CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

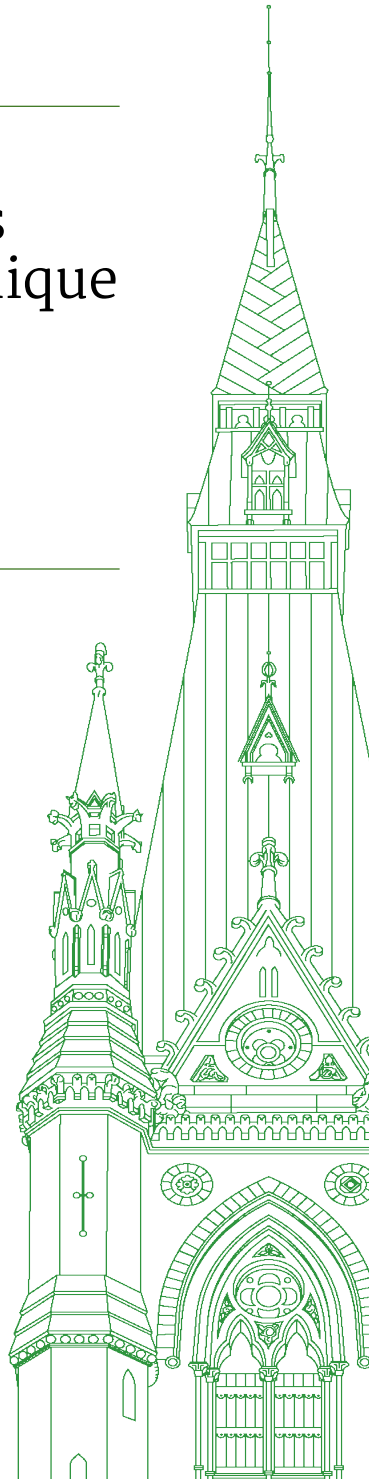
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 019

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 5 mai 2022



Président : M. Pat Kelly

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

Le jeudi 5 mai 2022

● (1535)

[*Français*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): Je déclare la séance ouverte.

Je vous souhaite la bienvenue à la 19e 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'alinéa 108(3)h) du Règlement et à la motion adoptée par le Comité le lundi 13 décembre 2021, le Comité reprend son étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale.

La réunion d'aujourd'hui se déroule en format hybride, conformément à l'ordre de la Chambre du 25 novembre 2021. Des membres sont présents en personne et d'autres participent à distance au moyen de l'application Zoom.

J'ai quelques commentaires à faire à l'intention des témoins. Nous avons des témoins dans la salle et des témoins qui participent par Zoom. Veuillez attendre que je vous identifie avant de prendre la parole. Si vous participez par Zoom, cliquez sur l'icône du microphone pour l'activer et mettez-le en sourdine lorsque vous ne parlez pas. Les participants dans la salle n'ont pas à appuyer sur le bouton, car quelqu'un d'autre assure le contrôle, mais soyez attentifs et assurez-vous que votre micro est allumé avant de parler. Je vous rappelle que vous devez vous adresser à la présidence.

J'aimerais maintenant souhaiter la bienvenue à nos témoins.

De Microsoft, nous accueillons Owen Larter, directeur responsable des politiques publiques en matière d'Intelligence artificielle; et du Conseil national des musulmans canadiens, nous avons Mustafa Farooq, président-directeur général, et Rizwan Mohammad, agent des services d'assistance judiciaire.

Nous allons commencer par M. Larter.

Vous avez un maximum de cinq minutes pour votre déclaration liminaire.

M. Owen Larter (directeur, Politiques publiques en matière d'Intelligence Artificielle responsable, Microsoft): Merci beaucoup.

[*Français*]

Bonjour à tous.

[*Traduction*]

Je remercie le président et les vice-présidents de me donner l'occasion d'apporter ma contribution aujourd'hui.

Je m'appelle Owen Larter. Je fais partie de l'équipe du Bureau des politiques publiques et de l'intelligence artificielle responsable de Microsoft.

Il y a vraiment trois points que je veux faire valoir dans mes observations aujourd'hui.

Premièrement, la reconnaissance faciale est une technologie nouvelle et puissante qui est déjà utilisée et pour laquelle nous avons maintenant besoin d'une réglementation.

Deuxièmement, il est particulièrement urgent de réglementer l'utilisation de la reconnaissance faciale par la police, étant donné que les décisions de la police ont des conséquences importantes.

Troisièmement, il existe une réelle occasion pour le Canada de montrer la voie à l'échelle mondiale en élaborant une réglementation de la reconnaissance faciale qui protège les droits de la personne et favorise la transparence et la responsabilisation.

Je tiens d'abord à saluer le travail du Comité sur ce sujet très important. Chez Microsoft, nous sommes des fournisseurs de la reconnaissance faciale. Nous sommes convaincus qu'elle peut apporter de réels avantages à la société. Elle peut notamment contribuer à sécuriser les appareils et aider les personnes aveugles ou malvoyantes à accéder à des expériences sociales plus immersives. Dans le contexte de la sécurité publique, elle peut contribuer à la recherche de victimes de la traite de personnes et être utilisée dans le cadre d'enquêtes criminelles.

Toutefois, nous sommes également conscients des risques que cette technologie peut présenter, notamment du risque de biais et de décisions injustes en matière de rendement, y compris dans différents groupes démographiques; du potentiel de nouvelles intrusions dans la vie privée des gens; et des menaces possibles pour les libertés démocratiques et les droits de la personne.

En réponse à cela, nous avons développé ces dernières années un certain nombre de mesures de protection internes chez Microsoft, dont nos principes de reconnaissance faciale. Ils comprennent la création de notre note sur la transparence pour l'interface de programme des applications FACE. Cette note sur la transparence explique, dans un langage destiné à un public non technique, comment fonctionne notre reconnaissance faciale, quelles en sont les capacités et les limites et quels sont les facteurs qui influent sur les performances, le tout dans le but d'aider les clients à comprendre comment l'utiliser de manière responsable.

Le travail sur la reconnaissance faciale s'appuie sur le programme plus étendu de responsabilisation en matière d'intelligence artificielle de Microsoft. Il s'agit d'un programme qui garantit que les collègues conçoivent et déploient l'intelligence artificielle d'une manière conforme à nos principes. Le programme comprend l'équipe de gouvernance de l'intelligence artificielle de l'entreprise et notre norme d'intelligence artificielle responsable, qui est une série d'exigences auxquelles les collègues qui conçoivent et déploient l'intelligence artificielle doivent se conformer. Il comprend également notre processus d'examen des utilisations délicates de l'intelligence artificielle.

Outre ces mesures de protection internes, nous pensons également que des dispositions réglementaires sont nécessaires. Ce besoin est particulièrement aigu dans le contexte de l'application de la loi, comme je l'ai mentionné. Nous pensons vraiment que l'importance du travail de ce comité ne peut être surestimée. Nous saluons la manière dont il réunit les parties prenantes de toute la société, y compris le gouvernement, la société civile, l'industrie et le monde universitaire, pour discuter de ce à quoi un cadre réglementaire devrait ressembler.

Nous soulignons qu'en effet, des avancées positives ont eu lieu dans des endroits comme l'État de Washington aux États-Unis, et que d'importantes discussions sont en cours dans l'Union européenne et ailleurs. Nous croyons cependant que le Canada a l'occasion de jouer un rôle de premier plan dans la création d'une réglementation en la matière.

Nous pensons que ce type de réglementation doit accomplir trois choses. Elle doit protéger les droits de la personne, favoriser la transparence et la responsabilisation, et assurer la mise à l'essai des systèmes de reconnaissance faciale de manière à démontrer qu'ils fonctionnent correctement.

En matière d'application de la loi, les dispositions réglementaires doivent prendre en compte d'importants aspects de la protection des droits de la personne, notamment l'interdiction d'utiliser la reconnaissance faciale pour la surveillance de masse sans discernement et l'interdiction de l'utiliser sur la base de la race, du sexe, de l'orientation sexuelle ou d'autres caractéristiques protégées d'une personne. Les dispositions réglementaires doivent également veiller à ce que l'utilisation de la reconnaissance faciale ne porte pas atteinte à des libertés importantes, telles que la liberté de réunion.

En ce qui concerne la transparence et la responsabilité, nous pensons que les organismes chargés de l'application de la loi devraient adopter une politique d'utilisation publique définissant la manière dont ils utiliseront la reconnaissance faciale; les bases de données dans lesquelles ils effectueront des recherches; et la manière dont ils désigneront et formeront les personnes chargées d'utiliser le système de sorte qu'elles le fassent convenablement et qu'un examen soit réalisé par un humain. Nous pensons également que les fournisseurs doivent donner de l'information sur le fonctionnement de leurs systèmes et sur les facteurs qui affecteront les performances.

Il est important que les systèmes soient également soumis à des tests garantissant l'exactitude des résultats. Nous recommandons aux fournisseurs de reconnaissance faciale comme Microsoft de soumettre leurs systèmes à des tests raisonnables réalisés par des tiers et de mettre en place des plans d'atténuation pour tout écart de performance, notamment parmi les groupes démographiques.

Nous pensons également que les organismes qui déploient la reconnaissance faciale doivent tester les systèmes dans des conditions opérationnelles, étant donné les effets que les facteurs environnementaux comme l'éclairage et le fond de scène ont sur les performances. Dans un contexte commercial, nous pensons que la réglementation devrait exiger un avis bien visible et un consentement explicite pour tout suivi.

Je vais conclure en disant que nous faisons l'éloge de nombreux éléments des recommandations que les commissaires provinciaux et fédéral à la protection de la vie privée ont formulées plus tôt cette semaine et qui établissent des éléments importants du cadre juridique de la reconnaissance faciale.

