CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

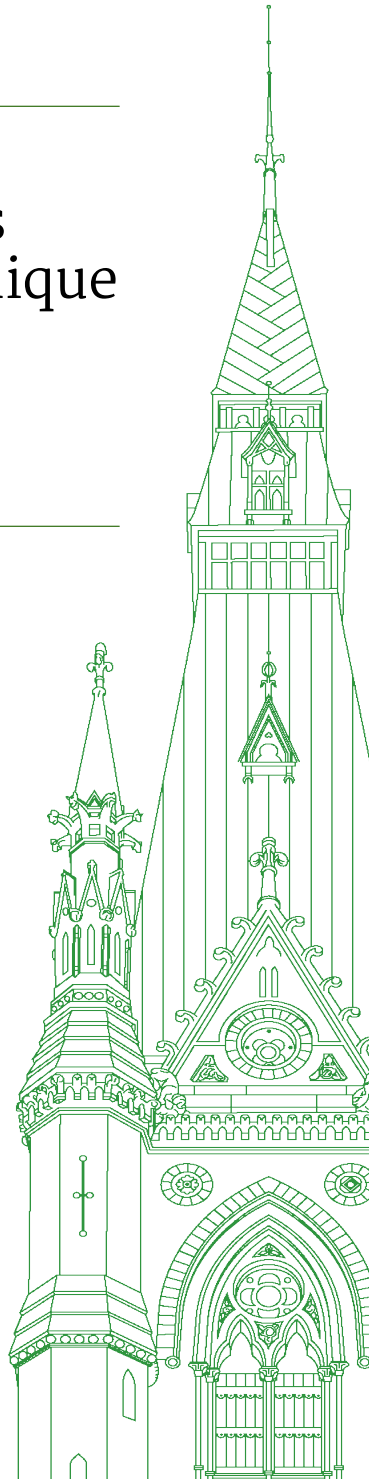
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 012

Le jeudi 24 mars 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 24 mars 2022

● (1530)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): Bienvenue à la 12e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Conformément à l'alinéa 108(3)h) du Règlement et à la motion adoptée par le Comité le lundi 13 décembre 2021, le Comité poursuit son étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale.

La réunion d'aujourd'hui se tient suivant une formule hybride, conformément à l'ordre de la Chambre adopté par le 25 novembre 2021. Des députés sont présents sur place et d'autres participent à distance au moyen de l'application Zoom. Sachez que la diffusion Web montrera toujours la personne qui parle, et non l'ensemble du Comité.

Je rappelle aux députés qui sont dans la salle que les règles habituelles de santé publique continuent de s'appliquer. Comme vous les avez entendues à plusieurs reprises, je ne vais pas les répéter, mais je vous invite néanmoins à les respecter.

Je vous rappelle également que vous ne pouvez pas faire de capture d'écran ni de photo de votre écran. Quand vous avez la parole, ralentissez le débit et articulez bien pour que les interprètes puissent vous suivre. Si vous n'avez pas la parole, mettez votre microphone en sourdine. Enfin, je demanderais aux députés et aux témoins de toujours s'adresser à la présidence.

J'aimerais maintenant souhaiter la bienvenue à nos témoins d'aujourd'hui. Nous recevons Mme Alex LaPlante, directrice principale, Engagement produit et commercial, de Borealis AI. Nous accueillons également Mme Brenda McPhail, directrice du Programme de la vie privée, de technologie et de surveillance au sein de l'Association canadienne des libertés civiles. Il y a ensuite M. Françoys Labonté, président-directeur général du Centre de recherche informatique de Montréal. Enfin, nous accueillons M. Tim McSorley, coordinateur national de la Coalition pour la surveillance internationale des libertés civiles.

Avant de céder la parole aux témoins, pour la gouverne des membres du Comité, j'ai décidé de réunir les témoins en seul groupe afin de réduire le plus possible le temps que nous perdons à passer d'un groupe à l'autre. Nous suivrons l'ordre habituel pour les séries de questions, et il y aura des tours supplémentaires, si le temps le permet, selon la formule prescrite pour l'ordre et la durée des interventions.

Sur ce, je donne la parole à nos premiers témoins, de Borealis AI.

Madame LaPlante, allez-y.

Mme Alex LaPlante (directrice principale, Engagement produit et commercial, Borealis AI): Je vous remercie, monsieur le président.

Je tiens à remercier le Comité de m'avoir invitée à témoigner au sujet de l'utilisation et des impacts de la technologie de reconnaissance faciale.

