection qui seraient mis en œuvre au titre de cette partie du projet de loi. Comme je l'ai mentionné, tous les arrêtés ministériels devront d'abord être approuvés par le commissaire au renseignement, qui s'assurera qu'ils sont raisonnables.

Cette partie inclut aussi un dispositif de protection explicite pour empêcher l'introduction de vulnérabilités systémiques dans les dispositifs de protection électroniques. Notre gouvernement s'oppose à la création de portes arrière.

Nous voulons que les Canadiens voient exactement comment ces pouvoirs sont créés et utilisés de sorte que leur exercice fait l'objet d'un contrôle démocratique étroit. Conformément aux lois actuelles, nos agents d'application de la loi et du renseignement essaient de lutter contre des criminels et des acteurs étatiques experts en technologies avec des outils qui datent de dizaines d'années. Le projet de loi C-22 comblerait cet écart tout en respectant les droits conférés par la Charte ainsi que la vie privée de tous les Canadiens.

[*Français*]

Je vous remercie et c'est avec plaisir que je répondrai à vos questions.

Le président: Merci, monsieur le ministre Anandasangaree.

Monsieur le ministre Fraser, vous avez la parole pour cinq minutes.

L'hon. Sean Fraser (ministre de la Justice): Merci, monsieur le président.

Avant de commencer mon discours, je voudrais remercier tout le monde d'être ici pour participer à ce débat très important.

Il est important, selon moi, de comprendre le contexte dans lequel s'inscrit ce projet de loi. Nous avons une stratégie pour améliorer la sécurité publique qui inclut trois piliers. Le premier est de renforcer les lois criminelles, notamment avec les projets de loi C-9, C-14 et C-16.

Cela dit, nous reconnaissons que ce n'est pas assez de seulement apporter des changements aux lois criminelles. Il faut aussi soutenir les personnes qui travaillent sur le terrain dans nos communautés, comme les organisations communautaires et les policiers. Ce n'est pas suffisant d'augmenter le nombre de personnes qui travaillent dans les communautés. Il faut aussi leur donner les outils nécessaires pour s'assurer qu'elles sont en mesure de répondre aux attentes que nous avons quant aux agents sur le terrain.

Nous devons aussi faire des investissements pour prévenir le crime et la violence à long terme. Cela comprend des investissements dans le logement abordable, des investissements pour que les personnes qui ont un problème de santé mentale puissent avoir des médicaments et des investissements pour soutenir les jeunes qui ont des problèmes dans leur vie.

[*Traduction*]

Ce projet de loi se concentre sur le deuxième pilier, et soutient ceux qui se trouvent en première ligne et qui essaient de faire du Canada un pays plus sûr tous les jours. Nous ne pouvons pas nous attendre à ce que les gens règlent des enjeux modernes à l'aide de technologies désuètes. C'est à cela que sert le projet de loi.

Quand nous comparons le Canada à d'autres partenaires ailleurs dans le monde, nous constatons que nous sommes très en retard pour ce qui est de nous attaquer aux enjeux modernes, surtout dans le contexte numérique. La technologie a changé. Le monde a changé. La criminalité a changé. Tout va plus vite. Cela traverse les frontières. Le numérique prend de plus en plus de place. Nous avons vu que d'autres administrations ont adopté ce dont nous discutons et ce que nous appelons l'« accès légal ». En termes très simples, c'est la capacité des organismes d'application de la loi d'accéder aux preuves dont ils ont besoin, lesquelles pourraient être de nature numérique, de la même façon dont nous leur permettons d'accéder à des preuves qui existent dans le monde physique. Vous ne pouvez pas arrêter une adresse IP ou un numéro de téléphone.

Nous devons fournir aux organismes d'application de la loi les outils qui leur permettront de découvrir l'identité de la personne coupable, quand il y a une enquête criminelle en cours, et de trouver un moyen de faire avancer l'enquête. Quand je regarde le processus actuel, je me dis qu'il est important de montrer aux Canadiens que nous avons bien réfléchi à la façon de nous assurer que les droits à la vie privée sont respectés et que nous tenons aussi compte des recommandations des organismes d'application de la loi visant à faciliter leur travail.

Plus précisément, pour commencer, en vertu de ce projet de loi, quand il y a une enquête qui concerne un numéro de téléphone ou une adresse IP, nous permettons aux organismes d'application de la loi de tout simplement demander au fournisseur de services: « Est-ce que cela fait partie de votre réseau? » Si le réseau répond par l'affirmative, nous pourrons alors entamer un processus, lequel serait approuvé par un juge, qui nous permettrait de dire oui, ce numéro de téléphone est associé à un nom et à une adresse. Actuellement, ce processus peut prendre des mois. Quand il s'agit de personnes qui participent aux activités du crime organisé — exploitation sexuelle d'enfants, trafic de stupéfiants, traite de personnes, invasions à domicile et vol organisé d'automobiles —, vous pouvez comprendre qu'il faut agir rapidement. C'est essentiel si nous voulons finir par atténuer les conséquences de la criminalité pour les collectivités canadiennes.

Selon moi, ce projet de loi fournit le bon cadre et offre aux organismes d'application de la loi les outils dont ils ont besoin pour préserver la sécurité des Canadiens, tout en se dotant de dispositifs de protection pour s'assurer que l'autorisation judiciaire est toujours essentielle, quand c'est approprié. Nous mettons un système en place afin que les fournisseurs de services puissent vraiment détenir l'information qui aidera à faire avancer ces enquêtes.

Laissez-moi vous résumer tout ça simplement: nous ne réglerons pas les problèmes de Netflix avec de la technologie de Blockbuster. Nous devons nous joindre aux économies avancées, ailleurs dans le monde, qui s'efforcent de régler ces problèmes depuis de nombreuses années. Je pense que, avec l'aide des différents partis représentés au Comité, nous pouvons envoyer un signal fort aux Canadiens pour leur montrer que, quand il est question de sécurité publique, nous ferons tout ce que nous pourrons pour que les organismes d'application de la loi aient les outils dont ils ont besoin pour préserver la sécurité des Canadiens.

● (1705)

[*Français*]

Merci, monsieur le président.

Le président: Merci, à vous deux.

Je passe maintenant la parole au député Caputo pour six minutes.

[*Traduction*]

Frank Caputo: Merci, monsieur le président.

Merci aux ministres et aux fonctionnaires.

J'aimerais faire remarquer que nous avons deux Kamloopsiens autour de la table aujourd'hui. C'est toujours extraordinaire.