Je vous remercie beaucoup.

● (1540)

Le président: Merci, monsieur Larter.

Nous allons maintenant écouter M. Farooq, qui dispose de cinq minutes.

M. Mustafa Farooq (président-directeur général, Conseil national des musulmans canadiens): Je vais en fait céder la parole à mon collègue, si vous le permettez, monsieur le président.

Le président: D'accord. Monsieur Mohammad, nous vous écoutons.

M. Rizwan Mohammad (agent des services d'assistance judiciaire, Conseil national des musulmans canadiens): Merci, monsieur le président, mesdames et messieurs les membres du Comité, de nous donner l'occasion de vous faire part de nos réflexions dans le contexte de cette étude.

Je m'appelle Rizwan Mohammad et je suis agent des services d'assistance judiciaire au Conseil national des musulmans canadiens, le CNMC. Je suis accompagné aujourd'hui par le président-directeur général du CNMC, Mustafa Farooq. Je tiens également à remercier Hisham Fazail, stagiaire au CNMC, d'avoir travaillé à la rédaction de notre mémoire.

Aujourd'hui, nous voulons nous pencher sur le cœur du problème de la technologie de reconnaissance faciale, ou TRF. Divers organismes de sécurité nationale et de maintien de l'ordre ainsi que d'autres organismes gouvernementaux sont venus témoigner devant votre comité pour vous dire à quel point la TRF est un outil important qui a un grand potentiel d'utilisation au sein du gouvernement. On vous a dit que la TRF peut contribuer à éviter les problèmes de cognition humaine et de partialité.

Je vais vous donner des noms que vous connaissez tous, des noms associés à des moments où ces mêmes organismes vous ont dit que la surveillance se ferait d'une manière conforme à la Constitution et équilibrée. Il s'agit de Maher Arar, Abdullah Almalki et Mohamedou Ould Slahi.

Les mêmes organismes qui ont menti à la population canadienne au sujet de la surveillance des communautés musulmanes se présentent maintenant devant vous pour affirmer que, même si la surveillance de masse n'aura pas lieu, la TRF peut et doit être utilisée de manière responsable. Le commissaire à la protection de la vie privée a déjà établi que ces organismes, dont la GRC, ont enfreint la loi en ce qui concerne la TRF.

Nous formulons donc les deux recommandations suivantes, et nous tenons à préciser que nos observations se limitent à l'exploration de la TRF dans un cadre autre que celui de la consommation.

Premièrement, nous recommandons au gouvernement d'adopter une loi claire et sans équivoque sur la protection de la vie privée qui limite rigoureusement la façon dont la TRF peut être utilisée dans un contexte autre que celui de la consommation, et qui ne permet que des exceptions approuvées par les tribunaux dans le contexte de la surveillance.

Deuxièmement, nous recommandons au gouvernement d'établir des sanctions claires pour les organismes qui violent les règles relatives à la protection de la vie privée et à la TRF.

Commençons par la première recommandation, qui demande une interdiction générale du recours à la TRF sans autorisation judiciaire à l'échelle du gouvernement, dans le contexte de tous les organismes de sécurité nationale, notamment, la GRC, le SCRS et l'ASFC. Vous en connaissez déjà les raisons. Un rapport de 2018 au Royaume-Uni a révélé de nouvelles données montrant que le logiciel de reconnaissance faciale utilisé par la police métropolitaine du Royaume-Uni produisait des correspondances incorrectes dans 98 % des cas. Une autre étude de 2019, fondée sur une méthodologie différente, a montré que la police métropolitaine fournissait un taux de correspondances incorrectes, ou un taux de faux positifs, de 38 %.

Nous sommes bien conscients que la TRF fonctionne différemment, et avec des degrés de précision différents, selon la technologie, mais nous reconnaissons tous qu'il existe des biais algorithmiques en matière de TRF. Compte tenu de ce que nous savons, des risques pour la vie privée que pose la TRF et des préoccupations exprimées par des Canadiens, y compris des membres d'autres comités de la Chambre, au sujet du racisme systémique dans les services de police, nous sommes d'accord avec d'autres témoins qui ont comparu devant ce comité pour demander un moratoire immédiat sur toute utilisation de la TRF dans le contexte de la sécurité nationale, notamment à la GRC, et ce, jusqu'à ce que soient rédigées des lignes directrices législatives.

Simultanément, nous recommandons l'adoption d'un seuil très élevé dans l'élaboration des lignes directrices législatives, notamment en ce qui concerne l'autorisation judiciaire, la surveillance et les délais.

Deuxièmement, nous sommes choqués par la désinvolture de la GRC dans sa façon d'aborder la question de l'utilisation de Clearview AI. La GRC a d'abord nié avoir utilisé Clearview AI, puis a confirmé avoir utilisé le logiciel après que la liste des clients de la société a été piratée. Elle a prétexté que l'utilisation de la TRF n'était pas largement connue au sein de la GRC. Elle a donné au commissaire à la protection de la vie privée une explication totalement inacceptable, aussi crédible que l'excuse du chien qui a mangé le devoir.

À la suite des conclusions formulées par le commissaire à la protection de la vie privée dans son rapport, la GRC a eu l'audace de déclarer qu'elle n'était pas nécessairement d'accord avec ces conclusions. La GRC a certes pris certaines mesures pour apaiser les préoccupations soulevées, mais tout manquement à l'obligation de rendre des comptes, lorsqu'il s'agit d'erreurs manifestes et de déclarations trompeuses, doit entraîner des sanctions claires. Sinon, comment pouvons-nous faire confiance à un tel processus ou à l'engagement d'éviter la surveillance de masse?

Nous encourageons le Comité à recommander que des sanctions sévères soient infligées aux organismes et aux agents qui enfreignent les règles créées en matière de TRF, peut-être par la modification de la Loi sur la GRC. Nous transmettrons au Comité un mémoire plus détaillé en temps voulu.

C'est ce que nous proposons. Vos questions seront bienvenues.

Merci.

● (1545)

Le président: Je vous remercie de cet exposé.

M. Williams sera le premier à poser des questions. Monsieur Williams, vous disposez de six minutes.

M. Ryan Williams (Baie de Quinte, PCC): Je remercie nos témoins de leur présence aujourd'hui.

Par votre intermédiaire, monsieur le président, j'ai quelques questions à poser à M. Larder.

On sait que vous avez interdit l'accès à la technologie de reconnaissance faciale aux services de police américains. Qu'est-ce qui s'est passé ou qu'est-ce qu'on a fait pour que Microsoft interdise aux services de police l'accès à la technologie de reconnaissance faciale?

M. Owen Larter: Je vous remercie beaucoup de votre question.

Il est vrai que nous ne vendons pas la reconnaissance faciale aux services de police locaux des États-Unis. Nous estimons qu'il est très important de mettre en place des dispositions législatives capables de protéger les droits de la personne dans le contexte de la reconnaissance faciale. Je pense que l'un des défis aux États-Unis est qu'il n'y a pas de loi en la matière. Il n'y a pas de loi sur la protection de la vie privée, comme il en existe dans beaucoup d'autres pays, y compris au Canada. Bien sûr, je suis au courant des discussions en cours sur la façon d'améliorer le régime de protection de la vie privée au Canada, et ce sont des discussions importantes à avoir également.

C'est notre position. C'est pourquoi nous nous exprimons de manière proactive, en participant à des discussions comme celle-ci et en contribuant à des efforts importants comme ceux que vous déployez. Nous voulons nous assurer de la mise en place d'une réglementation solide concernant l'utilisation de la reconnaissance faciale, en priorité pour la police, et nous souhaitons plus généralement veiller à ce que la technologie soit utilisée d'une manière transparente, responsable et respectueuse des droits.

M. Ryan Williams: Est-ce que vous refusez aussi cette technologie aux services de police canadiens?

● (1550)

M. Owen Larter: Ce n'est pas notre politique en ce moment.

M. Ryan Williams: Est-ce parce que nous avons des politiques différentes ici? Est-ce que le Canada a actuellement des politiques que vous aimez?

M. Owen Larter: Oui. Comme je l'ai dit précédemment, je pense qu'il existe un cadre législatif permettant de faire en sorte que la reconnaissance faciale soit utilisée d'une manière respectueuse des droits. Je pense que les dispositions législatives en matière de protection de la vie privée en font partie. Je pense qu'il est possible d'améliorer les cadres de protection de la vie privée dans le monde entier. Nous sommes conscients des discussions en cours au Canada également. L'absence de toute forme de lois générales sur la protection de la vie privée aux États-Unis est la principale raison de cette position.

M. Ryan Williams: Merci.

Vous venez de dire que votre programme de responsabilisation en matière d'intelligence artificielle s'accompagne d'un ensemble de directives à suivre pour son utilisation. Quelles sont ces directives?

M. Owen Larter: Nous avons notre programme plus général de responsabilisation en matière d'intelligence artificielle, que nous avons développé au cours des dernières années. Il comporte quelques éléments. Nous avons une équipe de gouvernance de l'intelligence artificielle à l'échelle de l'entreprise. Cette équipe regroupe de multiples parties prenantes et certains de nos chercheurs Microsoft. Il s'agit de chercheurs de renommée mondiale du domaine de l'intelligence artificielle qui partagent leurs connaissances sur l'état actuel de la technologie et sur son évolution. Ils collaborent à la supervision du programme général avec des personnes chargées des questions juridiques et politiques et des personnes qui ont une formation d'ingénieur.