Je m'appelle donc Alex LaPlante. J'occupe le poste de directrice principale chez Borealis AI, qui est le laboratoire de recherche et de développement de RBC pour l'intelligence artificielle. Les opinions que je m'apprête à exprimer aujourd'hui n'engagent que moi et ne reflètent pas le point de vue de Borealis AI, de RBC ou de toute autre institution à laquelle je suis affiliée.

J'ai passé les 15 dernières années à élaborer et à mettre en œuvre des solutions d'analyse avancée et d'intelligence artificielle à des fins universitaires et commerciales, et j'ai vu les résultats positifs que l'intelligence artificielle peut produire. Toutefois, je suis également très consciente d'une chose: si nous ne prenons pas soin d'évaluer correctement l'application, le développement et la gouvernance de l'intelligence artificielle, celle-ci peut avoir des effets négatifs sur les utilisateurs finaux, perpétuer et même amplifier la discrimination et les préjugés envers les communautés racisées et les femmes, et conduire à une utilisation non éthique des données et à des atteintes au droit à la vie privée.

Je me concentrerai principalement sur deux aspects: d'abord, la protection des données et, ensuite, la qualité des données et la performance algorithmique. Je conclurai en faisant des recommandations sur la gouvernance de cette technologie.

Les données biométriques font partie des données les plus sensibles qui existent. Le respect de la vie privée est donc primordial quand vient le temps de les recueillir, de les utiliser et de les entreposer en toute sécurité. Or, dans plusieurs cas, des données biométriques ont été recueillies et utilisées sans le consentement des personnes ou à leur insu. Songeons notamment à Clearview AI, qui a bafoué le droit à la vie privée des gens en mettant ces derniers à la merci de systèmes d'intelligence artificielle non réglementés et non validés. Cette situation est particulièrement préoccupante dans les cas d'utilisation à haut risque comme l'identification des criminels. Il y a également eu des cas de détournement d'usage, c'est-à-dire lorsque des entreprises obtiennent le consentement pour recueillir des données biométriques pour un usage particulier, mais qu'elles les utilisent ensuite à d'autres fins que celles initialement prévues.

Les meilleurs systèmes de reconnaissance faciale peuvent atteindre des taux de précision de 99,9 % et donner des résultats uniformes auprès de tous les groupes démographiques. Cependant, tous les algorithmes ne sont pas égaux et, dans certains cas, les taux de faux positifs peuvent varier par des facteurs de 10 jusqu'à même 100 pour les populations racisées et les femmes. Cet écart au chapitre de la performance est directement lié au manque de données représentatives et de haute qualité.

Parmi les domaines de recherche en matière d'intelligence artificielle, il y en a un qui mérite d'être souligné dans le contexte de la technologie de reconnaissance faciale: la robustesse antagoniste. C'est la pierre angulaire de pratiques comme le camouflage, c'est-à-dire des procédés qui visent à déjouer les technologies de reconnaissance faciale. Cela peut se faire par des manipulations physiques comme l'obscurcissement des traits du visage ou, de façon plus discrète, par des modifications apportées aux photos de visages, modifications qui sont indiscernables à l'œil humain, mais qui font en sorte que les photos ne sont plus identifiables.

Les organismes d'application de la loi au Canada et à l'étranger ont utilisé des technologies fondées sur des données non vérifiées, extraites du Web, qui peuvent être facilement manipulées de manière indétectable, sans aucun accès direct aux données sources. En l'absence d'une surveillance et d'une réglementation appropriées, ces entreprises peuvent facilement manipuler leurs données pour définir qui peut ou ne peut pas être identifié au moyen de leurs systèmes.

Au-delà des problèmes de qualité des données, la technologie de reconnaissance faciale, comme tout système d'intelligence artificielle à haut risque, devrait faire l'objet d'une validation approfondie afin que ses limites soient bien comprises et prises en compte lorsqu'elle est transposée dans le monde réel. Malheureusement, bon nombre des outils de reconnaissance faciale qui se trouvent sur le marché aujourd'hui sont de véritables boîtes noires et ne se prêtent pas à la validation ou à la vérification.

Bien que mes observations portent surtout sur les risques de la technologie de reconnaissance faciale, je crois tout de même que cette technologie est d'une grande valeur. Nous devons élaborer avec soin des règlements qui permettront d'utiliser la technologie de reconnaissance faciale en toute sécurité dans divers contextes et qui comblent les principales lacunes dans la législation canadienne, en plus de remédier aux préoccupations concernant les droits de la personne et la protection de la vie privée. Dans le cadre de mon travail dans le secteur financier, qui est hautement réglementé, j'ai participé à la gouvernance efficace de systèmes d'intelligence artificielle à haut risque, et il s'agit d'évaluer et d'étayer de manière exhaustive des questions comme la protection de la vie privée, l'utilisation, les répercussions et la validation algorithmique. Selon moi, des approches similaires peuvent répondre à bon nombre des principales préoccupations que soulève cette technologie.