Monsieur le ministre Anandasangaree, vous êtes tiré d'affaire, aujourd'hui. Nous ne vous poserons pas de questions sur les visas et sur qui a accordé un visa à des membres du corps des gardiens de la révolution islamique. Nous nous en tiendrons au projet de loi C-22.

J'aimerais revenir sur quelque chose que vous avez mentionné, monsieur le ministre. Vous avez dit que la loi était neutre en matière de chiffrement. Une des préoccupations principales dont on me parle souvent concerne ce chiffrement. Je vous demanderais de ne pas vous en remettre aux analystes. J'aimerais savoir ce que vous en pensez, vous. Ce projet de loi pourrait menacer les communications chiffrées, compte tenu du libellé ou de la façon dont on pourrait l'interpréter.

Pouvez-vous confirmer que l'objectif du projet de loi n'est pas de s'attaquer au chiffrement de bout en bout, soit quand une partie A se sert d'un programme pour s'occuper d'une partie B qui est chiffrée et qu'il est impossible de déchiffrer? Pouvez-vous confirmer que cela n'est pas prévu dans le projet de loi et que ce n'est pas son objectif?

L'hon. Gary Anandasangaree: Je peux le confirmer, oui.

Frank Caputo: Je vais seulement aller un peu plus loin dans ma confirmation: j'aimerais seulement confirmer que, dans ce cas, pour passer du point un au point deux, l'entreprise A n'est pas dans l'obligation de créer ce que nous pourrions appeler une porte arrière, un mécanisme qui permettrait d'accéder à cette information. Ai-je raison là-dessus aussi?

L'hon. Gary Anandasangaree: J'en ai parlé dans ma déclaration liminaire.

Frank Caputo: S'il y a de l'ambiguïté à cet égard, je suppose que vous allez faire les amendements qui s'imposent pour régler le problème, parce que cela change la donne, pour le projet de loi.

Je suppose donc que c'est le cas.

L'hon. Gary Anandasangaree: Je répéterais ce que je vous ai dit en privé, monsieur Caputo. Nous avons présenté ce projet de loi en misant sur des consultations avec différentes personnes, dont des collègues de différents partis. Nous travaillerons en collaboration pour renforcer le projet de loi. Si le Comité a des recommandations précises à présenter, nous les examinerons, évidemment. Nous avons hâte d'entamer ces discussions afin d'obtenir le bon résultat.

● (1710)

Frank Caputo: Je vais être franc, monsieur le ministre. Le gouvernement libéral est maintenant majoritaire. Ce qui est préoccupant, c'est que, s'il y a place à l'interprétation, ce ne sera pas réglé.

C'est pour cette raison que je vous demande, aux fins du compte rendu, s'il est possible que les communications chiffrées soient ciblées par le projet de loi. Si ce n'est pas son objectif — c'est ce que vous avez dit —, je ne crois pas que ce ne serait pas trop vous demander de dire, « Oui, monsieur Caputo, je soutiendrais un amendement visant à assurer que notre objectif est clair ». Par exemple, il pourrait s'agir d'un amendement qui comprend une définition de « données chiffrées », dans la partie 2, ou d'un amendement qui indique que la « vulnérabilité systémique » inclut une clé pour les données chiffrées et la création de telles clés.

Respectueusement, monsieur le ministre, je ne crois pas que ce soit difficile de dire, « Oui, c'est notre objectif ». N'êtes-vous pas d'accord?

L'hon. Gary Anandasangaree: Je le répète, nous sommes prêts à travailler ensemble, en collaboration, pour faire avancer le projet de loi.

J'étais au Sénat hier pour parler du projet de loi C-8, et 75 % des amendements adoptés avaient été présentés par l'opposition. Ce n'était pas des amendements du gouvernement.

Pour ce qui est du projet de loi dont nous discutons, je pense que nous avons tous deux dit clairement que nous travaillerons avec l'opposition pour faire avancer et renforcer le projet de loi, comme nous l'avons fait pour tous les autres.

Frank Caputo: Toutefois, monsieur le ministre, la différence entre le projet de loi C-8... Si vous voulez en parler, c'est exactement pourquoi je fais une mise en garde. Les libéraux se sont opposés à presque tous les amendements importants. Ce sont les conservateurs et le Bloc qui ont voté en faveur de ces amendements, qui ont permis leur adoption, et le gouvernement a souvent voté contre. Maintenant, les choses ont changé. Respectueusement, le projet de loi C-8 n'est pas un bon exemple. C'est pour cette raison que j'essaie d'obtenir des réponses aux fins du compte rendu.

Je pense que j'ai bien expliqué mon point et vous aussi, alors passons à autre chose.

Une des grandes questions concerne l'arrêté ministériel. Une autre, comme je l'ai dit, concerne le chiffrement, et une autre question importante, c'est la mesure dans laquelle la mise en œuvre et les définitions relèveront de la réglementation. Ce sont les critiques principales à propos du projet de loi.

Prenez par exemple l'article 5 proposé. On parle de vastes pouvoirs. Il est indiqué à l'alinéa 5(2)b) proposé « l'installation, l'utilisation, le fonctionnement, la gestion, l'évaluation, la mise à l'essai et l'entretien de tout dispositif ». Il est indiqué à l'alinéa 5(2)d) proposé « la conservation de catégories de métadonnées ». Monsieur le ministre, je comprends pourquoi le gouvernement veut que la portée soit large; c'est pour englober davantage de choses. Toutefois, si nous ne définissons pas les choses, où pouvons-nous le faire? Je suis convaincu que les experts nous diront, « Savez-vous quoi? Nous pouvons classer les métadonnées dans différentes catégories ». Nous pouvons classer les métadonnées dans différentes catégories, j'en suis sûr. Ce ne sont pas des choses qui changent tous les jours.

Seriez-vous ouvert à l'idée d'un amendement qui indique que, quand vous cherchez à obtenir des renseignements personnels, qui font l'objet d'attentes élevées en matière de vie privée...? Je suppose que vous seriez en faveur d'un amendement qui définirait ce genre de choses.

L'hon. Gary Anandasangaree: Je vais répéter ce que j'ai dit plus tôt, monsieur Caputo. Nous étudierons les amendements précis que vous proposerez. Je vous donne ma parole là-dessus. Cependant, je ne crois pas que je vais soutenir d'avance les amendements que vous proposez ici.

Frank Caputo: C'est seulement [*inaudible*].

L'hon. Gary Anandasangaree: Ce serait irresponsable de ma part de dire que j'accepterais tous les amendements. Je pense que ce qui est important, c'est de les étudier et d'envisager les conséquences qu'ils auraient sur le projet de loi. Nous serons toujours prêts à vous faire part de nos commentaires, comme je l'ai toujours fait.

Le président: Merci de votre débat respectueux et utile.

