CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

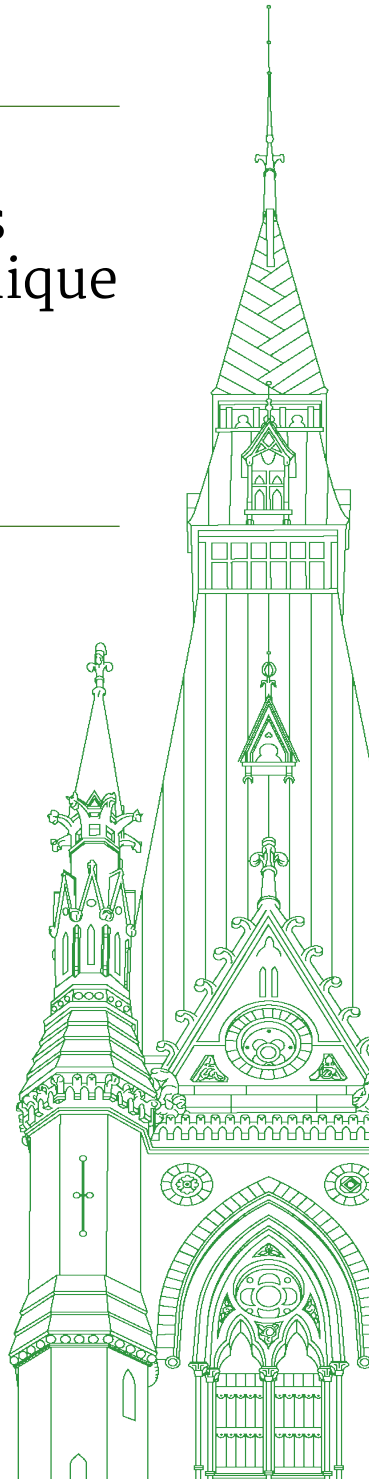
44e LÉGISLATURE, 1re SESSION

# Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

**NUMÉRO 094**

Le lundi 27 novembre 2023



Président : M. John Brassard

# Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

**Le lundi 27 novembre 2023**

● (1535)

[*Traduction*]

**Le président (M. John Brassard (Barrie—Innisfil, PCC)):** Bonjour à tous.

La séance est ouverte.

[*Français*]

Soyez les bienvenus à la 94e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

[*Traduction*]

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le mardi 31 janvier 2023, le Comité reprend son étude de l'utilisation des plateformes de médias sociaux pour la collecte de données et le partage non éthique ou illicite de renseignements personnels avec des entités étrangères.

[*Français*]

La réunion se déroule aujourd'hui sous forme hybride. Conformément au Règlement de la Chambre, les députés peuvent y participer en personne ou avec l'application Zoom.

[*Traduction*]

Je voudrais rappeler à tous les membres qu'il faut faire attention aux oreillettes pour l'interprétation. Veillez à ne pas placer votre oreillette à proximité du microphone, car cela peut entraîner une boucle de rétroaction susceptible de provoquer un choc acoustique qui pourrait à son tour blesser les interprètes.

Nous accueillons un témoin sur Zoom dans la première heure. Je rappelle aux membres que les tests ont été effectués avec lui et qu'il utilise le casque d'écoute approprié.

J'aimerais maintenant accueillir notre premier témoin, qui comparaît à titre personnel. Il s'agit de M. Anatoliy Gruzd, professeur et titulaire de la Chaire de recherche du Canada sur les technologies numériques de protection des renseignements personnels à la Toronto Metropolitan University.

Monsieur Gruzd, vous disposez de cinq minutes pour votre déclaration préliminaire.

Bienvenue, monsieur. Allezy, je vous en prie.

**M. Anatoliy Gruzd (professeur et titulaire de la Chaire de recherche du Canada sur les technologies numériques de protection des renseignements personnels, Toronto Metropolitan University, à titre personnel):** Monsieur le président, mesdames et messieurs, je vous remercie pour cette occasion de discuter de la menace d'ingérence étrangère et des risques associés à l'utilisation abusive des données provenant des médias sociaux.

Je suis Anatoliy Gruzd, titulaire d'une chaire de recherche du Canada et professeur à la Toronto Metropolitan University. Je suis également codirecteur du laboratoire des médias sociaux, où j'étudie l'effet des médias sociaux sur la société, la protection des renseignements personnels et la propagation de la mésinformation concernant des conflits comme la guerre entre la Russie et l'Ukraine.

Mes observations d'aujourd'hui sont les miennes, mais elles sont fondées sur les recherches menées au laboratoire des médias sociaux et s'appuient sur 15 années de travaux avec différents types de données issues des médias sociaux.

Comme l'ont dit les témoins précédents, on craint que TikTok ne soit vulnérable à l'ingérence étrangère, ce qui aurait de graves conséquences pour notre sécurité nationale et notre vie privée. Toutefois, je voudrais souligner qu'une arme chargée n'est pas une arme fumante. Bien qu'on présente l'application TikTok comme une menace pour la sécurité nationale, il n'existe à ce jour aucune preuve publique que le gouvernement chinois ait espionné des Canadiens en empruntant un accès dérobé, ou un accès privilégié, à l'application.

Cela ne veut pas dire qu'il n'y a pas lieu de s'inquiéter. Le risque que TikTok et d'autres plateformes soient exploitées par des acteurs malveillants à des fins de propagande et de radicalisation suscite des inquiétudes légitimes. Par exemple, la « Lettre à l'Amérique » d'Oussama ben Laden datant de 2002 a récemment refait surface sur TikTok et a été consultée par des millions de personnes. Toutefois, ces préoccupations ne se limitent pas à une seule plateforme. Elles représentent plutôt des défis plus vastes pour l'intégrité et la sécurité de notre environnement d'information.

Cela étant, nous devons adopter une approche globale pour résoudre ces problèmes en obligeant les plateformes à s'engager à adopter les principes de la protection de la vie privée dès la conception et par défaut; à investir dans l'élargissement de leurs équipes chargées de la confiance et de la sécurité; et à communiquer leurs données aux chercheurs et aux journalistes.

Je vais m'étendre sur chacun de ces points.

Il est important d'enseigner la culture numérique, mais il est injuste de faire peser toutes les responsabilités sur les utilisateurs. Les plateformes de médias sociaux sont complexes et les algorithmes qui décident de ce que les utilisateurs voient ou ne voient pas restent opaques. Le seul véritable choix qui s'offre à nous est de nous déconnecter des médias sociaux, mais ce n'est ni réaliste ni pratique, comme nos propres recherches l'ont montré, car la plupart des Canadiens ont au moins un compte de média social.

Il est important de changer de cible, de passer de la responsabilité individuelle à l'élaboration de stratégies qui obligent les entreprises à protéger les renseignements personnels dès la conception et par défaut. À l'heure actuelle, il n'est que trop fréquent que les plateformes collectent par défaut plus de données que nécessaire.

Cependant, même si les paramètres de protection des renseignements personnels sont activés, les Canadiens peuvent encore être vulnérables face à des acteurs malveillants et étatiques. Selon une enquête nationale publiée l'an dernier par notre laboratoire, la moitié des Canadiens ont déclaré avoir été confrontés à des récits pro-Kremlin sur les médias sociaux. Cela fait ressortir les préoccupations concernant la portée de la propagande et de la désinformation étrangères au Canada, qui ne se limite pas à une seule plateforme.

Voici un autre exemple: au début de l'année, Meta a fait état d'une opération d'influence sophistiquée menée par la Chine sur plusieurs plateformes, dont Facebook, Twitter, Telegram et YouTube. Leurs auteurs ont tenté d'usurper l'identité d'entreprises, de personnalités et d'institutions de l'Union européenne et des États-Unis en publiant des contenus correspondant à leur identité avant de passer à des commentaires négatifs sur les activistes ouïghours et les critiques de la Chine.

Pour lutter contre la désinformation, les plateformes devraient élargir leurs équipes chargées de la confiance et de la sécurité, s'associer à des organismes de vérification des faits et donner accès à des contenus d'organes de presse crédibles. Malheureusement, certaines plateformes, comme Meta et X, font exactement le contraire.

Pour évaluer dans quelle mesure les plateformes luttent contre la désinformation, le Canada devrait créer un code de pratique sur la désinformation calquée sur le code européen ainsi qu'un référentiel de transparence qui obligerait les grandes plateformes à rendre compte régulièrement de leurs activités en matière de confiance et de sécurité au Canada.

Pour renforcer encore la transparence et la surveillance, le Canada devrait rendre obligatoire l'accès aux données pour les chercheurs et les journalistes, un accès essentiel pour détecter de manière indépendante les tendances néfastes. Dans l'Union européenne, cet accès est prévu par la nouvelle Loi sur les services numériques.

Actuellement, TikTok n'accorde pas aux chercheurs canadiens l'accès à ses données, mais elle le fait pour ceux qui résident aux États-Unis et dans l'Union européenne. Malheureusement, TikTok n'est pas seule dans ce cas. Récemment, X a fermé son accès gratuit aux données pour les chercheurs.

En résumé, s'il est important de reconnaître l'impact de l'ingérence étrangère sur les médias sociaux, l'interdiction d'une seule application peut se révéler inefficace. Elle pourrait aussi miner la confiance dans le gouvernement, légitimer la censure et créer un environnement propice à la mésinformation.

Une approche plus nuancée devrait prendre en compte les différentes formes d'information et élaborer des stratégies pour les traiter directement, que ce soit sur TikTok ou d'autres plateformes. Il pourrait s'agir d'adopter plus largement le principe de protection des renseignements personnels dès la conception et par défaut, d'élargir les équipes chargées de la confiance et de la sécurité au Canada et d'obliger les plateformes à fournir leurs données aux chercheurs et aux journalistes en vue d'une plus grande transparence et d'un audit indépendant.

● (1540)

Je vous remercie de votre attention.

**Le président:** Merci, monsieur Gruzd.

Nous allons commencer notre série de questions de six minutes en cédant la parole à M. Kurek.

Allez-y, monsieur. Vous disposez de six minutes.

**M. Damien Kurek (Battle River—Crowfoot, PCC):** Merci beaucoup, monsieur le président.

Monsieur Gruzd, merci de vous joindre à nous et de nous faire part de vos réflexions. Je voudrais simplement mentionner qu'étant donné la structure de nos réunions, nous disposons de peu de temps, alors n'hésitez pas, surtout en ce qui concerne vos recommandations, à faire un suivi auprès du Comité si vous souhaitez recommander des mesures précises dans votre champ de compétences.

Vous avez parlé de TikTok et de l'arme chargée par rapport à l'arme fumante. Je suis curieux de savoir si vos recherches ont porté sur tout ce qui entoure WeChat. Je sais que des rapports font état d'un lien très étroit entre la structure de propriété de WeChat et l'État communiste à Pékin. Vos recherches ont-elles porté sur cette question?

**M. Anatoliy Gruzd:** Malheureusement, comme beaucoup d'autres applications de messagerie, WeChat est invisible pour la plupart des chercheurs. Il y a de bonnes raisons à cela: il s'agit généralement de conversations privées. Les chercheurs en médias sociaux s'intéressent au discours public sur les plateformes de médias sociaux publiques. Les plateformes disposent de moyens de fournir plus d'éléments probants et de données aux chercheurs pour les groupes publics qui utilisent ces plateformes. Malheureusement, nous n'avons pas cette possibilité.

Cela m'amène à l'une de mes recommandations: le Canada devrait rendre obligatoire l'accès des chercheurs indépendants à leurs données.

**M. Damien Kurek:** Je vous remercie.

Nous assistons en temps réel au conflit entre Israël et la Palestine et au ciblage d'Israéliens et de Gazaouis par le groupe terroriste Hamas, sous forme de mésinformation et de désinformation. Je me demande si vous avez eu l'occasion de suivre cette situation et si vous pouvez nous faire part de vos commentaires sur l'impact que cela pourrait avoir. Nous avons vu comment les renseignements diffusés en ligne ont contribué aux manifestations qui ont eu lieu dans les rues de notre pays.

Pourriez-vous apporter votre contribution à cette conversation par rapport aux médias sociaux et à ce que vivent plus généralement les Canadiens?

**M. Anatoliy Gruzd:** Oui. Malheureusement, les outils des médias sociaux, comme de nombreux témoins précédents l'ont souligné, ont été militarisés par divers acteurs étatiques et d'autres groupes d'intérêt. Ils sont trop accessibles au public, d'où la tentation d'orienter l'opinion publique. Dans certains cas, nous entendons parler de vastes réseaux de robots automatisés. Leur efficacité est parfois discutable, tout simplement parce qu'il est très difficile d'acquérir de la crédibilité sur les plateformes de médias sociaux. Dans certains cas, comme ceux des agences de recherche sur Internet, où nous avions effectivement des données fournies par Twitter aux chercheurs pour disséquer, enquêter et analyser rétrospectivement leur ensemble de données, nous avons remarqué comment ces comptes robots renforçaient leur crédibilité en publiant des contenus innocents sur des sites comme X, pour ensuite basculer vers des récits différents.

Cela signifie que les acteurs étatiques utilisent les plateformes de médias sociaux pour orienter nos récits et la perception que nous avons d'eux, mais ils exploitent également nos divisions et notre polarisation. Cela peut se faire ouvertement ou secrètement. Par exemple, l'an dernier, le compte Twitter de l'ambassade de la Russie à Ottawa diffusait des messages anti-LGBTQ sur sa plateforme. Ce n'était pas dissimulé. C'était explicite. Ils s'adressaient à un groupe de personnes dans ce pays susceptibles d'adhérer déjà à certaines de ces opinions.

C'est une réponse un peu longue, mais je pense que nous constatons un impact. Directement ou indirectement, un acteur étatique tente d'influer les récits et les opinions. Aussi...

● (1545)

**M. Damien Kurek:** Je vous remercie. Je déteste vous interrompre, mais notre temps est compté.

Il est intéressant que vous souleviez ce point. Comme plusieurs autres comités, nous nous sommes penchés sur l'ingérence étrangère dans les élections. L'utilisation des médias sociaux en a été un élément clé. Il est certain que si vous avez d'autres observations, je vous invite à nous les faire parvenir.

Je tiens à aborder une zone d'ombre. Des représentants de TikTok ont comparu devant nous et ils ont dit: « Oh, la protection des renseignements personnels, c'est fantastique ». Ils n'ont besoin de rien d'autre que de renseignements de base, et leurs paramètres sont configurés pour les enfants. Je paraphrase, évidemment, mais très peu de gens lisent l'intégralité des conditions d'utilisation. Très peu d'utilisateurs comprennent quels renseignements sont explicitement fournis. Je dirais même qu'ils sont encore moins nombreux à comprendre l'impact des renseignements qu'ils fournissent, qu'il s'agisse de photos de la façade de leur maison ou d'eux-mêmes en vacances.

Je me demande si vous pourriez nous donner des orientations, dans la minute qu'il vous reste, sur la manière d'équilibrer la liberté d'expression, les progrès réalisés dans la sphère sociale et la garantie de la protection des renseignements personnels et de la sécurité des Canadiens.

**M. Anatoliy Gruzd:** Cela revient à mon argument sur la protection des renseignements personnels non seulement dès la conception, mais par défaut. Lorsque j'ai installé l'application TikTok sur mon téléphone l'autre jour, je n'ai même pas créé de compte et elle avait déjà commencé à me suivre et à m'envoyer 102 demandes d'information, comme la durée de vie de ma pile, l'identifiant de mon appareil, etc. Je n'ai même pas de compte, alors pourquoi ont-ils besoin de ces renseignements?

Une façon d'y remédier est d'opter pour des plateformes et des places de marché qui hébergent ce type d'applications, car ce sont elles qui approuvent ce type d'applications.

Pour en revenir à votre remarque sur les conditions d'utilisation interminables, c'est un problème. Une initiative que j'aime beaucoup s'appelle « Terms of Service; Didn't Read ». Il s'agit d'une initiative communautaire qui existe depuis 10 ans environ. Elle évalue différentes conditions d'utilisation pour chaque fournisseur, y compris les plateformes de médias sociaux. La note E a été attribuée à toutes les grandes plateformes de médias sociaux, et pas seulement à TikTok. Il s'agit de la note la plus basse, A étant la note la plus élevée et E la plus basse...

**Le président:** Merci, monsieur Gruzd et monsieur Kurek.

Madame Khalid, vous disposez de six minutes. Allez-y.

**Mme Iqra Khalid (Mississauga—Erin Mills, Lib.):** Merci beaucoup, monsieur le président.

Merci, monsieur Gruzd, d'être venu. Nous sommes vraiment reconnaissants du temps que vous nous accordez.

Je vais d'abord poursuivre sur la lancée de M. Kurek.

