CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la justice et des droits de la personne

JUST • NUMÉRO 027 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 29 mai 2014

Président

M. Mike Wallace

Comité permanent de la justice et des droits de la personne

Le jeudi 29 mai 2014

● (1100)

[*Traduction*]

Le président (M. Mike Wallace (Burlington, PCC)): Mesdames et messieurs, bienvenue à la séance n° 27 du Comité permanent de la justice et des droits de la personne. Conformément à l'ordre du jour et à l'ordre de renvoi du lundi 28 avril 2014, nous poursuivons l'étude du projet de loi C-13, Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle.

Nous accueillons un certain nombre d'invités aujourd'hui.

À titre indicatif, j'ai cru comprendre que les cloches sonneront peut-être durant la séance. J'ai dit aux témoins que, si les cloches se font entendre, nous nous dépêcherons d'aller voter, puis nous reviendrons afin que leurs exposés de 10 minutes figurent bien au compte rendu.

J'ai une autre chose à dire avant de poursuivre. J'ai communiqué personnellement avec des représentants de Facebook et les ai invités à comparaître mardi, la journée où leur comparution était prévue, ou jeudi, la semaine prochaine. Nous n'avons pas eu de nouvelles quant à savoir s'ils acceptent l'invitation. Nous leur avons envoyé des copies de la motion du comité de la dernière fois.

Nous nous attendions à voir Global News, mais ils ne sont pas prêts. Comme les règles le prévoient, il est interdit de prendre des photos une fois la séance ouverte.

Nous allons commencer avec les exposés de 10 minutes. Nous accueillons aujourd'hui des représentants du Centre canadien de protection de l'enfance et du Bureau de l'ombudsman fédéral des victimes d'actes criminels. À titre personnel, nous accueillons M. Michael Geist. Nous rencontrons aussi un représentant de l'Association canadienne des professeures et professeurs d'université.

Afin de ne pas perdre de temps, nous allons commencer avec le Centre canadien de protection de l'enfance.

Madame McDonald, c'est à vous de commencer.

Mme Lianna McDonald (directrice générale, Centre canadien de protection de l'enfance): Merci.

Monsieur le président, membres distingués du comité, merci beaucoup de donner l'occasion à notre organisme de présenter un exposé sur le projet de loi C-13.

Je m'appelle Lianna McDonald. Je suis la directrice générale du Centre canadien de protection de l'enfance, un organisme de bienfaisance enregistré qui fournit des programmes et des services nationaux liés à la sécurité personnelle de tous les enfants.

Je suis accompagnée aujourd'hui de deux de mes collègues: Mme Signy Arnason, directrice de Cyberaide.ca; et Monique St. Germain, notre avocate générale.

Notre objectif, aujourd'hui, est de fournir des renseignements et d'exprimer notre appui à l'égard du projet de loi C-13, un projet de loi qui aidera à s'attaquer à la distribution non consensuelle d'images intimes. Nous allons livrer des témoignages découlant de notre rôle de gestionnaires de Cyberaide.ca, la ligne de dénonciation nationale du Canada où on peut déclarer les cas d'exploitation sexuelle en ligne des enfants.

Ce dont nous avons été directement témoins, et cela, trop souvent, c'est de l'intersection entre l'exploitation sexuelle, les technologies et l'intimidation. Depuis près de 30 ans, notre organisme travaille de près avec les familles, les forces de l'ordre, les éducateurs, les services de protection de l'enfance, l'industrie et d'autres intervenants pour assurer la protection de l'enfance. Dans le cadre de l'administration de Cyberaide.ca, nous avons reçu plus de 110 000 signalements de cas de violence sexuelle et d'exploitation des enfants. Ces signalements ont mené à plus de 550 arrestations par la police et au retrait de nombreux enfants d'environnements marqués par la violence.

C'est dans le cadre de ces travaux que nous avons été témoins des comportements les plus brutaux à l'égard des enfants, de l'enregistrement de scènes de violence sexuelle ou physique explicite contre de très jeunes enfants par des prédateurs adultes aux adolescents qui essaient de survivre aux conséquences sur les médias sociaux de l'affichage d'une photo de nature sexuelle en passant par des jeunes qui essaient de vivre avec les conséquences d'un crime sexuel qui a été enregistré. Il n'est pas facile d'être un jeune de nos jours.

Il y a plusieurs années, nous avons constaté un changement des types de signalements exposés sur la ligne de dénonciation. Nous avons commencé à remarquer que des jeunes qui avaient été victimes déclaraient eux-mêmes l'incident. Nous nous sommes vite rendu compte qu'il fallait intervenir et, par conséquent, nous avons créé un certain nombre de ressources de prévention. Nous avons rendu toutes ces ressources accessibles, avec deux ou trois exemples qui sont très pertinents pour cette question précise.

Même ces ressources et d'autres ressources sont importantes, nous savons que ce n'est pas suffisant. La technologie est devenue une arme puissante et la munition de choix des personnes qui veulent se cacher sous le couvert de l'anonymat. Les nouvelles technologies font en sorte qu'il est beaucoup plus facile de harceler les gens et de participer au Far-Web, où les préjugés continus au sujet de la délinquance sexuelle entrent en collision avec des attentes irréalistes touchant les comportements des adolescents, le tout alimenté par une utilisation inappropriée des technologies.

Même si, évidemment, nous en savons assez pour ne pas jeter le blâme uniquement sur les technologies, nous devrions vraiment être déterminés à comprendre son rôle dans la perpétration des infractions et à décider de quelle façon nous choisirons, en tant que pays, de régir et de moderniser nos lois de façon appropriée pour nous attaquer aux nouveaux types de comportements criminels.

Aujourd'hui, nous soulevons cette question du point de vue de la protection de l'enfance. De quelle façon protégeons-nous les droits à la vie privée des enfants? Et, plus précisément, de quelle façon nous attaquons-nous à l'atteinte à la vie privée de ces jeunes qui sont actuellement des victimes? Lorsque les jeunes deviennent des victimes et que les technologies ont été utilisées pour immortaliser le méfait sexuel, le traumatisme est encore plus profond. Le passé persiste dans le présent.

Pour ces raisons, nous sommes favorables au projet de loi C-13, et je veux souligner trois points principaux.

Premièrement, nous croyons fermement que l'infraction liée à la distribution d'images intimes est beaucoup plus appropriée qu'une infraction de pornographie juvénile lorsque la personne sur l'image et la personne qui la distribue ont toutes deux moins de 18 ans. Les infractions de pornographie juvénile ont été conçues et créées pour s'attaquer à un comportement et à des images qui sont vraiment différents de ce dont on parle aujourd'hui.

Deuxièmement, nous considérons que l'infraction doit s'appliquer aux victimes de tout âge. Notre organisme reçoit des signalements et des communications de nombreux jeunes adultes qui ont ce genre de problèmes. Les préjudices à la réputation et à la vie sexuelle découlant de la distribution non consensuelle d'images intimes sont importants, peu importe l'âge.

Troisièmement, il faut que de telles images soient retirées et effacées rapidement pour réduire au minimum les préjudices pour la personne qui en est le sujet.

Nous sommes favorables aux dispositions du projet de loi qui facilitent ces mesures. Selon nous, il est aussi extrêmement utile de permettre aux victimes potentielles de présenter une demande d'engagement imposé par un tribunal contre le distributeur potentiel pour prévenir toute distribution.

Je vais maintenant laisser ma collègue Signy Arnason vous présenter rapidement quelques statistiques et faits. Ensuite, Monique St. Germain abordera certaines critiques du projet de loi.

● (1105)

Mme Signy Arnason (directrice générale associée, Centre canadien de protection de l'enfance): Nous aimerions communiquer au comité des statistiques et des faits liés aux jeunes qui utilisent la ligne de dénonciation et qui étayent nos points de vue sur l'enjeu des jeunes qui partagent des images sexuelles et les répercussions de cette pratique.

Des 110 000 signalements que nous avons reçus jusqu'à présent sur la ligne de dénonciation, 4 % viennent d'une personne âgée de moins de 18 ans. Au cours des dernières années, un certain nombre de ces signalements ont été présentés par des jeunes et portaient sur des incidents d'auto-exploitation et d'exploitation par des pairs et de cyberintimidation. Nous continuons aussi de recevoir un certain nombre de déclarations dans nos comptes « Nous joindre ».

Les nombreux exemples dont nous avons été informés concernant l'échange d'images sexuelles vont de jeunes personnes qui partagent volontairement une image sexuelle dans le cadre d'une relation aux jeunes qui sont forcés à partager une image sexuelle en passant par des jeunes dont on a pris des photos à leur insu.

Que l'information soit présentée par le truchement de Cyberaide.ca ou AidezMoiSVP.ca, un site que nous avons conçu spécialement pour les jeunes, la principale demande de toutes les personnes dont une image à caractère sexuel a été distribuée en ligne est d'assurer le retrait du contenu. Ces jeunes sont désespérés et ils veulent que les photos ou les vidéos humiliantes d'eux-mêmes soient retirées d'Internet. Ils ne savent pas vers qui se tourner pour obtenir l'aide dont ils ont besoin.

AidezMoiSVP.ca, en tout juste un an, a reçu 65 000 visiteurs uniques. La page la plus populaire est celle qui décrit les mesures à prendre pour retirer du contenu sur Internet. Nous croyons que le projet de loi aidera à régler le dilemme des réseaux de contenu à qui on demande de retirer certains éléments du Web. Une telle mesure peut vraiment réduire la victimisation d'un jeune.

Au cours de la dernière année et demie, nous avons reçu au moins une dizaine de signalements de jeunes qui menaçaient de s'automutiler ou de se suicider en réaction à la distribution d'une image sexuelle. Dans un cas, nous avons dû garder une famille au bout du fil pendant que nous demandions l'intervention d'une unité de gestion de crise mobile.

Nous prenons chaque appel, chaque message à nos adresses « Nous joindre » et chaque signalement très au sérieux. Cependant, tant qu'il n'y aura pas de texte législatif qui s'attaquera à cette question, nous ne pourrons rien faire pour dissuader les jeunes de s'adonner à un tel comportement.

Mme Monique St Germain (avocate générale, Centre canadien de protection de l'enfance): Nous aimerions aussi exprimer certaines idées au sujet des quelques critiques qui ont été formulées au sujet du projet de loi.