Madame Sodhi, vous avez six minutes; allez-y, s'il vous plaît.

Amandeep Sodhi (Brampton-Centre, Lib.): Merci, monsieur le président.

Merci aux ministres d'être présents aujourd'hui.

Monsieur le ministre Anandasangaree, à Brampton, nous observons une augmentation inquiétante de la criminalité en tous genres, du vol d'automobiles, au vol qualifié en passant par les introductions par effraction, les meurtres et les fusillades en plein jour. Je suis préoccupée par la sécurité de mes électeurs et de tous les résidents de Brampton, et ils le sont aussi. Notre maire, Patrick Brown, et les chefs de police régionaux de Peel demandent depuis un certain temps une loi comme le projet de loi C-22, et ils ont salué le dépôt de celui-ci.

En pensant au contexte local, pourriez-vous décrire les menaces auxquelles s'attaque ce projet de loi et expliquer les lacunes opérationnelles concrètes avec lesquelles les organismes d'application de la loi, comme le SCRS doivent composer, aujourd'hui, et que le projet de loi C-22comblerait?

● (1715)

L'hon. Gary Anandasangaree: Laissez-moi saluer le travail de la police régionale de Peel, que nous avons consultée quand nous avons élaboré ce projet de loi. Les commentaires reçus nous ont grandement aidés. J'ai discuté avec le chef, Nishan Duraiappah, à maintes reprises.

C'est la priorité principale, comme les chefs de police l'ont souligné, pas seulement ceux de la municipalité de Peel, mais ceux de tout le Canada, à tous les échelons, qu'il s'agisse du commissaire Carrique de la police provinciale de l'Ontario ou du commissaire Duheme de la GRC, ainsi que les services de police régionaux. Ce dossier est de la plus haute importance.

Plus précisément, la technologie à notre disposition aujourd'hui n'est pas à la hauteur des enjeux auxquels nous faisons face. On se sert principalement des téléphones, d'Internet, des courriels et des appareils électroniques pour commettre des crimes, tous les jours. L'extorsion, par exemple, se pratique souvent au moyen d'un appel téléphonique ou d'un message texte, ou parfois d'un courriel. Au fil des ans, cela a créé beaucoup de retard, parce que les organismes d'application de la loi doivent obtenir des ordonnances de communication. Souvent, ils doivent attendre des semaines, parfois des mois, pour obtenir l'information dont ils ont besoin pour passer à la prochaine étape.

Essentiellement, ce que nous faisons ici... Je vais me servir de l'exemple du bottin téléphonique, qui peut être consulté dans une bibliothèque locale, et de la recherche inversée. Si vous avez un numéro de téléphone, vous pouvez consulter le bottin de Bower, inscrire le numéro de téléphone et obtenir l'adresse de la personne qui a ce numéro. À l'heure actuelle, ce sont souvent des numéros de téléphone anonymes, ce qui veut dire que nous devons nous adresser au fournisseur de services. Si c'est une entreprise de télécommunications, nous devons lui demander si un numéro de téléphone spécifique est associé à son service. Cela peut prendre des semaines, parfois des mois, pour obtenir cette information.

Au départ, le projet de loi C-22 permet aux organismes d'application de la loi d'obtenir ce que l'on appelle une confirmation de service, pour confirmer que ce numéro de téléphone est lié au réseau du fournisseur de services de télécommunications. La réponse affirmative ou négative. Si la réponse est non, on s'arrête là. Si c'est oui, on devra préparer une ordonnance de communication, un mandat, pour pouvoir obtenir l'information de la personne abonnée, celle dont le numéro de téléphone pourrait être lié à la compagnie de téléphone. Le mandat permettra d'obtenir des renseignements généraux sur la personne abonnée, soit son nom, son adresse courriel, et ainsi de suite.

Autrement, toute autre information supplémentaire nécessaire devra être obtenue selon le processus actuel, soit retourner devant les tribunaux et obtenir une autorisation judiciaire pour consulter le type d'information requis et poursuivre l'enquête. Essentiellement, une enquête qui prend des mois pourrait ne prendre que des semaines grâce aux dispositions supplémentaires prévues dans le projet de loi.

Amandeep Sodhi: Monsieur le ministre, vous avez dit avoir discuté longuement avec le chef Nish de la police régionale de Peel. Selon vous, y a-t-il un consensus? Est-ce que les services de police de toutes les administrations du Canada appuient le projet de loi C-22?

L'hon. Gary Anandasangaree: Je dirais que nous avons discuté avec bien des gens. L'honorable Murray Rankin a participé à des séances de médiation et nous a parlé d'un consensus presque total. Je ne dirais pas que tout le monde était d'accord, mais des représentants de l'industrie et d'organismes de défense des libertés civiles étaient présents. Nous avons également discuté avec des organismes d'application de la loi et des militants communautaires.

Je crois qu'il s'agit d'un état de choses que nous comprenons très bien et que nous acceptons, en général. Ce n'est pas parfait. Tout le monde ne l'appuie pas à 100 %. Les gens continuent d'exprimer leurs préoccupations, mais en général, cela reflète... Même avec les organismes d'application de la loi, nous avons dû réduire... Vous constaterez que des changements importants ont été apportés entre le projet de loi C-22 et le projet de loi C-2, par exemple, pour restreindre et définir certaines choses qui y étaient incluses.

Nous avons fait beaucoup de travail pour nous approcher le plus possible d'un consensus. Le projet de loi ne fera jamais l'unanimité. Je pense que, ce que nous devons faire, c'est nous assurer que tous les dispositifs de protection sont en place. Nous sommes convaincus que, dans le projet de loi, nous répondons à la fois aux préoccupations en matière de droits à la vie privée et à celles en matière de droits prévus par la Charte. Certaines personnes voudraient que nous en fassions plus. Certaines personnes souhaitent tout simplement tirer un trait sur le projet de loi, mais ce n'est pas une option pour nous.

● (1720)

Le président: Merci beaucoup, madame Sodhi.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille: Merci, monsieur le président.

Merci beaucoup, messieurs les ministres.

Monsieur Fraser, je n'ai pas vraiment de questions pour vous, mais je veux vous féliciter franchement pour votre français, qui s'est beaucoup amélioré.

Monsieur Anandasangaree, la Loi sur le soutien en matière d'accès autorisé à de l'information, édictée par la partie 2 du projet de loi, prévoit un rôle limité pour l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR. Or on a remarqué que, chez nos partenaires du Groupe des cinq, il y a des mécanismes comparables d'accès légal qui s'accompagnent d'un rôle plus formel de surveillance indépendante. À titre d'exemple, on peut nommer l'Australie. La Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 demade que l'organisme homologue à l'OSSNR soit avisé de la délivrance d'ordres d'assistance technique dans un délai précis.