Dans le contexte de la guerre israélo-palestinienne, nous avons vu des Canadiens, surtout des jeunes, être pris pour cible pour avoir publié leurs opinions en ligne, au point où cela se répercute sur leur emploi et leurs études. Il existe une sorte de culture de groupement en ligne, peu importe le côté qu'ils défendent, et un ciblage en ligne des personnes qui expriment leur point de vue.

Pensez-vous qu'il incombe aux entreprises de médias sociaux d'assurer la protection et de maintenir la liberté d'expression, surtout pour les jeunes en ligne?

**M. Anatoliy Gruzd:** Je prends une pause parce que cela va de pair avec le type de contenu produit par des influenceurs que les gens consomment sur ces plateformes et qui servirait de déclencheurs ou de catalyseurs à certaines expressions.

Une des préoccupations que nous avons observées au fil des ans en menant des enquêtes auprès des Canadiens est que nous sommes de plus en plus nombreux à nous tourner vers les médias sociaux pour nous renseigner sur des conflits comme la guerre en Ukraine ou la guerre en Palestine.

Que se passe-t-il s'il n'y a aucun organe de presse crédible pour fournir ce contenu? Les réactions que l'on voit assez souvent sur les plateformes de médias sociaux sont motivées par le contenu produit par l'influenceur qui fournit l'information.

Lorsque nous avons interrogé des utilisateurs de TikTok au Canada, la moitié d'entre eux ont déclaré qu'ils utilisaient la plateforme pour se renseigner sur la guerre entre la Russie et l'Ukraine. C'est inquiétant, car lorsque vous allez sur cette plateforme et que vous cherchez des sources d'information dignes de confiance, les plus populaires sont CTV, Global News et CBC, selon l'indice de confiance numérique. Elles ont 150 000 ou 160 000 abonnés. Elles ne peuvent pas rivaliser avec le contenu produit par des influenceurs.

La liberté d'expression est importante, mais il est tout aussi important de veiller à ce que lorsque nos concitoyens, les Canadiens, participent à ces plateformes, ils aient accès à des renseignements crédibles lorsqu'ils y réagissent en ligne.

● (1550)

**Mme Iqra Khalid:** Je vous remercie.

Vous avez également mentionné qu'il est injuste de confier aux utilisateurs la responsabilité de faire preuve de diligence raisonnable dans le contexte de la mésinformation, de la désinformation et des renseignements personnels qu'ils fournissent à ces plateformes de médias sociaux.

Que recommandez-vous? Parlons-nous d'un règlement officiel? Voulons-nous réglementer les plateformes de médias sociaux?

Sinon, s'agit-il d'imposer ou de retirer une partie de cette responsabilité individuelle aux utilisateurs qui doivent souvent lire des pages et des pages d'accords relatifs à la protection des renseignements personnels qu'ils peuvent ou non comprendre?

**M. Anatoliy Gruzd:** Ma remarque sur le fait de ne pas faire peser toute la responsabilité sur les utilisateurs a plusieurs sources. Tout d'abord, même si les utilisateurs savent modifier les paramètres de confidentialité, de nombreuses plateformes auront accès à leurs messages privés. Les utilisateurs se sentent protégés, mais ils ne le sont pas vraiment.

L'éducation est importante, mais il ne s'agit pas forcément de former chaque utilisateur. Il est difficile de modifier les comportements individuels, mais les plateformes peuvent intégrer des outils qui permettent aux utilisateurs de se protéger de façon plus efficace et efficiente.

Voici quelques exemples simples. Dans de nombreux navigateurs, un bouton apparaît lorsque vous passez la souris sur une image. Ce bouton vous permet de chercher des images connexes. C'est un outil simple sur lequel je suis heureux de former les utilisateurs, mais il est déjà incorporé dans la plateforme.

Nous n'avons pas parlé de l'IA générative, mais c'est la prochaine étape de cette évolution. Comment nous assurer que les outils que les différents utilisateurs peuvent utiliser pour détecter ce qui est réel et ce qui est authentique...? Cela ne fait pas partie de ces plateformes. Cela pourrait se faire au moyen d'une certification numérique ou autrement, mais ces outils devraient être incorporés dans les plateformes.

L'autre point bref concernant l'éducation est qu'il est beaucoup plus efficace d'institutionnaliser la formation.

Je vais vous donner un autre exemple. Lorsque je me préparais à participer à cette réunion, il y avait un test de Zoom et les instructions me disaient de passer en mode incognito dans ce navigateur. Fournir des instructions fait partie du processus, cela fait partie de l'institution. C'est beaucoup plus systématique et efficace.

**Mme Iqra Khalid:** Je vous remercie.

Pouvez-vous nous expliquer comment les entreprises de médias sociaux comme TikTok utilisent les renseignements qu'elles recueillent? Quel rôle l'intelligence artificielle et les algorithmes jouent-ils dans l'utilisation de ces données?

**M. Anatoliy Gruzd:** L'utilisation est très variable. Nous parlons d'entreprises privées qui font des profits; la plupart de leurs revenus proviennent de la publicité, c'est évident, et la plupart des données collectées le sont à cette fin. Comment livrent-elles des yeux aux entreprises et aux personnes qui sont prêtes à payer pour les obtenir?

En grande partie, il s'agit de connaître vos centres d'intérêt, ce que vous aimez et ce que vous n'aimez pas, de sorte que le moment venu, on vous montrera une publicité donnée qui est attrayante, et vous serez un acheteur bien disposé. Ce qui me préoccupe, c'est que ce type de données est lié à d'autres plateformes et à votre historique de navigation. L'interconnexion des données est très préoccupante.

Vous avez évoqué l'intelligence artificielle. Pouvez-vous répéter cette partie de la question?

**Mme Iqra Khalid:** Quel est le rôle de l'intelligence artificielle dans la collecte de données que les plateformes de médias sociaux utilisent, ainsi que celui des algorithmes?

Je vais développer un peu le sujet. De plus, quel est l'impact sur les droits et libertés garantis par la Charte canadienne des droits et libertés en ce qui concerne la façon dont ils peuvent se mobiliser, s'organiser ou s'exprimer en ligne?

**Le président:** Merci, madame Khalid.

Votre temps de parole est écoulé, mais je vais donner à M. Gruzd la possibilité de répondre à cette question.

Répondez très brièvement, si vous voulez bien, monsieur Gruzd.

**M. Anatoliy Gruzd:** L'apprentissage automatique dans le domaine de l'IA est très utilisé pour mettre du contenu devant des yeux. En ce qui concerne votre point, essentiellement, il est parfois inquiétant de se retrouver dans une chambre d'écho sur un sujet particulier et de ne rien voir d'autre. Si ces chambres sont remplies de mésinformation pilotée par un système de recommandations, c'est encore plus inquiétant. Je n'ai probablement pas le temps, mais je pourrai m'étendre sur ce point plus tard.

**Le président:** Merci, monsieur Gruzd.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

[*Traduction*]

Monsieur Gruzd, je tiens à m'assurer que vous avez choisi l'interprétation.

[*Français*]

Vous pouvez commencer, monsieur Villemure.

**M. René Villemure (Trois-Rivières, BQ):** Merci, monsieur le président.

Merci, monsieur Gruzd. Je suis très heureux de pouvoir avoir l'éclairage de quelqu'un qui a un curriculum vitæ aussi impressionnant que le vôtre à ce sujet.

Je vais commencer par vous poser une question très simple. Vous nous avez parlé du taux de confiance numérique.

Quel est, selon vous, le souci éthique des plateformes de médias sociaux? Est-il important ou faible?

● (1555)

[*Traduction*]

**M. Anatoliy Gruzd:** Lorsque vous dites « taux de confiance numérique », faites-vous référence à l'attribution de ce taux aux personnes, aux utilisateurs ou aux plateformes elles-mêmes?

[*Français*]

**M. René Villemure:** Je vais plutôt reformuler ma question.

Selon vous, les plateformes de médias sociaux ont-elles un souci éthique? Quelle en est la mesure? Est-ce un peu, peut-être, beaucoup? Est-ce important pour elles?

[*Traduction*]

**M. Anatoliy Gruzd:** Cela va directement dans le sens de ce que je disais à propos de l'élargissement de leurs services de confiance et de sécurité, et non de leur réduction. Il s'agit essentiellement de la section des grandes entreprises de médias sociaux qui supervise effectivement la modération du contenu, de sorte que le contenu nuisible, le contenu qui pose un problème, n'obtienne pas le public visé. Malheureusement, nous entendons dans les nouvelles que la taille de ces services diminue. Les équipes chargées de la confiance et de la sécurité sont laissées de côté, et certaines initiatives lancées il y a quelque temps sont abandonnées.

C'est inquiétant. Cela montre que ce service n'est peut-être pas si important, parce qu'il peut être facilement supprimé lorsque son besoin ne se fait plus sentir.

[*Français*]

**M. René Villemure:** Il nous semble, quand nous regardons les politiques des compagnies, qu'elles font le minimum requis, sans plus.

Quelles seront les conséquences de l'intelligence artificielle générative sur les médias sociaux? À quoi peut-on s'attendre?

[*Traduction*]

**M. Anatoliy Gruzd:** Il est évident que nous pouvons anticiper une confusion entre ce qui est authentique et ce qui ne l'est pas. Pour l'instant, nous n'en sommes pas là. En fait, dans plusieurs études dont j'ai pris connaissance, lorsqu'on demande à des participants humains s'ils reconnaissent ou non certains hypertrucages et autres artefacts créés par l'intelligence artificielle, les humains sont encore capables de les reconnaître.

Nous anticipons également que dans un avenir proche, il sera beaucoup plus difficile de faire la distinction entre un contenu généré par l'intelligence artificielle et un contenu ou une œuvre authentique. Je pense que c'est là que se situe la prochaine bataille. Nous voyons certaines plateformes explorer des options exigeant que leurs créateurs de contenu divulguent d'abord si des outils d'IA générative ont été utilisés pour produire ce contenu. C'est une mesure importante.

La mesure suivante consistera peut-être à apposer une sorte de certification ou de filigrane numérique sur le contenu, de sorte que nous sachions vraiment comment il a été créé. Il n'y a rien de mal à l'IA générative, mais si le contenu qu'elle peut créer est utilisé à des fins malveillantes, cela pose évidemment un problème.

[*Français*]

**M. René Villemure:** Croyez-vous que l'utilisation de l'intelligence artificielle générative sur les plateformes de médias sociaux contribuera à rendre plus flou le concept de vérité et, par conséquent, à rendre difficile la confiance des gens dans leurs interactions avec les plateformes en question?

[*Traduction*]

**M. Anatoliy Gruzd:** C'est tout à fait exact. Il s'agit de la confiance entre le contenu et les sujets précis, et c'est parfois suffisant pour créer de la confusion. Si vous avez un acteur étatique qui n'est peut-être pas en mesure de nous convaincre, ici au Canada, de certains discours, c'est peut-être suffisant pour créer une certaine confusion.

Dans mes recherches, je me concentre beaucoup sur la propagande du Kremlin, et cette stratégie est souvent utilisée.

[*Français*]

**M. René Villemure:** Avez-vous évalué l'impact de l'arrivée de QStar dans l'équation auprès des médias sociaux? Je comprends que ce n'en est qu'au début, mais connaissez-vous quelque chose à ce sujet, ou avez-vous des mises en garde à nous fournir à cet égard?

[*Traduction*]

**M. Anatoliy Gruzd:** Pouvez-vous m'en dire plus et essayer de me donner un peu de contexte?

[*Français*]

**M. René Villemure:** Il s'agit du plus récent projet d'OpenAI, qui est appelé QStar et qui, toujours selon OpenAI, rendrait dangereuse l'utilisation de la technologie.

[*Traduction*]

**M. Anatoliy Gruzd:** Tout emploi non réglementé de l'IA risque de donner lieu à des abus. Je pense qu'à l'heure actuelle, nous nous trouvons dans ce Far West, où de nombreuses erreurs seront commises, où les entreprises essaieront d'innover et où des acteurs malicieux utiliseront la technologie à mauvais escient.

Je suis heureux que votre comité, et d'autres comités éventuellement tentent d'examiner la question. C'est un peu le Far West en ce moment. C'est inquiétant, mais comme tout outil, il peut être utilisé à des fins éducatives comme à des fins malveillantes.

[*Français*]

**M. René Villemure:** Un marteau peut frapper un clou, mais peut également tuer, c'est sûr.

On parle beaucoup de TikTok ici aujourd'hui, mais il y a d'autres médias sociaux de pays étrangers qu'on connaît moins. On parle de ceux de la Russie, mais on parle aussi souvent des médias sociaux de l'Inde, du Pakistan et de l'Iran.

Quels sont les autres médias sociaux sur lesquels nous devrions peut-être porter un regard?

● (1600)

[*Traduction*]

**M. Anatoliy Gruzd:** Tous les deux ans, le Social Media Lab publie un rapport intitulé « The State of Social Media in Canada », dans lequel nous demandons aux Canadiens quelles plateformes ils utilisent. Il est certain que la plupart des neuf plateformes les plus utilisées sont nord-américaines et américaines, mais TikTok est la plateforme qui connaît la plus forte croissance. Environ un tiers des Canadiens l'utilisent.

Telegram est une autre plateforme qui n'a pas encore atteint un taux d'adoption de 10 % au Canada. Elle est adoptée assez largement dans le monde entier. En fait, en ce qui concerne le taux d'évaluation du service dont j'ai parlé, il est intéressant de constater qu'elle obtient un B, ce qui est assez élevé par rapport à E pour toutes les autres plateformes. Bien qu'elle protège les renseignements personnels ou qu'elle se soucie de ses utilisateurs, elle est remplie de discours de propagande du Kremlin, donc vous choisissez votre poison, malheureusement.

Je tiendrais certainement à l'œil Telegram et beaucoup d'autres applications de messagerie.

On m'a posé une question tout à l'heure sur WeChat et d'autres applications. Il est vraiment difficile de les étudier. Tout ce que votre comité peut faire pour aider à obliger les plateformes à fournir des renseignements sur elles-mêmes et leurs groupes publics, d'où provient ou d'où se propage la plus grande partie de ce genre de discours, ce serait très utile à l'avenir.

**Le président:** Merci, monsieur Gruzd.

[*Français*]

Merci, monsieur Villemure.

[*Traduction*]

Monsieur Green, vous disposez de six minutes. Allez-y.

**M. Matthew Green (Hamilton-Centre, NPD):** Merci beaucoup.

Je crois que dans votre déclaration préliminaire, vous avez parlé de l'efficacité ou de la justification de cibler une seule plateforme. Je pense que vous venez de régler une partie de la question en répondant aux observations de M. Villemure en disant qu'il faut les voir comme des outils. Je vous ai entendu dire à plusieurs reprises que la propagande du Kremlin est présente.

Je tiens à être clair. Dans toutes les régions — est, ouest, nord, sud — n'êtes-vous pas d'accord pour dire que tous les pays, y compris ceux d'Europe occidentale, utilisent la propagande, qu'il s'agisse d'acteurs étatiques ou d'intérêts privés, et qu'ils utilisent ces plateformes à des fins malveillantes?

**M. Anatoliy Gruzd:** En fait, nous constatons que c'est généralisé. Le cas que j'ai mentionné et que Meta a découvert était une opération d'information assez sophistiquée menée par l'intermédiaire de plusieurs plateformes, et non d'une seule. En fait, ce contenu incluait un élément de création de faux sites Web, et bien sûr, avec l'IA générative, il est assez facile d'en créer. Essentiellement, vous créez un faux contenu qui ressemble à un organe de presse et vous utilisez ensuite les médias sociaux pour attirer l'attention sur ce contenu, ou vous utilisez des publicités ciblées pour attirer l'attention.

Je pense que les acteurs étatiques utiliseront tous les outils disponibles, et toutes les plateformes de médias sociaux populaires au Canada seraient ciblées.

**M. Matthew Green:** Bien sûr, vous affirmeriez, et la logique voudrait que cette étude porte sur toutes les plateformes dans toutes les régions, y compris tous les acteurs, qu'ils soient considérés comme favorables à l'Occident ou comme des régimes plus autoritaires du monde entier. Pouvons-nous supposer sans risque de nous tromper que vous seriez favorable à un examen général de toutes les plateformes?

**M. Anatoliy Gruzd:** Je suis d'accord pour dire que nous devons examiner cette question de manière globale, en ne ciblant pas qu'une seule plateforme, à moins que vos futurs témoins fournissent des précisions sans équivoque ou des preuves justifiant le caractère particulier d'une plateforme donnée.

**M. Matthew Green:** Je vais vous poser la question.

Croyez-vous qu'il est judicieux de consacrer tout notre temps et toute notre attention à une seule plateforme parce qu'il se trouve qu'elle émane d'une certaine partie du monde, ou cette démarche nous fait-elle rater la cible pour ce qui est de comprendre parfaitement les risques d'ingérence, de profilage et d'orientation algorithmiques?