Les règlements doivent fournir aux développeurs, aux personnes chargées de la mise en œuvre et aux utilisateurs de la technologie de reconnaissance faciale des exigences et obligations claires concernant les utilisations précises de cette technologie. Cela devrait comprendre l'obligation d'obtenir un consentement explicite pour la collecte et l'utilisation de données biométriques, ainsi que la limitation de la finalité pour éviter le détournement d'usage. Les mesures législatives sur la technologie de reconnaissance faciale devraient s'appuyer sur les principes de nécessité et de proportionnalité en matière de protection de la vie privée, notamment dans le contexte des pratiques portant atteinte à la vie privée.

En outre, les exigences en matière de gouvernance doivent être proportionnelles à l'importance du risque. Les évaluations d'impact devraient être une pratique courante, et il devrait y avoir une surveillance contextuelle de questions comme la robustesse et la sécurité techniques, la protection de la vie privée et la gouvernance des données, la non-discrimination, l'équité et la responsabilisation. Cette surveillance ne devrait pas s'arrêter une fois qu'un système est en production, mais plutôt se poursuivre pendant toute la durée de vie du système, ce qui nécessite un suivi, des tests et une validation réguliers de la performance.

Enfin, il faut des cadres de responsabilisation plus clairs pour les développeurs et les utilisateurs finaux de la technologie de reconnaissance faciale, ce qui exigera une formulation législative transparente du poids des droits de la personne par rapport aux intérêts commerciaux.

Cela dit, ces règlements devraient chercher à adopter une approche équilibrée qui réduit, dans la mesure possible, les charges administratives et financières pour les entités publiques et privées.

● (1535)

Merci beaucoup. J'ai hâte de répondre à vos questions.

Le président: Merci beaucoup.

Nous passons maintenant à Mme McPhail pour un maximum de cinq minutes.

Mme Brenda McPhail (directrice, Programme de la vie privée, de technologie et de surveillance, Association canadienne des libertés civiles): Je remercie le président et le Comité d'avoir invité l'Association canadienne des libertés civiles à comparaître devant vous aujourd'hui.

La reconnaissance faciale — ou l'empreinte faciale, comme nous l'appelons souvent au sein de notre association, pour faire un parallèle avec un autre identificateur biométrique de nature sensible — est une technologie controversée. Dans le cadre de cette étude, vous entendrez des témoignages qui vantent ses avantages potentiels et d'autres qui mettent en garde contre les conséquences désastreuses pour la société, conséquences qui pourraient découler de certains cas d'utilisation, en particulier dans le contexte du maintien de l'ordre et de la sécurité publique. Les deux côtés du débat sont valables, ce qui rend votre travail en l'occurrence particulièrement difficile et extrêmement important. Je vous suis reconnaissante d'avoir entrepris cette étude.

L'Association canadienne des libertés civiles examine cette technologie sous l'angle des droits. Cette optique révèle que ce ne sont pas seulement les droits individuels et collectifs à la vie privée qui sont menacés par les diverses utilisations de la technologie de surveillance et d'analyse du visage dans les secteurs public et privé, mais aussi un large éventail d'autres droits. Je sais que vous avez entendu parler, dans des témoignages précédents, du grave risque pour les droits à l'égalité que présentent les versions défectueuses de cette technologie qui fonctionnent moins bien sur les visages noirs, bruns, autochtones, asiatiques, féminins ou jeunes — en somme, les visages non blancs et non masculins.

J'ajouterais à cette discussion la mise en garde suivante: si la technologie est corrigée et si elle devient plus précise pour tous les visages, quel que soit le sexe ou la race, elle risque de devenir encore plus dangereuse. Pourquoi? Parce que nous savons que, dans le contexte des forces de l'ordre, ces mêmes personnes sont surveillées de manière disproportionnée. Nous savons qui est souvent victime de discrimination dans les applications du secteur privé. Là encore, ce sont ces mêmes personnes. Dans les deux cas, une identification parfaite de ces groupes ou des membres de ces groupes, qui subissent déjà une discrimination systémique en raison de leur apparence, risque de faciliter des actes discriminatoires plus parfaitement ciblés.