De votre côté, selon le projet de loi C-22, vous devez donner un rapport non caviardé à l'Office un an après, et vous avez 90 jours, si je ne me trompe pas, pour le lui remettre. C'est donc à peu près un an et demi après les faits ou les décisions que vous remettez ça à l'Office de surveillance.

Quand vous vous inspirez du Groupe des cinq pour votre projet de loi, pourquoi ne voulez-vous pas donner à l'Office un rôle aussi important que celui que l'Australie a donné à un organisme de surveillance comparable?

L'hon. Gary Anandasangaree: Je vous remercie de la question.

[*Traduction*]

J'aimerais souligner que des dispositifs de protection sont prévus dans le projet de loi C-22. Par exemple, il faut obtenir l'approbation du commissaire au renseignement avant d'émettre un arrêté ministériel. Il y a des dispositions qui concernent le contrôle judiciaire dans certaines circonstances. Il y a aussi un renvoi à l'OSSNR après les faits, et c'est le processus d'examen normal...

[*Français*]

Claude DeBellefeuille: Je suis désolée de vous interrompre, mais j'ai déjà lu ça. Je me suis préparée.

Ce que je veux comprendre, c'est pourquoi l'Office canadien est comme un peu mis de côté, à mon avis. Je sais que le commissaire au renseignement a un rôle, mais pourquoi l'Office n'est-il pas avisé en temps réel? Quand on a les faits presque un an et demi plus tard, c'est dur de faire une enquête pour vérifier si les agences concernées, comme la GRC ou le Service canadien du renseignement de sécurité, sont conformes à la loi.

Je vous annonce que je vais proposer un amendement pour que l'Office de surveillance soit avisé en temps réel, un peu comme le modèle de l'Australie, parce que je considère que c'est notre garantie. C'est un peu comme une façon de donner notre confiance au gouvernement en nous assurant que l'Office de surveillance, dont la mission première est de faire de la surveillance, est avisé en temps réel, comme le commissaire au renseignement.

Je suis également surprise d'avoir appris par votre équipe que Mme Deschamps, qui est la présidente de l'Office, n'a pas du tout été consultée par les différents groupes de consultation qui ont été organisés pour l'étude du projet de loi C-22. Je vous le dis sincèrement, ça n'a pas sens pour moi. On s'inspire du Groupe des cinq pour les meilleurs pratiques, mais on omet d'inclure un rôle important pour l'Office dans le projet de loi C-22. Seriez-vous prêt à discuter de la question de pouvoir aviser l'Office en temps réel?

[*Traduction*]

L'hon. Gary Anandasangaree: Je dirais, d'une part, que, pour aller de l'avant avec un arrêté ministériel, il faut qu'il passe par le processus d'examen de l'OSSNR, lequel peut être assez long, donc un dispositif de protection a été prévu. Comme vous le savez, le rôle du commissaire au renseignement consiste davantage à réagir et à fournir des commentaires en temps réel. Le dispositif de protection vise à permettre au commissaire au renseignement d'approuver ou de rejeter un arrêté proposé...

[*Français*]

Claude DeBellefeuille: Cependant, qu'est-ce qui vous empêche d'en aviser l'Office de surveillance des activités en matière de sécurité nationale et de renseignement? C'est ça que je ne comprends pas. Je n'arrive pas à comprendre pourquoi vous l'excluez. Dans le fond, c'est sa mission première de surveiller, et vous la mettez de côté. Vous l'informez seulement un an après les faits.

Je vais vous répéter ma question. Je vais vous le présenter, l'amendement. Je sais que vous avez dit à la Chambre des communes que vous alliez être ouvert aux amendements. Pour moi, si vous avisez le commissaire, ce n'est pas plus compliqué d'aviser le bureau de la présidente de l'Office. Il me semble que ça aurait du sens, et c'est un peu ce que fait l'Australie. Cependant, vous semblez un peu résister à ça. Avez-vous des arguments pour me convaincre que je fais fausse route de vous demander cet amendement?

● (1725)

[*Traduction*]

L'hon. Gary Anandasangaree: Tout d'abord, j'ai effectivement rencontré le commissaire au renseignement, le commissaire à la protection de la vie privée et la présidente de l'OSSNR. J'ai discuté avec des gens tant à titre personnel qu'au nom de nos ministères.

Nous ne croyons pas que l'OSSNR peut approuver ou rejeter assez rapidement une demande d'arrêté ministériel précis, compte tenu de l'urgence de certains cas. C'est pour cette raison que nous faisons appel au commissaire au renseignement à cet égard. Le rôle de l'OSSNR est de faire un examen après le fait. Ce projet de loi s'aligne sur le mode de fonctionnement actuel de l'OSSNR, qui examine des dossiers et souligne les erreurs et les omissions possibles...

[*Français*]

Claude DeBellefeuille: Je vais vous interrompre, monsieur le ministre.

Vous savez que la présidence de l'Office n'est pas d'accord avec votre interprétation. Elle a informé les membres qu'elle pense qu'elle devrait être avisée. Il ne s'agit peut-être pas de demander qu'elle doive donner une autorisation, mais il faudrait au moins qu'elle soit informée quand il y a des arrêtés ministériels, au même titre que le commissaire. Ils n'ont peut-être pas le même rôle, mais elle pourrait au moins être informée. En ce sens, je pense que c'est important que l'Office ait plus d'importance pour gagner la confiance du public. C'est mon opinion.

Le président: Merci beaucoup, madame DeBellefeuille.

Madame Kirkland, vous avez la parole pour cinq minutes.

[*Traduction*]

Rhonda Kirkland (Oshawa, PCC): Merci, monsieur le président.

Messieurs les ministres, je vous remercie d'être ici.

Je vous comprends quand vous dites soutenir les agents en première ligne. On demande l'accès légal depuis de nombreuses années. Toutefois, je pense réellement que nous devons faire attention à ne pas aller trop vite. Nous devons bien faire les choses. En tant que parlementaires, nous devons garder à l'esprit notre devoir de diligence et le fait que nous devons protéger la vie privée et les renseignements personnels des Canadiens. Mes questions concerneront cela. Je pense que nous ne devons pas demander la sanction royale trop rapidement. Il faut bien faire les choses.