**M. Anatoliy Gruzd:** Je pense qu'en mettant l'accent sur une seule plateforme, on peut donner l'impression que les autres plateformes sont sûres alors qu'en fait, elles se livrent à des pratiques similaires de collecte et d'utilisation abusive de données, ou des acteurs étatiques peuvent les utiliser. Il est certain qu'élargir le champ de notre examen et nous pencher sur les stratégies utilisées pour exploiter l'information serait une approche beaucoup plus efficace, à moins que...

**M. Matthew Green:** Nous avons beaucoup parlé ici du capitalisme des données, du capitalisme de la surveillance et du capitalisme algorithmique. Je voudrais revenir sur ces sociétés privées, occidentales, américaines: Meta, Instagram et Twitter, évidemment, avec Elon Musk et X. N'est-il pas vrai que des sociétés privées collectent un grand nombre de nos profils d'information — à savoir les données sur nos clics, notre géolocalisation, nos tendances, nos préférences — puis les vendent à des tiers comme s'il s'agissait d'un produit, ce qu'ils sont effectivement, c'est-à-dire la marchandisation de l'utilisateur et non de la plateforme elle-même? Est-ce exact?

**M. Anatoliy Gruzd:** C'est ce qui se passe, et certaines mesures sont parfois contre-intuitives ou contre-productives, même le simple exemple d'aller sur un site Web qui vous demande si vous acceptez les témoins. Eh bien, quel est mon choix si je veux visiter ce site Web? Il y a aussi l'exemple que j'ai cité plus tôt concernant l'installation de l'application TikTok sans avoir un compte; quelqu'un essaie de traquer... Je pense qu'il s'agit d'une pratique omniprésente dans tous les domaines et dans toute l'industrie.

● (1605)

**M. Matthew Green:** Je voudrais revenir sur ce point pour être clair, cependant.

Quelle que soit l'origine de ces sociétés, lorsqu'elles vendent à des tiers, il y a toujours une probabilité, voire une forte probabilité, que les mêmes renseignements sensibles collectés par TikTok par l'entremise de ByteDance et de sociétés d'État chinoises puissent finir entre les mains de régimes oppressifs qui souhaitent obtenir des renseignements sur leurs citoyens, se renseigner sur la diaspora, les dissidents, les personnes qui ne partagent peut-être pas les opinions de ces régimes autoritaires. N'est-ce pas exact, qu'il s'agisse d'Instagram, de Facebook ou de X?

**M. Anatoliy Gruzd:** Ce n'est pas un secret. De nombreuses sociétés de collecte de données communiqueraient ce type de renseignements. Il y a aussi tout le Web clandestin qui recueille et échange des renseignements qui ont été divulgués ou piratés au moyen de différents référentiels. Malheureusement, c'est le monde dans lequel nous vivons. Nous devons en tenir compte.

**M. Matthew Green:** N'est-il pas vrai que ces autres acteurs, ces autres plateformes, ont aussi fourni un accès dérobé à des messages et à des renseignements, que ce soit par un accès quasi légal ou un accès dans la zone grise, en ce qui concerne l'absence de mandat et ce genre de choses?

**M. Anatoliy Gruzd:** Oui, comme je l'ai dit dans ma déclaration préliminaire, je pense qu'il est important de reconnaître les différents types d'ingérence. On peut imaginer une plateforme à laquelle un acteur étatique a un accès direct — comme VKontakte, qui fonctionnait à partir de la Russie et qui a été, en fait, interdite en Ukraine en raison de cette menace parce qu'il a été établi qu'elle était en fait gérée par l'État — par rapport au risque associé aux pratiques générales d'utilisation abusive de données, que ce soit par des plateformes ou par des tiers. Je sais que, dans le passé, vous et d'autres comités avez fait référence à Cambridge Analytica. Il arrive qu'un tiers accède aux plateformes et aux données par des moyens légaux, par exemple en passant par des applications de leurs développeurs. C'est une autre forme d'ingérence.

**Le président:** Merci, messieurs Gruzd et Green.

Monsieur Gruzd, avant que nous cédions la parole à M. Gourde pour la deuxième série de questions... Vous avez dit tout à l'heure que des acteurs étatiques utilisaient les médias sociaux aux fins de polarisation. J'aimerais que vous précisiez comment ils s'y prennent. Quelles méthodes utiliseraient-ils? Utiliseraient-ils les données pour cibler des individus ou des groupes favorables à une cause, par exemple? Comment cela se produirait-il?

**M. Anatoliy Gruzd:** En général, il ne s'agit pas de cibler une personne comme moi ou un collègue. Les acteurs étatiques visent en fait les groupes sympathisants. Ainsi, ils s'intéressent aux opinions politiques partisanes qui peuvent cadrer avec leurs objectifs. Par exemple, lorsque nous parlons de contenu pro-Kremlin, cela trouve généralement un écho très favorable chez les groupes conservateurs d'extrême droite, en particulier aux États-Unis. C'est le cas de Tucker Carlson, un ancien de *Fox News*. Il rediffusait des affirmations pro-Kremlin, car certaines d'entre elles sont en phase avec l'idéologie d'extrême droite.

J'ai mentionné plus tôt que des acteurs étatiques sont en mesure de créer des réseaux de robots, et ils l'ont fait, mais ces comptes n'ont pas de crédibilité. Ils n'auront probablement pas d'impact sur les utilisateurs ou les groupes. L'objectif d'une telle campagne est de toucher quelqu'un qui détient un pouvoir — soit un influenceur sur TikTok, soit un politicien qui brigue un poste — et utilise un microphone pour diffuser utilement les mêmes discours et ainsi de suite.

**Le président:** Merci, monsieur Gruzd.

[*Français*]

Monsieur Gourde, vous avez la parole pour cinq minutes.

**M. Jacques Gourde (Lévis—Lotbinière, PCC):** Merci, monsieur le président.

Je vais revenir à l'intelligence artificielle. C'est un outil très performant qui est utilisé dans les applications pour accélérer le transfert d'information, et pour nous étudier et établir notre profil, malheureusement.

Cet outil pourrait-il, à court terme, devenir une arme qui se retourne contre nous, les Canadiens, ou contre n'importe qui au monde qui se fait profiler à outrance? Cela pourrait-il constituer une certaine forme d'ingérence, par ricochet?

● (1610)

[*Traduction*]

**M. Anatoliy Gruzd:** La question est un peu vaste, mais je vais essayer de la situer dans son contexte.

Lorsque nous parlons explicitement d'outils d'IA générative, mon inquiétude du point de vue de la confidentialité des données serait que des Canadiens se rendent sur des sites Web comme ChatGPT. Ils étiquettent leurs renseignements privés et personnels dans la fenêtre sans se rendre compte qu'ils consentent à ce que ces données soient utilisées pour l'entraînement futur de l'application. Ils ne savent pas si ce contenu sera imprimé ou recraché dans le flux d'une autre personne. Je pense qu'il y a lieu de s'en inquiéter.

L'autre inquiétude, bien sûr, concerne les plateformes de médias sociaux qui s'appuient sur des outils d'IA pour détecter les contenus préjudiciables, simplement en raison de l'ampleur du problème. Au début de l'année, j'ai consulté certains tableaux du rapport de transparence de Meta, montrant qu'on supprimait automatiquement environ 65 % des contenus classés comme du harcèlement et de l'intimidation. Il reste un pourcentage important, environ 35 %, que les utilisateurs ont dû signaler pour que les plateformes agissent. De ce point de vue, il est important de signaler certains contenus problématiques que les modérateurs ou les vérificateurs de contenu humains ne seront pas en mesure d'examiner.

Lorsque nous nous penchons sur l'IA, je pense que nous devons différencier le type d'utilisation dont nous parlons.

[*Français*]

**M. Jacques Gourde:** Vous nous avez bien expliqué ce que l'intelligence artificielle pouvait faire en ce moment. D'après votre explication, c'est un outil de bienveillance.

Selon vous, à quoi pourrait ressembler l'intelligence artificielle sur les plateformes numériques dans trois, cinq ou dix ans?

[*Traduction*]

**M. Anatoliy Gruzd:** Il y aura davantage d'automatisation. Cependant, je me demande parfois dans quelle mesure. L'IA rédige déjà des courriels pour nous. Elle crée des sites Web pour nous. Il y aura des réactions négatives potentielles. Les gens voudront avoir des interactions authentiques.

C'est probablement une perspective plus futuriste. Je ne sais pas si vous voulez que je poursuive ma réflexion.

[*Français*]

**M. Jacques Gourde:** Nous tentons de légiférer sur les plateformes numériques ou sur l'intelligence artificielle, mais, dans l'avenir, je crois que l'intelligence artificielle sera le talon d'Achille de toutes les plateformes.

Devrions-nous légiférer là-dessus, plutôt que sur les plateformes?

[*Traduction*]

**M. Anatoliy Gruzd:** Le premier élément, bien sûr, consiste à savoir si des données canadiennes sont utilisées pour entraîner des applications d'IA générative, point à la ligne. Ce sera la priorité. Ensuite, lorsque les Canadiens voient du contenu sur des plateformes de médias sociaux ou d'autres actualités en ligne, ils doivent être en mesure de déterminer si le contenu a été créé par l'IA ou non. Ce sont les deux points sur lesquels je me concentrerais en premier lieu.

[*Français*]

**M. Jacques Gourde:** Selon vous, comment pourrions-nous nous y prendre pour trouver la façon la plus efficace d'obtenir des outils qui permettraient de légiférer ou de limiter les excès à l'échelle internationale?

[*Traduction*]

**M. Anatoliy Gruzd:** Certains outils de la législation sur la protection des renseignements personnels que vous envisagez pourraient être efficaces pour permettre aux Canadiens de demander que leurs données soient retirées de certains de ces services. Cette mesure pourrait être très efficace.

Les autres aspects que j'ai évoqués, dans ma déclaration préliminaire... Il s'agit de créer un référentiel et un code de conduite pour ces renseignements, en particulier. À l'heure actuelle, on le fait déjà et ça fonctionne. Les principales plateformes en ligne dans l'Union européenne — définies comme des plateformes comptant plus de 45 millions d'utilisateurs — rendent compte, généralement tous les six mois environ, de leurs activités et de ce qu'elles ont fait pour mettre fin à l'ingérence étrangère, pays par pays. Nous ne disposons d'aucune statistique à ce sujet au Canada.

En ce qui concerne votre question sur l'IA, lorsque les plateformes prennent des mesures à l'égard d'un contenu créé par l'IA, j'aimerais savoir quelle part de ce contenu... Quelle en était la finalité?

Je pense que cela orientera nos prochaines mesures.

**Le président:** Merci, monsieur Gruzd.

[*Français*]

Merci, monsieur Gourde.

[*Traduction*]

Monsieur Kelloway, vous disposez de cinq minutes. Allez-y.

**M. Mike Kelloway (Cape Breton—Canso, Lib.):** Merci, monsieur le président.

Monsieur Gruzd, c'est un plaisir de vous voir.

Les intervenants ont tous posé d'excellentes questions.

Je vais aborder la prochaine série de questions sous deux angles.

Premièrement, que peuvent faire les Canadiens moyens pour se protéger de la désinformation et de la mésinformation? Et d'un.

Cependant, vous avez aussi évoqué, à plusieurs reprises, ce que des communautés font par rapport aux conditions d'utilisation — une initiative. J'aimerais que vous nous fournissiez plus de détails à ce sujet, ainsi que sur le code d'éthique de l'Union européenne.

Y a-t-il trois mesures que le gouvernement du Canada peut prendre pour convaincre TikTok et d'autres plateformes de médias sociaux de s'asseoir à la table afin de réduire la mésinformation et la désinformation d'un point de vue économique, à l'échelle nationale et internationale? Je pense que le député Green l'a souligné. Il l'a fait très habilement à plusieurs reprises.

C'est la série de questions que j'ai à poser, et je pourrai les préciser au fil de votre réponse.

● (1615)

**M. Anatoliy Gruzd:** Nous avons l'éducation individuelle et les mesures que chaque Canadien peut prendre. Il faut savoir de quel groupe d'âge nous parlons. J'ai entendu plus tôt que votre comité s'intéresse surtout à la population mineure, un groupe très important et vulnérable. Cependant, nous oublions parfois les personnes âgées et d'autres groupes d'âge.

Franchement, l'éducation devrait être continuelle, mais nous ne pouvons pas préparer les gens à toutes les éventualités. C'est pourquoi j'ai mentionné plus tôt que les plateformes devraient être tenues d'incorporer des outils qui peuvent signaler les problèmes potentiels. Nous en avons eu un excellent exemple lors de la pandémie de la COVID, lorsque les plateformes se sont mobilisées et ont fait des interventions utiles, même des choses simples, comme l'ajout d'un lien vers Santé Canada lorsque quelqu'un parlait de la COVID, ou le signalement qu'une partie du contenu de l'article peut ne pas refléter fidèlement les connaissances scientifiques. Ces interventions sont effectivement utiles pour réduire la propagation de la mésinformation et de la désinformation. Malheureusement, ces derniers temps, nous constatons que ces initiatives ont été complètement abandonnées. Les enseignements tirés de ces initiatives ne sont pas applicables à d'autres domaines.

Si nous parlons explicitement des jeunes adultes ou des adolescents, nous ne pouvons pas nous contenter de penser au traditionnel... Nous pouvons enseigner ces compétences. Il faut aussi envisager des interventions intéressantes, comme des jeux qui montrent essentiellement... Mettez-les en situation de gérer une opération d'information. Plusieurs études intéressantes montrent l'efficacité de ces campagnes. Les participants doivent s'obliger à mener une telle campagne, et dans une telle situation, ils deviennent plus conscients de tout ce qui peut leur arriver dans leurs interactions de la vie réelle.

Pouvez-vous répéter les autres éléments de la question?

**M. Mike Kelloway:** Bien sûr. Je vous ai lancé quelques questions en rafale, je serais donc heureux de répéter les suivantes.

Dans l'une de vos réponses à une question posée par l'un des députés ici présents, vous avez parlé des conditions d'utilisation, si j'ai bien compris, comme d'une initiative communautaire. Vous me direz si je me trompe, en ce qui concerne la lutte contre la désinformation et la mésinformation.

Par ailleurs, pouvez-vous expliquer pourquoi le code d'éthique de l'Union européenne est la référence, ou en quoi il est utile pour lutter contre la désinformation et la mésinformation?

**M. Anatoliy Gruzd:** En ce qui concerne les conditions d'utilisation, l'initiative à laquelle j'ai fait référence s'appelle *Terms of Service: Didn't Read, ToS;DR*, ou Conditions d'utilisation: non lues. Elle existe depuis 10 ans. Elle est gérée par des bénévoles. Elle est financée par des organismes à but non lucratif. Des juristes et des technologues tentent de déconstruire les conditions d'utilisation de chaque plateforme et ils ont créé une rubrique. En gros, ils simplifient les conditions d'utilisation. Vous pouvez installer une extension de navigateur. Chaque fois que vous vous rendez sur une plateforme, qu'il s'agisse d'une plateforme de média social ou d'un autre site Web, si l'extension dispose d'information à son sujet, elle affichera ses cotes, mais elle détaillera aussi les principaux problèmes dans différentes catégories. Par exemple, il peut s'agir du fait que la plateforme a accès à vos messages privés ou qu'elle ne supprime pas réellement vos données, ou d'autres préoccupations. Vous pouvez ensuite pousser plus loin votre examen et cliquer sur ces préoccupations pour en savoir plus et vous rendre à l'endroit précis où il en est question dans les conditions d'utilisation.

J'aime cette initiative parce qu'il s'agit d'un contrôle indépendant. Cela m'amène à la deuxième question que vous m'avez posée. L'initiative de l'Union européenne s'appelle le Code de bonnes pratiques contre la désinformation. Au départ, ils ont créé un centre de transparence où les grandes plateformes en ligne doivent remplir un formulaire dans lequel elles doivent rendre compte à l'Union européenne de ce qu'elles font réellement pour lutter contre la désinformation. Elles doivent être très précises.

● (1620)

**Le président:** Je vous remercie.

Nous aurons des séries de questions de deux minutes et demie.

[*Français*]

Les conservateurs auront deux minutes et demie, et les libéraux aussi. Nous allons commencer par M. Villemure, qui sera suivi de M. Green.

Monsieur Villemure, vous avez la parole.

**M. René Villemure:** Merci beaucoup, monsieur le président.

Vous savez, je ne suis pas libéral.

Monsieur Gruzd, que doit-on penser du fait que OpenAI revoit ses conditions d'utilisation en distinguant l'usage qui sera fait des données aux fins d'affaires ou aux fins de recherche?