Outre les droits à l'égalité, les outils permettant une identification omniprésente auraient des répercussions négatives sur toute une série de droits protégés par la Charte canadienne des droits et libertés et d'autres lois, notamment la liberté d'association et de réunion, la liberté d'expression, le droit à la protection contre les fouilles, les perquisitions et les saisies abusives par l'État, la présomption d'innocence — si le visage de chacun, comme dans le cas de la technologie de Clearview AI, est soumis à une séance d'identification perpétuelle — et, enfin, les droits à la liberté et à la sécurité de la personne. Les enjeux sont donc énormes.

Il est également important de comprendre que cette technologie s'insinue dans la vie quotidienne d'une manière qui devient banale. Nous ne devons pas permettre à cette familiarité croissante d'engendrer un sentiment d'inévitabilité. Par exemple, beaucoup d'entre nous déverrouillent probablement leur téléphone à l'aide de leur visage. C'est pratique et, moyennant les bonnes protections intégrées, une telle fonctionnalité peut comporter relativement peu de risques pour la vie privée. D'ailleurs, le Parti libéral du Canada a récemment utilisé un outil similaire de reconnaissance faciale à correspondance biunivoque dans le cadre de son processus de vote pour l'investiture avant les dernières élections fédérales. En l'occurrence, il s'agissait d'une utilisation beaucoup plus risquée d'une technologie potentiellement défectueuse et discriminatoire, car c'était dans le contexte d'un processus qui est au cœur de la démocratie populaire.

La même fonctionnalité, utilisée dans des contextes très différents, soulève des risques différents. Voilà qui fait ressortir la nécessité d'accorder une attention particulière non seulement aux protections techniques de la vie privée, comme dans les exemples du téléphone et de l'application de vote, mais aussi aux protections contextuelles pertinentes pour l'ensemble des droits mis en cause par cette technologie.

Quelle est la voie à suivre? J'espère que cette étude examinera si — et pas seulement quand et comment — la reconnaissance faciale peut être utilisée au Canada, en tenant compte de ces questions contextuelles. L'Association canadienne des libertés civiles croit, comme la témoin précédente, qu'une réglementation s'impose pour les utilisations que les Canadiens jugent, en fin de compte, appropriées dans un État démocratique libre et équitable.

La reconnaissance faciale à des fins de surveillance de masse devrait être interdite. En ce qui concerne les utilisations plus ciblées, l'Association canadienne des libertés civiles continue, pour l'instant, à réclamer un moratoire, surtout dans le contexte policier, en l'absence d'une mesure législative complète et efficace qui fournit un cadre juridique clair pour son utilisation, qui contient des dispositions rigoureuses en matière de responsabilisation et de transparence, qui exige une surveillance indépendante et qui prévoit des mesures de coercition efficaces en cas de non-respect.

Il faut une loi intersectorielle sur la protection des données, qui s'appuie globalement sur le cadre des droits de la personne, surtout parce que les secteurs public et privé utilisent les mêmes technologies, mais sont actuellement soumis à des exigences juridiques différentes. Mieux encore, des lois ciblées régissant la biométrie ou les technologies algorithmiques à forte intensité de données pourraient être encore plus adaptées aux besoins. Il existe plusieurs exemples de pays où de telles mesures législatives ont été adoptées récemment ou sont à l'étude. Nous devrions nous en inspirer pour créer des lois canadiennes qui mettent en place des mécanismes de protection appropriés pour assurer l'utilisation potentiellement bénéfique de la technologie de reconnaissance faciale et protéger les gens partout au Canada contre un usage impropre ou abusif.

Merci. Je me ferai un plaisir de répondre à vos questions.

● (1540)

Le président: Merci.

Monsieur Françoys Labonté, vous avez cinq minutes tout au plus. Nous vous écoutons.

[*Français*]

M. Françoys Labonté (président-directeur général, Centre de recherche informatique de Montréal): Mesdames et messieurs les députés membres du Comité, cela me fait plaisir de participer à cette importante étude.

Je commence par me présenter brièvement. Je suis Françoys Labonté, président-directeur général du CRIM, soit le Centre de recherche informatique de Montréal. J'ai une formation technique, en l'occurrence un doctorat spécialisé en vision par ordinateur de l'École polytechnique de Montréal. En 2010, je me suis joint au CRIM, pour en devenir le PDG en 2015. Le CRIM est un organisme qui travaille en intelligence artificielle depuis de nombreuses années, soit presque depuis sa création, et qui a eu l'occasion, de façon très pratique, de travailler à l'évolution des technologies de la reconnaissance de la parole dans les années 2000 et de la reconnaissance faciale dans les années 2010.