Il y a plus de 10 ans — je ne sais pas si vous le savez —, votre parti nous a mis en garde contre un projet de loi très similaire à celui-ci. C'était un projet de loi sur l'accès légal. Votre parti a dit que le projet de loi risquait de transformer le Canada en État de surveillance. Aujourd'hui, non seulement vous proposez des pouvoirs similaires, mais vous étendez de beaucoup leur portée avec le projet de loi C-22. En fait, M. Francis Scarpaleggia, le Président actuel de la Chambre, était alors le porte-parole libéral en matière de sécurité publique. Il nous a prévenus qu'une loi similaire sur l'accès légal risquait, et je traduis ses propos, « de créer un service d'État orwellien ».

Voici ma question: avait-il tort?

L'hon. Gary Anandasangaree: Je dirais que les gouvernements qui se sont succédé n'ont pas su promouvoir l'accès légal comme un outil et un cadre essentiels, indispensables...

Rhonda Kirkland: Oui. Je sais que cela n'a pas abouti. Ma question, c'est est-ce que le gouvernement libéral a une opinion différente de celle qu'il avait il y a plus de 10 ans, ou croyez-vous que M. Scarpaleggia avait tort à cette époque?

L'hon. Gary Anandasangaree: Madame Kirkland, cela n'a rien à voir avec M. Scarpaleggia. Cela concerne la sûreté et la sécurité des Canadiens. Comme vous le savez, le nouveau gouvernement canadien, sous le premier ministre Mark Carney, a travaillé pour concrétiser ces trois piliers, comme le ministre Fraser l'a si bien souligné. Cela constitue une partie très importante de ce pilier.

Peut-être que M. Fraser pourrait vous en dire plus.

Rhonda Kirkland: Je vais passer à autre chose. Je vais poser des questions à M. Fraser, sous peu.

Monsieur Anandasangaree, pouvez-vous garantir que le projet de loi, tel que libellé, ne sera pas utilisé à des fins qui dépassent son objectif initial? J'ai entendu des fonctionnaires du ministère dire que le projet de loi ne vise pas à faire X, Y et Z. Toutefois, si le projet de loi permet au gouvernement de faire ces choses, qu'est-ce qui empêcherait un futur gouvernement, dont la stratégie en matière de protection de la vie privée et des libertés civiles pourrait différer de la vôtre, d'abuser de ce pouvoir?

L'hon. Gary Anandasangaree: Je dirais que nous avons longuement réfléchi pour nous assurer de mettre en place des dispositifs de protection, tant pour assurer la protection de la vie privée que pour garantir la conformité avec la Charte. Nous sommes convaincus que le projet de loi, tel que libellé, a ces dispositifs de protection.

Rhonda Kirkland: À l'époque, il y a plus d'une décennie, lorsque nous avons essayé de faire cela, on nous a prévenus que l'adoption précipitée de lois complexes en matière de surveillance, sans évaluation adéquate de l'opinion des Canadiens, pouvait se solder par un échec. Vous avez dit que vous étiez convaincu que le projet de loi, dans sa forme actuelle, tient compte des questions de protection de vie privée et de sécurité.

Votre gouvernement s'est fondé sur des consultations menées par Murray Rankin pour élaborer le projet de loi C-22, mais vous n'avez pas publié ce rapport. Allez-vous publier le rapport de M. Rankin et le transmettre au Comité?

● (1730)

L'hon. Gary Anandasangaree: Je dirais que le rapport de M. Rankin — et je suis reconnaissant du travail qu'il a accompli — a été préparé... Il est avocat. Nous sommes collègues. Le rapport m'a été présenté, et M. Fraser s'en est servi par mon intermédiaire, pour orienter nos décisions.

Le projet de loi n'a aucun lien avec le rapport de M. Rankin. Je dirais que...

Rhonda Kirkland: Monsieur, j'aimerais simplement vous le demander. Vous n'allez pas publier le rapport au Comité, ou allez-vous le faire?

L'hon. Gary Anandasangaree: Je demande le privilège à ce sujet. Je ne crois pas que le rapport sera rendu public, non.

Rhonda Kirkland: Il y a plus de 10 ans, le gouvernement libéral disait que la rhétorique du gouvernement mettait fin à un débat important sur cette version, les dispositions du projet de loi C-30 sur l'accès légal, mais, aujourd'hui, on demande au Comité d'examiner des pouvoirs similaires alors qu'il n'a pas accès au rapport de consultation qui a orienté la réforme de l'accès légal dans le projet de loi C-22. Ce rapport est indispensable à tout examen approfondi et à la capacité du Parlement à exercer ses fonctions législatives fondamentales. En ne publiant pas le rapport, le gouvernement demande essentiellement aux députés d'adopter un projet de loi sans leur communiquer l'ensemble des données probantes sur lesquelles il repose.

Monsieur, pourquoi refusez-vous de publier ce rapport, tout en insistant pour que nous autorisions ces pouvoirs?

L'hon. Gary Anandasangaree: Je dirais...

Rhonda Kirkland: Pourquoi insistez-vous là-dessus.

L'hon. Gary Anandasangaree: Madame Kirkland, si vous me permettez de répondre...

Rhonda Kirkland: Merci. Je veux simplement que vous répondiez à la question.

L'hon. Gary Anandasangaree: Votre question comportait un préambule. Je devrais pouvoir vous donner une réponse complète.

Si vous me le permettez, ce que je dirais, c'est que, dans le cadre de la procédure normale de dépôt d'un projet de loi, le ministère se fonde sur une foule d'informations pour élaborer le projet de loi et obtenir les autorisations nécessaires pour le présenter. La grande majorité du temps, aucune de ces informations n'est communiquée. Cela fait partie du processus décisionnel du gouvernement.

Madame Kirkland, vous êtes la bienvenue...

Rhonda Kirkland: La différence entre le Groupe des cinq et notre pays est que nous avons une Charte...

Le président: Désolé de vous interrompre, tous les deux.

Nous allons maintenant passer à M. Casey; vous avez cinq minutes, allez-y, s'il vous plaît.

Sean Casey (Charlottetown, Lib.): Merci beaucoup, monsieur le président.

Je siégeais au Parlement le jour où Francis Scarpaleggia s'en est pris à Vic Toews à propos du projet de loi sur l'accès légal de l'époque, et je me souviens très bien que le ministre Toews avait dit que soit vous êtes avec le gouvernement, soit vous êtes avec les producteurs de pornographie juvénile. Je me souviens de la popularité du mot-clic « TellVicEverything », dites tout à Vic, car, à l'époque, beaucoup estimaient que le projet de loi allait trop loin. Dans tous les coins du pays, des gens disaient au ministre Toews qu'ils avaient avalé leur soupe de travers parce qu'ils croyaient que le ministre s'intéressait à tout ce qu'ils faisaient, étant donné les mesures qu'il prenait pour empiéter sur leur vie privée et les discours exagérés qu'il tenait, à ce moment-là, pour les défendre.