En ce qui concerne les autres composantes, nous disposons également d'une norme d'intelligence artificielle responsable. C'est un ensemble d'exigences liées à nos six principes de l'intelligence artificielle — je pourrai vous les présenter en détail — qui garantissent que toutes les équipes chargées de concevoir ou de déployer des systèmes d'intelligence artificielle le font d'une manière conforme à nos principes.

Le dernier élément est également un processus d'examen des utilisations délicates. Ce processus entre en jeu lorsque la conception ou le déploiement éventuel d'un système répond à l'un des trois éléments déclencheurs potentiels. Chaque fois qu'un système est utilisé d'une façon qui affecte les perspectives juridiques ou le statut juridique d'une personne, chaque fois qu'il y a un risque de préjudice psychologique ou physique, ou chaque fois qu'il y a risque d'atteinte aux droits de la personne, l'équipe de gouvernance que j'ai mentionnée se réunit et vérifie si nous pouvons aller de l'avant avec le déploiement ou la conception d'une forme d'intelligence artificielle particulière, et veille ainsi à ce que cela se fasse de manière responsable.

Vous pouvez imaginer que ces discussions se tiennent pour tous nos systèmes, y compris les discussions que nous avons sur la reconnaissance faciale.

M. Ryan Williams: Merci.

Vous avez parlé de protocoles de test appropriés. Quelles recommandations feriez-vous à notre comité concernant les protocoles de test que vous utilisez? Est-ce qu'ils comportent aussi un contrôle humain pour cette technologie?

M. Owen Larter: Nous pensons que c'est une partie très importante de la réflexion, et ce, pour plusieurs raisons.

La précision de la reconnaissance faciale s'est nettement améliorée ces dernières années. De très bonnes recherches sont menées par le National Institute of Standards and Technology aux États-Unis, ou NIST. Elles montrent que la précision s'est nettement améliorée ces dernières années pour les systèmes les plus performants. Il existe toutefois un écart très important entre les systèmes les plus performants et les systèmes les moins performants, et les systèmes les moins précis ont tendance à être plus discriminatoires également. C'est la raison pour laquelle nous pensons que les tests sont vraiment importants.

Il y a deux composantes à cela. Nous pensons que des fournisseurs tels que Microsoft devraient permettre que leurs systèmes soient testés de manière raisonnable par des tiers indépendants, ce que nous permettons actuellement au moyen d'une IPA, ou interface de programme des applications. Une tierce partie peut tester notre système pour voir s'il est précis. Nous pensons que les fournisseurs devraient être tenus de répondre à tout test et de corriger tout écart de performance important, y compris sur le plan démographique. Donc, les fournisseurs doivent agir sur le plan des tests.

Nous pensons aussi qu'il est vraiment très important que les organisations qui déploient un service de reconnaissance faciale le testent dans des conditions opérationnelles. Si vous êtes un client de la police et que vous utilisez un système de reconnaissance faciale, vous ne devez pas vous contenter de croire sur parole le fournisseur qui vous dit que le système sera précis dans l'abstrait; vous devez également le tester dans des conditions opérationnelles. En effet, les facteurs environnementaux tels que la qualité de l'image ou la position de la caméra ont une incidence considérable sur la précision.

Vous pouvez imaginer que si vous avez une caméra qui fixe le dessus de la tête d'une personne et qu'il y a des saletés sur l'objectif, ou que des images de mauvaise qualité entrent dans le système en général, les performances en seront très réduites. Par conséquent, les organisations qui déploient la reconnaissance faciale devraient également être tenues de procéder à des tests garantissant que le système fonctionne correctement dans l'environnement où il sera utilisé.

M. Ryan Williams: Merci beaucoup, monsieur Larter.

Le président: C'est maintenant au tour de Mme Hepfner, pour six minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci beaucoup.

Je remercie tous les témoins de leur présence parmi nous aujourd'hui. J'aimerais également commencer par vous, monsieur Larter.

J'ai lu un article écrit en 2018 par Brad Smith, de Microsoft. Il aborde beaucoup de questions semblables à celles dont vous parlez aujourd'hui. La technologie de reconnaissance faciale était mise au point, et Microsoft demandait au gouvernement de réglementer l'industrie.

Je me demande si vous pouvez parler de la façon dont cela fonctionne lorsque des géants de la technologie mettent au point cette technologie et demandent ensuite aux gouvernements de la réglementer. Est-ce la bonne façon de procéder? Y a-t-il de meilleurs moyens pour faire participer les gouvernements lorsque la technologie est mise au point?

J'aimerais juste que vous en parliez un peu.

● (1555)

M. Owen Larter: C'est une question très importante, et nous sommes convaincus que le gouvernement doit jouer un rôle de premier plan dans la création d'un cadre réglementaire pour la technologie en général, y compris des technologies comme la reconnaissance faciale.

Nous avons essayé deux ou trois choses au cours des dernières années. Nous avons d'abord pris des mesures internes de protection, pour apporter notre contribution en tant que vendeur de systèmes de reconnaissance faciale afin que la technologie soit utilisée de manière responsable. J'ai parlé de notre programme de responsabilisation en matière d'intelligence artificielle. Nous avons aussi notre note sur la transparence pour l'interface de programme des applications FACE. Je crois que c'est un aspect très important de la discussion pour répondre au besoin de transparence quant à la façon dont la reconnaissance faciale est mise au point et élaborée.

La note sur la transparence est un document que nous avons rendu public, et il indique clairement le fonctionnement d'un système pour ce qui est de certaines capacités de la technologie, les limites de la technologie ainsi que les usages à proscrire et les facteurs qui nuisent au rendement, pour que le client qui se sert de la technologie soit bien informé et en mesure de prendre des décisions éclairées et responsables relativement à son déploiement.

C'est une partie de ce que nous faisons à l'interne. Nous croyons également qu'un cadre réglementaire est nécessaire, car il est très important d'instaurer la confiance dans la technologie en général et plus particulièrement dans la reconnaissance faciale, compte tenu de certains risques qu'elle peut présenter et dont j'ai parlé dans mes observations.

Nous tenons à appuyer ces discussions. C'est la raison pour laquelle nous sommes ravis de prendre part à des discussions comme celle-ci. Nous voulons vraiment mettre à contribution nos connaissances sur le fonctionnement et l'orientation de la technologie pour pouvoir créer, sous la direction des gouvernements et en collaboration avec d'autres intervenants comme la société civile, un cadre réglementaire solide pour la technologie afin de pouvoir tirer parti des avantages de cette technologie puissante tout en s'attaquant à certains des problèmes qu'elle présente.

Mme Lisa Hepfner: Merci.

Dans vos observations liminaires, vous avez énuméré toutes sortes de façons d'utiliser la reconnaissance faciale pour de bonnes raisons et peut-être aussi pour de mauvaises raisons. Pouvez-vous dire au Comité, en vous adressant à la présidence, dans quelle mesure la technologie de reconnaissance faciale est actuellement répandue dans notre société? Quelle est son incidence sur la vie des Canadiens?

M. Owen Larter: C'est une très bonne question. Je dirais qu'on s'en sert de plus en plus. C'est une technologie qui peut présenter de nombreux avantages, et je pense que les gens et les organisations s'en rendent compte.

Il y a quelques applications différentes. Elles sont souvent liées à la sécurité, comme la vérification de l'identité à l'aide de la reconnaissance faciale. Par exemple, lorsqu'on ouvre une session sur son téléphone ou son ordinateur, c'est maintenant souvent à l'aide d'un outil de reconnaissance faciale. L'enregistrement aisé et sans contact à l'aéroport est un autre exemple de la façon dont la reconnaissance faciale est utilisée. Cette utilisation a d'ailleurs été particulièrement importante au cours des dernières années, dans le pire de la crise attribuable à la COVID, de toute évidence.

Au-delà de la sécurité, je pense qu'il y a des applications très bénéfiques en matière d'accessibilité. Un certain nombre d'organisations font des travaux de recherche très intéressants sur la façon d'utiliser la reconnaissance faciale pour aider les personnes aveugles ou malvoyantes à mieux comprendre le monde qui les entoure et à mieux interagir. Nous avons le projet Tokyo, dans lequel on a recours à la reconnaissance faciale. Une personne aveugle équipée d'un casque d'écoute peut balayer la pièce — disons une cafétéria ou un espace ouvert au travail — et être en mesure d'identifier les personnes qui ont accepté de faire partie de son système de reconnaissance faciale, ce qui lui permettra de prendre les devants et d'entamer une conversation, ce qui aurait été très difficile autrement.

Une autre application à laquelle je pense et qui emballe les gens du milieu de l'accessibilité s'adresse aux personnes atteintes d'Alzheimer ou de maladies similaires qui font en sorte qu'il leur est de plus en plus difficile de reconnaître des amis ou des êtres chers. Vous pouvez imaginer la manière dont on se penche sur la reconnaissance faciale pour aider ces personnes à reconnaître leurs amis et leurs proches.

La réponse devient longue, mais je vais terminer en disant qu'il y a aussi des applications utiles dans le contexte de l'application de la loi. Nous pensons que, dans le cadre d'une enquête criminelle, la reconnaissance faciale, de pair avec de solides mesures de protection, peut être un outil utile. On s'en sert aussi pour identifier en ligne des personnes disparues ou victimes de la traite, y compris des enfants, d'une manière qui s'est également avérée très utile.

La technologie procure des avantages concrets, mais, encore une fois, il y a les problèmes dont j'ai aussi parlé. C'est pour cette raison que vous avez besoin d'un cadre réglementaire qui permet de profiter de ces avantages tout en s'attaquant aux problèmes connexes.

● (1600)

Mme Lisa Hepfner: Merci beaucoup.