À l'image du CRIM, ma présentation se veut très pragmatique. D'entrée de jeu, il est essentiel de comprendre qu'à la base, les technologies de reconnaissance faciale ne requièrent et n'impliquent aucun renseignement personnel. Ces technologies se limitent à indiquer si une nouvelle image d'un visage qui n'a jamais été présentée auparavant à un système correspond à un visage qui a déjà été présenté à ce système.

Dans le contexte de votre étude, je comprends qu'on désire déterminer dans quel contexte il est acceptable ou non d'associer des renseignements personnels à un visage et de permettre ainsi d'identifier un individu à partir d'une ou de plusieurs images de son visage. Un des grands défis auxquels votre comité fait face est de trouver un juste équilibre entre les préoccupations relatives au respect de la vie privée, l'acceptation sociale et les avantages pour la société.

Nous faisons face à un phénomène un peu paradoxal: pour un nombre important de Canadiens, une ou plusieurs images de leur visage auxquelles leur nom est directement associé, sans compter d'autres renseignements personnels qui peuvent parfois y être associés, se trouvent déjà dans le domaine public, que ce soit dans des réseaux sociaux, dans des médias numériques ou dans d'autres applications numériques. Souvent, ces images ont été fournies par les gens alors qu'ils avaient une utilisation précise en tête, mais ces derniers ont accepté des clauses de consentement de portée très large et des droits d'utilisation très étendus. Même si une personne fournit une image de son visage dans l'intention, par exemple, de bonifier son profil d'utilisateur dans une application numérique, en pratique, il est relativement facile pour des tierces parties d'accéder à cette image et aux autres données qui y sont associées et de les utiliser à diverses autres fins en toute impunité, tellement les consentements obtenus sont vastes. De façon pratique, il est quasi impossible de renverser cette situation et de faire disparaître d'Internet ces images, ou même de dissocier les renseignements personnels qui y sont associés.

Voici une question sur laquelle votre comité devrait se pencher: étant donné que des images du visage de la plupart des Canadiens, auxquelles sont associés leurs renseignements personnels, sont accessibles dans le domaine public, quelles utilisations de ces images impliquant la reconnaissance faciale devraient être proscrites ou strictement encadrées?

Il y a probablement un fort consensus dans la population canadienne quant à l'interdiction d'utiliser les technologies de reconnaissance faciale dans un contexte à la Big Brother, où des bases de données d'images du visage de l'ensemble des citoyens seraient utilisées et où des caméras de surveillance publique feraient des suivis arbitraires des déplacements ou des comportements des citoyens. De même, utiliser la reconnaissance faciale en conjonction avec des drones dans un contexte militaire, pour des assassinats ciblés, va certainement à l'encontre de toutes les initiatives visant à promouvoir une utilisation éthique de l'intelligence artificielle.

Je veux délibérément vous amener à voir les choses un peu différemment dans un contexte d'utilisation où les réponses sont probablement plus floues et où la technologie de reconnaissance faciale ne fait que remplacer d'autres technologies existantes ou se substituer à celles-ci.

Prenons l'exemple de l'utilisation de la reconnaissance faciale pour des personnes qui se trouvent dans un commerce de détail ou un centre commercial. On peut facilement faire un parallèle avec le commerce en ligne, qui, sans nécessairement faire l'unanimité, jouit tout de même d'une grande acceptation sociale. Lorsqu'on magasine en ligne d'une façon qu'on qualifie d'anonyme, c'est-à-dire en n'étant pas connecté au moyen d'un compte d'utilisateur, des témoins de connexion laissent quand même des traces de notre passage sur le Web. Ces traces sont par la suite utilisées pour nous pousser de la publicité ciblée en fonction de nos préférences. Cela est-il très différent d'un système de reconnaissance faciale dans un centre commercial qui, sans connaître explicitement votre identité, pourrait, en fonction d'éléments pouvant facilement être inférés à partir de votre visage ou de vos comportements, vous pousser de la publicité ciblée?

● (1545)

Toujours dans la même logique, quand on magasine en ligne, mais cette fois-ci au moyen d'un compte d'utilisateur pour lequel on fournit des informations...

[*Traduction*]

Le président: Je vais devoir vous demander de conclure très rapidement. Vous avez déjà un peu dépassé votre temps.

[*Français*]

M. Françoys Labonté: D'accord.

De façon générale, je pense que les gens se font une idée favorable de l'utilisation des technologies de reconnaissance faciale pour des applications ciblées et clairement balisées, lorsqu'il est facile de comprendre à quelles fins les données sont utilisées et de voir les avantages qui en découlent.

Toutefois, il reste d'énormes défis à relever pour bâtir la confiance du public et le convaincre que la technologie de reconnaissance faciale et les images seront effectivement utilisées uniquement à des fins qui respectent ce qui a été accepté initialement.