Premièrement, certains craignent que le projet de loi ait un impact négatif sur les jeunes et que plus de jeunes soient accusés et envoyés en prison. En tant qu'organisation vouée à la protection de tous les enfants, nous préférerions que ce problème puisse être réglé grâce à la prévention, l'éducation et la sensibilisation. Malheureusement, parfois, des outils supplémentaires sont requis pour dissuader les jeunes d'adopter de tels comportements, s'attaquer aux préjudices et protéger les victimes actuelles et futures qui, dans de nombreux cas, sont aussi des enfants.

Ce qui n'a pas encore été mentionné, c'est que, si l'accusé est un jeune, la Loi sur le système de justice pénale pour les adolescents s'applique. Cette loi prévoit des mesures de protection de fonds uniques, conceptuelles et procédurales conçues spécialement pour protéger les intérêts des jeunes. Il y a des dispositions détaillées dans cette loi qui obligent tous les intervenants qui interagissent avec le jeune, des forces de l'ordre à la Couronne en passant par le juge, à tenir compte du niveau de maturité et de développement du jeune et à envisager des solutions de rechange et des mécanismes de réparation durant l'ensemble du processus.

Deuxièmement, des objections ont été soulevées auprès du comité au sujet du fait que la norme d'insouciance est trop faible. Cette norme était une recommandation précise du Groupe de travail sur la cybercriminalité du CCHF dans son rapport aux ministres FPT responsables de la justice et de la sécurité publique. Nous reprenons ce qu'a exprimé David Butt, de l'Association pour la sécurité Internet des enfants. La norme d'insouciance, dans un contexte criminel, n'est pas une norme de manque de diligence. C'est tout à fait la même chose que les règles de droit relatives à la négligence. Nous encourageons le comité à s'assurer que toute décision prise sur la question de l'insouciance est fondée sur une évaluation complète de la façon dont cette notion s'applique dans un contexte de droit criminel.

Troisièmement, certains ont dit craindre que le projet de loi C-13 n'empiète sur les droits des Canadiens aux termes de l'article 8 de la Charte. Le projet de loi prévoit deux mesures de protection importantes: l'obligation de demander un mandat, et la discrétion judiciaire de lancer ou non un tel mandat. La police a le devoir de communiquer pleinement, franchement et de façon équitable tous les faits importants au juge compétent lorsqu'elle demande un mandat. Selon nous, un juge est la personne la mieux placée pour évaluer la demande à la lumière de ces faits. Le seul élément du projet de loi qui n'exige pas de mandat est celui sur la préservation, mais la préservation n'est pas la même chose que la communication. Selon nous, le projet de loi a trouvé le juste équilibre entre les droits à la vie privée et la protection des Canadiens.

● (1110)

Mme Lianna McDonald: Pour terminer, nous savons que les enjeux auxquels les jeunes sont confrontés aujourd'hui sont beaucoup plus importants que ce que nous avons pu imaginer. Nous savons que trop de jeunes souffrent en silence, et nous avons perdu trop d'enfants en raison de suicides, ceux qui estimaient qu'il n'y avait aucune façon de s'en sortir, aucune aide et personne pouvant changer les choses. C'est inacceptable.

Aucune famille n'est à l'abri de ce problème croissant. C'est maintenant qu'il faut régler rapidement ce dossier. Nous comprenons que les discussions sur l'accès autorisé ont cours depuis bien plus de 10 ans. Du point de vue de notre organisme, c'est la protection de l'enfance qui en a souffert. Même si nous acceptons et reconnaissons qu'il faut débattre de façon constructive de la question, nous encourageons toutes les parties à relever leurs manches et à s'entendre. Les enfants ne méritent rien de moins.

Merci.

Le président: Merci beaucoup pour l'exposé du Centre canadien de protection de l'enfance.

Notre prochaine invitée, que nous connaissons tous, est Mme O'Sullivan du Bureau de l'ombudsman fédéral des victimes d'actes criminels.

La parole est à vous pour les 10 prochaines minutes.

Mme Sue O'Sullivan (ombudsman fédérale des victimes d'actes criminels, Bureau de l'ombudsman fédéral des victimes d'actes criminels): Je vous remercie de m'accueillir parmi vous aujourd'hui pour venir vous parler du projet de loi C-13, la Loi sur la protection des Canadiens contre la cybercriminalité.

J'aimerais commencer avec un bref aperçu du mandat de mon bureau.

Créé en 2007, le Bureau de l'ombudsman fédéral des victimes d'actes criminels reçoit et examine les plaintes des victimes. Nous favorisons et facilitons l'accès aux programmes et aux services fédéraux pour les victimes d'actes criminels en les renseignant et en les aiguillant, nous faisons la promotion des principes fondamentaux de la justice auprès des victimes d'actes criminels, nous sensibilisons les intervenants dans le domaine de la justice pénale et les décideurs au sujet des besoins et des préoccupations des victimes et nous déterminons les questions systémiques et les questions nouvelles qui ont une incidence négative sur les victimes d'actes criminels. En fait, nous aidons les victimes individuellement et collectivement.

Le projet de loi C-13 couvre de nombreuses questions liées aux télécommunications et à la criminalité, y compris la création d'une nouvelle infraction au Code criminel concernant la distribution non consensuelle d'images intimes; la modernisation du Code criminel; et la prestation de nouveaux outils d'enquête aux organismes chargés de l'application de la loi. Étant donné mon mandat et le temps limité dont nous disposons aujourd'hui, je limiterai mes commentaires aux articles du projet de loi qui touchent directement les victimes, et j'aborderai brièvement l'importance pour les organismes d'application de la loi d'avoir à leur disposition les outils dont ils ont besoin pour empêcher la perpétration d'actes criminels.

Ceci étant dit, j'appuie entièrement les dispositions du projet de loi C-13 que créent une nouvelle infraction relative à la distribution non consensuelle d'images intimes ainsi que les nouvelles mesures du Code criminel qui sont liées à cette infraction, y compris accorder le pouvoir aux juges de rendre une ordonnance d'interdiction pour limiter l'accès du délinquant à Internet ou à des réseaux numériques; accorder le pouvoir aux juges d'ordonner que des images intimes soient retirées d'Internet; permettre à un juge d'ordonner la confiscation d'ordinateurs, de téléphones cellulaires ou de tout autre appareil utilisé dans la perpétration de l'infraction; rembourser les dépenses engagées par les victimes pour retirer les images intimes d'Internet ou d'un autre média; et accorder le pouvoir aux juges de rendre une ordonnance interdisant à une personne de diffuser des images intimes.

Si le projet de loi est adopté, il aidera à fournir les outils nécessaires pour réduire la cyberintimidation et à offrir aux victimes le soutien dont elles ont grandement besoin.

La cyberintimidation est un problème assez récent, mais dont les conséquences sont dévastatrices. Les Canadiens peinent à trouver les meilleures façons de la comprendre et, surtout, d'y mettre fin. La cyberintimidation, comme nous l'avons entendu, touche énormément de personnes: dans un sondage mené en 2007 auprès de jeunes de 13 à 15 ans, plus de 70 % ont déclaré avoir subi de l'intimidation en ligne, et 44 % ont déclaré avoir intimidé une personne au moins une fois. Les enseignants canadiens ont classé la cyberintimidation au premier rang d'une liste de six enjeux préoccupants; 89 % ont indiqué que l'intimidation et la violence sont des problèmes graves dans nos écoles publiques. Je sais que des témoins sont venus vous parler de leur expérience personnelle intense avec la cyberintimidation.

Je tiens à prendre quelques instants pour souligner le courage et le leadership dont ils ont fait preuve afin de participer à cet important dialogue public, malgré toutes les émotions que cela ait pu éveiller chez eux. À travailler directement avec les victimes, j'ai appris que peu importe les difficultés qu'elles doivent surmonter, les victimes sont prêtes à venir parler de leur expérience pour le bien-être collectif, pour s'assurer que d'autres n'aient pas à souffrir comme elles.

Nous savons tous que l'intimidation, y compris la cyberintimidation, peut avoir des répercussions graves et permanentes sur les victimes. Ce qui distingue la cyberintimidation, c'est la vitesse fulgurante et la portée du méfait. En quelques minutes seulement, des images intimes ou personnelles peuvent inonder les réseaux et parcourir le monde, exposant de façon permanente les victimes.

Nous savons aussi qu'essayer de contenir une image qui est devenue « virale » est tout un exploit, et c'est même parfois impossible. Même lorsque les victimes travaillent avec des professionnels pour supprimer une image, on ne peut jamais être certain qu'il n'y a pas quelqu'un quelque part qui l'a encore et qui la diffusera de nouveau. Ce que nous ne comprenons pas encore réellement, c'est le sentiment d'être à jamais vulnérable et exposé, et les répercussions à long terme du fardeau émotionnel qui vient avec.

Les crimes liés à la technologie et les crimes connexes évoluent plus rapidement que notre capacité à comprendre pleinement leurs répercussions sur les victimes à long terme. Les personnes qui se font harceler montrent une perte d'intérêt pour les activités scolaires et un plus grand taux d'absentéisme, présentent des travaux scolaires de qualité inférieure et obtiennent des notes inférieures, et ont plus tendance à abandonner des cours et à faire l'école buissonnière.

Faire face au problème peut être tout aussi difficile. Pour cette raison, j'appuie l'ajout des « images intimes » à l'article 164.1 du Code criminel tel que le propose le projet de loi, car cela permettra aux juges d'ordonner le retrait d'images intimes du Web, ainsi que la proposition du projet de loi d'accorder aux juges le pouvoir de rendre une ordonnance interdisant à une personne de diffuser des images intimes.

Mais lorsqu'une ordonnance n'est pas rendue, retirer les images du Web n'est pas une mince affaire. Pour bien des gens, l'idée de retirer les images du Web peut être déconcertante; comment ça fonctionne? Comment je m'y prends? Qui peut m'aider?

Dans certains cas, il vaut mieux faire appel aux connaissances et aux services de professionnels pour obtenir des résultats plus certains et efficaces. Cependant, le recours à des sociétés privées peut entraîner des coûts importants, et les victimes ne devraient pas en être responsables. Une victime ne devrait jamais avoir à acquitter les coûts liés au retrait d'images. Une telle situation serait tout simplement inacceptable.

Ainsi, j'appuie la disposition du projet de loi C-13 qui prévoit le remboursement des dépenses engagées par les victimes pour retirer l'image intime d'Internet ou d'un autre média.