Monsieur le président, il me reste environ 30 secondes. J'aimerais donner de vive voix un avis de motion, celle que j'ai distribuée hier. La voici:

> Que, conformément à l'article 108(3)h)(vii) du Règlement, le comité entreprenne une étude en vue d'examiner la question de la surveillance numérique par les employeurs des Canadiens qui travaillent à domicile, y compris : a) la prévalence de la surveillance numérique par les employeurs; b) le type de surveillance recueillie; c) la façon dont les données de surveillance personnelle sont stockées et sécurisées; d) les règles en place pour protéger le droit à la vie privée des employés qui travaillent à domicile; e) les droits de divulgation et de permission des employés en matière de collecte de données; que le comité fasse rapport de ses conclusions et recommandations à la Chambre; que conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au rapport.

Merci.

Le président: Merci. Vous donnez avis de cette motion, n'est-ce pas?

Mme Lisa Hepfner: Je le fais de vive voix. Merci.

Le président: Nous l'avons reçue, et elle est donc...

Mme Lisa Hepfner: Je l'ai tout simplement lue pour le compte rendu. Merci beaucoup.

Le président: Bien sûr. Merci.

[*Français*]

Monsieur Villemure, vous avez maintenant la parole pour six minutes.

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

Mes questions s'adresseront à M. Larter.

Monsieur Larter, vous avez dit que Microsoft ne vendait pas sa technologie aux services policiers. Maintenant est-ce que Microsoft a comme client les agences militaires, les agences de surveillance ou les services de renseignement?

[*Traduction*]

M. Owen Larter: Nous pensons que la reconnaissance faciale peut avoir des applications dans le domaine de la sécurité et celui de l'application de la loi. Je pense que ce qu'il faut vraiment retenir, c'est que nous utilisons une approche axée sur les risques en ce qui a trait à notre façon de procéder à une évaluation au moyen d'un système et au genre de clients avec lesquels nous travaillons.

Nous avons notre processus d'examen des utilisations délicates dont j'ai parlé, qui compte trois éléments déclencheurs. Chaque fois que nous déployons un système — qu'il s'agisse de la reconnaissance faciale ou d'un autre — d'une façon qui mène à un de ces trois éléments déclencheurs, nous avons recours à un solide processus d'examen des utilisations délicates.

Notre technologie de reconnaissance faciale peut servir à appliquer la loi et à assurer la sécurité. Nous pensons qu'elle a des applications utiles dans ces scénarios, mais il est très important d'avoir de solides mesures de protection liées à cette utilisation, y compris les mesures de protection internes de Microsoft dont j'ai parlé, mais aussi un cadre réglementaire pour qu'il ne plane aucun doute sur la façon dont la technologie est utilisée, pour que nous sachions qu'elle est utilisée de manière fiable et responsable.

[*Français*]

M. René Villemure: Pourriez-vous, plus tard et par écrit, fournir au Comité des exemples des mesures de sauvegarde en question?

[*Traduction*]

M. Owen Larter: Oui, bien sûr. Je le ferai avec plaisir.

[*Français*]

M. René Villemure: C'est parfait. Merci beaucoup.

La question peut vous sembler étrange, mais Microsoft cherche-t-elle à ce que ce soit réglementé afin de pouvoir dire, plus tard, qu'elle a même milité pour un encadrement, et que ce n'est pas grave si certaines choses se produisent?

Cela peut sembler non pertinent, mais est-ce que le fait d'avoir un tel encadrement protège Microsoft?

[*Traduction*]

M. Owen Larter: La présence d'un cadre protège Microsoft, mais pas nécessairement pour les raisons évoquées. De façon générale, nous considérons qu'il est crucial d'établir dans le domaine de la technologie un cadre de réglementation qui engendre la confiance et montre que la technologie est utilisée de manière fiable.

Nous sommes en activité depuis un bon bout de temps maintenant. Notre entreprise a presque 50 ans, et nous comprenons qu'il faut que la technologie inspire la confiance pour que la société en profite et pour que les gens l'utilisent. La réglementation joue un rôle de premier plan dans l'établissement d'un cadre de fiabilité. Voilà ce que nous préconisons en général et, en particulier, ce pour quoi nous investissons du temps pour tenter de préconiser l'établissement de mesures de protection solides au sujet de la reconnaissance faciale, puisqu'il s'agit d'une puissante technologie qui a des applications très bénéfiques, comme je l'ai souligné, mais qui s'accompagne également de défis potentiels.

La création d'un cadre en matière de reconnaissance faciale faisant en sorte que cette dernière puisse être utilisée de façon fiable — et de manière jugée fiable par la population — est très importante pour que la société puisse profiter de ses bienfaits et pour que cette technologie soit utilisée à long terme.

[*Français*]

M. René Villemure: J'aime beaucoup votre approche, d'ailleurs.

Nous vous serions reconnaissants si vous pouviez nous envoyer, par la suite, tout renseignement que vous auriez sur les mesures de sauvegarde, sur les types de programmes et sur la responsabilité de la technologie de reconnaissance faciale, ou ce qui s'y rapporte.

Ma prochaine question peut vous sembler un peu étonnante.

Y a-t-il un lien entre la technologie de reconnaissance faciale et le nouvel univers du métavers?

[*Traduction*]

M. Owen Larter: C'est une bonne question. Je vous remercie de m'inviter à fournir des documents. Nous serions heureux d'avoir l'occasion de le faire. Nous pensons que les travaux du Comité sont très importants et nous voulons apporter tout le soutien et toute l'aide possible. Je vous remercie de me demander de fournir des documents, et nous vous en enverrons.

En ce qui concerne le métavers, les possibilités qu'il offre suscitent un enthousiasme généralisé, et avec raison, selon moi. La création du métavers mettra à contribution un certain nombre de technologies pour qu'il fonctionne conformément aux attentes des gens et de manière responsable.

Je pense que la reconnaissance faciale fera partie de ces technologies, aux côtés de bien d'autres technologies. Le métavers — que, chez Microsoft, nous appelons « multivers » — offre une myriade de possibilités que notre société commence à peine à explorer. Nous devrons discuter sérieusement de ce que nous voulons qu'il soit et des mesures de protection que nous devrons instaurer pour profiter des avantages de cette technologie et résoudre certains problèmes.

La reconnaissance faciale jouera certainement un rôle de toutes sortes de façons que nous ne pouvons probablement même pas comprendre pleinement à l'heure actuelle.

● (1605)

[*Français*]

M. René Villemure: Je vous remercie beaucoup de votre réponse. C'est une conversation que nous aurons probablement dans un autre comité, mais c'est très intéressant.

Pourriez-vous me dire dans quels secteurs d'activités se situent les principaux clients de Microsoft dans le domaine de la reconnaissance faciale?

[*Traduction*]

M. Owen Larter: Il y en a dans une panoplie de secteurs. Nous utilisons nous-mêmes de nombreuses applications, comme Windows Hello sur nos appareils Microsoft. Si quelqu'un a un appareil Surface ou Windows, Windows Hello y joue un grand rôle.

Mais de façon générale, il y a beaucoup d'applications de sécurité et de vérification, qui intéressent particulièrement le secteur bancaire et le domaine de l'aviation. À titre d'exemple, nous connaissons des banques australiennes qui envisagent d'utiliser la reconnaissance faciale pour que les gens utilisent les guichets automatiques sans numéro d'identification personnel, ne s'identifiant qu'avec leur visage pour effectuer un retrait.

Cette technologie a de nombreuses applications, qui tendent à être dans les domaines de la vérification et de la sécurité pour accorder l'accès à des appareils et à autre chose.

[*Français*]

M. René Villemure: Merci beaucoup.

[*Traduction*]

Le président: Sur ce, nous accorderons la parole à M. Green pour six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Ma première question, que je poserai par votre entremise, monsieur le président, s'adresse à M. Larter.

Monsieur Larter, je vais vous mitrailler de questions. Quand vous m'entendez dire « merci », c'est parce que je reprends la parole pour passer à la prochaine question. Ne le prenez pas comme un affront personnel, mais je vais devoir poser mes questions rapidement.

J'ai entendu dire aujourd'hui que vous n'avez pas interdit l'utilisation de la technologie de reconnaissance faciale dans le domaine de l'exécution de la loi au Canada. Avec quels organismes de l'armée, de la police et du domaine de l'exécution de la loi avez-vous conclu des contrats, par le passé et actuellement?

M. Owen Larter: Au Canada?

M. Matthew Green: Oui.

M. Owen Larter: Je ne pense pas que nous en ayons à l'heure actuelle, mais je veux m'assurer de fournir une réponse juste à votre question, donc...

M. Matthew Green: Monsieur Larter, avez-vous eu des contrats avec la GRC?

M. Owen Larter: Je devrai le vérifier. Dans le domaine de la reconnaissance faciale, je ne le pense pas, mais je devrai m'en assurer.

M. Matthew Green: Monsieur Larter, rappelons que vous êtes directeur des politiques publiques au bureau de l'intelligence artificielle de Microsoft. Si vous aviez conclu des contrats avec des organismes d'exécution de la loi au Canada, se seraient-ils retrouvés sur votre bureau de directeur? Auriez-vous été informé de ces contrats? Auriez-vous été appelé à les autoriser et à les signer?

M. Owen Larter: Oui. Je n'aurais pas eu à les autoriser et à les signer, mais nous en aurions certainement discuté au sein de l'entreprise, notamment au bureau de l'intelligence artificielle responsable, qui serait probablement intervenu dans le processus, mais...