En effet, à compter du 14 décembre, si on veut utiliser ChatGPT, toutes nos données seront susceptibles d'être utilisées par les entreprises.

[*Traduction*]

**M. Anatoliy Gruzd:** La question est délicate, car pour toute entreprise en démarrage, la recherche utilisée peut déboucher sur des utilisations commerciales. Nous ne savons pas si l'ensemble de données collectées dans le cadre de la recherche servira ensuite à d'autres projets lucratifs. Je pense que nous devons appliquer des principes similaires. Si le cadre législatif applicable est la LPRPDE, elle devrait s'appliquer de la même manière à l'utilisation des données à des fins de recherche et à des fins commerciales. La seule exception que je ferais pour la recherche, essentiellement, concerne les chercheurs et les journalistes indépendants agréés, et cela renvoie en fait à des questions antérieures sur ce que nous pouvons faire pour rendre obligatoire l'accès à ce type de données que les entreprises collectent déjà, pour qu'elles fassent l'objet d'une vérification plus indépendante.

Ces mesures sont possibles. Les plateformes vous diront que par souci de protéger les renseignements personnels ou la propriété intellectuelle, elles ne peuvent communiquer des données à des chercheurs. Je l'ai entendu très souvent, mais en réalité, il y a de nombreuses façons de communiquer ce type de données en utilisant une technologie qui préserve la vie privée, de sorte que les chercheurs puissent en rendre compte.

[*Français*]

**M. René Villemure:** Si c'était possible, j'aimerais que vous regardiez les nouvelles modalités d'utilisation de OpenAI et que vous nous disiez ce que vous en pensez par courriel, parce que c'est très inquiétant, vu d'ici.

Vous avez mentionné quelques applications plus tôt, dont Telegram et WeChat. Toutefois, parmi toutes ces applications de messagerie que nous-mêmes, députés, utilisons, quelle est la plus sécuritaire? Nous sommes tous sur WhatsApp, Telegram, entre autres.

Qu'est-ce que, nous, nous devrions faire?

[*Traduction*]

**M. Anatoliy Gruzd:** La solution la plus sûre est de se déconnecter des médias sociaux et d'Internet, mais ce n'est pas une option, comme nous l'avons vu. Sérieusement, nous devons vraiment nous demander si une application de messagerie utilise le cryptage et le type de cryptage auquel les plateformes n'ont pas accès à l'heure actuelle. Cela devrait être précisé dans toute application de messagerie. Si une application de messagerie avait accès à vos messages privés, je ne l'utiliserais pas, car cela pose un problème très grave.

**Le président:** Merci, monsieur Gruzd, c'est un sage conseil.

Monsieur Green, allez-y, pour deux minutes et demie.

**M. Matthew Green:** Merci beaucoup, monsieur le président.

Je vous remercie de votre témoignage. Je le trouve très utile.

Nous avons une occasion exceptionnelle. L'ancienne présidente du Conseil du Trésor fait partie de notre comité. Nous savons que la décision d'interdire TikTok a été prise par la dirigeante principale de l'information, qui comparaîtra devant nous. Dans des témoignages précédents, des représentants du SCRS et du Centre de la sécurité des télécommunications nous ont dit qu'ils conseillaient le dirigeant principal de l'information, ou DPI. Ils n'ont pas voulu entrer dans les détails de leurs conseils, mais ils donnent des conseils et, au bout du compte, il a été décidé, le 27 février dernier je crois, d'interdire l'utilisation de cette application sur les appareils gouvernementaux.

Monsieur, je vous donne l'occasion de répondre à la question suivante, compte tenu de votre compétence en la matière: si vous deviez conseiller la DPI à propos de cette interdiction proposée de TikTok, quels conseils lui donneriez-vous, et quels autres domaines ou sujets auriez-vous pu couvrir?

**M. Anatoliy Gruzd:** J'ai entendu ce témoignage. Je pense qu'il avait été question d'un niveau de risque inacceptable, et c'est tout ce que nous savons à ce stade. J'espère que le prochain témoin pourra vous donner un peu plus d'information.

Dans le domaine public, nous ne savons rien de plus que ce que nous venons de dire, donc...

**M. Matthew Green:** Je parle des renseignements qu'en tant qu'expert en la matière, vous fourniriez à la DPI sur les plateformes des médias sociaux et les questions relatives à la protection des renseignements personnels et à l'accès à l'information sur les appareils gouvernementaux.

Quelle information lui communiqueriez-vous, sachant ce que les plateformes peuvent faire et quelle devrait être la priorité?

**M. Anatoliy Gruzd:** Si la recommandation concerne la protection des données des utilisateurs, nous devrions traiter toutes les plateformes de médias sociaux de la même manière, qu'elles soient petites ou grandes, et nous devrions alors les vérifier de la même manière. C'est ce que je conseillerais.

En ce qui concerne l'interdiction d'une plateforme, comme je l'ai dit dans ma déclaration préliminaire, à moins qu'il n'y ait des preuves évidentes d'actes malveillants commis par des acteurs étatiques qui empruntent des accès dérobés... À défaut, en l'interdisant, nous minons nos processus démocratiques, et cela crée une perception de politisation du sujet.

Que se passera-t-il si une autre plateforme... ou de nouvelles preuves montrent qu'en fait, l'acteur étatique disposait d'un accès dérobé? Nos concitoyens auront-ils confiance dans cette nouvelle décision?

● (1625)

**M. Matthew Green:** C'est très important.

Je tiens à vous remercier d'avoir pris le temps de venir nous voir. Dans les 10 secondes qu'il me reste, j'aimerais vous inviter... Si vous voyez autre chose dans les autres témoignages ou si vous souhaitez apporter un éclairage, vous êtes toujours le bienvenu pour nous faire part d'autres observations par écrit pour que nous puissions les examiner à l'étage du rapport.

Merci beaucoup.

**Le président:** Merci, monsieur Green.

Merci, monsieur Gruzd.

Nous cédons la parole à M. Barrett pour deux minutes et demie.

**M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC):** Merci, monsieur le président.

Monsieur Gruzd, en ce qui concerne la protection des mineurs et l'utilisation des médias sociaux, que diriez-vous de l'idée que les sociétés qui exploitent les magasins d'applications, comme l'App Store d'Apple et Google Play, exigent qu'un adulte — idéalement un parent, mais un adulte — approuve tous les téléchargements pour les personnes âgées de moins de 16 ans?

**M. Anatoliy Gruzd:** Je pense que c'est un bon conseil sur le rôle parental. Dans mon travail, je me concentre davantage sur la population adulte, les 18 ans et plus, donc je ne pourrais probablement pas en parler plus en détail.

La seule chose qui me préoccupe est que l'adulte chargé de la surveillance n'est peut-être pas en mesure de déterminer si une application est malveillante ou non. Je pense que les magasins dont vous parlez ont la responsabilité de vérifier les plateformes qu'ils hébergent.

**M. Michael Barrett:** Oui. Je pense que cette double obligation concerne bien sûr l'hébergement de la plateforme de l'application par les magasins d'applications, mais aussi l'adulte responsable dans la vie d'un mineur qui doit l'approuver.

J'aime bien que vous disiez qu'il s'agit d'un bon conseil sur le rôle parental. Je pense que c'est potentiellement aussi une bonne politique publique, et c'est ce que je cherchais à savoir. Étant donné l'omniprésence de messages, surtout lorsqu'ils sont parrainés par des acteurs étatiques étrangers, des acteurs malveillants ou des prédateurs, je pense que nos enfants courent un grand risque avec la configuration actuelle et leur capacité à accéder à ces renseignements, et je vous remercie donc de vos commentaires à ce sujet.

Merci, monsieur le président.

**Le président:** Merci, monsieur Barrett.

Monsieur Gruzd, aviez-vous quelque chose à ajouter en 20 secondes?

**M. Anatoliy Gruzd:** Oui, cela concerne simplement les parents. Nous partons du principe qu'ils sont des adultes avertis, ce qui me ramène à l'idée qu'il ne faut pas trop insister sur les responsabilités individuelles. Les plateformes doivent jouer leur rôle. Les enfants peuvent avoir un deuxième appareil.

**Le président:** Nous cédons la parole à Mme Fortier pour deux minutes et demie.

[*Français*]

**L'hon. Mona Fortier (Ottawa—Vanier, Lib.):** Merci, monsieur le président.

[*Traduction*]

Je vous remercie d'être ici aujourd'hui.

M. David Lieber a comparu devant nous le 18 octobre. Il est le chef des Politiques publiques en matière de vie privée pour les Amériques. Il a dit: « Les données des Canadiens sont conservées aux États-Unis, à Singapour et en Malaisie. C'est à ces endroits que leurs serveurs sont situés ».

Est-ce que cela déclenche des signaux d'alarme chez vous? Pouvez-vous commenter cette affirmation générale?

**M. Anatoliy Gruzd:** Tout d'abord, je n'ai pas la capacité de vérifier de manière indépendante où les données sont effectivement stockées, il s'agit donc de propos tenus publiquement. Sachant à quel point les systèmes en ligne sont interconnectés, nous voudrions voir une forme d'audit de la destination réelle des données.

Nous avons parlé de l'IA, et je vais expliquer pourquoi c'est pertinent. Dans un souci d'innovation, de nombreuses plateformes de médias sociaux et d'autres services en ligne incorporeront des interfaces applicatives de programmation, c'est-à-dire l'accès à des applications d'intelligence artificielle, afin d'améliorer les recommandations. Essentiellement, il peut arriver que les données quittent les serveurs, ce qui explique qu'il soit parfois difficile d'en avoir le cœur net. Des plateformes comme TikTok et d'autres ont des partenaires, et ils s'échangent des données pour améliorer leurs services respectifs.

● (1630)

**L'hon. Mona Fortier:** Comme il me reste environ une minute, vous pouvez peut-être terminer de répondre aux autres questions qu'on vous a posées. Je sais que vous voudrez peut-être nous faire part d'autres réflexions avant la fin de notre discussion.

**M. Anatoliy Gruzd:** Je pense que nous avons bien couvert tous les sujets. Je pense qu'il s'agit simplement de souligner que lorsque nous parlons d'ingérence étrangère, elle se présente sous différentes formes.

De mon point de vue, c'est l'impact des influenceurs en ligne et des politiciens qui ont des plateformes. Ils sont souvent les plus grands diffuseurs de désinformation, mais il arrive parfois que cela corresponde aux intérêts d'autres États.

**Le président:** Merci, madame Fortier.

Monsieur Gruzd, merci beaucoup d'avoir comparu devant nous. Je sais que vous avez porté le fardeau à vous seul. Vous étiez le seul témoin. Des problèmes techniques nous ont malheureusement forcés à reporter la comparution d'un témoin, mais je vous remercie d'être venu seul aujourd'hui et d'avoir répondu aux questions du comité.

Nous allons suspendre la séance pour quelques minutes pour nous préparer à accueillir le prochain groupe.

La séance est suspendue.

● (1630)

(Pause)

● (1635)

**Le président:** Nous reprenons nos travaux. Encore une fois, bienvenue à tous.

J'aimerais maintenant accueillir nos témoins pour la deuxième partie de notre réunion.

Tout d'abord, de la Gendarmerie royale du Canada, nous accueillons le sous-commissaire Bryan Larkin, responsable des Services de police spécialisés. Bienvenue, monsieur le sous-commissaire.

Nous accueillons aussi Brigitte Gauvin, la commissaire adjointe par intérim de la Police fédérale, à la Sécurité nationale.

Nous accueillons aussi, du Secrétariat du Conseil du Trésor, Catherine Luelo, sous-ministre et dirigeante principale de l'information.

Monsieur Larkin, je comprends que vous avez une déclaration liminaire.

Madame Luelo, je veux simplement confirmer que vous n'avez pas de déclaration liminaire. Est-ce exact?

**Mme Catherine Luelo (sous-ministre et dirigeante principale de l'information du Canada, Secrétariat du Conseil du Trésor):** J'aimerais faire quelques observations, mais je serai brève.

**Le président:** C'est très bien. Je vous céderai la parole après M. Larkin.

Allez-y, monsieur. Vous disposez de cinq minutes pour vous adresser au comité.

**Sous-commissaire Bryan Larkin (sous-commissaire, Services de police spécialisés, Gendarmerie royale du Canada):** Merci beaucoup.

[*Français*]

Bonjour, monsieur le président.

[*Traduction*]

Bonjour, monsieur le président et honorables membres du Comité.

Je m'appelle Bryan Larkin. Je suis le sous-commissaire aux Services de police spécialisés. Je suis accompagné de la commissaire adjointe, Brigitte Gauvin.

D'abord, j'aimerais vous remercier de me donner l'occasion de discuter de la question. Au nombre de ses mandats, la GRC accorde la plus haute priorité à l'exploitation des données personnelles des Canadiens par des protagonistes de l'étranger et à la perpétration de crimes dans l'espace numérique.

L'ingérence étrangère touche tous les aspects de notre vie: des fondements de notre démocratie et de notre prospérité économique aux infrastructures essentielles à notre bien-être, sans oublier les valeurs et les droits fondamentaux qui nous définissent en tant que société. Cette ingérence est une menace à plusieurs niveaux. En effet, des acteurs étrangers cherchent à atteindre leurs objectifs de multiples façons, notamment par le harcèlement et l'intimidation de personnes et de communautés, avec le soutien d'un État, et ce, partout au Canada.

Ne vous y trompez pas: des gouvernements étrangers tirent parti de données recueillies sur les plateformes de médias sociaux populaires pour établir le profil de certaines personnes et mener des campagnes de mésinformation et de désinformation au Canada. Une des activités qui constituent une menace consiste à utiliser des données en ligne pour identifier et réprimer les dissidents politiques qui cherchent refuge au Canada.

Des acteurs de l'ingérence étrangère établissent également d'infâmes liens avec des organisations criminelles pour faciliter la perpétration d'activités illicites comme la fraude en ligne, le cyberespionnage, l'exploitation des enfants et le vol de propriété intellectuelle, et en tirer profit.

En gardant à l'esprit ces considérations, nous parlerons brièvement aujourd'hui du rôle de la GRC dans la protection du Canada et des Canadiens contre l'ingérence étrangère dans le cyberespace.

En tant que service de police national du Canada, la GRC a pour mandat d'enquêter sur les activités criminelles liées aux crimes graves, à la criminalité organisée et à la sécurité nationale, ce qui comprend les cas d'ingérence étrangère en ligne. Par l'entremise de son Centre national de coordination contre la cybercriminalité, la GRC collabore avec tous les organismes d'application de la loi et d'autres partenaires, y compris le Centre antifraude du Canada, en vue de réduire la menace posée par la cybercriminalité au Canada, ses répercussions et le nombre de victimes.

En 2022, parmi plus de 30 000 signalements de fraudes et d'escroqueries liées à la cybercriminalité, 35 % avaient un lien avec les plateformes de médias sociaux. Nous travaillons également en étroite collaboration avec les services de police dans tout le pays, qui sont souvent les premières entités d'application de la loi à être informées des activités cybercriminelles soutenues par un État, qui ciblent des Canadiens.

Si la GRC enquête sur les cybermenaces et ses acteurs, les Canadiens doivent reconnaître eux aussi les dangers ainsi que les conséquences d'une activité en ligne. Plus particulièrement, il est essentiel que nous comprenions tous que tout ce que nous transmettons en ligne est recueilli et stocké sur des serveurs, souvent situés à l'extérieur de nos frontières nationales, où les droits relatifs à la protection des renseignements personnels pourraient ne pas avoir la même signification qu'ici. En fait, nous laissons une empreinte numérique partout dans le pays.

Dans certains pays, les lois sur la sécurité nationale obligent les entreprises de médias sociaux à transmettre les données personnelles recueillies auprès d'utilisateurs étrangers aux gouvernements locaux. Ces données sont ensuite utilisées pour harceler, contraindre ou menacer des voix dissidentes, des dirigeants politiques et nos communautés diversifiées à l'étranger, ou pour faciliter la cybercriminalité.

Les jeunes sont particulièrement vulnérables. Ils sont vulnérables à la cybercriminalité, car ils ont tendance à faire confiance à l'environnement numérique sans en comprendre pleinement les risques qui sont associés aux plateformes numériques. Leur utilisation intensive des plateformes de médias sociaux, conjuguée à leur tendance à donner trop de renseignements personnels, en font des cibles particulièrement attrayantes pour les cybercriminels.

Nos Services nationaux à la jeunesse communiquent avec les jeunes et les sensibilisent à la question de la sécurité en ligne, en collaboration avec des policiers éducateurs et divers organismes. De plus, la GRC s'engage et continue à travailler avec nos communautés diverses et les nouveaux arrivants pour leur fournir des renseignements, y compris des conseils de sécurité sur la façon de reconnaître les appels frauduleux et les tactiques d'hameçonnage.