Bien que j'appuie les éléments du projet de loi liés au dédommagement, je crois qu'il faut: prolonger la période pouvant être visée par une demande de dédommagement; envisager la mise en place de mesures de rechange pour aider les familles qui ne peuvent payer les coûts directs liés au retrait d'une image; et inclure une disposition sur la façon dont les victimes recevront de l'information et une orientation en ce qui concerne les options relatives au retrait d'une image et le moment où elles les recevront et pour ce qui est du moment où elles peuvent demander un remboursement ou examiner ces questions.

● (1115)

Je crois comprendre qu'au titre du projet de loi, les dédommagements ne s'appliqueraient qu'aux dépenses engagées avant le prononcé de la peine. Une telle approche est problématique à quelques égards.

Notamment, il est possible qu'une victime dont la capacité financière est restreinte n'ait pas recours à des services de professionnels étant donné la possibilité qu'il n'y ait pas de déclaration de culpabilité ou qu'elle n'obtienne pas de remboursement dans le cadre du dédommagement.

Également, même si elles sont prêtes à courir un tel risque, certaines victimes n'ont pas les fonds nécessaires ou une carte de crédit leur permettant d'absorber la dépense temporairement. Autrement dit, les victimes qui n'ont pas les moyens de payer les services directement ou d'attendre un remboursement n'auront pas accès au même niveau de service et de protection que les autres. Il y aurait donc une inégalité au chapitre de l'aide offerte aux victimes.

Enfin, comme un certain temps pourrait s'écouler avant que la victime apprenne l'existence d'une aide professionnelle ou que l'entreprise en question effectue et facture les travaux, il est probable que certaines dépenses seront engagées après le prononcé de la peine. Selon ce que je comprends, au titre du projet de loi, les dépenses engagées par les victimes après cette étape ne pourraient pas faire l'objet d'un remboursement.

Bien que j'appuie les intentions qui sous-tendent le projet de loi, je recommande au comité d'envisager la modification de la section sur le dédommagement afin de mieux répondre aux besoins de toutes les victimes, peu importe leur situation financière, pour ce qui est de l'aide au retrait d'images.

Pour ce qui est des victimes qui ont les moyens et la possibilité de retenir les services de professionnels afin de retirer les images et de demander un dédommagement, il sera essentiel de leur fournir bien à l'avance des renseignements sur leurs droits et les processus à cet égard. Je ne vois pas très bien comment et quand on signalera aux victimes leur droit de demander une ordonnance de retrait ou de présenter une demande de dédommagement. Je comprends par contre qu'il s'agit de détails liés à la mise en oeuvre du projet de loi et qu'il est possible qu'on ne les examine qu'à cette étape. Cependant, je crois qu'il est important de souligner aux députés que si on ne met pas les victimes au courant de leurs droits et options suffisamment à l'avance, il est possible qu'elles ne puissent pas profiter d'importantes occasions de traiter les préjudices subis et d'obtenir l'aide dont elles ont besoin et qu'elles méritent.

Avant de conclure, je souhaite parler brièvement des éléments du projet de loi qui semblent être les plus sujets à controverse, à savoir ceux qui portent sur les outils d'enquête et l'équilibre entre les pouvoirs et la protection de la vie privée.

Les questions relatives à la protection de la vie privée et les outils d'enquête techniques ne relèvent généralement pas de mon mandat. Il est bien de souligner que les victimes avec qui nous avons discuté ne s'entendent pas sur ce volet du projet de loi. J'ai parlé à des victimes qui appuient fortement des mesures accrues pour aider les forces de l'ordre à mener des enquêtes et selon qui les outils inclus dans le projet de loi sont équilibrés et nécessaires. Mais, tout comme vous, j'ai également entendu le point de vue de victimes qui ne souhaitent pas que ces éléments soient adoptés, car elles craignent qu'ils minent le droit à la vie privée des Canadiens.

À mon avis, il faut établir un équilibre, et le dialogue que tiennent les Canadiens est très utile. Afin de favoriser une réduction de la cyberintimidation et de protéger les éventuelles victimes, il faut fournir aux agents d'application de la loi les bons outils pour qu'ils soient en mesure de mener des enquêtes rapidement et efficacement. Je crois que le projet de loi C-13 prévoit des outils importants qui aideraient les forces de l'ordre à enquêter sur ces cas et j'appuie l'ensemble des modifications législatives qui visent la conservation des données nécessaires aux enquêtes et qui permettraient ainsi à des affaires importantes d'aboutir.

En conclusion, j'appuie de nombreux éléments du projet de loi C-13 et je félicite le gouvernement d'avoir déposé un projet de loi qui pourrait faciliter le traitement des affaires de cyberintimidation et aider les victimes à retirer des images intimes du domaine public. Toutefois, comme je l'ai déjà mentionné, je recommande qu'on amende les dispositions portant sur le dédommagement afin de garantir que toutes les victimes aient les mêmes droits et possibilités d'avoir recours à de l'aide professionnelle et au remboursement des dépenses. Je recommande également qu'on précise comment et quand on informera les victimes de leurs droits.

Je vous remercie de votre attention.

[*Français*]

Merci.

● (1120)

[*Traduction*]

Le président: Merci, madame O'Sullivan, pour votre exposé.

Notre prochain invité est un habitué de la Colline, M. Michael Geist. Il est ici à titre personnel, mais il est titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique à l'Université d'Ottawa.

Bienvenue à nouveau. Vous avez 10 minutes, monsieur Geist.

M. Michael Geist (titulaire de la chaire de recherche du Canada, Droit d'Internet et du commerce électronique, Université d'Ottawa, à titre personnel): Merci, monsieur le président.

Bonjour, comme vous venez de l'entendre, je m'appelle Michael Geist. Je suis professeur en droit à l'Université d'Ottawa. J'ai comparu à de nombreuses reprises devant des comités dans le cadre de séances qui portaient sur les politiques numériques, y compris celles touchant la vie privée, mais je suis ici aujourd'hui à titre personnel pour vous parler de mes propres points de vue.

Comme vous le savez peut-être, j'ai été critique des projets de loi sur l'accès légal qui ont été présentés par les gouvernements libéraux et conservateurs. Cependant, je veux commencer en soulignant que le fait de critiquer les projets de loi sur l'accès légal ne signifie pas qu'on est opposé à s'assurer que les organismes d'application de la loi ont les outils dont ils ont besoin pour lutter contre la criminalité en ligne.

Comme Mme McDonald peut le confirmer, lorsque son organisation a lancé le projet Cleanfeed Canada en 2006, j'ai appuyé publiquement cette initiative, qui ciblait la pornographie juvénile en tentant d'établir un système pour protéger les enfants, maintenir la liberté d'expression et contenir un cadre de surveillance efficace.

Dans le cadre du projet de loi C-13, il y a un travail semblable à faire afin de s'assurer de ne pas sacrifier indûment et inutilement notre droit à la vie privée au nom de la lutte aux méfaits en ligne. Comme Mme O'Sullivan vient de le dire, il faut trouver un juste équilibre, et comme Carol Todd l'a dit au comité, nous ne devrions pas avoir à choisir entre la vie privée et notre sécurité.

Puisque j'ai peu de temps, permettez-moi de commencer en affirmant que je suis favorable aux demandes des témoins précédents, qui souhaitent que le projet de loi soit divisé afin qu'on puisse s'attaquer à la cyberintimidation de façon efficace, comme nous venons de l'entendre, et que nous puissions examiner de plus près la question de l'accès légal. De plus, je suis favorable aux demandes que l'on a entendues relativement à un examen exhaustif de la vie privée et de la surveillance au Canada.

Je pourrai discuter davantage de ces enjeux durant la période de questions, mais je veux me concentrer sur les préoccupations liées à la vie privée associées au projet de loi. Ainsi, je vais laisser la question des dispositions sur la cyberintimidation à d'autres, comme les témoins que nous venons d'entendre.

En ce qui concerne la protection de la vie privée, j'aimerais me concentrer sur trois enjeux: la disposition sur l'immunité en cas de communication volontaire; le faible seuil lié aux mandats pour les données de transmission; et l'absence d'exigences redditionnelles et en matière de communication.

Pour commencer, il y a la création d'une disposition sur l'immunité en cas de communication volontaire de renseignements personnels. Je crois que cette disposition sur l'immunité doit être examinée à la lumière de cinq faits. Pour commencer, la loi permet déjà à des intermédiaires de communiquer des renseignements personnels volontairement dans le cadre d'une enquête. C'est le cas dans la LPRPDE et le Code criminel.

Deuxièmement, les intermédiaires communiquent des renseignements personnels de façon volontaire sans mandat de façon excessivement fréquente. La récente révélation touchant les 1,2 million de demandes présentées à des entreprises de télécommunications pour obtenir des renseignements sur leurs clients en 2011 seulement, touchant ainsi au moins 750 000 comptes d'utilisateurs, nous donne une idée de l'impact sur la protection de la vie privée des cas de communication volontaire.

Troisièmement, les renseignements communiqués ne se limitent pas aux renseignements de base des abonnés. En effet, le comité a reçu un témoin du milieu de l'application de la loi, un représentant de la GRC qui a souligné ce qui suit:

> À l'heure actuelle, certains types de données, comme les données de transmission et de suivi, peuvent être obtenus par la divulgation volontaire d'un tiers...

En fait, puisque la LPRPDE est aussi ouverte, le contenu peut aussi être divulgué volontairement tant que cela n'exige pas d'interception.

Quatrièmement, les intermédiaires n'informent pas les utilisateurs de la communication, ce qui fait en sorte que des centaines de milliers de Canadiens ne sont pas informés. Contrairement à certaines des discussions que nous avons entendues, il n'y a pas d'exigence liée à l'information dans le projet de loi pour régler ce problème.

Cinquièmement, cette disposition sur la communication volontaire devrait aussi, je crois, être examinée parallèlement au manque de modifications importantes dans le projet de loi S-4 qui, ensemble, permettraient d'appliquer les dispositions sur la communication volontaire sans mandat à toutes les organisations.

Compte tenu de ce contexte, j'aimerais faire valoir que la disposition est une erreur et devrait être retirée. Elle accroît de façon incontestable la probabilité de communication volontaire au moment où, justement, les Canadiens sont de plus en plus préoccupés par de telles activités. En outre, on le fait sans définir d'exigences redditionnelles, sans surveillance ni transparence.

À ceux qui font valoir que cela ne fait que confirmer le droit actuel, permettez-moi de dire qu'il y a au moins deux changements importants, tous les deux préoccupants.