M. Matthew Green: Je vous remercie beaucoup.

Dans votre allocution, vous avez indiqué que vous avez eu des contrats; la reconnaissance faciale n'est donc pas interdite au Canada, car je pense que vous avez affirmé que nous disposons de lois suffisantes et d'un cadre plus solide que celui des États-Unis. Je vais maintenant vous donner l'occasion d'expliquer, à titre de directeur des politiques publiques, quelles parties de nos lois en matière de protection de la vie privée, comme la Loi sur la protection des renseignements personnels et les documents électroniques, justifient l'utilisation de la reconnaissance faciale, advenant que vous concluiez des contrats avec des organismes d'exécution de la loi, l'armée et d'autres organismes, comme il en a été question.

M. Owen Larter: Je pense que certaines mesures entrent en jeu ici, notamment les mesures de protection internes dont j'ai parlé, comme le processus d'examen de l'utilisation responsable. Le déploiement de la technologie chez le genre de clients dont vous parlez aurait fait l'objet d'un tel processus pour veiller à ce que...

M. Matthew Green: Il s'agit de mesures internes à Microsoft?

M. Owen Larter: [*Inaudible*]

M. Matthew Green: Oui, mais il en irait de même aux États-Unis, n'est-ce pas?

M. Owen Larter: Oui, exactement. C'est...

M. Matthew Green: Pourquoi la différence de politique, alors?

M. Owen Larter: C'est parce que nous procédons au cas par cas. Au Canada, nous examinerions chaque déploiement pour nous assurer que tout est fait dans les règles de l'art. Je dirais...

M. Matthew Green: Pourtant, monsieur Larter, vous avez interdit cette technologie dans un marché de la taille des États-Unis. Vous attendez l'instauration d'un cadre de réglementation. Or, notre comité a été formé parce que notre pays n'aurait pas de cadre de réglementation, comme nous l'avons entendu dire dans de précédents témoignages.

Je vous demande, vous qui êtes directeur des politiques publiques d'intelligence artificielle chez Microsoft, pourquoi la norme diffère entre notre marché et celui des États-Unis.

● (1610)

M. Owen Larter: C'est une question importante, mais nous ne pensons pas que la norme diffère.

Si nous témoignons aujourd'hui, c'est parce que nous voulons jouer un rôle de participant dans la création de la reconnaissance faciale en général. Nous considérons qu'il existe une réelle occasion dans ce domaine au Canada. Selon nous, les États-Unis n'ont pas de cadre général de protection de la vie privée, ce qui pose un problème au chapitre de la protection des droits de la personne qui...

M. Matthew Green: Monsieur Larter, je vais reprendre la parole. Je vous remercie de cette explication. Je vous encourage à écouter le reste des témoignages, car vous pourriez découvrir que dans les faits, nos cadres actuels ne sont pas adéquats au Canada.

Sur ce, je tournerai mon attention vers nos amis du Conseil national des musulmans canadiens et M. Mohammad, qui a, selon moi, soulevé des points fort pertinents dans son allocution d'ouverture.

Monsieur, votre site Web indique que vous avez reçu des centaines de plaintes en matière de droits de la personne de la part de membres du public qui considèrent avoir fait l'objet de discrimination. Au cours de mes questions précédentes, j'ai établi un lien entre l'utilisation de la reconnaissance faciale et le profilage racial, les contrôles de routine et d'autres mesures. À votre avis, cette technologie est-elle utilisée comme méthode de profilage racial?

M. Rizwan Mohammad: Je voudrais inviter notre président-directeur général à répondre à votre question.

M. Matthew Green: Bien sûr. Nous disposons de deux minutes, et j'ai d'autres questions à poser.

M. Mustafa Farooq: Je vous remercie beaucoup.

Je pense qu'en réalité, la réponse est oui, je pense qu'il est fort probable que ce soit le cas.

Le fait est que nous recevons tout le temps des appels — dont les gens n'entendent pas parler — de personnes qui font l'objet de surveillance de la part du Service canadien du renseignement de sécurité ou de la GRC, en raison des problèmes qui en découlent. En réalité, cette technologie est utilisée dans l'ensemble du secteur. Nous savons déjà que l'Agence des services frontaliers du Canada a procédé à un projet pilote dans les aéroports pour mettre à l'essai une technologie appelée AVATAR, qui était censée être une sorte de détecteur de mensonges. Cette technologie qui a été utilisée est interdite dans d'autres pays, soit dit en passant. Nous nous préoccupons vivement de la manière dont elle peut être exploitée comme une arme afin d'établir le profil des gens pour terrorisme potentiel.

M. Matthew Green: Vu la nature de vos efforts de défense des droits de la personne au sein de la communauté, votre organisation a-t-elle reçu des plaintes en matière de droits de la personne ayant un lien avec la technologie artificielle, y compris la reconnaissance faciale?

M. Mustafa Farooq: Pas jusqu'à maintenant, mais je pense que c'est dû en bonne partie au fait que les gens ne savent pas nécessairement qu'ils sont captés avec ce genre de technologies. Nous avons parfois vent de préoccupations au sujet de gens qui assistent à des rassemblements pacifiques, que ce soit à Vancouver, à Hamilton ou ailleurs, où les organismes d'exécution de la loi prennent des photos. On ne connaît pas toujours l'usage qui est fait de ces données, mais si nous ne recevons pas de plaintes, c'est en grande partie en raison d'un manque de divulgation.

M. Matthew Green: Si je me souviens bien, beaucoup de travail a été accompli au sein de la communauté concernant les listes de personnes interdites de vol et le ciblage de profils et de noms aux consonances musulmanes. Parfois, des enfants d'à peine 6 ou 8 mois sont inscrits sur ces listes et ne peuvent prendre l'avion.

Selon vous, le gouvernement pourrait-il utiliser subrepticement cette technologie pour commettre les mêmes genres d'actes ciblés de discrimination et de profilage racial envers votre communauté?

M. Mustafa Farooq: Absolument.

M. Matthew Green: Je vous remercie beaucoup.

Je vous remercie, monsieur le président.

Le président: Je vous remercie. Vous ne lui avez laissé que deux ou trois secondes pour répondre, mais nous avons eu le temps d'entendre sa réponse.

Sur ce, nous passerons à la prochaine intervention de cinq minutes. C'est M. Kurek qui a la parole.

M. Damien Kurek (Battle River—Crowfoot, PCC): Je vous remercie beaucoup, monsieur le président. Je remercie également nos témoins de comparaître aujourd'hui.

Permettez-moi de commencer, comme je le fais souvent, en invitant les témoins à fournir des documents supplémentaires au Comité s'ils n'ont pas l'occasion de fournir des réponses exhaustives au cours de la séance d'aujourd'hui. Ces documents seraient certainement les bienvenus et nous aideraient.

Monsieur Larter, à titre d'exemple pour préparer le terrain en vue de ma question, lorsque les caméras ont été initialement créées, les produits chimiques utilisés étaient expressément conçus pour capter le visage de personnes blanches, de façon générale. J'ai fait quelques lectures et vu certains documents indiquant que c'était le cas. Il y a donc des limites techniques dans le domaine de la reconnaissance faciale.

Je me demande si vous pourriez nous indiquer si Microsoft en a tenu compte dans le développement de sa technologie de reconnaissance faciale et nous expliquer les implications que ces limites pourraient avoir sur le plan des différentes races, des divers genres, etc.

M. Owen Larter: C'est une question vraiment importante. Je vous remercie donc de l'avoir posée.

Comme je l'ai indiqué, je considère qu'un des principaux risques qu'il faut prévenir avec la réglementation est celui de l'utilisation discriminatoire potentielle de la technologie de reconnaissance faciale. Au cours du développement de notre technologie, nous avons pris grand soin d'avoir un ensemble de données représentatif afin de mettre au point la technologie pour qu'elle fonctionne adéquatement, y compris entre les divers groupes démographiques.

Nous dirions que c'est à cet égard que les mises à l'essai sont très importantes et qu'il ne faut pas tout bonnement nous croire sur parole. Selon nous, il importe que les vendeurs fassent tester la technologie de reconnaissance faciale par un tiers indépendant et raisonnable, comme je l'ai indiqué, pour vérifier ce que font les entreprises qui vendent la technologie de reconnaissance faciale au chapitre des algorithmes. Je pense que ce genre de surveillance est cruciale afin d'élever la barre...

● (1615)

M. Damien Kurek: Je vous remercie. Comme M. Green, je ferais remarquer que nous disposons de peu de temps. En une trentaine de secondes, pourriez-vous expliquer au Comité la relation entre la reconnaissance faciale et l'intelligence artificielle?

M. Owen Larter: Oui, volontiers. L'intelligence artificielle englobe un large éventail de systèmes, dont la reconnaissance faciale fait partie. La reconnaissance faciale est un type de technologie qui peut effectuer une observation ou une reconnaissance comme le ferait un humain. Nous considérerions la reconnaissance faciale comme un genre d'intelligence artificielle, aux côtés d'autres systèmes d'intelligence artificielle.

M. Damien Kurek: Je vous remercie beaucoup.

Je m'adresserai maintenant à nos amis du Conseil national des musulmans canadiens. Nous vous avons entendus dire qu'il fallait modifier la Loi sur la Gendarmerie royale du Canada. Est-il nécessaire, selon vous, de modifier d'autres lois pour résoudre certains des problèmes, comme celui du profilage racial?

M. Mustafa Farooq: Il conviendrait d'examiner la Loi sur le Service canadien du renseignement de sécurité également.

M. Damien Kurek: Bien sûr.

M. Mustafa Farooq: Je pense qu'en réalité, on ne sait toujours pas — et à ce que je sache, le Comité ne s'est pas fait dire— si le Service canadien du renseignement de sécurité utilise la reconnaissance faciale. Les Canadiens méritent d'avoir une réponse à cette question. Selon les réponses reçues, on pourrait envisager l'imposition de sanctions en cas de non-divulgation.