Merci.

[*Traduction*]

Le président: Sur ce, nous allons entendre Tim McSorley, qui fera la dernière déclaration préliminaire avant que nous passions aux questions des députés.

Allez-y, monsieur McSorley.

● (1550)

M. Tim McSorley (coordinateur national, Coalition pour la surveillance internationale des libertés civiles): Monsieur le président, mesdames et messieurs les membres du Comité, merci beaucoup de m'avoir invité à comparaître devant vous aujourd'hui.

Je suis très heureux de vous parler aujourd'hui au nom de la Coalition pour la surveillance internationale des libertés civiles. Nous sommes une coalition de 45 organisations de la société civile canadienne qui se consacrent à la protection des libertés civiles au Canada et à l'étranger dans le contexte des activités canadiennes en matière de lutte contre le terrorisme et de sécurité nationale.

Compte tenu de notre mandat, nous nous intéressons particulièrement à la technologie de la reconnaissance faciale en raison de son utilisation par les organismes d'application de la loi et les services de renseignement, surtout au niveau fédéral. Nous avons fait état de l'augmentation rapide et continue de la surveillance étatique au Canada et à l'étranger au cours des deux dernières décennies. Ces activités de surveillance, qui présentent des risques importants, ont brimé les droits des gens au Canada et dans le monde.

La technologie de reconnaissance faciale est particulièrement inquiétante en raison des risques inouïs qu'elle présente pour la vie privée et parce qu'elle allie la surveillance biométrique à la surveillance algorithmique. Notre coalition a dégagé trois raisons particulières qui suscitent des inquiétudes.

Premièrement, comme l'ont souligné d'autres témoins aujourd'hui et plus tôt cette semaine, de nombreuses études ont révélé que certaines des technologies de reconnaissance faciale les plus utilisées reposent sur des algorithmes qui sont biaisés et inexacts. C'est particulièrement vrai pour les images faciales des femmes et des personnes de couleur, qui font déjà l'objet d'un degré accru de surveillance et de profilage par les organismes d'application de la loi et les services de renseignement au Canada.

Cette situation est particulièrement préoccupante dans le domaine de la sécurité nationale et de la lutte contre le terrorisme, où l'on a déjà recensé de nombreux cas de racisme systémique et de profilage racial. Une technologie inexacte ou biaisée ne fait que renforcer et aggraver ce problème, puisque les gens courent ainsi le risque d'être faussement associés au terrorisme et à des menaces pour la sécurité nationale. Comme beaucoup d'entre vous le savent, même une seule allégation de la sorte peut stigmatiser la personne accusée de façon profonde et durable.

Deuxièmement, la reconnaissance faciale permet une surveillance de masse sans discernement et sans mandat. Même si on réglait les graves problèmes de partialité et de précision, les systèmes de surveillance par reconnaissance faciale continueraient à soumettre les gens à une surveillance intrusive et sans discernement. Ce constat est vrai, que ces systèmes soient utilisés pour surveiller les voyageurs dans un aéroport, les piétons sur une place publique ou les activistes lors d'une manifestation.

Même si les forces de l'ordre doivent obligatoirement demander une autorisation judiciaire pour surveiller des individus en ligne ou dans des lieux publics, les lois actuelles comportent des lacunes puisqu'il n'est pas clair si elles s'appliquent à la surveillance ou à la désanonymisation au moyen de la technologie de reconnaissance faciale. À cause de ces lacunes, les forces de l'ordre peuvent soumettre tous les passants à une surveillance de masse injustifiée dans l'espoir de pouvoir identifier une seule personne d'intérêt, en temps réel ou après coup.

Troisièmement, il y a un manque de réglementation de la technologie et un manque de transparence et de responsabilisation de la part des organismes d'application de la loi et des services de renseignement au Canada. Le cadre juridique actuel régissant la technologie de reconnaissance faciale est tout à fait inadéquat. L'ensemble disparate de règles en matière de protection de la vie privée à l'échelle provinciale, territoriale et fédérale ne garantit pas que les forces de l'ordre utilisent la technologie de reconnaissance faciale dans le respect des droits fondamentaux. De plus, le manque de transparence et de responsabilisation signifie que cette technologie est adoptée à l'insu du public, en l'absence de débat public ou de surveillance indépendante.

Nous en avons vu des exemples patents au cours des deux dernières années.