Le Centre national de coordination contre la cybercriminalité et le Centre antifraude collaborent aussi à la campagne « Pensez cybersécurité » lancée par le gouvernement du Canada pour sensibiliser le public. Cette initiative vise à informer tous les Canadiens, y compris les jeunes, au sujet des cybermenaces et des mesures de prévention.

La GRC produit également des bulletins opérationnels et des outils de signalement de crimes à l'intention des agents de police de première ligne, des partenaires stratégiques et du public dans le but d'accroître le nombre de signalements de crimes à l'échelle fédérale et de mobiliser les diverses communautés culturelles.

La protection du Canada et la sécurité de ses citoyens et de ses résidents sont primordiales pour la GRC, et il sera important que toutes sphères de la société travaillent ensemble pour se protéger contre l'ingérence étrangère dans cet environnement.

Je vous remercie de votre attention.

● (1640)

**Le président:** Merci, monsieur Larkin.

Madame Luelo, vous avez cinq minutes, s'il vous plaît.

**Mme Catherine Luelo:** Merci beaucoup. J'ai l'intention de ne prendre que quelques minutes. Je veux laisser le temps aux membres du Comité de poser toutes les questions qu'ils pourraient avoir sur ce sujet important.

Je vous remercie de m'accueillir virtuellement aujourd'hui.

Je pense que le sous-commissaire a très bien décrit un certain nombre de choses. Je prendrai juste une minute pour situer mon rôle.

En tant que dirigeante principale de l'information du Canada, j'ai la responsabilité de veiller à ce que nous ayons des règles et des lignes directrices explicites concernant l'utilisation des appareils du gouvernement du Canada. C'est dans cette optique que j'ai pris la décision concernant TikTok.

Lorsque nous prenons des décisions sur ce qui constitue une utilisation acceptable des appareils du gouvernement, nous tenons compte de toute une série d'éléments, notamment la protection de la vie privée, l'usage acceptable dans un environnement professionnel et le coût. Tous ces éléments entrent en ligne de compte pour décider ce que nous autorisons sur les appareils.

En dernière observation, je vous conseille de continuer à resserrer notre environnement en ce qui concerne l'utilisation des appareils du gouvernement du Canada. Nous avons un environnement assez ouvert, dans lequel environ 90 % des appareils du gouvernement du Canada autorisent le téléchargement de tout ce que l'utilisateur souhaite.

Nous avons cloisonné l'usage sur les appareils, une portion réservée à l'usage professionnel et une autre à l'usage personnel, sur un seul appareil. À ma connaissance, ce n'est pas chose habituelle dans le secteur privé, et c'est pourquoi je vous conseille à nouveau — et c'est la direction dans laquelle je fais évoluer l'organisation —, de resserrer davantage cet environnement au point que les appareils du gouvernement sont utilisés uniquement pour les affaires du gouvernement. Ce faisant, nous aurons un effet d'entraînement qui, je pense, permettra de mieux protéger la confidentialité des renseignements.

Je répondrai avec plaisir à vos questions, et vous rends la parole pour que vous disposiez d'autant de temps que possible.

Je vous remercie de votre attention.

**Le président:** Nous vous remercions, madame Luelo.

Nous allons commencer le premier tour de six minutes. J'ai M. Brock pour six minutes.

Allez-y, monsieur.

**M. Larry Brock (Brantford—Brant, PCC):** Merci, monsieur le président, et merci aux témoins d'être venus aujourd'hui.

Si le temps le permet, je reviendrai sur l'objet de cette réunion, à savoir les médias sociaux et l'ingérence étrangère, mais il y a une autre question urgente à laquelle les Canadiens veulent une réponse.

Monsieur Larkin, toutes mes questions s'adresseront à vous.

Vous conviendrez qu'il existe des principes juridiques fondamentaux dans le droit pénal, à savoir qu'ignorer la loi n'est pas une excuse et qu'aucun Canadien n'est au-dessus de la loi. Cela inclut tous les députés et le premier ministre lui-même.

Convenez-vous de cela?

● (1645)

**S.-comm. Bryan Larkin:** C'est le fondement de la démocratie et des institutions démocratiques que nous soutenons en appliquant le Code criminel du Canada et d'autres lois de compétence, telles que les lois provinciales et municipales.

**M. Larry Brock:** Je vous remercie.

Bien qu'un premier ministre en exercice n'ait jamais été accusé d'une infraction au Code criminel du Canada ou condamné pour une infraction criminelle, si le service de la GRC avait des motifs raisonnables et probables de croire que le premier ministre Minister Justin Trudeau a commis une infraction criminelle, le service porterait des accusations en conséquence, n'est-ce pas?

**L'hon. Mona Fortier:** Monsieur le président, j'invoque le Règlement. Nous avons des témoins qui ont été invités aujourd'hui pour débattre du sujet dont nous sommes saisis. Il me semble que nous devrions rester sur le sujet et ne pas nous en éloigner. Je vous serais reconnaissante, monsieur le président, de faire en sorte que nous poursuivions le sujet à l'étude.

**Le président:** M. Brock est un avocat plaidant d'expérience, et il a dit dès le départ qu'il irait là où il doit aller; je veux donc lui laisser une certaine latitude.

En règle générale, comme vous le savez, je laisse à chaque député le temps de parler de ce qu'il veut. Si cela aboutit à un certain point — et je suppose que c'est là où M. Brock veut en venir —, alors il a la parole et il peut poser toutes les questions qu'il veut.

Monsieur Brock, j'ai arrêté votre temps de parole. Je ne l'ai pas arrêté tout de suite, mais je vous donne 10 secondes d'avance, puis je relance le chronomètre.

**L'hon. Mona Fortier:** Monsieur le président, puis-je contester votre décision?

Nous parlons de la pertinence du sujet, et je crois que nous devrions...

**Le président:** Le problème avec la pertinence, madame Fortier, c'est qu'elle est plutôt subjective.

Monsieur Brock...

**L'hon. Mona Fortier:** Est-ce subjectif, lorsque nous sommes dans un comité travaillant à une étude sur les médias sociaux, que nous parlions du premier ministre? Nous devrions peut-être revenir au sujet que nous avons devant nous à l'étude.

**Le président:** Monsieur Brock, vous avez la parole. Je m'attends à ce que vous arriviez au point que vous visez.

**M. Larry Brock:** Je pense que la pertinence sera établie si je ne suis pas interrompu par les députés libéraux.

Merci, monsieur le président.

**Le président:** Bien, merci.

Allez-y, monsieur Brock.

**M. Larry Brock:** Monsieur Larkin, puis-je avoir une réponse à cette question?

Si le service a des motifs raisonnables et probables de croire que Justin Trudeau a commis une infraction criminelle, il l'inculpera en conséquence, n'est-ce pas?

**S.-comm. Bryan Larkin:** Je vous remercie de cette question.

Elle est évidemment très hypothétique. Notre mandat est d'enquêter sur des dossiers criminels, quelle qu'en soit la cible. Nous avons une section chargée des enquêtes délicates et internationales, dont le mandat est d'enquêter dans les affaires délicates et à haut risque qui menacent gravement l'intégrité politique, économique et sociale du Canada. Là encore, ce sont les enquêteurs de première ligne, en consultation avec les procureurs et d'autres responsables, qui en décident. Il serait hypothétique de parler d'un scénario précis.

**M. Larry Brock:** Avec tout le respect que je vous dois, je ne suis pas d'accord avec vous. Le mandat de chaque policier, qu'il soit de première ligne...

**L'hon. Mona Fortier:** Monsieur le président, j'invoque le Règlement, s'il vous plaît.

**Une voix:** Qu'est-ce que cela a à voir avec les médias sociaux?

**Le président:** Quel est votre rappel au Règlement?

**L'hon. Mona Fortier:** Le même que j'ai mentionné plus tôt. Il porte sur la pertinence. Malheureusement, nous ne débattons pas du sujet qui nous occupe, monsieur le président. Je conteste les faits; nous devrions vraiment nous concentrer sur cette étude aujourd'hui, ce que ne fait malheureusement pas M. Brock. La pertinence devrait être invoquée et nous devrions revenir au sujet qui nous occupe.

**Le président:** Je vais lui donner plus de temps pour établir où il veut en venir. En ce qui concerne la question de la pertinence, comme je l'ai dit plus tôt, elle est subjective. M. Brock a indiqué qu'il allait arriver aux médias sociaux, et je m'attends à ce qu'il le fasse.

Allez-y, monsieur Brock.

**M. Larry Brock:** Je vais revenir au sous-commissaire Larkin.

C'est une question hypothétique, mais je pense qu'il est facile d'y répondre, car chaque service policier dans ce pays — et vous serez d'accord avec moi — a un seuil juridique précis à partir duquel porter une accusation, allant du méfait ou vol à l'étalage, à l'homicide.

Le service a-t-il des motifs raisonnables et probables de croire qu'une infraction a été commise? Seriez-vous d'accord avec moi, monsieur, pour dire qu'il s'agit là du seuil légal pour le maintien de l'ordre dans ce pays?

**S.-comm. Bryan Larkin:** C'est le seuil de toute enquête criminelle, qui consiste à suivre les preuves pour s'assurer que l'on mène des enquêtes et des entretiens exhaustifs et que l'on examine la situation globalement. C'est le seuil auquel comparer les faits et les enjeux de l'infraction qui fait l'objet de l'enquête.

● (1650)

**M. Larry Brock:** Je vous remercie.

Je suis heureux que votre service dispose d'une unité des affaires délicates, qui fait enquête sur le premier ministre pour accusation, éventuellement, d'entrave à la justice...

**L'hon. Mona Fortier:** Une fois de plus, monsieur le président, j'invoque le Règlement au titre de la pertinence.

**Le président:** Allez-y, madame Fortier.

**L'hon. Mona Fortier:** Encore une fois, monsieur le président, il l'a dit au début. M. Brock a dit que ses paroles ne porteraient pas sur le sujet de cette étude. J'aimerais qu'on revienne à l'étude dont nous sommes saisis. Il serait souhaitable que nous nous concentrions sur... vous savez que nous essayons depuis longtemps de nous concentrer sur cette étude. Nous avons ici d'excellents invités qui peuvent répondre à de nombreuses questions. Si le député veut parler d'une autre étude, il pourra le faire à un autre moment. Mais aujourd'hui, ses questions ne sont pas pertinentes.

**Le président:** Merci, madame Fortier.

**M. Larry Brock:** Puis-je répondre?

**Le président:** Sur le rappel au Règlement, allez-y.

**M. Larry Brock:** Si Mme Fortier ou tout autre député libéral souhaite continuer à invoquer le Règlement à propos de mes questions avant même que la question ne soit posée au témoin, nous allons à l'encontre de l'objectif pour lequel nous sommes ici. J'entends que Mme Fortier souhaite aborder les questions relatives aux médias sociaux et à l'ingérence étrangère. Si elle et ses collègues continuent à m'interrompre, ils n'auront que très peu de temps pour aborder ce qu'ils estiment être des questions pertinentes.

Je suis d'accord avec vous, monsieur le président, pour dire que la pertinence est un art très subjectif. Je l'ai dit dès le départ. Si le temps le permet, je reviendrai sur l'objet de cette réunion, mais je m'oppose à cette ingérence constante des libéraux.

**Des députés:** Oh, oh!

**M. Larry Brock:** Ils rient. Oui, vous pouvez bien rire, Carolyn Bennett, mais ce n'est pas drôle pour les Canadiens.

**Le président:** Monsieur Brock, je vais vous demander de poursuivre.

**L'hon. Carolyn Bennett (Toronto—St. Paul's, Lib.):** Les Oscars ont déjà été remis cette année.

**Le président:** Vous avez dit que vous alliez traiter du sujet en question. Je vais vous demander, dans les deux minutes et 10 secondes qu'il vous reste, d'aller dans cette direction.

Je vous remercie.

**M. Larry Brock:** Monsieur Larkin, ce à quoi nous voulions en venir avant d'être interrompus, et ce pour la troisième fois, c'est au concept du seuil juridique. Bien que jamais un premier ministre n'ait été accusé au criminel, en ce qui concerne l'enquête de la GRC, qui n'est pas un secret pour les députés libéraux...

**L'hon. Mona Fortier:** J'invoque à nouveau le Règlement, monsieur le président, au sujet de la pertinence.

Vous avez dit clairement que nous allions parler de l'étude en cours. Je n'ai pas vraiment entendu, dans l'introduction, que nous allions vers cela. Avant que nos invités n'aient à répondre aux questions, il serait bon de revenir sur la pertinence de cette étude.

**Le président:** Je vous remercie, madame Fortier. Comme je l'ai dit au début, j'accorde généralement beaucoup de latitude en ce qui concerne les questions, en espérant que nous finirons par traiter de l'étude. Je suppose que c'est là que M. Brock veut en venir.

Sur le rappel au Règlement, la parole est à M. Barrett.

Il est suivi par vous, monsieur Green.

Allez-y, monsieur Barrett, pour le rappel au Règlement.

**M. Michael Barrett:** Monsieur le président, je m'attendrais à ce que si nous n'avions pas eu quatre interruptions de M. Brock en moins de quatre minutes, ou quatre minutes de temps de parole — le chronomètre a dû être arrêté plusieurs fois —, nous aurions pu arriver là où il veut aller, mais il est désavantagé lorsque, chaque fois que le chronomètre est arrêté, il doit reprendre la même question.

Si on lui donnait la possibilité de poser sa question sans avoir à la répéter, le Comité pourrait peut-être entendre l'intégralité de ce qu'il cherche à faire, mais on ne lui en donne pas la possibilité.

**Le président:** Merci, monsieur Barrett.

Monsieur Green, allez-y.

**M. Matthew Green:** Merci beaucoup, monsieur le président.

Monsieur le président, vous savez que j'ai beaucoup de respect pour vous. Je pense que vous faites du bon travail dans ce fauteuil. Je vais vous faire part de ce qui me préoccupe dans ce qui se passe actuellement.

Ce qui me préoccupe, c'est qu'en tant que personne qui a souvent recours à la procédure... je sais que mon ami M. Brock saura reconnaître cela, car nous avons passé beaucoup de temps ensemble au sein du comité DEDC. Ce qui me préoccupe, c'est que lorsqu'il y a de l'obstruction — et il y en a —, vous savez que je réfléchis souvent à l'aspect pertinence. Si ce que nous faisons maintenant crée un précédent qui permet de débattre de n'importe quel sujet à n'importe quel moment, cela nuira à mes interventions futures sur la pertinence en circonstances d'obstruction.

Je sais que M. Brock a un profond respect et une grande considération pour les règles de procédure, et je demanderais que nous revenions à l'étude en cours, afin que dans les débats futurs, lorsque j'invoquerai la pertinence, vous ne repensiez pas à aujourd'hui et ne disiez pas que tout et n'importe quoi sont de bonne guerre.

● (1655)

**Le président:** Oui. Comme vous le savez, monsieur Green, j'ai généralement essayé d'accorder une grande latitude dans les questions, quel que soit le sujet. Je crois fondamentalement que les six minutes d'un député sont ses six minutes. S'il veut parler d'arcs-en-ciel et de licornes, il peut le faire.

Monsieur Brock, je vous demande de revenir au sujet qui nous occupe, si vous le pouvez.

**M. Larry Brock:** J'en ai l'intention. Merci, monsieur le président.

**Le président:** Vous avez la parole pour 1 minute et 40 secondes. Allez-y.

**M. Larry Brock:** Encore une fois, monsieur Larkin, j'espère pouvoir poser cette question.

Mes médias sociaux sont en pleine effervescence avec des préoccupations concernant ce domaine particulier.

**Des députés:** Oh, oh!

**M. Larry Brock:** Je peux mentionner les médias sociaux un millier de fois pour satisfaire mes collègues libéraux, mais selon les médias sociaux, voici ce que les Canadiens veulent savoir: la GRC est-elle imperméable à l'idée que le premier ministre ne peut être accusé d'une infraction criminelle...

Je sais que le sujet est délicat, mais je vous ai demandé une réponse précise, et je n'en obtiens pas.

Si la GRC avait des motifs raisonnables et probables de croire que notre premier ministre, Justin Trudeau, avait été impliqué dans une infraction criminelle qui atteint votre seuil juridique — des motifs raisonnables et probables —, et que vous avez consulté les autorités juridiques appropriées — le ministère de la Justice, les procureurs de la Couronne provinciaux et territoriaux —, si celles-ci vous ont indiqué que les faits et les preuves étaient là et que votre seuil juridique était atteint, pouvez-vous dire aux Canadiens si, dans cette hypothèse, vous pourriez porter une accusation d'infraction criminelle contre le premier ministre, Justin Trudeau? Oui ou non, monsieur.