M. Damien Kurek: Notre comité a évidemment passé beaucoup de temps à examiner les implications pour le gouvernement. Je serais toutefois curieux de savoir si vous avez d'autres réflexions au sujet des implications privées. Je présume que nous utilisons probablement tous la technologie de reconnaissance faciale pour accéder à nos téléphones et à autre chose. Nous utilisons déjà un peu la technologie de reconnaissance faciale, en un certain sens.

Auriez-vous des observations à formuler sur les implications non seulement publiques, mais aussi privées de l'utilisation de cette technologie, que ce soit sur des appareils électroniques personnels ou autre chose, comme dans des magasins et des lieux de ce genre?

M. Mustafa Farooq: Nous ne sommes malheureusement pas des experts pour pouvoir dire quelles seraient les implications pour un consommateur ou une entreprise. Sachez toutefois que notre communauté se préoccupe fort de la manière dont les grandes entreprises technologiques recueillent ces données, les utilisent, les vendent et pourraient potentiellement les donner à des régimes autoritaires. Je ne fais pas référence à une entreprise technologique en particulier, mais ce sont certainement des préoccupations que nous entendons de la part de notre communauté.

M. Damien Kurek: Je sais que mon temps est presque écoulé; je vous poserai donc peut-être simplement la question suivante. Vous avez proposé d'instaurer des balises judiciaires. Si vous pouviez fournir au Comité plus d'information sur ce que vous considérez comme une balise judiciaire appropriée pour l'application de la technologie de reconnaissance faciale, par exemple, dans le contexte de l'exécution de la loi, notre comité vous en saurait gré. Je vous remercie beaucoup.

Sur cette dernière remarque, mon temps est écoulé. Je remercie les témoins.

Le président: Je vous remercie.

Nous accordons maintenant la parole à M. Bains pour cinq minutes.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Je vous remercie, monsieur le président. Je remercie également les témoins qui se joignent à nous aujourd'hui.

Ma question s'adresse au représentant du Conseil national des musulmans canadiens.

Des témoins ont affirmé au Comité que des organismes d'exécution de la loi utilisent la technologie de reconnaissance faciale. Vous avez également indiqué au cours de votre témoignage que ces technologies sont utilisées à Vancouver ou dans d'autres régions du pays lors de rassemblements ou d'autres activités où les gens se réunissent. Quelqu'un a fait savoir que la police de Vancouver les utilisait également en Colombie-Britannique.

La question éveille ma curiosité. À ce que vous sachiez, dans quelle mesure ces organismes utilisent-ils la technologie? J'aurai ensuite une question de suivi.

● (1620)

M. Mustafa Farooq: Je ne voudrais pas parler au nom d'un organisme en particulier. À ma connaissance, la police de Vancouver a imposé un moratoire sur la technologie de reconnaissance faciale après avoir reçu des plaintes sur son utilisation.

Toutefois, nous savons que ce n'est pas une règle universelle. Une personne a beau dire qu'elle fait quelque chose, on continue toujours à se demander si elle tient sa parole.

M. Parm Bains: Je vous remercie.

Des autorités policières canadiennes ont-elles engagé un dialogue avec vous au sujet de la technologie de reconnaissance faciale?

M. Mustafa Farooq: Seulement très accessoirement.

M. Parm Bains: Avez-vous présenté des observations ou des recommandations pour améliorer l'encadrement juridique de la technologie d'intelligence artificielle au Canada?

M. Mustafa Farooq: Votre comité est le seul groupe auquel nous avons présenté officiellement des recommandations, mises à part des réserves que nous avons émises au sujet de la réglementation relative aux préjudices en ligne et au rôle de l'intelligence artificielle dans ce dossier.

M. Parm Bains: Y a-t-il une raison pour laquelle vous n'avez pas été en mesure d'engager un dialogue avec les organismes? Avez-vous tenté de communiquer avec eux?

M. Mustafa Farooq: Pour le dire simplement, c'est très difficile d'engager un dialogue en l'absence de données fondamentales.

Comme le SCRS refuse de répondre à une question fondamentale — une question à laquelle il n'a pas répondu non plus pour le Comité —, à savoir s'il utilise la technologie de reconnaissance faciale, c'est très difficile de croire en la reddition de comptes. C'est aussi très difficile d'avoir une discussion. De plus, comme la GRC ne tient pas les mêmes propos selon qu'elle s'adresse à la population canadienne, au commissaire à la protection de la vie privée ou à notre organisation, c'est très difficile d'avoir une discussion franche et de bonne foi sur ce à quoi pourrait ressembler l'avenir.

Je pense que nous souhaitons tous un avenir où les organismes d'application de la loi utilisent la technologie de reconnaissance faciale de manière responsable. Les gens ont raison d'affirmer que cette technologie peut être utilisée à de bonnes fins, surtout dans des domaines comme la lutte contre la pornographie juvénile. La réalité, c'est que les organismes canadiens ne répondent pas aux attentes de la population, pour toutes les raisons que vous connaissez, qui sont liées au racisme systémique et à nombre d'autres difficultés.

M. Parm Bains: Je vous remercie.

Si le temps le permet, j'ai une petite question pour M. Larter.

Plusieurs témoins ont soulevé des préoccupations à l'égard du fait qu'il a été démontré que la technologie de reconnaissance faciale peut entraîner plus d'erreurs d'identification pour les personnes racialisées que pour les personnes blanches. Ce sujet a été abordé ici à plusieurs reprises. Quelles mesures votre organisation prend-elle pour réduire ce risque?

M. Owen Larter: C'est une question très importante et un des risques majeurs posés par l'utilisation de la technologie de reconnaissance faciale qu'il faut s'employer à éliminer.

Je vais revenir sur les mesures de protection internes dont nous avons déjà parlé. Les mises à l'essai comptent parmi les plus importantes. Nous soumettons notre système de reconnaissance faciale à des essais réalisés par des tiers indépendants afin de nous assurer qu'il est bien mis au point, qu'il n'entraîne pas d'erreurs et qu'il réduit les écarts entre les divers groupes démographiques.

Je tiens absolument à insister sur le fait que les mises à l'essai sont essentielles pour éviter les erreurs commises par la technologie. La technologie peut fonctionner adéquatement. Les meilleurs algorithmes ont énormément évolué au cours des dernières années, mais nombre d'algorithmes laissent à désirer. Il faut les mettre à l'essai pour s'assurer, par exemple, que les services de police qui y ont recours utilisent les meilleurs systèmes qui soient.

Le président: Je vous remercie.

M. Parm Bains: Merci. Me reste-t-il du temps?

Le président: J'ai bien peur que non, monsieur Bains.

Nous passons maintenant à M. Villemure. Vous disposez de deux minutes et demie.

[*Français*]

M. René Villemure: Monsieur Larter, je vais me tourner de nouveau vers vous. Puisque nous ne disposons que de deux minutes et demie, soyons prompts.

Pour Microsoft, qu'est-ce qui constitue de la surveillance?

[*Traduction*]

M. Owen Larter: Je dirais que la surveillance, c'est l'action d'observer des personnes ou des groupes.

[*Français*]

M. René Villemure: Est-ce avec ou sans leur consentement?

[*Traduction*]

M. Owen Larter: Cela pourrait être sans leur consentement, ce qui poserait problème. Cela pourrait aussi être avec leur consentement. De façon générale, quand on pense à la surveillance, on suppose qu'elle est faite sans le consentement des personnes surveillées.

[*Français*]

M. René Villemure: Lorsque l'on sait que, parfois, la reconnaissance faciale peut indiquer — ce ne sont pas toutes les études qui le soutiennent — les préférences politiques ou sexuelles d'une personne, d'une certaine façon, on peut dire qu'il n'y a plus de liberté possible. Nous sommes surveillés en tout temps.

● (1625)

[*Traduction*]

M. Owen Larter: À mon avis, ces préoccupations sont fondées, et des mesures doivent être prises à leur égard. Je le répète, c'est la raison pour laquelle nous recommandons la mise en place de réglementation.

Nous avons des doutes quant à la validité de certaines affirmations sur ce que la reconnaissance faciale peut faire — par exemple, deviner les préférences politiques d'une personne à partir de sa seule apparence —, d'où l'importance d'avoir une discussion sur la mise en place de réglementation stipulant quelles utilisations sont autorisées et, surtout, lesquelles ne le sont pas.

[*Français*]

M. René Villemure: Devant l'absence de réglementation au Canada, pour le moment, est-ce que Microsoft est sous contrat avec une agence gouvernementale canadienne, une agence de sécurité, de surveillance ou de renseignement, actuellement?

[*Traduction*]

M. Owen Larter: Avez-vous demandé si Google ou Microsoft... Désolé.

[*Français*]

M. René Villemure: Je parle de Microsoft, évidemment.

[*Traduction*]

Mr. Owen Larter: Pas à ma connaissance, non. Pas pour des services de reconnaissance faciale au Canada.

[*Français*]

M. René Villemure: Vous ne travaillez donc avec aucune agence gouvernementale, aucune agence de sécurité, aucune organisation militaire ni aucune agence de surveillance.

[*Traduction*]

M. Owen Larter: Non, pas à ma connaissance.

[*Français*]

M. René Villemure: Faites-vous le commerce de données? Je parle à la fois de l'achat et de la vente de celles-ci.

[*Traduction*]

M. Owen Larter: Pas dans le domaine de la reconnaissance faciale. Nous ne vendons pas les données utilisées dans nos systèmes de reconnaissance faciale. Voilà ma réponse.

[*Français*]

M. René Villemure: Je vous remercie.

[*Traduction*]

Le président: Merci.

Le prochain intervenant sera M. Green; il disposera de deux minutes et demie. Je précise qu'il y aura une autre série de questions après. Nous passerons une heure complète avec les témoins.