Le premier, c'est qu'on élargit la teneur de la notion de « fonctionnaire public » pour y inclure des intervenants comme les employés du CSTC et du SCRS et d'autres fonctionnaires. Après les révélations de Snowden, des préoccupations se font sentir à l'échelle mondiale au sujet du manque de responsabilité lié aux activités de surveillance, et cela risquerait d'accroître la fréquence de ces activités.

Deuxièmement, le Code criminel inclut actuellement une exigence de bonne foi et de raisonnabilité de la part de l'organisation qui communique volontairement l'information. Cette nouvelle disposition sur l'immunité n'inclut pas ces exigences, ce qui fait qu'on pourrait accorder l'immunité même lorsque la communication de renseignements n'est pas raisonnable.

Bref, cette disposition n'est pas nécessaire pour lutter contre la cyberintimidation et ce n'est pas non plus une disposition qu'il faut mettre à jour pour combattre la cybercriminalité. En fait, j'aimerais faire valoir qu'elle va à l'encontre des affirmations du gouvernement touchant la surveillance par les tribunaux. Je crois qu'il faut la retirer du projet de loi.

Le deuxième enjeu sur lequel j'aimerais m'arrêter, est le faible seuil touchant la délivrance d'un mandat relatif aux données de transmission. Comme vous le savez, le projet de loi C-13 contient un faible seuil touchant les « motifs de soupçonner » relativement aux mandats concernant les données de transmission, et, comme beaucoup de personnes l'ont souligné, le genre d'informations visées par de tels mandats est plus couramment appelé des métadonnées. Certains ont essayé de faire valoir que les métadonnées ne sont pas des renseignements de nature délicate, mais ce n'est tout simplement pas le cas.

● (1125)

Il y a eu un peu de confusion, pendant les séances, au sujet du volume de métadonnées incluses dans les données de transmission. Je tiens à dire que cela dépasse de loin la question de savoir qui a téléphoné à qui et combien de temps a duré la conversation. Cela comprend des informations très délicates touchant les communications entre ordinateurs, comme l'ont justement expliqué les représentants des services d'application de la loi aux membres de votre comité.

Ce type de métadonnées ne reflète peut-être pas le contenu du message, mais son contenu en renseignements personnels est très important. À la fin de l'année dernière, la Cour suprême du Canada, dans l'arrêt *R.* c. *Vu*, a statué sur l'importance des renseignements personnels associés aux métadonnées générées par un ordinateur. Elle a noté ce qui suit:

> Dans le contexte d'une enquête criminelle, cependant, elles peuvent également donner aux enquêteurs accès à des détails intimes sur les intérêts, les habitudes et les identités d'un utilisateur en fonction d'un registre créé involontairement par l'utilisateur...

Des représentants du milieu de la sécurité ont également commenté l'importance des métadonnées.

Le général Michael Hayden, ancien directeur de la NSA et de la CIA, a dit: « Nous tuons des gens à cause des métadonnées. »

Stewart Baker, ancien avocat général à la NSA, a déclaré ceci:

> Les métadonnées disent absolument tout sur la vie d'une personne. Quand vous avez suffisamment de métadonnées, vous n'avez pas vraiment besoin de contenu.

De nombreuses études ont confirmé les commentaires de MM. Hayden et Baker. Par exemple, certaines études font état d'appels à des organismes religieux qui permettent de tirer des inférences concernant la religion d'une personne et d'appels à des organismes médicaux qui permettent de tirer des inférences touchant l'état de santé de cette personne. De fait, un mémoire à un tribunal américain récent, signé par quelques-uns des plus grands experts mondiaux de l'informatique, relatait ce qui suit:

> Les métadonnées téléphoniques révèlent des informations à caractère privé et délicat au sujet des gens. Elles peuvent révéler leur affiliation politique, leurs pratiques religieuses et leurs fréquentations les plus personnelles. Elles permettent de savoir qui a téléphoné à une ligne d'aide de prévention du suicide et qui a téléphoné à son député; qui téléphone au bureau local du Tea Party et qui téléphone au service de planification des naissances. Le regroupement des métadonnées téléphoniques — touchant une seule personne sur une période donnée, des groupes de personnes, ou d'autres ensembles de données — augmente davantage le caractère délicat de l'information.

Voilà quels sont leurs commentaires — les commentaires des experts en sécurité de ce milieu.

De plus, la commissaire à la protection de la vie privée du Canada vient de publier une étude sur les répercussions sur les renseignements personnels des adresses IP, où elle dit qu'elles peuvent servir à observer les gens de façon très personnelle.

En outre, on voit jusque dans un rapport du ministre de la Justice, qui semble servir de fondement stratégique au projet de loi C-13, une recommandation visant la création de nouveaux outils d'enquête qui « garantiraient que le degré de protection augmente avec l'étendue du droit à la vie privée en jeu ».

Étant donné l'étendue du droit à la vie privée lié aux métadonnées, l'approche proposée dans le projet de loi C-13 en ce qui concerne les mandats visant les données de transmission devrait être modifiée et remplacée par la norme des « motifs raisonnables de croire ».

Ma troisième question concerne la transparence des rapports. Il faut se préoccuper de l'absence de transparence, de divulgation et d'exigence redditionnelle touchant la communication sans mandat. Cette question s'appuie à la fois sur la LPRPDE et les principes de l'accès légal, mais le projet de loi C-13 empire les choses. Les révélations fracassantes que nous avons obtenues au sujet des demandes et de la divulgation de renseignements personnels — dans la plupart des cas, sans surveillance des tribunaux ni mandat — montrent du doigt une faiblesse extraordinairement troublante des lois canadiennes sur la protection des renseignements personnels.

La plupart des Canadiens n'étaient pas au courant de ces divulgations et ils ont été choqués d'apprendre à quelle fréquence elles étaient utilisées. Les projets de loi présentés au Parlement visent l'élargissement de leur portée. À mon avis, cela fait de nous tous des victimes, car des renseignements personnels nous concernant pourraient être divulgués souvent sans que nous en ayons connaissance ou sans notre consentement explicite. Quand nous demandons aux entreprises de télécommunications du Canada d'être plus transparentes, comme c'est le cas dans d'autres pays, elles rétorquent que les règlements adoptés par le gouvernement les en empêchent.

J'espère que le comité modifiera les dispositions qui rendent davantage possible la divulgation sans mandat. Mais, même dans le cas contraire, il devrait assurément augmenter le niveau de transparence en rendant obligatoires les avis aux abonnés, la tenue d'un registre des demandes d'accès à des renseignements personnels et la publication régulière de rapports sur la transparence. Ces exigences pourraient être ajoutées au projet de loi C-13 en vue d'atténuer les préoccupations associées à la divulgation volontaire sans mandat. De plus, de tels rapports ne nuiraient pas aux enquêtes et seraient susceptibles d'augmenter la confiance du public à l'égard des organismes d'application de la loi ainsi qu'à l'égard des fournisseurs de services de communication.

J'aimerais, pour conclure, avec tout le respect que je lui dois, rappeler un incident personnel impliquant un membre de votre comité, M. Dechert, qui met en relief la pertinence de ces questions.

Nombre d'entre vous se souviendront qu'il y a plusieurs années, M. Dechert a lui-même été victime d'une atteinte à la vie privée: ses courriels personnels ont été envoyés aux journalistes et ont par la suite été largement repris par les médias. Cet incident relie ensemble plusieurs enjeux que j'ai essayé de mettre en lumière.

Premièrement, la question du droit à la vie privée se pose même quand vous n'avez rien à cacher et que vous n'avez rien fait de mal. Le préjudice causé dans le cas qui nous occupe, même s'il n'y a pas eu d'acte répréhensible, prouve que la victimisation est possible si les renseignements personnels ne sont pas protégés de manière adéquate.

Deuxièmement, une grande partie de ces renseignements risquent d'être dévoilés de manière volontaire. De fait, l'élargissement de la définition d'agent de police signifie que, en théorie, les adversaires politiques eux-mêmes pourraient demander la divulgation volontaire d'informations de ce type et avoir quand même l'immunité. En outre, dans de tels cas, aucun avis n'est prévu.

● (1130)

Troisièmement, et c'est peut-être ce qui est le plus important, le contenu des courriels qui ont été divulgués était dans la plupart des cas non pertinent. Ce sont les métadonnées — avec quelle personne le sujet a communiqué, à quel moment, à quel endroit et combien de temps a duré la conversation — qui auraient permis de tirer les inférences qui l'ont été par erreur dans le cadre de cet incident. Le droit à la vie privée résidait dans ces métadonnées, et c'est pourquoi un seuil trop bas est à ce point inapproprié.

Ce type de préjudice visant les renseignements personnels peut faire de quiconque une victime. Comme je l'ai déjà dit, nous savons qu'au moins 750 000 comptes d'utilisateurs canadiens font l'objet chaque année d'une divulgation volontaire — c'est un cas toutes les 27 secondes. Voilà pourquoi nous devons nous assurer que les lois prévoient des mesures de protection appropriées contre l'utilisation à mauvais escient de nos renseignements personnels, et voilà pourquoi il faudrait modifier le projet de loi C-13.

Le président: Merci, monsieur Geist, pour cet exposé.

Le prochain intervenant est M. Turk, de l'Association canadienne des professeures et professeurs d'université.

Vous avez la parole pour 10 minutes.

M. James L. Turk (directeur général, Association canadienne des professeures et professeurs d'université): Merci beaucoup.

Je m'appelle James Turk. Je suis le directeur général de l'Association canadienne des professeures et professeurs d'université. Cette association représente 68 000 professeurs qui travaillent dans 124 universités et collèges du Canada.

Cela fait longtemps que nous nous préoccupons de la législation en matière d'accès légal et de ses formulations successives. J'aimerais attirer votre attention sur trois points qui nous préoccupent dans le projet de loi C-13.

Le premier point, comme M. Geist l'a mentionné, touche la réduction du seuil juridique s'appliquant à la communication de dossiers personnels. Le second point concerne le fait que le projet de loi C-13 prévoit que les fournisseurs de services Internet qui conservent des données ou qui les communiquent de manière volontaire ne pourront pas être poursuivis au civil ni au criminel. Le troisième point qui nous préoccupe, c'est l'ajout des mots « origine nationale » dans la définition de « groupe identifiable » du Code criminel. Cette section du Code criminel est celle qui traite des discours haineux. Elle rend possible la criminalisation du discours politique.