**Le président:** En 20 secondes, monsieur Larkin...

**L'hon. Mona Fortier:** J'invoque de nouveau le Règlement sur la pertinence, monsieur le président.

**Le président:** Je vous remercie. Comme je l'ai dit, la pertinence est subjective.

Monsieur Larkin, vous avez 20 secondes pour répondre à cette question si vous le souhaitez.

**S.-comm. Bryan Larkin:** Encore une fois, c'est un scénario hypothétique, mais, quel que soit le suspect, nous suivons le seuil juridique. Nous sommes fidèles à notre serment et nous suivons les preuves de toute enquête criminelle. C'est notre mandat.

Merci.

**Le président:** Merci, monsieur le sous-commissaire.

Monsieur Bains, vous avez six minutes.

**M. Parm Bains (Steveston—Richmond-Est, Lib.):** Merci, monsieur le président.

Je pense que vous savez maintenant pourquoi il est très important de faire une étude sur la mésinformation et la désinformation, tant nationales qu'étrangères.

Une grande inquiétude pour moi... Je suis père d'un enfant de 15 ans et d'un autre de 12 ans. Il s'agit donc d'un risque générationnel pour lequel nous tentons d'apaiser certaines des inquiétudes que nous avons tous.

Ma question s'adresse au sous-commissaire.

Je m'adresserai d'abord à vous, s'il vous plaît. Compte tenu de l'abondance des renseignements que les gens reçoivent, quels sont les défis communs auxquels sont confrontées les forces de l'ordre dans la lutte contre la cybercriminalité sur les plateformes de médias sociaux?

**S.-comm. Bryan Larkin:** Je pense que l'un des défis est l'amplification dans les médias sociaux des objets d'enquêtes criminelles. D'une manière générale, dans la majorité des enquêtes que nous menons actuellement, qu'il s'agisse d'un délit mineur, d'un délit contre les biens, d'un délit violent ou d'exploitation, il y a une forme d'entité numérique liée à l'enquête.

Pour nous, en tant que service de police national, et pour nos partenaires et nos services de police compétents, notre capacité a changé par rapport à ce qui était une enquête fondamentale menée dans un quartier, dans une cour d'école ou ailleurs.

Ce que nous voyons, en particulier dans ce cas, ce sont des acteurs étrangers qui utilisent et amplifient les médias sociaux pour cibler des citoyens canadiens ou des citoyens étrangers qui vivent dans notre pays. Cela représente un défi de taille. Nous ne surveillons pas les médias sociaux. Nous les utilisons évidemment comme outil ou capacité d'enquête, mais si vous regardez toutes les plateformes de médias sociaux, vous pourrez constater que l'amplification des enquêtes criminelles dans les médias sociaux a un impact sur tout ce que nous faisons, tous les jours.

**M. Parm Bains:** Vous ne surveillez pas les médias sociaux, mais vous les consultez en cas de plaintes. Y a-t-il des protocoles établis pour le partage de renseignements entre la GRC et les entreprises de médias sociaux?

Je vais prendre un exemple. Sur X, un major de l'armée indienne a déclaré: « Cela fait longtemps que » — il mentionne une victime de meurtre ici au Canada — « a été “condamné à l'enfer”. Il est temps d'en éliminer quelques autres... » C'est un major de l'armée indienne qui a fait cette déclaration sur Twitter, qui s'appelle X maintenant.

Qu'avez-vous établi avec les entreprises de médias sociaux qui autorisent ce genre de menaces?

● (1700)

**S.-comm. Bryan Larkin:** Pour être clair, nous ne surveillons pas activement les médias sociaux; toutefois, nous les utilisons dans le cadre de nos enquêtes pour des renseignements venant de sources ouvertes. Nous utilisons des logiciels qui affinent nos recherches dans le cadre de nos enquêtes criminelles ou de notre travail.

Par l'intermédiaire de notre Centre national de coordination contre la cybercriminalité, nous entretenons des relations suivies avec toutes les plateformes de médias sociaux. Nous avons mis en place des protocoles, notamment en ce qui concerne l'exploitation des enfants et les préjudices causés aux jeunes. Ce sont toutes des choses que nous faisons.

Évidemment, nous travaillons à l'interne avec le gouvernement du Canada sur la sécurité en ligne et les projets de loi à venir, et autre chose du genre. Cependant, encore une fois, la nature même de ce travail est que nous travaillons avec d'autres services policiers. Des renseignements nous sont communiqués. Nous les utilisons évidemment pour faire avancer les enquêtes. Nous suivons l'aspect de l'accès légitime, les ordonnances de production ou les mandats de perquisition pour obtenir des renseignements supplémentaires des plateformes de médias sociaux. Nous avons des ententes permanentes avec leurs services de sécurité pour recevoir et récupérer ces renseignements.

Chaque élément de média social que nous repérons et suivons ou utilisons dans le cadre de nos enquêtes constitue une preuve. Cela a également augmenté la demande au sein de notre organisation. La demande en matière de maintien de l'ordre est assez importante.

**M. Parm Bains:** D'autres témoins nous ont appris des choses. Nous avons entendu dire que Telegram était associé au Kremlin et que la Russie, pendant des générations, ciblait une génération de personnes et essayait graduellement de l'influencer et de lui laver le cerveau.

Pouvez-vous nous donner des preuves que des pays autres que la Russie tentent d'influencer les générations futures de Canadiens, à partir des renseignements que vous avez déjà fournis dans votre préambule ou dans vos exposés précédents?

**Mme Brigitte Gauvin (commissaire adjointe par intérim, Police fédérale, Sécurité nationale, Gendarmerie royale du Canada):** Je vais répondre à cette question, monsieur le président.

Le programme de sécurité nationale enquête sur les activités criminelles. Nous n'enquêtons pas sur les médias sociaux et nous ne cherchons pas à savoir s'il y a mésinformation, désinformation ou tentative d'influence. Si les activités criminelles ont trait à l'ingérence étrangère, nous enquêterons, certainement, selon notre mandat.

Dans nos enquêtes, nous pouvons obtenir des renseignements par le truchement des données sur les abonnés aux médias sociaux et d'autres renseignements que nous pouvons obtenir dans les sources ouvertes ou au moyen d'autorisations judiciaires. Dans le cas du programme de sécurité nationale, l'activité criminelle doit être liée à l'ingérence d'un acteur étranger, par exemple.

**M. Parm Bains:** Y a-t-il des agents chargés de surveiller les plateformes de médias sociaux?

**S.-comm. Bryan Larkin:** Non.

**M. Parm Bains:** Bien. Y a-t-il des agents spécialement formés pour naviguer sur les plateformes à tout moment afin de détecter des activités illégales?

**S.-comm. Bryan Larkin:** Par l'intermédiaire du président, oui, nous avons certainement des agents qui sont formés à la cybercriminalité et qui peuvent évidemment aller trouver différents renseignements, mais nous n'utilisons pas activement l'intelligence artificielle. Nous n'utilisons pas l'apprentissage machine. Nous ne faisons pas une surveillance permanente.

Je pense que je vais comparer le cybermonde à un quartier. Ce n'est pas le quartier traditionnel où nous avons une voiture de patrouille. Comme dans le cas des quartiers de notre analogie, nous enquêtons activement, mais nous ne surveillons pas réellement 24 heures sur 24, sept jours sur sept.

**Le président:** Merci, monsieur Larkin et monsieur Bains.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

**M. René Villemure:** Merci, monsieur le président.

Monsieur Larkin, je vous remercie beaucoup d'être venu nous voir aujourd'hui.

J'aime toujours vos réponses, qui sont claires. Je vais poursuivre sur ce dont vous parliez à l'instant.

Pourriez-vous nous dire de quelle façon vous voyez l'ingérence étrangère depuis l'avènement des médias sociaux?

**Mme Brigitte Gauvin:** Je vais répondre à cette question, monsieur le président.

Je vous remercie de votre question, monsieur Villemure.

Il y a certainement eu, au cours des dernières années, une augmentation de l'ingérence étrangère. Les médias sociaux servent de véhicules aux entités étrangères pour propulser leurs activités.

● (1705)

[*Traduction*]

C'est certainement une tendance que nous observons. Nous estimons qu'il y a eu une augmentation considérable les dernières années. Il est certain que les médias sociaux sont utilisés.

[*Français*]

**M. René Villemure:** Quelles sont les répercussions de la croissance de l'utilisation des médias sociaux sur la sécurité des Canadiens?

**Mme Brigitte Gauvin:** Cette ingérence est beaucoup plus difficile à détecter. Voilà pourquoi l'éducation est importante. Les gens doivent être au courant du fait qu'ils peuvent être surveillés par les entités étrangères par l'intermédiaire des médias sociaux. Par conséquent, il est important que nous, les gens s'occupant de la sécurité nationale et les membres de la GRC en général, ayons des programmes d'engagement avec le public, les entités privées et les communautés plus vulnérables pour éduquer les gens à propos des différentes façons ou des divers mécanismes utilisés par les entités étrangères pour effectuer des activités d'ingérence.

**M. René Villemure:** Habituellement, les gens ne savent pas qu'ils courent des risques, dans bien des cas.

J'aime que vous ayez amené le sujet de l'éducation. Les témoins qui sont venus ici se sont dits d'avis qu'il fallait éduquer les gens. Ce que je remarque, c'est qu'il faut demander l'éducation.

Je sais que ce n'est pas directement lié à votre rôle, mais comment peut-on éduquer la population quant à un danger qu'elle ignore?

**Mme Brigitte Gauvin:** Vous soulevez un aspect important, monsieur Villemure.

Je pense qu'il faut, malgré ce fait, continuer à éduquer les gens. On ne peut pas cesser d'éduquer les gens en s'appuyant sur cette prémisse. Il est important de poursuivre cette éducation et d'utiliser différentes façons pour le faire. C'est un problème qui affecte le gouvernement en général. Il y a de nombreuses agences, et nous devons travailler ensemble pour continuer de faire cette éducation afin de protéger la population canadienne.

**M. René Villemure:** Je ne sais pas vers qui je dirige cette question.

Constatez-vous un accroissement du danger depuis l'arrivée de l'intelligence artificielle en général ou de l'intelligence artificielle générative, qui est active depuis environ un an avec l'arrivée de ChatGPT?

L'intelligence artificielle a-t-elle un effet sur l'ingérence étrangère?

Les dangers sont-ils accrus ou différents?

**Mme Brigitte Gauvin:** La présence d'intelligence artificielle crée assurément de gros obstacles.

[*Traduction*]

Cela remet en question la façon dont nous menons nos enquêtes. Je vais vous donner un exemple. Si vous enquêtez sur une menace affichée sur les médias sociaux, ou si quelqu'un profère une menace sur une plateforme en ligne, une partie de notre enquête consiste à authentifier la vidéo. C'est un élément de preuve très important. L'intelligence artificielle rend cette tâche encore plus difficile.

[*Français*]

**M. René Villemure:** L'autorité de la GRC s'exerce sur un territoire donné. Une vidéo ou une application peuvent avoir été créées sur un autre territoire, où elle n'a aucune autorité.

Cela constitue-t-il un problème?

**Mme Brigitte Gauvin:** Nous nous penchons sur cette question. Toutefois, si on menace un Canadien, une Canadienne ou la sécurité publique canadienne ou la sécurité nationale du Canada, cela nous donne l'autorité d'agir.

**M. René Villemure:** Cela varie en fonction de l'objet de la menace, donc à qui ou à quoi elle est destinée, et non pas de son origine comme telle.

**Mme Brigitte Gauvin:** Voilà.

**M. René Villemure:** D'accord.

Qu'apporte l'intelligence artificielle à l'ingérence étrangère? Quels sont les exemples de danger accru que cela a apporté?

**Mme Brigitte Gauvin:** Je ne peux pas vous donner des exemples précis d'ingérence étrangère causée par l'intelligence artificielle, mais je peux certainement noter cette question et vous faire parvenir une réponse plus complète.

**M. René Villemure:** D'accord, j'aimerais beaucoup cela. C'est très bien.

Je reviens à l'éducation, parce que cela me fascine et me préoccupe.

Faut-il donner à l'école des cours de médias sociaux ou de savoir-vivre virtuel?

**Mme Brigitte Gauvin:** Tout à fait. Ce serait une excellente idée.

À ma connaissance, éduquer les jeunes aux dangers des réseaux sociaux fait partie du programme scolaire.

● (1710)

**M. René Villemure:** D'accord.

Quels réseaux sociaux devrait-on utiliser? On a parlé de TiKToK, mais élargissons le spectre. Nous sommes des députés, nous communiquons entre nous sur des plateformes dites sécurisées. Lesquelles devrions-nous utiliser?

**Mme Brigitte Gauvin:** C'est une bonne question, mais je ne peux pas y répondre avec précision.

**M. René Villemure:** Je reviens à vous, monsieur le sous-commissaire.

**S.-comm. Bryan Larkin:** Je crois que cette question devrait s'adresser à Mme Luelo, la dirigeante principale de l'information au Secrétariat du Conseil du Trésor du Canada.

**M. René Villemure:** J'aimerais bien avoir une brève réponse.

**Le président:** Madame Luelo, vous avez la parole.

Pourriez-vous répondre très brièvement, s'il vous plaît?

[*Traduction*]

**Mme Catherine Luelo:** Je pense qu'il est très difficile de répondre à cette question, à moins de comprendre la classification des renseignements que vous utilisez. La réponse n'est pas simple. Je pense qu'il faut s'en tenir à l'ensemble des outils autorisés que nous fournissons à nos politiciens.

**Le président:** Je vous remercie.

[*Français*]

Merci, monsieur Villemure.

[*Traduction*]

Monsieur Green, vous avez six minutes.

**M. Matthew Green:** Merci beaucoup.

Je vais poser une série de questions, madame Luelo, respectueusement.

Elles concernent votre mandat de dirigeante principale de l'information. J'ai cru comprendre — vous pouvez le confirmer aujourd'hui — selon certains bruits, que votre mandat de dirigeante principale de l'information prend fin à la fin de ce mois. Est-ce exact?

**Mme Catherine Luelo:** À la fin du mois de décembre. C'est exact.

**M. Matthew Green:** J'ai mentionné tout à l'heure que nous avions l'ancienne présidente du Conseil du Trésor. Je sais que vous êtes ici devant nous.

Je vais vous demander de faire preuve d'un peu de franchise, si vous voulez bien, sur la période pendant laquelle vous avez été dirigeante principale de l'information. À un moment ou à un autre des décisions ou des consultations sur l'interdiction de TikTok, avez-vous ressenti une pression politique?

**Mme Catherine Luelo:** Pas du tout.

**M. Matthew Green:** Comment caractériseriez-vous la période pendant laquelle vous avez été dirigeante principale de l'information? Je pense que vous y avez fait référence dans une déclaration publique, ou quelque part dans des paroles qui ont circulé au sein de la fonction publique.

Considérez-vous que la mission est accomplie? Que pensez-vous de l'état de la sécurité du renseignement au Canada et du travail que vous avez accompli en tant que dirigeante principale de l'information?

**Mme Catherine Luelo:** Je crois que le Bureau du vérificateur général vient de publier un rapport sur l'état de la modernisation des technologies de l'information. Je n'ai pas eu l'occasion de le lire. Je pense qu'il reflète bien et fidèlement l'état actuel de notre technologie. Nous n'avons fait aucun progrès au cours des 13 dernières années. Je ne pense pas que ce soit une victoire pour les Canadiens.

En ce qui concerne ma période de service, j'ai le sentiment qu'elle est ce qu'elle a toujours été censée être. J'espère que d'autres dirigeants du secteur privé feront de même. C'est une occasion incroyable. Je pense que plus nous encouragerons les partenariats public-privé...

**M. Matthew Green:** Je vais revenir à la question qui nous occupe, à savoir l'étude de TikTok et la décision de l'interdire purement et simplement. Vous avez entendu... vous avez peut-être entendu les témoins précédents, et savez donc quelles questions j'ai posées au Service canadien du renseignement de sécurité et au Centre de la sécurité des télécommunications.

Pourquoi interdire TikTok uniquement?

**Mme Catherine Luelo:** Nous avons commencé par TikTok. Depuis, vous noterez que nous avons interdit WeChat et Kaspersky Lab. L'orientation que j'ai donnée à mon équipe est de continuer à serrer la vis. Nous devons continuer à réduire le nombre d'applications différentes que nous...

**M. Matthew Green:** Je pense, pour être clair, que vous avez déclaré qu'il devrait y avoir une séparation entre l'utilisation personnelle sur les médias sociaux — et soyons honnêtes, c'est à des fins politiques qui sont souvent très partisanes, lorsqu'il s'agit de personnes élues de toute façon — et nos outils de travail.