Monsieur Green, la parole est à vous. Vous disposez de deux minutes et demie.

M. Matthew Green: Je vous remercie.

Monsieur le président, je veux m'assurer que la demande que j'ai faite à M. Larter est parfaitement claire.

Monsieur Larter, je vous demande de nous fournir, aux fins de notre étude, une liste de l'ensemble des contrats, actuels et passés, que vous avez conclus avec les organismes canadiens de sécurité publique — les organismes du gouvernement, de l'armée, du domaine de l'application de la loi et de la police —, étant donné que vous n'avez pas été en mesure de fournir ces renseignements au Comité aujourd'hui. Comprenez-vous la demande?

M. Owen Larter: Oui. À ma connaissance, nous n'avons conclu aucun contrat de cette nature, mais je comprends la demande.

M. Matthew Green: Merci beaucoup. Je vous en suis reconnaissant.

Je m'adresse maintenant à M. Farooq, par l'entremise de la présidence. Monsieur Farooq, durant votre déclaration préliminaire, je crois que vous avez parlé de modifications législatives. Ma perception de l'état actuel de la réglementation au Canada repose sur les témoignages que nous avons reçus d'autres invités. J'aimerais savoir si votre mémoire contient des recommandations précises quant aux mesures à prendre pour resserrer notre cadre réglementaire afin que nous ayons connaissance de l'utilisation, que des comptes soient rendus par rapport à l'utilisation et que la technologie soit utilisée en conformité avec les droits garantis par la Charte.

Pouvez-vous nous fournir plus de détails sur les améliorations législatives que vous recommandez?

M. Mustafa Farooq: Certainement. Je vous remercie pour cette question très importante.

Nous fournirons plus de détails dans notre mémoire, mais ce que je dirais en premier lieu, de façon générale, c'est qu'il faut interdire l'utilisation de la technologie de reconnaissance faciale en temps réel dans des endroits comme les aéroports et les postes frontaliers.

En ce qui concerne les outils d'enquête, nous demandons l'imposition d'un moratoire jusqu'à la mise en place des politiques. À notre avis, le processus devrait ressembler de près à celui que la police doit suivre pour obtenir tout mandat de perquisition: elle doit se présenter devant un juge et lui soumettre son argumentaire, un scénario idéal et des documents clairs; ensuite, le tout est rendu public. Nous fournirons des détails sur les dispositions particulières que nous recommandons de modifier.

M. Matthew Green: Merci beaucoup, monsieur le président, et merci aux témoins.

Le président: Je vous remercie.

Nous passons maintenant à M. Bezan. Vous disposez de cinq minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Je vous remercie, monsieur le président, et je m'excuse de ne pas être avec vous en personne aujourd'hui. Je suis aux prises avec une inondation dans ma circonscription et dans ma propre cour.

Mes premières questions s'adressent à MM. Farooq et Mohammad. Je veux creuser encore plus pour être certain de n'oublier aucune mesure législative dans notre examen de la réglementation.

Vous avez déjà mentionné le SCRS et la GRC. Vous avez aussi parlé des modifications qu'il faudra apporter au Code criminel, ainsi qu'à la Loi sur la protection des renseignements personnels et à la Loi sur la protection des renseignements personnels et les documents électroniques. Je sais que dans le domaine de la défense nationale, le CST surveille principalement les messages envoyés en ligne. Le CST a peut-être la formule qu'il nous faut, car il ne peut pas utiliser des moyens détournés pour faire ce qu'il n'a pas le droit de faire par des moyens directs, comme surveiller tout citoyen canadien ou tout allié du Groupe des cinq. Il doit obtenir des mandats ou des autorisations ministérielles pour toute question liée à la sécurité et à la défense nationales.

Nous recommandez-vous de prendre les mêmes mesures pour protéger les droits des Canadiens garantis par la Charte?

● (1630)

M. Mustafa Farooq: D'abord, nous espérons tous que vous allez bien, vous, vos voisins et tous les autres.

M. James Bezan: Je peux vous dire qu'il y a beaucoup d'eau autour d'ici.

M. Mustafa Farooq: De façon générale, si la question est de savoir si nous sommes d'avis que, sur le plan législatif, les critères à remplir pour obtenir un mandat dans le cadre d'enquêtes devraient être les mêmes pour la technologie de reconnaissance faciale, je dirais qu'il y a quelques nuances à apporter. Globalement, la réponse est oui, il devrait y avoir une procédure judiciaire...

M. James Bezan: Quelles sont les nuances, alors?

M. Mustafa Farooq: Les nuances se rapportent principalement à l'article 8, qui concerne les fouilles, les perquisitions et les saisies. Des éléments de preuve seraient présentés à un juge. C'est là que le processus commencerait.

M. James Bezan: Des témoins nous ont dit que de nombreux organismes canadiens d'application de la loi utilisaient la technologie de reconnaissance faciale de Clearview AI, y compris la GRC et l'ASFC. Ce n'est plus le cas aujourd'hui puisque Clearview dit ne plus offrir ce service aux organismes canadiens.

Connaissez-vous IntelCenter Check? Cette entreprise a aussi de la technologie de reconnaissance faciale, et j'ai l'impression qu'elle a peut-être conclu des contrats avec la GRC et le SCRS.

M. Mustafa Farooq: J'ai seulement connaissance de ce qui est public, des renseignements qui ont été publiés à son sujet. Je n'ai pas de connaissances particulières.

M. James Bezan: Nous parlons de l'équilibre des pouvoirs. Il faut d'abord veiller à protéger les droits garantis par la Charte en modifiant les différentes lois contenant des dispositions pertinentes. Comme nombre de mes collègues l'ont mentionné, la question se résume aux préjugés intégrés à la technologie: étant donné que la technologie de reconnaissance faciale a été mise au point en employant des visages blancs, elle commet beaucoup plus d'erreurs dans le cas des visages bruns et des visages noirs. Diverses sociétés du renseignement ont suggéré que les services de police accroissent le rôle de l'intervention humaine dans le processus.

Cette solution répondrait-elle aux préoccupations de votre communauté et d'autres au Canada?

M. Mustafa Farooq: Me demandez-vous si une plus grande intervention humaine aiderait à régler les problèmes liés à la technologie de reconnaissance faciale? Ai-je bien compris votre question?

M. James Bezan: C'est ce que je vous demande. Toute désignation de personne d'intérêt par la technologie de reconnaissance faciale et l'intelligence artificielle ferait l'objet d'une vérification humaine.

M. Mustafa Farooq: Sauf votre respect, je ne crois pas que ce serait suffisant.

Certes, les vérifications humaines sont importantes, mais nous savons aussi qu'il y a un problème de racisme et de préjugés systémiques au sein des services de police. Je ne pense pas qu'il suffirait de procéder à des vérifications humaines. À notre avis, les tribunaux sont l'endroit indiqué pour assurer l'équilibre des pouvoirs, avec de l'information claire. Dans quelle mesure tel organisme a-t-il recours à la technologie de reconnaissance faciale? Comment les données sont-elles stockées? Les délais de destruction des données devraient aussi être fournis aux parlementaires. Nous trouvons cela très important.

Le président: Je vous remercie.

Nous passons maintenant à Mme Khalid. Vous disposez de cinq minutes.

● (1635)

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Je vous remercie, monsieur le président. Ma première question s'adresse à M. Larter.

Monsieur Larter, le CNMC a proposé aujourd'hui qu'un moratoire soit imposé sur la technologie de reconnaissance faciale. Quelle est l'opinion de votre organisation par rapport à l'imposition d'un moratoire à l'égard des utilisations non commerciales de la technologie de reconnaissance faciale?

M. Owen Larter: Nous sommes convaincus qu'il faut mettre en place de la réglementation, comme nous l'avons recommandé aujourd'hui. Nous vous conseillons d'investir du temps et des ressources dans l'élaboration de la réglementation. Comme il faut beaucoup de temps et d'investissements pour faire avancer toute initiative, nous vous conseillons de mettre l'accent sur la mise en place de la réglementation, en commençant par les utilisations faites par les organismes d'application de la loi.

De plus, nous recommandons l'adoption d'une approche progressive à l'égard de la réglementation dans ce domaine. La technologie évolue rapidement; elle s'est nettement améliorée au cours des dernières années. Plutôt que d'investir du temps et des efforts dans l'imposition d'un moratoire, nous vous recommandons de commencer par réglementer les utilisations faites par les organismes d'application de la loi, car nous considérons ce besoin comme étant le plus pressant. C'est ce que nous suggérons.

Mme Iqra Khalid: Je vous remercie.

Monsieur Farooq, êtes-vous d'accord avec M. Larter?

M. Mustafa Farooq: Sauf le respect que je lui dois, je pense que nous sommes en désaccord là-dessus.

Compte tenu des risques posés par la technologie de reconnaissance faciale pour la population canadienne, et étant donné l'absence regrettable de réponses adéquates de la part des organismes canadiens d'application de la loi, nous sommes d'avis qu'un moratoire est la mesure qui s'impose dans le contexte non commercial. D'autres témoins que vous avez reçus ont pris la même position. C'est ce que nous recommandons jusqu'à la mise en place de réglementation sur la protection des renseignements personnels et tout le reste.

Mme Iqra Khalid: Je vous remercie.

Vous avez expliqué à quel point il est difficile d'obtenir une réponse ouverte et transparente de la part de tous les ordres d'organismes d'application de la loi. D'après vous, quelles mesures précises devraient être prises pour instaurer un moratoire et le faire respecter?

M. Mustafa Farooq: Je pense qu'il y a plusieurs mesures à prendre. Bien entendu, il faudrait probablement apporter des modifications réglementaires ou législatives.