Je vais d'abord parler de la première question, c'est-à-dire l'abaissement du seuil. Les dispositions actuelles du projet de loi C-13 touchant les ordonnances de communication des données de transmission et des données de localisation rabaissent le seuil — comme vous le savez, je l'espère — des « motifs raisonnables de croire » aux « motifs raisonnables de soupçonner ». Il s'agit possiblement de l'étape qui suivra un ordre ou une ordonnance de préservation des données de transmission. Le seuil plus élevé — le seuil actuel —, les « motifs raisonnables de croire », s'applique toujours aux ordonnances de communication qui excluent les données de transmission; cela veut dire que, si vous voulez avoir accès au contenu, votre demande doit respecter la norme des « motifs raisonnables de croire ». Mais si vous désirez obtenir les métadonnées, il vous suffit de respecter le critère des « motifs raisonnables de soupçonner ».

Étant donné le nombre de requêtes présentées au Canada, récemment, et compte tenu de ce que nous savons sur ce qui se passe aux États-Unis... Vous vous rappellerez qu'en juin 2013, la cour constituée en vertu de la FISA, aux États-Unis, avait demandé à l'entreprise Verizon de fournir à la NSA les métadonnées de tous ses clients des États-Unis, y compris les métadonnées associées aux appels téléphoniques locaux. Ainsi, la NSA a pu recueillir et conserver toutes les métadonnées associées aux appels téléphoniques faits aux États-Unis, qui ont abouti ou non, à partir d'un téléphone, d'un téléphone cellulaire ou d'un téléphone intelligent.

Je suis d'accord avec M. Geist sur le fait que les métadonnées peuvent réduire la pertinence du contenu. Les données que nous laissons derrière nous quand nous utilisons les technologies de la communication et qui touchent l'heure et la durée de la communication, l'appareil utilisé et la géolocation, entre autres, sont un formidable moyen de porter atteinte au droit à la vie privée d'une personne.

Prenons un exemple: un membre de votre comité téléphone à quelqu'un et, une semaine plus tard, se rend dans un édifice à bureaux. Un peu plus tard, il téléphone à une autre personne et, une semaine plus tard, se rend dans un autre édifice à bureaux. Dans cet exemple, quelles informations pourrions-nous tirer de l'analyse des métadonnées? Eh bien, quand on les compare à un profil donné, les métadonnées concernant le téléphone et les appareils utilisés par ce politicien permettraient aux intervenants d'un organisme gouvernemental de savoir que le premier interlocuteur était un médecin et le premier édifice à bureaux abritait le cabinet de ce médecin. Le deuxième interlocuteur était un médecin spécialiste et le second bureau, le cabinet de ce spécialiste.

Et maintenant? Nous savons que ce politicien a consulté deux médecins. Tout ce que les intervenants de l'organisme gouvernemental auraient à faire, ensuite, c'est d'examiner les activités du politicien sur Internet pour avoir une bonne idée de la maladie dont il souffre ou qui le préoccupe. Il est peut-être allé sur Internet pour s'informer sur le cancer colorectal, la maladie de Parkinson ou le VIH.

On peut facilement soutenir que, dans cet exemple, les métadonnées — deux appels à deux médecins, deux visites à deux médecins, l'activité sur Internet pendant la même période — sont aussi explicites que le contenu des communications. Le projet de loi C-13 abaisse le seuil s'appliquant à la surveillance par l'État des visites de ce politicien aux médecins, mais conserve un seuil plus élevé pour les courriels que ce politicien pourrait envoyer à son épouse au sujet de son problème de santé.

Je peux vous donner une foule d'autres exemples pour montrer que l'analyse des métadonnées peut être considérée comme une invasion. Les communications entre un époux et une épouse peuvent révéler de nombreux aspects de leur relation — l'endroit où ils vivent, l'endroit où ils travaillent, l'heure à laquelle ils se couchent, l'heure à laquelle ils se lèvent, le moment où ils quittent la maison, leur présence ensemble à la maison.

L'accès aux métadonnées permet également de déterminer selon une probabilité raisonnable que deux personnes ont noué des liens étroits, par exemple lorsque les appareils qu'ils utilisent se trouvent au même endroit plusieurs soirs de suite. Il permet également de savoir si une personne a un problème de consommation, par exemple si elle téléphone fréquemment aux Alcooliques anonymes. Il permet également de savoir si une personne envisage de se faire avorter, si elle téléphone à une clinique d'avortement, ou si elle a des problèmes de jeu, si elle téléphone fréquemment à un preneur de paris ou à un service d'aide.

● (1135)

Autrement dit, les fournisseurs de services Internet conservent les métadonnées pendant de longues périodes. La collecte et l'analyse de ces données, compte tenu du grand bassin des métadonnées, permet de faire des associations avec des événements qui se produisent dans le monde réel. Il est ainsi plus facile d'établir un profil et de porter atteinte au droit à la vie privée de certaines personnes sans avoir à demander à un niveau supérieur la permission de mettre un téléphone sur écoute. Un seuil moins élevé, quand il est question des métadonnées, ouvre la porte à une surveillance de masse.

Notre seconde préoccupation est l'immunité des fournisseurs de services Internet qui communiquent des données personnelles. La Cour suprême, comme vous le savez, a réservé son jugement quant à la constitutionnalité des requêtes de l'État visant à obtenir des renseignements sur un abonné sans mandat en vertu de la LPRPDE. Nous nous attendons à ce que la Cour rende sa décision bientôt, dans l'affaire *R.* c. *Spencer*.

Les progrès de la technologie et la valeur des métadonnées pour la surveillance par l'État font que les fournisseurs de services Internet constituent, à bien des égards, les chiens de garde des renseignements personnels des Canadiens. En prévoyant une exemption de responsabilité pénale ou civile pour les fournisseurs de services Internet, on invite ces derniers à favoriser une surveillance invasive par l'État plutôt que de les inciter à protéger les renseignements personnels des Canadiens par des moyens politiques et légaux. Je m'attendrais à ce que Telus, Bell ou Rogers considèrent qu'il est dans leur intérêt primordial de protéger le caractère confidentiel et privé des renseignements sur leurs abonnés. Ce projet de loi les encouragerait à se considérer comme des partenaires de la surveillance exercée par l'État sur leurs propres clients.

Mon dernier commentaire concerne l'expansion de la définition de discours haineux qui englobe le discours politique. Le projet de loi C-13, comme je l'ai dit en commençant, ajoute les mots « origine nationale » à la définition de « groupe identifiable » du Code criminel. Cette section du Code criminel porte sur le discours haineux. En incluant l'origine nationale à la définition des groupes identifiables, on fait en sorte que certains types de discours — par exemple les discours critiques à l'égard d'un gouvernement national, celui d'Israël, de Cuba ou de l'Ukraine — pourraient être considérés comme des discours haineux. Nous n'avons pas à revenir très loin en arrière, seulement aux années 1980, pour voir une disposition semblable utilisée pour poursuivre des personnes qui critiquaient le régime de l'apartheid en Afrique du Sud.

Comme l'ont fait d'autres témoins qui ont comparu devant votre comité, nous vous encouragerions à scinder le projet de loi. Combattre la cyberintimidation, c'est un objectif louable, mais donner à un gouvernement davantage de pouvoirs de surveillance sur ses citoyens pourrait perturber l'équilibre entre la liberté et l'autonomie individuelles et le pouvoir de l'État. Cette tension fondamentale des sociétés démocratiques doit être examinée avec prudence sans se priver de multiplier les consultations et en se préoccupant de la protection des renseignements personnels.

Faire le contraire — refuser de scinder le projet de loi et de tenir compte des préoccupations que M. Geist et moi-même avons soulevées — représentera pour le gouvernement du Canada, au mieux, un exercice futile. Des lois excessives seront contestées devant les tribunaux pendant les 5 ou 10 prochaines années et, à notre avis, seront au bout du compte déclarées invalides parce qu'elles violent les droits constitutionnels des Canadiens. Dans le pire des cas, le refus de scinder le projet de loi et de revoir ces sections entraînera une augmentation des pouvoirs de surveillance du gouvernement au détriment de la liberté et de l'autonomie individuelles, et les citoyens canadiens en paieront le prix.

Merci beaucoup.

● (1140)

Le président: Merci de ces commentaires, monsieur Turk.

Nous allons maintenant passer à la période de questions.

La première à prendre la parole sera Mme Borg, du Nouveau Parti démocratique.

[*Français*]

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Merci beaucoup.

J'aimerais vous remercier de vos témoignages.

Nous entendons deux types de témoignages différents: d'une part, on parle de la partie du projet de loi touchant la cybercriminalité; d'autre part, on parle des dispositions qui pourraient avoir des répercussions sur la vie privée. Voilà qui explique l'importance, selon nous, de diviser le projet de loi afin de bien étudier ces deux aspects séparément.

Ma première question s'adresse à M. Geist. M. Turk pourrait peut-être émettre lui aussi ses commentaires là-dessus.

Vous avez tous les deux parlé du fait d'accorder une immunité légale aux compagnies de télécommunication. On sait qu'en une seule année, les agences gouvernementales ont fait 1,2 million de demandes à des compagnies de télécommunication. Ce projet de loi ferait en sorte qu'on n'ait plus à prendre le temps de réfléchir et de se demander si on risque d'être poursuivi si on partage certaines informations. Personnellement, cela me préoccupe extrêmement.

J'aimerais entendre vos commentaires là-dessus. Le fait que ce projet de loi retire cette petite responsabilité légale risque-t-il de faire augmenter le partage de renseignements personnels sans mandat entre le gouvernement et les compagnies de télécommunication?

[*Traduction*]

Le président: Monsieur Geist, je crois que la question vous a été posée à vous, d'abord; M. Turk pourra répondre à son tour.

M. Michael Geist: Merci d'avoir posé la question.

Je crois qu'on se préoccupe énormément des cas de divulgation dont nous avons parlé. Je devrais souligner que ce chiffre de 1,2 million de demandes ne reflète peut-être pas tout à fait fidèlement les demandes qui sont présentées. Comme vous le savez, le Commissariat à la protection de la vie privée du Canada a présenté cette demande, et les entreprises de télécommunications ont refusé de fournir des réponses individuelles. Certaines ont été obligées de le faire, mais les informations ont été regroupées avant d'être transmises.