Voici le premier exemple, et c'est aussi le plus connu: l'absence de réglementation a permis à la GRC d'utiliser le logiciel de reconnaissance faciale de Clearview AI pendant des mois à l'insu du public, puis de mentir à ce sujet avant d'être forcée d'admettre la vérité. De plus, nous savons maintenant que la GRC a utilisé une forme ou une autre de reconnaissance faciale au cours des 20 dernières années sans que le public en soit informé et sans qu'il y ait de débat ou de surveillance claire. Le commissaire à la protection de la vie privée du Canada a conclu que l'utilisation de l'outil de Clearview AI par la GRC était illégale, mais la GRC a rejeté cette conclusion, arguant qu'elle ne peut être tenue responsable de la légalité des services fournis par des tiers. Cela lui permet, en gros, de continuer à passer des contrats avec d'autres services qui enfreignent la loi canadienne.

Ce que l'on sait moins, c'est que la GRC a également passé un contrat pour l'utilisation d'un système américain privé de « reconnaissance faciale des terroristes », connu sous le nom d'IntelCenter. Cette entreprise prétend offrir un accès à des outils de reconnaissance faciale et à une base de données de plus de 700 000 images de personnes associées au terrorisme. Au dire de l'entreprise, ces images sont extraites du Web, tout comme celles de Clearview AI. La stigmatisation qui accompagne le fait d'être associé à une soi-disant base de données de reconnaissance faciale des terroristes ne fait qu'accroître les préjugés et les répercussions sur les droits qui s'y rattachent.

Comme dernier exemple, je me contenterai de dire que le Service canadien du renseignement de sécurité, ou SCRS, a refusé de confirmer s'il utilise ou non la technologie de reconnaissance faciale dans le cadre de son travail, en déclarant qu'il n'a aucune obligation de le faire.

Compte tenu de toutes ces préoccupations, nous formulons trois grandes recommandations: premièrement, que le gouvernement fédéral interdise immédiatement l'utilisation de la surveillance par reconnaissance faciale et qu'il entreprenne des consultations sur l'utilisation et la réglementation de la technologie de reconnaissance faciale en général; deuxièmement, à partir de ces consultations, que le gouvernement procède à la réforme des lois sur la protection des renseignements personnels dans les secteurs privé et public afin de combler les lacunes relatives à la reconnaissance faciale et à d'autres formes de surveillance biométrique; enfin, que le commissaire à la protection de la vie privée se voie accorder plus de pouvoirs coercitifs en ce qui concerne les violations des lois canadiennes sur la protection des renseignements personnels dans les secteurs public et privé.

● (1555)

Merci, et j'ai hâte aux discussions et aux questions.

Le président: Je remercie les témoins de leurs déclarations préliminaires.

Le premier intervenant sera M. Kurek, qui dispose de six minutes.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup.

Permettez-moi de commencer par faire une demande à tous nos témoins. Tout d'abord, je vous remercie de l'expertise et des renseignements que vous nous avez fournis aujourd'hui. C'est très précieux. Chose certaine, alors que je me préparais pour cette réunion... Je vous suis très reconnaissant d'être venus nous faire part de ces renseignements aujourd'hui. Je sais qu'un certain nombre d'entre vous ont formulé des recommandations, et cela s'avère très utile, d'un point de vue pratique, pour le travail que le Comité accomplira en prévision du rapport.

Pour en revenir à ma demande, au-delà des questions que je compte poser dans un instant, voici ce que je propose: puisque le temps est limité, si vous avez d'autres recommandations ou renseignements, n'hésitez pas à les transmettre aux membres du Comité afin que nous puissions les inclure dans le rapport que nous préparerons dans les mois à venir. Considérez cela comme une invitation ouverte, car votre expertise est d'une très grande utilité.

Madame LaPlante et monsieur McSorley, vous nous avez donné quelques exemples. Clearview AI est l'un des exemples les plus évidents.

Commençons par Mme LaPlante.

Y a-t-il d'autres exemples dont vous pourriez parler brièvement et qui mettent en évidence certains des défis posés par ces systèmes?

Mme Alex LaPlante: Clearview AI est l'un des cas les plus préoccupants. Ce qui est si inquiétant à son sujet, c'est la collecte de quantités massives de données. Ces données, qui se rapportent à l'identité des gens, sont utilisées dans des contextes où le résultat final peut être lourd de conséquences pour les individus. À mon avis, nous devons tenir compte de cet aspect lorsque nous appliquons des systèmes d'intelligence artificielle de toutes sortes dans ce genre de contextes.