Affirmez-vous qu'il devrait y avoir une interdiction générale de tous les médias sociaux sur les appareils gouvernementaux pour aider à prévenir toute violation de la sécurité, si l'on tient compte de toutes les atteintes à la sécurité des données qui se sont produites chez Facebook, Instagram et d'autres plateformes? Est-ce la même conclusion logique que dans le cas de TikTok?

**Mme Catherine Luelo:** Je pense que s'il y a une raison acceptable d'utiliser une plateforme de médias sociaux à des fins professionnelles... Nous communiquons avec certaines catégories de personnes au moyen des médias sociaux. Je pense à mes enfants de 21 et 24 ans. Ils utilisent les médias sociaux, nous devons donc utiliser ce mécanisme pour leur transmettre des renseignements.

En règle générale, cependant, vous avez tout à fait raison. J'aimerais que nous resserrions la vis sur l'usage des médias sociaux. Leur utilisation sur les appareils mobiles entraîne des coûts, et nous devons faire un équilibre entre la confidentialité des données, l'utilisation acceptable...

**M. Matthew Green:** Qu'est-ce que le « risque acceptable »? J'ai trouvé ce terme intéressant. Qu'est-ce qui est acceptable?

**Mme Catherine Luelo:** Pour moi, un risque est acceptable lorsque la valeur de l'action l'emporte sur le risque d'un inconvénient éventuel.

**M. Matthew Green:** Qui décide de la valeur?

**Mme Catherine Luelo:** La valeur pourrait être des choses comme, s'il s'agit du vaccin contre la COVID, par exemple, atteindre des groupes démographiques afin d'aider...

**M. Matthew Green:** En ce qui concerne le vaccin contre la COVID, alors, le ministère de la Santé pourrait être sur TikTok, distribuant ou publiant des renseignements, en utilisant ses algorithmes pour les transmettre au plus grand nombre de Canadiens possible. Est-ce que c'est acceptable?

● (1715)

**Mme Catherine Luelo:** Ce serait un exemple de risque acceptable. Il y a un certain nombre d'autres exemples de ce qui serait acceptable, et je pense que cela dépend de la situation.

**M. Matthew Green:** D'accord, c'est logique.

Je vais aller un peu plus loin. En aucun cas, pendant votre mandat — je sais que c'est gênant, puisque nous avons ici l'ancienne présidente du Conseil du Trésor —, vous n'avez ressenti de pression politique sur vos décisions, dans un sens ou dans un autre?

**Mme Catherine Luelo:** Non.

Pour être claire, l'ancienne présidente du Conseil du Trésor a été d'un grand soutien, en tout cas pendant la période où j'ai travaillé au Conseil du Trésor.

Je dirais, si je peux me le permettre, que j'aimerais que nous allions plus vite. Nous devons aller plus vite. Je pense qu'il y a des coûts, liés à toutes les strates de gouvernement passées et présentes, qui nous amènent là où nous sommes.

**M. Matthew Green:** Il y a quelque chose qui m'a un peu agacé. Je vais vous en faire part.

Je travaillais aux comptes publics et aux opérations gouvernementales, et l'une de mes premières études était un audit de l'état actuel de la technologie. Je me souviens d'avoir posé la question suivante: est-ce que nous fonctionnons encore en DOS? La technologie est-elle si vieille que cela? Dans certains cas, la réponse était oui, elle était aussi vieille même que cela.

Bien sûr, à l'époque, nous avions un gouvernement libéral qui affirmait qu'il allait inaugurer une nouvelle ère d'ouverture et de transparence. Il y avait un ministère de la gouvernance numérique, et puis, sans tambour ni trompette, il a tout simplement disparu en 2019.

Le regrettez-vous? Pensez-vous que si nous avions conservé ce mandat et cette approche pangouvernementale — pour utiliser le jargon libéral —, il y aurait peut-être eu une avancée, une intervention fiscale ou un investissement de la part de ce gouvernement pour arriver là où vous vouliez aller?

**Mme Catherine Luelo:** Je pense que je répondrais à cette question en disant que, d'après mon expérience, le numérique est la responsabilité de tout le monde. L'objectif est de fournir des programmes et des services aux Canadiens, qu'il s'agisse d'entreprises ou de particuliers, et lorsqu'on n'en fait la responsabilité que d'une seule personne, le travail ne se fait pas.

**M. Matthew Green:** Bien sûr, mais cela exclut votre poste, n'est-ce pas? Nous garderons quand même celui-ci.

**Mme Catherine Luelo:** Je pense que vous devriez garder le poste de dirigeant principal de l'information, certainement.

**M. Matthew Green:** Eh bien, vous l'avez dit. Je devais établit le lien, parce qu'il y a des gens qui aiment l'austérité et qui pourraient vous couper lors de leur prochain passage.

**Le président:** Merci, monsieur Green et madame Luelo.

Monsieur Barrett, pour le deuxième tour, vous avez cinq minutes.

Allez-y.

**M. Michael Barrett:** Madame Luelo, j'aimerais revenir rapidement, si possible, sur votre échange avec l'intervenant précédent.

Vous avez dit que le numérique était la responsabilité de tous, mais nous avons vu des exemples d'une énorme externalisation en ce qui concerne le développement de produits numériques au sein du gouvernement, au point que nous ne pouvons même pas savoir combien de sous-traitants travaillent dans le cadre d'un contrat donné. Diriez-vous que c'est une façon responsable pour le gouvernement de gérer les systèmes informatiques?

**Mme Catherine Luelo:** Je ne peux pas parler de l'approche en approvisionnement, ce n'est pas mon domaine, mais je peux vous dire que le monde dans lequel nous pourrons régler ce problème sans devoir travailler avec des entrepreneurs et des sociétés de services professionnels n'existe pas.

Nous n'avons pas la capacité, au sein du gouvernement, de résoudre le problème nous-mêmes. Ayant joué ce rôle dans un certain nombre de grandes entreprises au Canada, j'ai toujours compté sur un équilibre entre notre propre personnel et les entreprises qui sont bien équipées pour faire ce qu'il faut pour produire le numérique.

**M. Michael Barrett:** Avec tout le respect que je vous dois, je dirais qu'il y a une absence totale d'équilibre. Nous avons des entreprises comme GC Strategies, qui utilisent un nombre illimité de sous-traitants pour cacher qui fait réellement le travail, au point que le gouvernement ne le sait pas. Tout le monde pointe du doigt: « Ce n'est pas ma responsabilité. » L'approvisionnement n'est pas de votre responsabilité, et les approvisionnements disent que le numérique n'est pas de leur responsabilité. En fin de compte, les Canadiens se retrouvent avec une facture énorme, et de tous les côtés, les intéressés disent qu'ils ne sont pas responsables de leur avoir imposé cette facture.

Monsieur le président, ma prochaine question s'adresse au sous-commissaire.

La sécurité des données des Canadiens peut-elle être garantie si les données sont conservées dans des serveurs à l'étranger?

J'ai besoin d'une réponse rapide, si vous voulez bien, monsieur.

**S.-comm. Bryan Larkin:** Encore une fois, c'est une question difficile, car cela dépend des niveaux de cryptage, des serveurs réels, etc.

**M. Michael Barrett:** Il n'y a aucune certitude.

**S.-comm. Bryan Larkin:** Je ne crois pas qu'il existe un système qui puisse nous garantir quoi que ce soit. Je veux dire que nous faisons tout ce qu'il est possible de faire, mais il y a un risque.

**M. Michael Barrett:** Est-ce que Pékin utilise les médias sociaux pour cibler les dissidents au Canada?

Pouvez-vous répondre rapidement?

**Mme Brigitte Gauvin:** Monsieur le président, la Chine et d'autres acteurs étrangers utilisent divers moyens pour cibler les dissidents et mener des activités d'ingérence étrangère. L'utilisation des médias sociaux est certainement l'un de ces moyens.

● (1720)

**M. Michael Barrett:** Les soi-disant postes de police illégaux dirigés par la dictature de Pékin... L'information qu'ils utilisaient pour cibler la communauté de la diaspora au Canada provenait-elle de la collecte de données dans les médias sociaux?

**Mme Brigitte Gauvin:** Les postes de police présumés... L'enquête très active, elle est en cours. Je ne peux donc pas donner plus de détails à ce sujet, car cela pourrait compromettre l'enquête.

**M. Michael Barrett:** Veuillez répondre très rapidement: croyez-vous que c'est une bonne idée, monsieur le sous-commissaire, d'exiger que les vendeurs d'applications comme Apple App Store et Google Play obtiennent l'approbation d'un adulte responsable — un parent — avant de procéder au téléchargement d'une application dans le cas des personnes de moins de 16 ans? Pensez-vous que ce serait une bonne pratique et que cela pourrait réduire l'exploitation et l'exposition des enfants?

**S.-comm. Bryan Larkin:** Je pense que ce serait un dialogue progressiste sur le plan politique, oui.

**M. Michael Barrett:** Merci.

Je cède le temps qu'il me reste à M. Gourde.

[*Français*]

**Le président:** Vous disposez d'une minute et demie.

**M. Jacques Gourde:** Merci.

Compte tenu de l'ingérence étrangère qui a eu lieu au cours des élections de 2019 et de 2021, aurez-vous le mandat d'intervenir s'il y a des cas d'ingérence étrangère évidents ou démontrés lors de la prochaine période électorale?

**Mme Brigitte Gauvin:** Je vais répondre à cette question, monsieur le président.

La GRC n'avait pas d'enquête en cours lors des élections de 2019 et de 2021. Si, lors d'une prochaine élection, il y a des allégations d'ingérence étrangère, nous pourrons intervenir sur une base ad hoc ou sur demande.

Nous partageons ce mandat avec le Bureau du commissaire aux élections fédérales. La GRC, dans le cadre de son programme de sécurité nationale, a certainement un mandat à cet effet.

**M. Jacques Gourde:** J'aimerais parler du temps que cela vous prend pour intervenir, car une élection dure seulement 35 jours, ce qui est très court. Or, c'est souvent une question d'heures. S'il vous faut deux mois pour intervenir, ce sera trop tard. Est-il possible de le faire en deux jours?

**Mme Brigitte Gauvin:** Parlez-vous d'une enquête?

**M. Jacques Gourde:** Je parle de l'enquête pour déterminer s'il est nécessaire d'intervenir. Il faut que ce soit rapide et efficace.

**Mme Brigitte Gauvin:** En ce qui a trait à nos interventions, nous enquêtons sur toutes les allégations d'activités criminelles que nous recevons. Dès que nous les recevons, un dossier est ouvert et une équipe y est affectée.

**M. Jacques Gourde:** Que pouvez-vous faire pour intervenir? Allez-vous divulguer qu'il y a eu de l'ingérence dans telle ou telle circonscription et que tel ou tel message a été envoyé?

Il faut que ce soit su en temps réel.

**Le président:** Veuillez répondre brièvement, s'il vous plaît.

**Mme Brigitte Gauvin:** Nous disposons d'une variété de moyens pour avertir les gens. Naturellement, il y a des techniques d'enquête que nous ne pouvons pas dévoiler, puisqu'il s'agit d'information délicate, mais la communication avec la société et les personnes concernées, entre autres, est une façon de lutter contre l'ingérence étrangère.

**Le président:** Merci.

[*Traduction*]

Madame Khalid, vous avez cinq minutes.

**Mme Iqra Khalid:** Merci beaucoup, monsieur le président, et merci à nos témoins d'être avec nous aujourd'hui.

Je vais d'abord m'adresser au sous-commissaire Larkin.

Vous avez mentionné plus tôt que la majorité du travail que vous faites sur ce problème en particulier est surtout de nature investigatrice et réactive.

Croyez-vous que la GRC devrait adopter une approche plus proactive relativement à la protection de l'information, surtout pour les plateformes de médias sociaux?

**S.-comm. Bryan Larkin:** Il est très difficile pour notre organisation de réagir à l'amplification et à l'impact des médias sociaux. Une grande partie de notre travail est de nature réactive.

Grâce à notre Centre national de coordination contre la cybercriminalité, nous sommes très proactifs pour tenter de mettre en place des mesures de prévention, et de sensibiliser par l'entremise du Centre antifraude. Notre Centre national contre l'exploitation d'enfants propose une série de campagnes de sensibilisation axées sur la protection des personnes vulnérables. Cependant, une loi appuyant d'autres paramètres relativement à la protection des personnes vulnérables et la modernisation nous aiderait beaucoup. L'un des défis est que nous sommes toujours en évolution — c'est continu — pour ce qui est de l'impact des médias sociaux sur notre société.

Encore une fois, même si nous aimerions faire la transition, la réalité est que notre capacité est limitée.

**Mme Iqra Khalid:** Je vous remercie de votre réponse.

Pour revenir à une éventuelle loi, serait-il utile, à votre avis, que des bureaux comme le vôtre, la GRC et d'autres organismes d'application de la loi puissent compter sur un registre national de toutes les applications de l'intelligence artificielle ou de leur utilisation par les plateformes de médias sociaux pour savoir ce qui existe dans cet univers? Je crois que c'est peut-être la moitié du défi que représente la protection des collectivités vulnérables, si vous ne savez pas exactement quels types d'applications ou de systèmes d'intelligence artificielle sont utilisés par les plateformes de médias sociaux, par exemple.

● (1725)

**S.-comm. Bryan Larkin:** Ce sont des discussions et des dialogues progressistes sur les politiques qui devraient avoir lieu, car ils informeraient le grand public et les utilisateurs des médias sociaux. En bref, oui, je suis d'avis qu'en tant que nation, nous devons continuellement évoluer dans notre façon de gérer les médias sociaux et leurs impacts sur nos institutions, mais aussi sur notre vie quotidienne. Oui, je le répète, ce sont des discussions politiques modernes et progressistes qui devraient avoir lieu.

**Mme Iqra Khalid:** Merci beaucoup.

Je vais poser la même question à la dirigeante principale de l'information, si vous le voulez bien.

Pensez-vous qu'un registre national répertoriant toutes les applications de l'intelligence artificielle et leurs utilisations au Canada serait utile pour assurer la protection de la vie privée et la sécurité des Canadiens?

**Mme Catherine Luelo:** Je vais m'en remettre au sous-commissaire pour le volet externe, mais du point de vue interne, il est certain que les directives que nous donnons au gouvernement visent à assurer la transparence relativement à l'utilisation de l'IA et, certainement, à faire la même chose pour l'IA générative. Nous venons de publier des lignes directrices à ce sujet.

**Mme Iqra Khalid:** Merci.

Monsieur le président, pendant le temps qu'il me reste, j'aimerais proposer une motion, si cela vous convient.

Je vais la lire à voix haute:

> Que, nonobstant toute motion adoptée antérieurement par ce comité, en ce qui concerne l'étude du comité sur les médias sociaux et les entités étrangères:
>
> (a) Que le comité envoie des invitations à tous les témoins qui n'ont pas encore été invités et réinvite, au besoin, les témoins pour lesquels nous attendons toujours une réponse à comparaître;
>
> (b) Que le comité envoie une citation à comparaître aux témoins suivants dans les plus brefs délais:
>
> (i) Garrick Tiplady, VP Global Business Group et directeur national, Meta Canada;
>
> (ii) Sabrina Geremia, vice-présidente et directrice générale nationale, Google Canada;
>
> (iii) Paul Burns, directeur général, Twitter Canada;
>
> (iv) Shou Zi Chew, PDG, TikTok;
>
> (c) Que le comité consacre autant de réunions que possible pour compléter les témoignages, et que le comité n'entende aucun témoin sur des études liées à un autre sujet jusqu'à ce que le comité soit satisfait que tous les témoins en A) et B) aient témoigné, que le comité fixe une date limite du mardi 28 novembre à 12 h HNE pour soumettre de nouveaux témoins au greffier du comité,—

Et, c'est très important, monsieur le président:

> — que tous les témoins reçoivent un préavis raisonnable pour se préparer et assister aux réunions du comité.

Je crois qu'une copie de cette motion a été envoyée à la greffière.

**M. Michael Barrett:** Pouvons-nous suspendre la séance, monsieur le président?

**Le président:** Nous allons suspendre la séance pendant une minute. Je dois consulter la greffière.

● (1725)

_____(Pause)_____

● (1730)

**Le président:** La séance reprend.

Mme Khalid a proposé une motion. Tous les membres du Comité devraient l'avoir reçue. La motion est liée à l'étude en cours, et elle est donc recevable.

Avant de passer au débat — et je vois que vous levez la main, monsieur Kurek —, je vais vous libérer, madame Gauvin et monsieur Larkin. Je tiens à vous remercier d'avoir comparu aujourd'hui et de nous avoir fourni de précieux renseignements.

Madame Luelo, vous pouvez également partir.