Je trouve frappante la différence entre le Canada et les États-Unis quand il est question de la transparence associée à ce type d'activités. Aux États-Unis, de grandes entreprises de télécommunications, comme Verizon et AT&T, déposent maintenant des rapports sur la transparence qui présentent des informations regroupées sur la situation. Nous ne voyons rien de semblable, au Canada, en ce qui concerne nos propres entreprises de télécommunications. Certaines ont fait valoir qu'elles n'avaient pas le droit de le faire, qu'il y avait pour cela des motifs juridiques. Je crois qu'il faudrait y voir.

De la même façon, du point de vue de la personne, le fait qu'aucune notification ne soit donnée, dans de tels cas, pose un énorme problème. Dans de nombreux cas, on ne sait pas s'il y a une restriction de nature juridique, si le bâillon a été imposé. Ça s'est passé ainsi, dans d'autres législations. Ce n'est pas nécessairement en vertu de la LPRPDE que le bâillon a été imposé, dans nombre de ces cas-là. C'est tout simplement qu'on refuse de donner suite à ces requêtes ou qu'on a décidé de ne pas en parler.

Je ferais valoir que dans des cas délicats touchant l'application de la loi, il est possible d'obtenir le mandat requis ou l'ordonnance requise pour s'assurer qu'aucun renseignement ne sera divulgué, si on estime que cela pourrait causer un préjudice, mais, dans d'autres cas, il est tout à fait approprié que l'entreprise de télécommunications ou l'intermédiaire concerné doive aviser son abonné ou son client du fait que des renseignements personnels le concernant ont été communiqués.

Le président: Monsieur Turk.

M. James L. Turk: Je suis d'accord pour dire que le chiffre de 1,2 million est probablement une sous-estimation des demandes.

Plutôt que de simplement répéter ce que M. Geist a dit, parce que je suis d'accord avec lui, je pense que, actuellement, la police dispose des outils dont elle a besoin pour faire ce qu'elle a à faire. Je pense que la norme des motifs raisonnables de croire, qui est la condition pour avoir accès aux données de transmission ou au contenu, est une norme raisonnable et qu'elle devrait être maintenue.

Je suis également profondément préoccupé par le fait que le Canada semble faire preuve de moins de transparence que les États-Unis et qu'il semble accorder moins d'importance à la responsabilité de protéger ses clients que les fournisseurs de services Internet canadiens semblent le faire. Ce projet de loi ne fera qu'aggraver la situation.

● (1145)

[*Français*]

Mme Charmaine Borg: Merci.

On constate que le manque de transparence semble être un gros enjeu. Je conviens qu'on est arrivé à ce chiffre de 1,2 million sans même que toutes les compagnies de télécommunication répondent à la question de la commissaire. Sans cette question, on ne l'aurait jamais su, ce qui est fort problématique.

Lorsqu'on débat de ces enjeux à la Chambre des communes, on finit toujours par nous dire qu'on peut retrouver ces données dans un annuaire téléphonique. Or c'est complètement faux. Une adresse IP peut révéler énormément de choses sur une personne, tout comme les métadonnées.

Monsieur Geist, vous nous avez donné une certaine idée de ce qu'est une adresse IP et de ce qu'elle peut révéler sur une personne. Pouvez-vous nous donner plus de précisions là-dessus?

[*Traduction*]

M. Michael Geist: En ce qui concerne la question précise sur ce qu'est une adresse IP, il s'agit, d'une certaine façon, de l'endroit où nous nous trouvons sur Internet. Cette même adresse IP peut révéler — et je félicite la commissaire à la protection de la vie privée pour son rapport sur le sujet — davantage que simplement l'ordinateur ou le dispositif que nous utilisons, parce que cette information figure à de nombreux endroits dans Internet. Par exemple, si vous contribuez à la rédaction d'un article sur Wikipedia, votre adresse IP est enregistrée et devient disponible publiquement. Il est même possible d'utiliser ce genre d'informations pour commencer à créer un profil des activités en ligne d'une personne.

Vous l'avez souligné, mais je pense qu'il est important d'insister sur le fait que, aux termes de la LPRPDE, l'exemption qui s'applique aux organismes d'application de la loi, telle qu'elle est définie aujourd'hui, n'est d'aucune façon limitée aux renseignements de base sur les abonnés. Cette notion est propagée encore et encore, et, je m'excuse, mais elle est tout simplement fausse. L'ouverture vise à permettre la divulgation, un point c'est tout. En fait, votre comité a entendu de la part de la GRC que cela comprend les données de transmission et de localisation, mais, franchement, cela pourrait également inclure, en théorie, le contenu qu'un intermédiaire a en sa possession, si cela fait partie d'une enquête licite.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

[*Traduction*]

Le président: Je vais maintenant céder la parole à M. Dechert, notre premier intervenant du Parti conservateur.

M. Bob Dechert (Mississauga—Erindale, PCC): Merci, monsieur le président.

Merci à chacun de nos témoins d'être ici, aujourd'hui.

Monsieur Geist, j'aimerais vous répondre. Vous avez parlé d'une chose qui s'est produite relativement à des messages entre moi et un autre parti, qui ont été volés par un tiers et rendus publics. Certains de mes amis dans les médias se sont bien amusés dans cette affaire.

Cependant, ce dont ce projet de loi traite, monsieur, c'est la protection des jeunes à l'égard de la cybercriminalité. Je suis un adulte, je suis un avocat, je suis un représentant élu. J'ai été envoyé ici deux fois par des milliers de gens de ma circonscription afin de les représenter, et je suis encore assis ici, en train de vous parler, aujourd'hui, contrairement à Rehtaeh Parsons ou Amanda Todd ou Jamie Hubley. Voilà la différence. Je n'ai pas souffert. Bien sûr, ça m'a mis un peu dans l'embarras, mais, je vous le dis, je n'ai pas souffert.

Si j'avais souffert, j'aurais eu les moyens d'y faire face. J'aurais pu poursuivre la personne. J'aurais pu poursuivre les médias. Je sais comment faire cela. Je suis certain que les gens de ma circonscription m'appuient, mais je suis ici en train de vous parler, et il y a d'autres gens qui ne le sont pas. Ce que nous devons faire, c'est donner aux organismes d'application de la loi les outils leur permettant de protéger les gens qui ne peuvent pas se protéger.

J'aimerais m'adresser à Mme O'Sullivan...

Une voix: [*Note de la rédaction: inaudible*]

Le président: La parole est à lui, monsieur Geist. Il peut faire ce qu'il veut.

Les cloches sonnent, donc je vais suspendre la séance. Nous allons arrêter le temps ici pour vous, monsieur Dechert. Nous serons de retour après ce vote, puis nous allons continuer avec les questions et les réponses. Nous allons essayer de faire en sorte que nous terminions au moins une série de questions.

La séance est suspendue.

● _____ (Pause) _____ ●

● (1235)

Le président: La séance est ouverte.

Chers témoins, merci de votre patience. Nous avons procédé au vote, et nous sommes de retour. Nous devrions réussir à terminer la première série de questions, donc chaque parti aura la possibilité de poser des questions.

Monsieur Dechert, vous avez encore la parole.

M. Bob Dechert: Merci, monsieur le président.

Madame O'Sullivan, au moment où la séance a été suspendue, je m'apprêtais à vous poser une question au sujet du juste équilibre entre le fait de répondre aux besoins et préoccupations des victimes et, également, le fait de protéger les libertés civiles. Comme vous le savez, nous avons tous de la difficulté à y arriver, ici. Où traçons-nous la limite entre la publication de ce que certaines personnes, certains défenseurs des libertés civiles, disent être des renseignements personnels et le fait de pouvoir agir suffisamment rapidement pour sauver la vie de personnes vulnérables?

Mardi, à la réunion du comité, nous avons accueilli M. Gilhooly, qui est un avocat et une victime lui-même. C'est un homme brave, et il est venu nous raconter son histoire, comment il a été victimisé par Graham James.

Je lui ai posé la même question, et il a dit: « Je mets mon espoir dans une police dotée des outils appropriés pour intervenir », et que, en ce qui a trait aux cas liés au projet de loi C-13 où les droits à la vie privée ne sont pas bafoués de façon flagrante, « nous, les victimes... ne voulons pas que les droits soient bafoués, mais il faut ici privilégier la victime ». Laissez-moi continuer pendant une petite minute, parce que je veux également que vous sachiez ce que l'autre côté a dit. Le représentant de la Criminal Lawyers' Association a dit que: « Il ne faut pas faire pencher la balance vers la victime ». Il a dit: « Mais plutôt vers la Charte, qui est la loi suprême à respecter ».

Seriez-vous d'accord pour dire que le gouvernement a la lourde tâche de trouver le juste équilibre entre les libertés civiles et la protection des Canadiens et des victimes? Seriez-vous d'accord pour dire que, dans les cas où il n'y a pas de violation grave des droits de la protection des renseignements personnels, la balance doit pencher vers la victime? Qu'en pensez-vous?

● (1240)

Mme Sue O'Sullivan: J'aimerais commencer en disant que, tout d'abord, je pense qu'il est absolument nécessaire que nous respections toutes les opinions qui sont formulées au cours de cette conversation ainsi que le besoin, comme vous le dites, d'établir cet équilibre. J'aimerais également reconnaître, tout particulièrement, qu'il y a eu de nombreuses familles de victimes, notamment sur le plan de la cybercriminalité, qui se sont exprimées de façon très publique à propos de leur leadership, de leur bravoure, ainsi que du leadership dont elles ont fait preuve en vue de s'assurer que nous, dans notre pays, avons cette conversation — cette conversation très importante — à propos de cet équilibre.

Cette conversation n'est pas uniquement liée à ce projet de loi. Il s'agit d'une chose à laquelle nous devons constamment prêter attention, mais, selon moi, les outils dont il est question dans ce projet de loi sont nécessaires pour s'assurer que les organismes d'application de la loi peuvent mener cette enquête. Ce que j'en comprends, c'est simplement qu'il y a de l'information qui peut être pertinente dans le cadre d'une enquête. Alors, ils demandent aux fournisseurs de services de télécommunications de préserver cette information, puis ils obtiennent une autorisation judiciaire afin d'y avoir accès. Donc, je pense que cela... Ce que je veux dire, lorsqu'on parle de freins et contrepoids... je pense vraiment qu'une autorisation judiciaire est un mécanisme de contrôle approprié.