J'aimerais que M. Fraser se joigne à la conversation.

Monsieur le ministre, dans votre déclaration préliminaire, vous avez parlé de la protection de la vie privée et de la conformité avec la Charte, à cet égard. Pourriez-vous nous en dire plus sur la protection de la vie privée et la conformité avec la Charte, ainsi que sur les efforts qui ont été déployés dans le cadre de ce projet de loi sur ces deux aspects?

L'hon. Sean Fraser: Écoutez, pour mieux comprendre, j'aimerais vous donner un peu de contexte.

Mme Kirkland a mentionné dans ses questions que ce débat dure depuis plusieurs années. Il ne dure pas depuis plusieurs années; il dure depuis 30 ans.

J'invite tout le monde à visionner la vidéo du commissaire Carrique résumant l'importance du projet de loi lors de son dépôt. On sent bien la frustration des agents des forces de l'ordre. Je crois qu'ils s'entendent pour dire que nous devons aller de l'avant, car ils en ont assez des organisations criminelles responsables de la traite de personnes, des vols de véhicules et du trafic de drogues. Ils sont au courant de ces activités, et ils essaient de faire leur travail avec une main attachée derrière le dos. Quand ils reçoivent des informations d'un gouvernement étranger, y compris sur un sujet aussi sensible que l'exploitation sexuelle d'enfants, ils veulent agir rapidement. Ils ne veulent pas porter atteinte à la vie privée des gens pendant leur intervention.

Heureusement, il y a eu plusieurs progrès, au Canada et à l'échelle du globe, qui montrent que nous pouvons mieux protéger la vie privée. Le Comité a parlé des différences entre les approches de nos partenaires du Groupe des cinq et celles du Canada. Aucun de nos partenaires du Groupe des cinq — ni la France, l'Allemagne, la Finlande ou l'Espagne, d'ailleurs — n'a besoin d'une autorisation judiciaire pour obtenir des renseignements relatifs à un abonné. Nous parlons des renseignements que l'on trouvait autrefois dans un bottin téléphonique. Nous exigerions tout de même qu'un tribunal autorise l'accès à ces renseignements. Cela faciliterait l'accès sans compromettre la vie privée de façon significative.

Si vous voulez aller plus loin, même dans des situations d'urgence... La seule exception serait une situation d'urgence quand le délit peut encore être empêché, ou si des preuves risquent d'être détruites. Il y aurait même des possibilités en aval de... Le critère devra tout de même être satisfait, mais le préjudice pourrait être réparé, pour ainsi dire, si le tribunal exclut des éléments de preuve, si cela est nécessaire, s'il y a eu atteinte à la vie privée.

Nous l'avons d'ailleurs amélioré après avoir consulté différents députés de différents partis, ainsi que des experts qui nous ont conseillé de préciser les renseignements relatifs à l'abonné que nous recherchons, c'est pourquoi nous avons exclu les informations médicales et les conseils juridiques. Il s'agit de découvrir la personne qui est rattachée à un numéro de téléphone ou à une adresse IP si nous soupçonnons qu'elle a pris part à des activités criminelles.

À chaque étape du processus, nous avons essayé de donner aux agents des forces de l'ordre les outils dont ils ont besoin pour lutter contre la criminalité moderne. À chaque étape du processus, nous nous sommes demandé comment faire cela de manière à respecter les droits en matière de protection de la vie privée conférés par la Charte canadienne des droits et libertés. Je suis convaincu que nous avons trouvé un juste équilibre, après de nombreuses années de débats et de nombreux mois de discussion avec les députés de différents partis. Nous avons atteint un équilibre qui nous permettra de défendre les intérêts des Canadiens et de protéger nos collectivités, tout en respectant les droits à la vie privée des Canadiens.

● (1735)

Sean Casey: Monsieur le ministre Anandasangaree, avez-vous quelque chose à ajouter à ce que nous venons d'entendre?

L'hon. Gary Anandasangaree: Je crois que le ministre Fraser a bien fait état du travail que nous avons accompli et de l'urgence de la situation.

Je tiens à souligner une chose. Les technologies se développent et de nouvelles technologies apparaissent constamment — nous savons que nous avons déjà 30 ans de retard à ce chapitre —, avec l'intelligence artificielle et d'autres outils, à une échelle et à un rythme auxquels, à mon avis, notre monde n'est pas prêt à faire face; il est donc essentiel d'avoir au Canada un cadre en matière d'accès légal, à tout le moins, pour rester à jour et évoluer.

Le président: Merci beaucoup de votre réponse.

[*Français*]

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

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur le ministre, vous avez confirmé à M. Caputo que l'intention du projet de loi C-22 n'est pas de permettre la création de portes dérobées dans les systèmes de chiffrement, ni maintenant ni à l'avenir. Vous l'avez confirmé.

Cette même question, soit l'affaiblissement possible du chiffrement, nous a inquiétés quand nous avons étudié le projet de loi C-8. La ministre Joly nous a alors dit que même si, dans le projet de loi, il y avait une certaine intention exprimée, elle accepterait d'ajouter au projet de loi un article qui dirait clairement qu'il n'y aura pas d'affaiblissement du chiffrement.

Je vais vous dire sincèrement que l'affaiblissement du chiffrement, c'est vraiment une crainte très, très généralisée. Peut-être que vous pourriez rassurer la population en indiquant clairement dans le projet de loi que vous ne porterez pas atteinte aux systèmes de chiffrement.

Est-ce que vous pensez qu'il y a de la place dans le projet de loi pour clarifier encore plus votre intention, puisque vous avez affirmé à M. Caputo tantôt que ce n'était pas votre intention d'affaiblir le chiffrement?

[*Traduction*]

L'hon. Gary Anandasangaree: Comme je l'ai dit, nous allons examiner chaque amendement. Il y a une procédure, pour les amendements. Une fois que vous avez terminé le travail, le Comité présentera des recommandations. Je peux vous dire que nous allons examiner chacune de ces propositions et vous donner des commentaires. Comme d'habitude, je vais communiquer avec vous, monsieur Caputo, et avec tous ceux qui souhaitent faire avancer ce dossier.

C'est l'engagement que je peux prendre envers vous aujourd'hui.

[*Français*]

Claude DeBellefeuille: Monsieur le ministre, quand la ministre Joly a comparu, elle s'est engagée à ce que le gouvernement dépose un amendement au projet de loi C-8 pour y ajouter qu'il n'y aurait pas d'affaiblissement du chiffrement. Elle l'a dit publiquement lors de l'étude du projet de loi C-8.