Ce n'est pas aussi facile pour moi. Vous devez cliquer sur « annuler » ou « quitter la réunion », mais je vous remercie tous de nous avoir consacré du temps aujourd'hui. Merci.

**Mme Catherine Luelo:** Je vous remercie de m'avoir invitée.

**Le président:** Vous pouvez parler de votre motion, madame Khalid, et M. Kurek aura ensuite la parole.

**Mme Iqra Khalid:** Merci.

J'espère que les députés ont eu l'occasion de lire le texte de la motion. Je tiens à préciser que l'objectif de cette motion est que nous terminions cette étude. Nous avons commencé l'étude en octobre. Nous sommes maintenant en décembre. Nous n'avons pas vraiment respecté l'esprit de la motion adoptée au départ.

Je tiens à préciser que le point (c) ne signifie pas que l'étude se poursuivra indéfiniment. S'il faut deux ou trois réunions pour entendre les témoins que nous recevrons et rédiger un rapport efficace, c'est ce que je veux que nous fassions, monsieur le président. Je veux vraiment que cette étude progresse le plus tôt possible, afin que nous puissions préparer et déposer un rapport à la Chambre et trouver des solutions concrètes aux enjeux très importants dont nous discutons.

Encore une fois, je répète que cela ne signifie pas que je veux que cette étude se poursuive indéfiniment.

**Le président:** Merci, madame Khalid.

Pour la gouverne du Comité, je veux vous préciser que nous avons des ressources jusqu'à environ 17 h 45. Nous avons eu quelques retards. Notre greffière me l'a rappelé.

Monsieur Kurek, vous avez la parole concernant la motion.

**M. Damien Kurek:** Merci beaucoup, monsieur le président.

Je trouve cela intéressant. La lecture de cette motion montre une obstruction systématique sous un autre nom... Je n'ai jamais vu — et je suis député depuis plusieurs années et j'ai passé pas mal de temps à notre comité, et à d'autres — de motion qui dit « autant de réunions que possible pour compléter les témoignages ».

Certes, je comprends que le gouvernement n'est pas à l'aise avec certains sujets examinés par le Comité, mais je crois que c'est une motion d'une grande portée qui dit essentiellement que le travail pourrait ne jamais se terminer. Je trouve que c'est inquiétant et que nous pouvons y voir un motif caché.

Je ne veux pas minimiser l'importance du sujet à l'étude, mais je pense, monsieur le président, que nous avons déjà dit que nous ne pouvons pas marcher et mâcher de la gomme en même temps.

Si vous me le permettez... je ne veux pas céder mon temps de parole, monsieur le président, mais je sais que le Comité a consacré du temps à l'élaboration d'un plan de travail. Je crois comprendre que les deux prochaines réunions seront consacrées à cette question, alors pour ce qui est de l'information recueillie par le Comité, je crois que ce serait pertinent... et j'aurai ensuite d'autres commentaires, alors je vais certainement poursuivre là-dessus.

Toutefois, monsieur le président, j'aimerais que vous demandiez à la greffière ou aux analystes de nous communiquer les détails du plan de travail, en particulier pour ce qui est des deux prochaines réunions, et j'aurai ensuite quelques autres commentaires.

● (1735)

**Le président:** Je vous remercie de votre question, monsieur Kurek. Vous aurez encore la parole lorsque nous reviendrons.

Nous avons des témoins le 29. Nous avons travaillé pour avoir des témoins le 4 décembre. En fait, l'avis de convocation est prêt à communiquer. Il y aurait M. Caraway, qui, malheureusement, a éprouvé des problèmes techniques; Mme Emily Laidlaw, professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité de l'Université de Calgary; M. Matt Malone devrait comparaître; et nous recevrons deux représentants de The Dais: M. Sam Andrey, directeur général et M. Joe Masoodi, analyste principal des politiques.

Je vais demander à la greffière de vous parler précisément de la réunion du 4 décembre.

Avons-nous des témoins pour le 4 décembre, madame la greffière, ou attendons-nous encore des réponses?

**La greffière du Comité (Mme Nancy Vohl):** Je dois envoyer les invitations et les confirmations. Par ailleurs, j'aimerais connaître les directives du Comité...

**Le président:** D'accord. Bien sûr, le 11 décembre, nous avons convenu dans le cadre de notre plan de travail — peut-être que nos analystes pourront nous en dire plus à ce sujet — d'inviter le commissaire de la GRC dans le cadre de la motion adoptée par le Comité concernant SNC-Lavalin.

Aimeriez-vous ajouter quelque chose?

**Mme Alexandra Savoie (attachée de recherche auprès du Comité):** Je voudrais simplement ajouter que, comme Mme Vohl vient de le dire, nous aimerions avoir des directives, que ce soit par le biais de la motion de Mme Khalid... parce que, techniquement, comme vous l'avez remarqué, certains témoins ont refusé l'invitation. Cependant, pour ce qui est du plan de travail qui a été distribué, l'information se trouve à la fin du plan de travail, et c'est pourquoi nous avons besoin de directives pour savoir qui nous devrions inviter ensuite.

**Le président:** Voilà la réponse à cette question, monsieur Kurek.

Vous avez toujours la parole. Allez-y.

**M. Damien Kurek:** Merci, monsieur le président.

Il est très révélateur, à mon avis — et le Comité étudie l'importante question des médias sociaux et de leurs répercussions sur le Canada et les jeunes Canadiens — que l'adoption de la motion dans sa forme actuelle, monsieur le président, aurait pour effet de passer outre au plan de travail dans lequel il est prévu que le commissaire de la GRC se présente pour témoigner au sujet de SNC-Lavalin. Je pense qu'il est évident qu'il y a un motif caché.

De plus, je tiens à souligner que les témoins à recevoir sont des gens de Meta-Facebook. Il y a un vice-président de Google et un directeur général de Twitter Canada. Cependant, le directeur général de TikTok serait aussi invité. Par souci de cohérence, il serait également très raisonnable d'inviter les membres de la haute direction de ces organisations à participer à cette discussion.

Cela mis à part, monsieur le président, je propose un amendement à la motion de Mme Khalid. Il s'agirait simplement de supprimer le point (c) de la motion.

**Mme Iqra Khalid:** Voulez-vous dire (c) au complet?

**M. Damien Kurek:** Oui.

**Le président:** L'amendement proposé par M. Kurek à la motion de Mme Khalid est de supprimer le point (c).

Y a-t-il des commentaires sur l'amendement? N'oubliez pas que nous avons jusqu'à 17 h 45.

Nous vous écoutons, monsieur Barrett.

**M. Michael Barrett:** Monsieur le président, je crois qu'il serait utile de connaître le nombre de témoins qui ont refusé de comparaître. Ce serait une information importante. Si vous pouviez nous fournir ce renseignement, j'aimerais ensuite parler de l'amendement.

**Le président:** Je vais revenir à la semaine dernière. Je crois que la greffière nous a transmis une liste sur la situation concernant les témoins.

Cette liste a-t-elle été transmise à tous les membres du Comité?

**La greffière:** Mme Fortier a demandé la liste, mais elle n'a pas été transmise à tout le monde.

**Le président:** C'est Mme Fortier qui l'a demandée.

**La greffière:** Je peux l'envoyer.

**Le président:** Nous pouvons certainement vous la transmettre, si vous voulez des renseignements à ce sujet maintenant. Aimeriez-vous la recevoir, monsieur Barrett, ou...?

**M. Michael Barrett:** J'aimerais beaucoup, oui, mais pour le nombre de témoins, si vous pouviez...

**Le président:** Si nous pouvons faire un calcul approximatif...

**M. Michael Barrett:** Ce serait une excellente idée.

● (1740)

**Le président:** D'accord, madame la greffière, si vous voulez bien...

**La greffière:** Vous voulez savoir, approximativement, combien de personnes ont refusé.

**Le président:** Oui. Combien de personnes ont refusé?

**La greffière:** Neuf personnes ont refusé, mais il y a des doubles car certaines personnes ont été proposées par les conservateurs et les libéraux.

**Le président:** Au total, neuf d'entre elles ont refusé. Certaines figuraient sur des listes de plusieurs partis.

Pouvez-vous préciser ce que signifie cette ligne jaune?

**La greffière:** Ce sont les personnes avec lesquelles nous n'avons pas pu communiquer.

**Le président:** D'accord, nous attendons une réponse.

D'après ce que je vois, environ cinq ou six personnes n'ont pas encore répondu. Neuf ont refusé, ont dit « non », et nous attendons une réponse d'environ cinq personnes.

**Mme Iqra Khalid:** Je veux préciser que parmi ces neuf personnes, certaines sont nommées dans ma motion.

**Le président:** La greffière vient de me rappeler que certaines d'entre elles n'ont pas été invitées parce qu'elles ne figuraient pas dans le plan de travail approuvé par le Comité.

Je rappelle également aux membres du Comité que si le commissaire de la GRC doit comparaître le 11 décembre, c'est parce qu'il s'est libéré pour comparaître à cette date. Nous avions convenu de commencer l'étude sur SNC après l'étude sur les médias sociaux, mais le commissaire de la GRC a dit qu'il était disponible le 11 décembre, et c'est pourquoi nous avons accepté qu'il témoigne ce jour-là. Évidemment, nous devons aussi tenir compte de son horaire.

Monsieur Barrett, allez-y.

**M. Michael Barrett:** Compte tenu du temps dont nous disposons, monsieur le président, j'aimerais savoir si vous avez cherché à obtenir un consensus au sujet du point (a) de la motion de Mme Khalid — simplement un consensus — et d'inviter ces personnes conformément au plan de travail qui a été approuvé par le sous-comité. Si vous avez le temps de le faire dans les trois minutes qu'il nous reste avant que nous manquions de ressources, nous pourrions ensuite nous occuper de l'amendement de M. Kurek et de la motion principale.

Je ne crois pas qu'il soit nécessaire de présenter une motion pour demander au président de simplement envoyer des invitations à toutes les personnes inscrites sur la liste des témoins. Cela peut se faire par consensus.

**Un député:** D'accord.

**Le président:** Nous allions y arriver de toute façon.

Actuellement, notre problème est que nous devons nous prononcer sur un amendement.

Si le Comité est d'accord pour que nous envoyions...

**Mme Iqra Khalid:** Non, monsieur le président.

**Le président:** Ce n'est pas le cas. D'accord, oublions cela.

**M. Michael Barrett:** D'accord.

**Le président:** Nous parlons encore de l'amendement, monsieur Barrett.

Nous vous écoutons.

**M. Michael Barrett:** Monsieur le président, que nous consacrions le plus grand nombre de réunions possible pour compléter les témoignages... L'expression « autant de réunions que possible » est, je suppose, limitée uniquement par les ressources de la Chambre. Cela ne signifie pas autant de réunions que nécessaire.

Je ne pense pas que nous réunir simplement pour avoir des réunions nous permettra d'accomplir le travail que nous devons faire. De plus, il sera important de nous assurer d'avoir suffisamment de matière pour nous occuper pendant « autant de réunions que possible ».

Si nous envoyons une assignation à des gens qui ont déjà refusé... Notre comité s'est déjà retrouvé dans cette situation, et avec le même résultat, en convoquant des représentants de sociétés qui n'ont pas de siège social au Canada. Nous l'avons vu avec le PDG de Meta. Je suppose que dans le cas du PDG de TikTok, si la société mère n'est pas au Canada, nous recevrons une réponse semblable.

Il est important de ne pas avoir un nombre illimité de réunions. Nous avons déjà des réunions planifiées, et nous avons...

Je suis désolé, monsieur le président...

**Une voix:** [*Inaudible*]

**Le président:** En fait, nous ne pouvons pas passer au vote. Il a toujours la parole.

**M. Michael Barrett:** Je ne comprends pas ce qu'ils disent.

**Le président:** Poursuivez, monsieur Barrett.

**M. Michael Barrett:** Je ne crois pas que d'avoir un nombre illimité de réunions soit une bonne façon d'utiliser le temps du Comité alors que nous n'arrivons même pas à trouver des témoins pour les réunions déjà prévues.

Vous venez de voir que le Comité n'a même pas la volonté de donner suite à la motion proposée avec amendement ou à la motion non amendée, alors qu'il est simplement question d'envoyer des invitations à tous les témoins. Supprimer simplement le point (a) en demandant au Comité de l'approuver par consentement unanime... La personne qui a proposé la motion n'est même pas d'accord pour le point (a). Je ne sais pas comment nous allons nous y prendre pour l'adopter.

Pour ce qui est du point (c), je crois qu'il est important que nous votions parce que l'expression « autant de réunions que possible » n'est pas un libellé raisonnable. Ce n'est pas une directive raisonnable pour le Comité.

● (1745)

**Le président:** Nous parlons encore de l'amendement visant à supprimer le point (c).

Nous devons nous arrêter ici. Je vais devoir lever la séance, parce qu'on vient de dire...

**M. Damien Kurek:** Je passe mon tour.

**Le président:** Je vais vous donner une seconde.

Allez-y.

**Mme Iqra Khalid:** Monsieur le président, je vous implore de mettre aux voix l'amendement. Votons sur cette motion le plus rapidement possible.

**M. Michael Barrett:** Avons-nous le temps ou non?

**Mme Iqra Khalid:** Encore une fois, cela retarde l'étude, monsieur le président.

**Le président:** C'est là le problème. S'il y a d'autres interventions sur l'amendement ou sur la motion... Je ne peux pas forcer la tenue d'un vote, madame Khalid. Je ne peux tout simplement pas.

Y a-t-il d'autres commentaires sur l'amendement?

**M. Michael Barrett:** Avons-nous encore des ressources pour poursuivre la réunion?

**Le président:** Pas maintenant. Nous avons terminé à 17 h 45.

**Mme Iqra Khalid:** Monsieur le président, serait-il possible de demander des ressources?

**Le président:** Je vais laisser la greffière vous répondre.

Nous avons envoyé des courriels à des techniciens, et on nous a dit que nous devions nous arrêter à 17 h 45. Nous avons maintenant dépassé ce point.

**M. Michael Barrett:** Nous devrions lever la séance.

**Mme Iqra Khalid:** Je ne sais pas, monsieur le président, s'il y a quelqu'un d'autre sur la liste des intervenants.

**Le président:** M. Kurek est sur la liste des intervenants.

Vous avez la parole, monsieur Kurek.

**M. Damien Kurek:** Merci, monsieur le président.

Pour ce qui est de mon amendement, je crois qu'il est assez clair et qu'il permettra d'établir si la motion est de bonne foi ou s'il s'agit simplement d'une tentative de se soustraire à la reddition de comptes. Je vais m'en tenir à ces commentaires.

Je pense que le point (c) de la motion de Mme Khalid est non seulement sans précédent, mais aussi une tentative claire d'empêcher le Comité d'examiner d'autres importantes questions prévues.

Sur ce, je cède mon temps de parole au prochain intervenant inscrit sur la liste pour ce qui est de l'amendement.

**Le président:** Je n'ai personne d'autre sur la liste.

**Mme Iqra Khalid:** Vous pouvez mettre l'amendement aux voix.

**Le président:** Je vais mettre la question aux voix.

**M. Michael Barrett:** Pouvons-nous avoir un vote par appel nominal, s'il vous plaît?

**Le président:** Nous allons procéder un vote par appel nominal sur l'amendement.

Nous devons agir très rapidement, madame la greffière. Allez-y.

(L'amendement est rejeté par 7 voix contre 3. [*Voir le Procès-verbal*])

**Le président:** L'amendement a été rejeté.

Je ne peux pas faire cela. Je ne peux pas accepter d'autres... Nous avons différents comités ici ce soir. Il y le comité des Finances et l'OGGO qui s'en occupent. La greffière me dit que je ne peux pas...

Nous en sommes à la motion principale. Je ne peux pas le faire, alors je vais devoir...

**M. Damien Kurek:** Allez-vous maintenir la liste des intervenants pour la prochaine fois?

**Le président:** La greffière m'informe que si vous souhaitez poursuivre, je dois simplement confirmer la liste des intervenants pour la reprise de cette discussion et confirmer si nous voulons reprendre la discussion le 4 décembre. Nous recevons des témoins le 29.

Souhaitez-vous avoir une liste d'intervenants à la reprise des travaux? Je vois plusieurs mains levées.

Je vais lever la séance.

**Un député:** Oui.

● (1750)

**Mme Iqra Khalid:** Monsieur le président, si vous êtes d'accord, je veux dire, s'il s'agit simplement d'un vote rapide sur la motion principale, pouvons-nous…

**M. Michael Barrett:** Est-ce que nous ajournons ou non?

**Le président:** La séance est levée. Écoutez, j'ai des intervenants sur la motion principale.

**Mme Iqra Khalid:** Excusez-moi.

**Le président:** Je ne peux pas continuer, alors je lève la séance.