Donc, à mesure que nous progressons — et j'ai parlé, dans ma déclaration préliminaire, de la technologie et de son impact —, ce ne serait pas la fin de ces conversations. Il s'agit d'une conversation, je pense, que non seulement les parlementaires et les gouvernements continuent d'avoir, mais que les Canadiens doivent avoir, parce que nous participerons ainsi à un débat très public, qui nous permet, en tant que Canadiens, de véritablement s'assurer... D'une certaine façon, le fait que les Canadiens participent à ce débat très important est un autre moyen de surveillance. Mais, à mon avis, ces outils sont essentiels pour aider les organismes d'application de la loi à veiller à ce que nous ayons la capacité de recueillir et de préserver ces éléments de preuve.

M. Bob Dechert: Madame McDonald, qu'avez-vous à dire là-dessus?

Mme Lianna McDonald: Eh bien, comme, je pense, nous l'avons indiqué d'entrée de jeu, nous croyons assurément que ce projet de loi permet d'atteindre ce juste équilibre. Du point de vue de notre organisme, nous nous sommes beaucoup appuyés sur ce qui avait été mis de l'avant. Nous avons un rapport très approfondi du Groupe de travail sur la cybercriminalité du CCHF. Nous croyons comprendre que des consultations ont été effectuées pendant des années sur cette question. Nous avons donc eu l'occasion, au fil des années, d'en discuter avec un grand nombre d'intervenants concernés dans le cadre de nos travaux sur ces sujets délicats. Encore une fois, nous croyons que ce projet de loi permet d'atteindre un juste équilibre et qu'il est temps de prendre les mesures qui s'imposent.

M. Bob Dechert: Me reste-t-il du temps? D'accord.

J'ai une petite question pour Mme O'Sullivan. Vous avez déjà été policière.

Mme Sue O'Sullivan: Oui, je l'ai été.

M. Bob Dechert: Un des commentaires qui ont été formulés concernant ce projet de loi, c'est que la personne dont les renseignements personnels sont divulgués devrait être avisée au moment où la demande est présentée. En tant que policière, qu'adviendrait-il des données, selon vous, si cela se produisait? Seraient-elles détruites? Seraient-elles effacées?

Mme Sue O'Sullivan: Tout d'abord, je ne suis plus policière depuis cinq ans, et je sais que vous avez accueilli un groupe d'experts sur l'application de la loi, ici, alors je m'en remettrais certainement aux organismes d'application de la loi pour obtenir de l'information à ce sujet. Cela relève vraiment de leur domaine de compétence, mais, au bout du compte, je pense qu'on pose les bonnes questions. Comme je l'ai dit, je sais que le chef Chu et plusieurs hauts fonctionnaires responsables de l'application de la loi en ont parlé.

M. Bob Dechert: Merci.

Le président: Merci beaucoup.

Maintenant, du Parti libéral, nous avons M. Casey.

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

Monsieur Geist, au début de cette série de questions, M. Dechert s'est un peu acharné sur vous, et vous n'avez pas eu la chance de répondre. Vous pouvez utiliser une partie de mes sept minutes pour le faire, si vous le souhaitez.

M. Michael Geist: Merci pour cela.

La seule chose que je voulais dire, c'est que nous sommes d'accord. Nous sommes tous les deux d'accord pour dire que les victimes, particulièrement dans le contexte de la cyberintimidation, doivent pouvoir exercer un recours et disposer d'outils appropriés.

La seule chose que je voulais dire relativement à cette question, c'est qu'il y a des victimes d'atteintes à la vie privée de tous les âges et de tous les milieux. En fait, dans de nombreux cas, celles-ci se produisent lorsque les gens sont parfaitement inconscients de ce qui se passe.

Je dirais que, dans le contexte de ce projet de loi, comme la cyberintimidation comporte ce qui est très clairement un élément important de protection de la vie privée, nous ne devrions pas, pour la contrer, oublier la protection des renseignements personnels. Il y a de meilleures façons de régler deux ou trois petits détails préoccupants très précises, alors que, pour être honnête, il y a un consensus plutôt important sur bon nombre de dispositions du projet de loi.

● (1245)

M. Sean Casey: Merci.

Je veux me pencher sur le fait qu'on permet la distribution non consensuelle de renseignements personnels sur un client avec l'immunité et sans mandat. Plusieurs d'entre vous en ont parlé.

Monsieur Geist, il y a deux ou trois choses que vous avez dites dans votre déclaration préliminaire qui portaient sur les compagnies de téléphone, et, si vous me le permettez, j'aimerais approfondir un peu la question. Une des choses que vous avez dites, en ce qui a trait aux rapports sur la transparence, c'était que les compagnies de téléphone indiquent qu'il y a, en fait, certaines règles gouvernementales qui l'interdisent.

Nous avons entendu le ministre à ce sujet. Je lui ai posé directement une question concernant les rapports sur la transparence ou la communication d'informations par les compagnies de communications. Je voulais savoir à quelle fréquence elles divulguent de l'information sans consentement et sans mandat, et si elles ont l'obligation d'en faire part à leurs clients. La réponse que j'ai obtenue, c'est qu'il s'agissait d'une modalité contractuelle entre le client et la compagnie de communications.

J'aimerais, si vous le voulez bien, que vous m'aidiez à comprendre. Si les compagnies de communications disent que le gouvernement les empêche de faire preuve de plus de transparence, et que le gouvernement dit qu'il s'agit d'une entente entre elles et leur client, qui devons-nous croire, et à qui devons-nous nous adresser?

M. Michael Geist: Je pense qu'il y a deux ou trois choses que nous devons faire. Plus tôt cette année, on a demandé à toutes les grandes compagnies de communications, dans une lettre envoyée par de nombreux intervenants du milieu de la protection des renseignements personnels au Canada, de divulguer certaines de leurs pratiques. Il faut reconnaître qu'elles ont toutes décliné la demande en citant les règles du solliciteur général et en disant, de façon générale, que, si le gouvernement leur demandait de procéder à ce genre de divulgations liées à la transparence, elles le feraient, mais, autrement, qu'elles ne s'estimaient pas à l'aise de le faire, même en regroupant les données.

Leur opinion, actuellement, c'est qu'ils ne progressent pas à cet égard. Nous pourrions faire en sorte que le gouvernement dise qu'il juge que ce type d'information regroupée est importante, même de façon regroupée. Il convient de noter que, même en ce qui a trait aux personnes, M. Dechert, avec sa dernière question, a laissé entendre que, d'une certaine façon, ceux qui sont en faveur de l'envoi d'avis veulent que ces avis soient envoyés immédiatement, tandis que les organismes d'application de la loi sont au beau milieu de l'enquête. Je ne crois pas que c'est ce que j'ai dit ni ce que bon nombre d'autres personnes ont dit.

Nous avons dit qu'un client devrait avoir le droit, à un moment ou à un autre, d'être avisé si ses renseignements personnels sont divulgués — le fait de décider de ce que serait le moment approprié est, je pense, une question importante et dont on devrait débattre —, mais je n'ai entendu personne dire que le client en cause devrait être avisé si cela devait nuire à l'enquête ou la mettre en péril.

M. Sean Casey: Plusieurs d'entre vous ont parlé de l'immunité, et c'est un sujet qui a passablement été abordé dans le cadre d'autres audiences, également. Je ne sais pas si vous allez pouvoir m'aider. Cette question est pour M. Geist et pour M. Turk, également.

Pourquoi est-il question de cela? Était-ce à la demande des compagnies de téléphone? Qu'est-ce qui a justifié l'insertion de l'immunité — particulièrement lorsque le gouvernement affirme que cette disposition n'a aucune importance et qu'elle y figurait déjà — dans ce projet de loi? J'aimerais entendre ce que, tous les deux, vous avez à dire là-dessus, je vous prie.

M. James L. Turk: Je ne sais pas pourquoi on a voulu l'inclure. Je soupçonne que le principal intérêt des compagnies de téléphone et des fournisseurs de services Internet, c'est que cela pourrait empêcher le dépôt de recours collectifs contre eux. Ils sont relativement peu vulnérables.

Je pense qu'il y a un aspect plus important lié à son inclusion, dont j'ai essayé de parler, et c'est qu'elle constitue, essentiellement, une mesure qui incite les fournisseurs de services Internet à réfléchir à leur relation avec le gouvernement, et non à leurs obligations à l'égard de leurs abonnés.

M. Michael Geist: Bien sûr, je serais certainement d'accord avec M. Turk à cet égard. Je pense que c'est probablement cette responsabilité éventuelle liée aux recours collectifs, mais, en même temps, je dirais que, si nous examinons l'ensemble de la situation concernant les questions sur la protection de la vie privée, tant en ce qui a trait à ce projet de loi qu'au projet de loi S-4, ceux-ci, en fait, laissent entendre que le gouvernement favorise la divulgation davantage volontaire et sans mandat. Nous le constatons avec l'élargissement de ce type de dispositions figurant dans le projet de loi S-4, et nous le voyons ici, maintenant, avec l'immunité concernant les divulgations qui ont lieu.

Cela a pour effet d'envoyer un signal, je pense, à ceux qui recueillent de l'information, les compagnies de communications et les autres, que nous allons créer et adopter un cadre qui favorisera cette coopération volontaire, cette divulgation volontaire, sans l'intervention des tribunaux.

Nous avons constamment entendu dire, je pense, de la part d'autres intervenants que ce projet de loi permettra l'atteinte d'un juste équilibre. Ils disent cela de façon uniforme, à condition que les tribunaux interviennent. Il faut reconnaître que, dans ces situations, le tribunal n'intervient pas lorsque ces divulgations volontaires ont lieu.

● (1250)

Le président: Votre temps est écoulé, monsieur Casey. Merci beaucoup.

Notre prochain intervenant du Parti conservateur est M. Seeback.

M. Kyle Seeback (Brampton-Ouest, PCC): Merci, monsieur le président.

Je vais essayer de procéder rapidement. J'ai très peu de temps.

Madame St. Germain, je pense que vous avez parlé de la norme d'insouciance. Un autre témoin s'est présenté à la séance de mardi, M. Butt, et voici ce qu'il a dit au comité:

> Au risque d'une simplification à outrance, je dirai qu'il ne s'agit pas de négligence. La négligence est de l'étourderie, un manque de réflexion sur le risque. L'insouciance connaît le risque, mais ça n'empêche pas d'agir. Comment peut-on avoir tort de dire, même à un adolescent, que, malgré le risque dont il était conscient, il a quand même distribué des images intimes inappropriées d'un tiers.

Je présume que vous êtes d'accord avec l'évaluation qu'il a faite mardi.