Alors, je vous pose la même question. Êtes-vous prêt à demander à votre équipe d'ajouter dans le projet de loi de la certitude par rapport au fait qu'il n'y aura pas d'atteinte aux systèmes de chiffrement afin de rassurer le public?

● (1740)

[*Traduction*]

L'hon. Gary Anandasangaree: Je travaille en étroite collaboration avec vous depuis maintenant près d'un an, et je crois que vous connaissez généralement l'approche que j'ai adoptée dans le cadre de cette collaboration. Je suis tout à fait disposé à vous rencontrer et à examiner votre proposition.

Nous serions ravis d'entendre toute proposition visant à renforcer le projet de loi.

[*Français*]

Le président: Merci, madame DeBellefeuille.

Monsieur le député Lloyd, vous avez la parole pour cinq minutes.

[*Traduction*]

Dane Lloyd: Merci, monsieur le président.

Merci aux ministres d'être ici.

Monsieur le ministre Anandasangaree, vous avez refusé de renoncer au droit au secret sur le rapport présenté par Murray Rankin, sur le processus consultatif du rapport. On m'a dit que le rapport a été largement diffusé auprès des personnes qui ont pris part à la consultation. Je présume que les personnes qui n'ont pas communiqué le rapport ont signé une entente de non-divulgation.

Pouvez-vous confirmer si les députés ayant participé aux consultations ont dû signer une telle entente pour consulter le rapport?

L'hon. Gary Anandasangaree: Monsieur Lloyd, je ne sais pas.

La discussion d'aujourd'hui ne porte pas sur le rapport de M. Rankin; nous discutons d'un projet de loi dont la Chambre est actuellement saisie. Il n'y a aucun précédent où des gouvernements auraient communiqué les informations recueillies avec le contenu des discussions qui se déroulent en Comité. Je crois que nous nous éloignons du sujet principal dont nous sommes censés discuter, le projet de loi lui-même.

Dane Lloyd: Merci. Je vous ai laissé suffisamment de temps, monsieur le ministre.

Le rapport a joué un rôle déterminant dans l'élaboration du rapport de votre gouvernement. Il serait très utile pour nous, en tant que membres du Parlement, d'y avoir accès. Je crois que les gouvernements doivent impérativement instaurer la confiance chez les Canadiens. Monsieur le ministre, votre comportement, ici, ne semble ni responsable ni transparent, surtout puisque nous traitons d'un projet de loi controversé qui concerne les droits à la vie privée des Canadiens.

Qu'essayez-vous de cacher, monsieur le ministre? Pourquoi refusez-vous de publier le rapport?

L'hon. Gary Anandasangaree: Vous pouvez convoquer M. Rankin à comparaître devant le Comité, et il pourra vous donner l'information.

Ce qui se passe en ce moment, c'est une tentative pour détourner l'attention du sujet principal, le projet de loi lui-même.

Dane Lloyd: Monsieur le ministre, c'est vous qui détournez l'attention de la question en refusant de nous remettre le rapport. Le fait que nous en parlions aujourd'hui... Même les gens qui ont lu le rapport — qu'ils soient pour ou contre le projet de loi C-22 ne comprennent pas pourquoi le rapport n'a pas été publié.

Monsieur le ministre, cela devient une source de distraction parce que vous en faites une source de distraction. Pourquoi ne pas simplement publier le rapport?

L'hon. Gary Anandasangaree: Monsieur Lloyd, cela n'a rien à voir avec le rapport. Vous le savez. Nous parlons du projet de loi lui-même, tel que présenté par M. Fraser et moi-même. Si vous avez des questions spécifiques sur le projet de loi, je serais tout à fait disposé à y répondre, mais je ne vais pas vous donner des informations confidentielles que je crois avoir recueillies auprès de M. Rankin et qui ont éclairé nos décisions.

M. Fraser et moi-même avons aussi rencontré une foule d'autres personnes. Nous consultons plusieurs personnes lors de l'élaboration d'un projet de loi...

Dane Lloyd: Monsieur le ministre, je vous ai donné amplement de temps pour répondre.

Pourquoi les intervenants concernés, comme l'Association canadienne des libertés civiles et d'autres intervenants, auraient-ils davantage droit de consulter le rapport que les députés à qui on demande de voter sur ce projet de loi?

L'hon. Gary Anandasangaree: Vous pouvez inviter M. Rankin à comparaître, il sera ravi.

Dane Lloyd: Je vais passer à autre chose, monsieur le ministre.

Je parlais avec vos fonctionnaires, plus tôt. Il semble y avoir une contradiction. On dit que le projet de loi ne vise pas à affaiblir le chiffrement ou à créer des vulnérabilités systémiques, mais d'autres parties du projet de loi indiquent qu'un arrêté ministériel vise à créer les capacités très techniques indispensables pour venir à bout du chiffrement.

Si l'un des résultats recherchés par ce projet de loi, c'est-à-dire l'accès légal, ne peut pas être réalisé sans créer des vulnérabilités systémiques, votre gouvernement ordonnera-t-il quand même aux entreprises de télécommunications et aux fournisseurs de services de courrier électronique de créer ces capacités de chiffrement?

L'hon. Gary Anandasangaree: Comme je l'ai déjà dit, le projet de loi est neutre en ce qui concerne le chiffrement. Il ne vise ni ne prévoit d'aucune manière le décryptage. Les arrêts ministériels prévus devront être approuvés par le commissaire au renseignement, et cela fait partie des dispositifs de protection en place.

Dane Lloyd: Vous avez été assez direct dans votre réponse à ma question pendant le débat sur la rémunération des fournisseurs. Vous avez dit vous attendre à ce que, pour répondre aux conditions d'octroi d'une licence par le CRTC, les entreprises obtempèrent sans indemnisation.

Est-ce vraiment ce que vous avez dit à la Chambre?

L'hon. Gary Anandasangaree: Ce que je vais dire, c'est que...

● (1745)

Dane Lloyd: C'est ce que vous avez dit, oui ou non?

L'hon. Gary Anandasangaree: Monsieur Lloyd, je ne m'en souviens plus.

Dane Lloyd: D'accord.

L'hon. Gary Anandasangaree: J'ai fait des commentaires à ce sujet, donc je peux...

Dane Lloyd: Votre réponse est non pour ce qui est de l'indemnisation. Est-ce exact? Je veux que cela soit clair.

L'hon. Gary Anandasangaree: Le projet de loi... L'indemnisation fait partie des demandes possibles...

Dane Lloyd: D'accord.

L'hon. Gary Anandasangaree: ... mais, à mon avis, les entreprises qui exercent leurs activités au Canada sont de bons citoyens corporatifs. Les pays du Groupe des cinq ne payent pas nécessairement...