Nous serions ravis de vous fournir une réponse plus détaillée dans notre mémoire, y compris des formulations précises des modifications législatives proposées.

Mme Iqra Khalid: Merci, je vous en serais reconnaissante.

Monsieur Larter, votre entreprise fait des affaires partout dans le monde. À votre connaissance, y a-t-il des États qui utilisent la technologie de reconnaissance faciale pour surveiller sa population?

M. Owen Larter: Je suis désolé, les lumières dans la pièce se sont éteintes. J'espère que vous me voyez et que vous m'entendez toujours bien.

Je suis sûr que plusieurs pays, en particulier des pays non démocratiques, utilisent la technologie de reconnaissance faciale pour surveiller sa population; ils emploient probablement des moyens qu'aucun d'entre nous ne trouverait acceptables. Nous ne fournissons pas de services qui soutiennent ce type de surveillance.

Mme Iqra Khalid: Nous aimerions, si vous le pouvez, que vous nommiez certains de ces pays et que vous nous disiez comment ils exercent cette surveillance exactement.

Deuxièmement, vous êtes très favorable à la réglementation des technologies de reconnaissance faciale. Selon vous, y a-t-il dans le monde un régime de réglementation que le Canada devrait adopter pour s'assurer que les technologies de reconnaissance faciale sont utilisées à bon escient, non seulement dans le secteur non commercial, mais aussi dans le secteur commercial?

M. Owen Larter: Oui. Je pense qu'il y a eu des avancées positives aux États-Unis, au niveau des États.

J'aimerais notamment attirer l'attention du Comité sur l'État de Washington où une loi entrée en vigueur en juillet dernier comprend d'importantes mesures de transparence et de reddition de comptes. Elle prévoit les mises à l'essai dont j'ai parlé et aussi une surveillance humaine avant la prise de décision, ce qui est très important, de façon à s'assurer que tout résultat du système fait l'objet d'une analyse par un humain ayant reçu une formation adéquate à cette fin.

Le modèle de l'État de Washington est certainement un modèle qu'il convient d'étudier.

Mme Iqra Khalid: Monsieur le président, combien de temps me reste-t-il?

Le président: Vous avez 25 secondes.

Mme Iqra Khalid: Dans ce cas, je vais donner avis de la motion suivante:

> Que, nonobstant les motions adoptées par le Comité le 13 décembre 2021 et le 31 janvier 2022 concernant les réunions régulières prévues du comité concernant la production de rapports ce printemps, compte tenu des questions importantes soulevées au cours de nos délibérations sur les technologies de reconnaissance faciale, que le Comité prolonge ses audiences sur l'étude sur la reconnaissance facile de trois réunions et que le Comité entreprenne l'étude d'un rapport en septembre 2022.

● (1640)

Le président: Merci, madame Khalid.

Encore une fois, je pense que cette motion était mise en avis, comme d'autres motions dont nous avons reçu avis aujourd'hui. Je vous remercie.

Cela dit, nous passons maintenant à M. Villemure, pour deux minutes et demie.

[*Français*]

M. René Villemure: Merci, monsieur le président.

Je vais encore une fois m'adresser à M. Larter, de Microsoft.

Monsieur Larter, vous excuserez ma pugnacité, mais ce que vous faites m'intéresse beaucoup.

Est-il possible que des entités criminelles, une puissance étrangère ou une quelconque tierce partie puissent infiltrer et falsifier des données obtenues à l'aide de l'intelligence artificielle?

[*Traduction*]

M. Owen Larter: C'est une bonne question.

Je pense que la technologie en général doit assurément s'accompagner de mesures de cybersécurité robustes. Microsoft fait d'importants investissements sur ce plan pour sécuriser sa gamme de technologies et protéger la clientèle. De toute évidence, il existe des menaces dont nous devons tous être conscients pour veiller à ce que la technologie soit développée et utilisée...

[*Français*]

M. René Villemure: À votre connaissance, y a-t-il déjà eu de tels bris de sécurité dans les technologies de Microsoft quelque part dans le monde?

[*Traduction*]

M. Owen Larter: Je me concentre davantage sur les systèmes d'intelligence artificielle et leur utilisation responsable. Donc, la question s'éloigne quelque peu de mon domaine d'expertise. Toutefois, je pense que la menace d'acteurs malveillants existe toujours. Par conséquent, j'estime que réagir de façon énergique en faisant d'importants investissements, comme nous le faisons, est la bonne chose à faire.

Je crains de ne pouvoir vous donner une réponse plus précise, car la question est hors de mon domaine d'expertise.

[*Français*]

M. René Villemure: Merci beaucoup.

Si vous pouviez nous fournir cette information en consultant vos collègues, nous vous en serions reconnaissants.

Quelles seraient, selon vous, les limites à ne pas franchir en matière de reconnaissance faciale?

[*Traduction*]

M. Owen Larter: Je pense que c'est une question fondamentale dans cette discussion sur la réglementation. Je pense qu'il est très important de déterminer ce qui est une utilisation autorisée et ce qui ne l'est pas.

Nous avons des suggestions à cet égard. Nous sommes d'avis que la surveillance de masse systématique ne devrait pas être autorisée. Nous pensons aussi que toute discrimination fondée sur la race, le sexe, l'orientation sexuelle ou d'autres caractéristiques protégées devrait être interdite.

En outre, la question des libertés démocratiques, dont nous avons discuté aujourd'hui, est très importante, et je suis heureux de constater qu'elle fait partie de la discussion. Il faut aussi veiller à ce que l'utilisation de la technologie ne porte pas atteinte aux libertés fondamentales comme la liberté de réunion. Voilà quelques principes de base que nous suggérons.

Plus particulièrement dans le contexte de l'application de la loi, nous considérons qu'il est important que les résultats de la reconnaissance faciale ne soient pas le seul motif ou le seul élément de preuve dans la prise de décisions importantes, notamment les arrestations.

Le président: Je dois passer au prochain intervenant; nous avons largement dépassé le temps imparti à M. Villemure.

Pour les dernières questions, nous avons M. Green.

M. Matthew Green: Merci, monsieur le président.

Je pense que dans sa série de questions, Mme Khalid a soulevé un point très important concernant la création d'un cadre juridique, et c'est ce que j'appellerai « l'obligation de franchise » des organismes de sécurité, des services de police, des forces armées et de l'ASFC quant à l'utilisation de ces technologies.

Par votre intermédiaire, monsieur le président, j'aimerais attirer l'attention de M. Farooq sur un reportage du *Globe and Mail* datant du 31 août 2021 dans lequel on indique que la cour a encore une fois semoncé le SCRS concernant son obligation de franchise. On mentionne aussi d'autres violations liées aux méthodes du SCRS pour obtenir des mandats et surveiller subrepticement des Canadiens, ce qui est illégal, pour parler franchement.

La question est pour M. Farooq, monsieur le président, par votre intermédiaire. Selon votre expérience, dans votre travail de défense des droits — puisque nous parlons maintenant de l'aspect humain de l'utilisation de cet outil —, pourriez-vous parler de cas où nos organismes de sécurité nationale et de sécurité publique pourraient avoir manqué de franchise quant à la surveillance des membres de la communauté musulmane?

M. Mustafa Farooq: Bien sûr. Je pense que le cas le plus probant — et le plus pertinent pour le Comité — est une décision du juge Gleeson de la Cour fédérale, il y a environ un an et demi. Dans une décision stupéfiante, le juge Gleeson a taillé le SCRS en pièces, essentiellement, pour son habitude persistante d'essayer d'induire la cour en erreur. La plupart d'entre nous se souviennent de cette phrase, mais chez les avocats, nous appelons cela une « violation de l'obligation de franchise ». Cette habitude n'a pas seulement été relevée par le juge Gleeson, mais aussi par le juge Mosley dans une série de décisions à la Cour fédérale.

Le directeur du SCRS, David Vigneault, a fini par admettre qu'il y avait peut-être eu des problèmes, mais étonnamment — et je pense que nous avons clairement indiqué notre position à ce sujet — et malheureusement, ce gouvernement a choisi de porter cette décision en appel. La cause est toujours en instance. Je pense que la question demeure donc de savoir quelles mesures seront prises pour obliger les organismes de sécurité nationale à rendre des comptes lorsqu'elles induisent les gens en erreur.

● (1645)

M. Matthew Green: Merci.

Par votre intermédiaire, monsieur le président, j'aimerais savoir si M. Farooq est d'avis que toute réflexion sur la réglementation des aspects techniques de ces technologies doit également porter sur la mise en place de cadres connexes et d'un cadre d'éthique pour le gouvernement et les organismes d'application de la loi afin d'assurer la conformité et une transparence totale dans l'utilisation de ces outils?

Le président: Veuillez répondre très brièvement.

M. Mustafa Farooq: Je suis désolé. Pourriez-vous répéter la question?

M. Matthew Green: Toute réflexion sur la réglementation de la technologie, dans le contexte du présent rapport, devrait porter aussi sur un cadre de conformité, de surveillance et de reddition de comptes pour les intervenants humains, y compris nos organismes d'application de la loi et les services policiers, en particulier pour assurer le respect de l'obligation de franchise.

M. Mustafa Farooq: Oui, tout à fait.

M. Matthew Green: Merci beaucoup.

Je n'ai pas d'autres questions.

Le président: Merci beaucoup.

Je remercie tous nos témoins d'aujourd'hui.

Sur ce, je vais suspendre la séance. Nous reprendrons à huis clos.

Je demanderais à nos témoins de quitter la salle assez rapidement. Je vous remercie. Nous reprendrons à huis clos sous peu.

La séance est suspendue.

[*La séance se poursuit à huis clos.*]