Mme Monique St Germain: Si elle est interprétée dans un contexte criminel, la norme d'insouciance comporte un élément subjectif. La personne qui commet l'infraction doit en fait reconnaître qu'un risque est associé à ce qu'elle fait, ce qui est un peu différent du simple fait d'être négligent. C'est une norme beaucoup moins élevée, donc, oui.

M. Kyle Seeback: Donc, vous approuveriez ce qu'il avait à dire dans son analyse.

Mme Monique St Germain: Oui.

M. Kyle Seeback: Excellent. Merci.

Monsieur Turk, je veux vous parler au sujet de votre préoccupation à l'égard de la norme des motifs raisonnables de soupçonner par rapport à la norme des motifs raisonnables de croire en ce qui a trait aux données de transmission. Nous entendons toujours dire que cela concerne les métadonnées, mais je vais exprimer respectueusement mon désaccord. Je pense que les données de transmission forment une catégorie plus restreinte que celle des métadonnées. On obtient moins d'informations qu'on en obtiendrait grâce à des métadonnées, lorsqu'il s'agit des données de transmission.

Vous dites que cela abaisse la norme. Dans d'autres circonstances, ce sont les motifs raisonnables de croire. Mais, si vous voulez obtenir un enregistreur, qui vous donnera l'information sur l'origine d'un appel téléphonique, le destinataire de l'appel téléphonique et la durée de la conversation, il s'agit du paragraphe 492.2(1) du Code criminel, et, pour l'obtenir, il faut des motifs raisonnables de soupçonner.

Il ne s'agit pas d'abaisser la norme. En fait, c'est la même norme. Les gens disent, comme vous, que le principal problème, c'est que, dans un courriel, on peut découvrir que la personne a écrit à un médecin et, par conséquent, obtenir des renseignements personnels, et que ce devrait être une norme plus élevée. Eh bien, on obtient ces renseignements d'un appel téléphonique aussi. Tout ce qu'on a à faire, c'est aller voir quel était le numéro de téléphone sur le site de Canada 411.

Ainsi, en réalité, la norme ne change pas. C'est exactement la même.

M. James L. Turk: Je pense que vous êtes la première personne que je rencontre qui laisse entendre que le genre d'informations qu'on peut obtenir d'un relevé de téléphone conventionnel équivaut à celles qu'on obtient au moyen de métadonnées Internet.

M. Kyle Seeback: Mais ce ne sont pas des métadonnées. Ce sont...

M. James L. Turk: Eh bien...

M. Kyle Seeback: Ce qu'on obtient des données de transmission, ce sont le type, la date, l'heure, l'origine, la destination ou la fin de la communication. Elles ne comprennent pas le contenu. Ce qu'on obtient d'un relevé de téléphone, c'est l'heure, la date, l'origine et la destination de l'appel.

Je ne vois pas de différence gigantesque qui requiert un niveau de preuve plus élevé, puisqu'on doit tout de même obtenir une autorisation judiciaire, même si on a des motifs raisonnables de soupçonner. Les policiers doivent se rendre devant un juge et le convaincre du fait qu'ils soupçonnent qu'un acte criminel a été commis avant qu'ils puissent obtenir les données de transmission.

M. James L. Turk: Tous les juristes que je connais estiment qu'il y a une différence importante entre les motifs raisonnables de croire et les motifs raisonnables de soupçonner.

M. Kyle Seeback: Il y en a une. C'est exact.

M. James L. Turk: C'est mon premier point. Deuxièmement, j'ai tenté de donner des exemples de cas, en me servant de vous pour les illustrer, du genre d'informations qu'on peut recueillir en vertu de cette disposition et qui révéleraient une bonne quantité de renseignements personnels.

M. Kyle Seeback: Vous avez dit supposons que j'enverrais un courriel à un médecin, n'est-ce pas?

M. James L. Turk: Oui.

M. Kyle Seeback: Puis, après, si j'en envoie un autre à un autre médecin, ils découvrent que je suis allé consulter un spécialiste du cancer du côlon ou peu importe.

Ne pourrait-on pas obtenir exactement les mêmes renseignements à la lumière des appels téléphoniques que j'aurais faits pour communiquer avec ces personnes, c'est-à-dire que j'ai téléphoné à deux médecins différents?

● (1255)

M. James L. Turk: C'est la combinaison de tous ces renseignements: qui vous avez appelé, quand vous l'avez appelé et de vos autres activités sur Internet liées à ces communications, durant cette période; c'est ce qui est si révélateur. On ne peut pas faire cela simplement à partir de...

M. Kyle Seeback: Avec une autorisation judiciaire, par conséquent, la police...

M. James L. Turk: La norme des motifs raisonnables de soupçonner...

Ce que je veux dire, c'est, regardez: si la police a effectivement des motifs raisonnables de croire, ce n'est pas une norme impossible à respecter, alors pourquoi l'abaisser?

M. Kyle Seeback: Ce n'est pas l'abaisser. Parce que, si on obtient ces renseignements d'un appel téléphonique...

M. James L. Turk: Elle l'est. Si elle n'est pas abaissée, pourquoi n'êtes-vous pas prêts à faire des motifs raisonnables de croire la norme?

M. Kyle Seeback: Nous devrions donc la changer pour les numéros de téléphone également.

M. James L. Turk: Oui.

M. Kyle Seeback: Ce devrait être les motifs raisonnables de croire; ainsi, vous dites qu'il faut changer le paragraphe 492.2(1).

M. James L. Turk: Si vous vous servez de cela pour justifier ce changement, alors oui, il faut le changer.

Le président: Il vous reste une minute.

M. Kyle Seeback: L'argument que je pense que les gens comme vous n'arrêtent pas de me donner, c'est que vous supposez que les policiers vont s'adresser à un juge — parce qu'ils doivent le faire, n'est-ce pas? — pour obtenir cette ordonnance du tribunal et convaincre un juge qu'il y a des motifs raisonnables de soupçonner qu'un acte criminel a été commis, que, d'une manière ou d'une autre, ils vont...

M. James L. Turk: Ou qu'il sera commis.

M. Kyle Seeback: ... ou qu'il sera commis, et que les policiers réussiront à utiliser ces motifs pour obtenir des renseignements sur des Canadiens ordinaires. Ainsi, la police aurait le temps de courir dans tous les sens, de s'adresser à un juge, après être passée par toute la chaîne de commandement afin d'être en mesure d'obtenir l'autorisation de s'adresser à un juge, seulement pour obtenir des renseignements sur des Canadiens au hasard. C'est ce qui me préoccupe.

Le président: Veuillez donner une réponse assez courte.

M. James L. Turk: Je ne suis pas en train de formuler un commentaire ni d'essayer d'attaquer la police. Nous établissons nos lois, et nous établissons nos normes en fonction de ce qui, selon nous, est approprié. Nous n'attribuons pas de motivation. Le juge doit respecter ces normes, et nous disons qu'une norme assez élevée devrait être respectée avant que ce genre de renseignements puissent être communiqués.

Le président: D'accord. Je vous remercie de cette précision. Votre temps est écoulé.

Il nous reste environ deux minutes. C'est le tour du Nouveau Parti démocratique.

Par conséquent, madame Boivin, je vais vous interrompre d'ici deux minutes.

[*Français*]

Mme Françoise Boivin (Gatineau, NPD): D'accord, je vais essayer de faire ça vite. C'est dommage, parce que ce groupe de témoins est extrêmement intéressant. J'aurais aimé poser des questions à chacun d'eux.

[*Traduction*]

Nous avons parlé de la notification. Je pense qu'il est important de supprimer certains des sous-entendus que je crois avoir entendus du côté du gouvernement. Personne ne demande que la police ou le fournisseur avise la personne qui fait l'objet d'une enquête à ce moment-là.

Ai-je raison de penser que cela s'applique davantage à

[*Français*]

l'écoute électronique, par exemple? Serait-ce dans ce genre de cas qu'on demanderait que des rapports soient faits, que les gens soient informés dans un délai donné, à la suite des enquêtes, et ainsi de suite? Est-ce bien de ça qu'il est question quand on parle de notification?

[*Traduction*]

M. Michael Geist: Le problème que, selon moi, beaucoup de gens ont soulevé est à la fois lié au contexte du projet de loi et à celui de la révélation selon laquelle plus d'un million de demandes sont présentées relativement à ces renseignements. Ainsi, même si M. Turk a demandé si les gens faisaient du hameçonnage et des choses du genre, je n'accuse personne de hameçonnage, mais je sais qu'il y a des demandes de communication concernant 750 000 comptes d'utilisateurs chaque année. Cela fait beaucoup de renseignements sur les gens qui sont communiqués.

Mme Françoise Boivin: Et ce n'est pas déraisonnable...

M. Michael Geist: ... et tous les fournisseurs, chacun d'entre eux, ont dit qu'ils n'avaient pas avisé le client visé par ces divulgations.

Mme Françoise Boivin: Et il ne serait pas déraisonnable d'aviser ces personnes en disant: « Écoutez, vos renseignements ont été communiqués ». C'est une question que je voulais poser.

L'autre que nous n'avons pas eu le temps d'aborder avec vous et qui, selon moi, est importante, c'est la

[*Français*]

définition des termes « agent de la paix » et « fonctionnaire public ». On donne la définition de « fonctionnaire public » juste un peu en haut de l'article 487.012 proposé. Quant au terme « agent de la paix », il est défini à l'article 2 du Code criminel, or le fait que ce soit une très longue définition m'inquiète un peu.

Croyez-vous qu'on devrait circonscrire la définition qui détermine qui a le pouvoir de faire ce qui est indiqué dans ces dispositions?

[*Traduction*]

Le président: Monsieur Geist, ce que je vous propose, c'est de donner votre réponse par l'entremise du greffier en ce qui a trait à cette question particulière concernant la définition du terme « agent de la paix ». Merci beaucoup.

Je veux remercier nos intervenants de leur présence.

Je tiens à vous dire qu'il nous reste une semaine, mardi et jeudi prochains, à entendre des témoins sur ce sujet particulier, sur ce projet de loi. Ensuite, pour la semaine suivante, le mardi et le jeudi, on prévoit procéder à une étude article par article ainsi que de tous les amendements prévus. Si vous avez des suggestions pour nos collègues d'un côté ou de l'autre de la Chambre concernant des amendements que vous aimeriez proposer, veuillez nous les transmettre, et nous allons nous en occuper.

Merci beaucoup pour cette excellente discussion, et je m'excuse de l'interruption liée au vote.

Sur ce, la séance est levée.