Dane Lloyd: C'est très différent de la réponse que vous avez donnée à la Chambre.

Selon vous, dans quelle situation l'indemnisation serait-elle possible?

L'hon. Gary Anandasangaree: À ce stade-ci, je ne prévois pas de situation particulière. S'il y avait des circonstances atténuantes où la situation financière d'une entreprise limitait ses capacités, ce serait une considération ponctuelle, mais, en général, nous ne prévoyons pas d'indemnisation.

Le président: Merci, monsieur Lloyd.

Nous avons ensuite Mme Acan; allez-y, s'il vous plaît, vous avez cinq minutes.

Sima Acan: Merci, monsieur le président.

Je tiens à parler de certains aspects techniques des métadonnées dont mes collègues devraient tenir compte avant de proposer des amendements qui pourraient avoir une incidence significative sur l'efficacité du projet de loi.

Les enquêtes criminelles modernes, surtout celles impliquant l'exploitation d'enfants, la traite de personnes, l'extorsion, le crime organisé et la cybercriminalité, dépendent fortement des métadonnées numériques pour reconstruire les événements, identifier les suspects et cartographier des réseaux complexes. Ces affaires sont souvent rapportées longtemps après les faits, et c'est pourquoi les données historiques sont essentielles pour déterminer la chronologie des événements et établir des liens qui ne sont pas évidents à première vue.

Il pourrait donc être risqué de restreindre le type de données conservées. Différents types de métadonnées ont différentes fonctions pour les enquêtes et la TI: l'attribution, la cartographie des communications et la reconstruction des activités multi-plateformes. Si des catégories clés sont exclues, cela peut rompre la chaîne des preuves et limiter la capacité à faire des liens entre les activités d'un système à un autre et d'une administration à une autre. Dans le domaine des enquêtes et de l'informatique médico-légale, les métadonnées manquantes réduisent la capacité à effectuer des analyses des structures et des réseaux, qui sont essentielles pour les activités policières modernes axées sur le renseignement et les enquêtes cybercriminelles. Cela peut aussi compromettre l'exhaustivité des preuves devant le tribunal. Bon nombre de crimes graves sont signalés bien après qu'ils se sont produits. Si certaines catégories de métadonnées n'ont jamais été stockées, elles ne peuvent pas être récupérées plus tard, même avec un mandat ou une ordonnance du tribunal.

Monsieur le président, je demande à mes collègues de bien vouloir consulter la transcription de mes remarques quand ils examineront des amendements visant à réduire le type de métadonnées pouvant être recueillies ou à limiter la période de conservation, puisque ces changements pourraient affaiblir significativement l'efficacité de l'accès légal.

Mon collègue, M. Caputo, a soulevé des préoccupations non seulement sur les types de métadonnées, mais aussi sur le cadre relatif à la conservation des données de 12 mois énoncé dans la partie 2.

Pendant mes rencontres avec les responsables des organismes de l'application de la loi, ils ont précisé les paramètres généraux. Les enquêtes complexes posent toutefois un défi pratique. Bon nombre de dossiers graves, comme l'exploitation d'enfants, la traite de personnes, le crime organisé et l'extorsion, sont par nature chronophages, et s'étendent souvent bien au-delà de six ou même de neuf mois, en raison de leur caractère interadministratif et numérique.

Est-ce que le SCRS ou la GRC pourraient en dire plus sur l'importance opérationnelle de la conservation des données pour soutenir ce type d'enquêtes complexes? De plus, de quelle manière l'accès aux données et la période de conservation des données affectent-ils la capacité des forces de l'ordre de mener des enquêtes efficaces en temps opportun dans un contexte numérique?

Merci.

Nicole Giles (directrice adjointe, Service canadien du renseignement de sécurité): Les ministres me font des signes, donc j'imagine que c'est à moi de répondre.

Je peux vous donner deux exemples. Le SCRS pourrait essayer de suivre les déplacements d'un groupe terroriste, et nous avons reçu le mandat de suivre le cellulaire d'une personne d'intérêt. Le fournisseur des services électroniques n'avait pas la capacité de suivre l'appareil, donc nous ne pouvons pas faire grand-chose si ces capacités n'existent pas. C'est l'une des capacités clés qui serait fournie au titre de la partie 2, qui obligerait les fournisseurs de services de courrier électronique à développer et à maintenir des capacités de géolocalisation, qui sont, bien honnêtement, la norme dans les pays du Groupe des cinq et les pays européens.

Prenons un autre exemple. Nous pourrions recevoir des renseignements d'un partenaire étranger qui mène une enquête à l'extérieur du Canada où certains sujets ont un numéro de téléphone canadien; le partenaire étranger souligne que la menace semble près d'entrer sur le territoire canadien. Nous pouvons confirmer que les numéros de téléphone cellulaire ont été obtenus auprès d'un revendeur, mais, les revendeurs ne tiennent pas souvent un registre de leurs ventes et ne suivent pas non plus les activités de leurs clients. La partie 2 ferait entrer cela en jeu en impliquant les revendeurs dans le processus, ce qui nous permettrait d'intervenir dans ce genre de demandes.

● (1750)

Sima Acan: Me reste-t-il encore du temps?

Le président: Vous avez 30 secondes.

Sima Acan: D'accord.

Le projet de loi C-22 apporte un changement législatif important, précisant que...

J'ai changé d'avis, monsieur le président, je n'ai pas suffisamment de temps. Je vais m'arrêter ici.

L'hon. Sean Fraser: Monsieur le président, s'il reste 20 secondes...

Sima Acan: Monsieur le ministre, avez-vous quelque chose à ajouter?

L'hon. Sean Fraser: Si je peux me le permettre, ce ne sont pas des crimes fictifs. Si vous parlez vraiment aux organismes d'application de la loi, surtout pour ce qui est du deuxième exemple, les gens ne le savent pas, mais ces organismes reçoivent un déluge de renseignements sur les menaces potentielles, y compris l'exploitation sexuelle d'enfants. L'application de la loi est inégale entre les provinces, car le régime régissant l'utilisation des preuves numériques lors des enquêtes et à des fins de prévention de la criminalité n'est pas clairement défini.

Ce sont des menaces réelles à...

Le président: Désolé d'avoir à interrompre un collègue ministre, mais le temps est malheureusement écoulé.

[*Français*]

Je remercie les ministres d'avoir pris le temps de se préparer et de se déplacer pour comparaître aujourd'hui.

Je remercie tous les fonctionnaires d'avoir fait le travail nécessaire.

Nous allons maintenant lever la séance, et nous nous reverrons jeudi pour d'autres travaux.