Pour ce qui est des autres exemples, Facebook est un incontournable. Son programme est mis en veilleuse pour un certain temps, mais je pense que vous êtes tous bien conscients, si vous utilisez Facebook, qu'il y avait une fonction qui permettait essentiellement d'identifier au préalable un ami sur une photo. Cette fonction utilise directement les données contenues dans votre profil et toutes les photos que vous et vos amis avez publiées et balisées. Il s'agit peut-être d'un cas un peu plus inoffensif et, à certains égards, une telle fonction peut être considérée comme quelque chose d'utile ou de pratique, mais je tiens également à souligner que c'est une pente glissante parce que ces bases de données appartiennent à des sociétés privées, alors qu'il n'y a aucune réglementation ou vérification de leur utilisation.

M. Damien Kurek: Je vous remercie.

Je sais qu'il me reste peu de temps.

Monsieur McSorley, y a-t-il d'autres exemples que vous pourriez citer rapidement et qui mériteraient d'être examinés de plus près par le Comité?

M. Tim McSorley: J'insiste à nouveau sur la question d'Intel-Center, une entreprise américaine avec laquelle nous savons que la GRC a passé un contrat. Nous avons très peu d'information sur ce qu'elle a fait avec cette entreprise et avec cette base de données.

C'est la seule autre entreprise que je peux mentionner, mais elle vient amplifier les préoccupations que nous avons à l'égard de Clearview AI parce qu'elle utilise des tactiques similaires, notamment la collecte d'images en ligne et leur inclusion dans une base de données. Toutefois, elle pousse plus loin la stigmatisation en affirmant savoir que ces personnes ont des liens avec le terrorisme, sans que l'on vérifie comment elle est arrivée à cette conclusion, et ces données sont ensuite transmises aux forces de l'ordre. Il y a déjà des préjugés sans fondement qui sont associés à des gens, et voilà que les forces de l'ordre se servent de telles données pour essentiellement qualifier ces personnes de terroristes.

M. Damien Kurek: Je vous remercie.

Madame McPhail, j'ai bien aimé votre observation lorsque vous avez dit, et je vais vous paraphraser, que l'amélioration de la technologie ne résout pas vraiment le problème. C'est un message très important qu'il fallait entendre ici.

Notre travail au sein du Comité nous a permis de constater l'importance d'intégrer et de définir le consentement et de prévoir des fonctions que la population comprend bien, comme les dispositions d'adhésion et de retrait.

Aujourd'hui, à l'ère des médias sociaux et en raison de la présence de caméras presque partout, comment pouvons-nous, en tant que législateurs, protéger les Canadiens de certains des défis associés à la reconnaissance faciale et à l'intelligence artificielle dans le contexte dont nous discutons ici aujourd'hui?

Mme Brenda McPhail: Je vous remercie de cette question, qui est très importante.

Il faut partir du bon point de départ. Je suis respectueusement en désaccord avec M. Labonté. Les systèmes de reconnaissance faciale utilisent notre visage. Il s'agit de l'un des renseignements personnels les plus sensibles que nous ayons. Les visages sont reconnus dans le droit canadien comme un élément d'information permettant d'identifier une personne; ils sont donc visés par la loi.

La meilleure façon de protéger les gens au Canada contre les utilisations inappropriées de cette technologie, c'est vraiment de réfléchir à la façon dont elle doit être réglementée. Comme première étape, le Comité pourrait envisager d'examiner un exemple positif contenu dans le projet de loi proposé par le Sénat américain, le projet de loi S.3284, c'est-à-dire la loi sur l'utilisation éthique de la reconnaissance faciale, qui établirait un comité ou une commission du Congrès pour étudier et créer des lignes directrices sur l'utilisation de la technologie de reconnaissance faciale aux États-Unis.

● (1600)

M. Damien Kurek: Je n'ai presque plus de temps, alors je vous remercie beaucoup de votre réponse. Vous avez écrit un texte — et je n'entrerai pas dans les détails, faute de temps — dans lequel vous dites: « Clearview AI a quitté le marché canadien, mais son modèle d'affaires demeure. » Existe-t-il dans notre pays d'autres exemples semblables à celui de Clearview AI dont notre comité devrait avoir connaissance?

Le président: Pouvez-vous répondre en 10 ou 15 secondes, s'il vous plaît?

Mme Brenda McPhail: Je pense que pratiquement tous les fournisseurs de technologie de reconnaissance faciale du secteur privé ont un modèle similaire. J'attire votre attention sur l'enquête menée par le commissaire à la protection de la vie privée du Canada sur le centre commercial Cadillac Fairview. Cette enquête portait sur l'utilisation non consensuelle, par le secteur privé, de l'analyse d'images faciales, qui avait été jugée appropriée dans les conversations en coulisses entre une entreprise du secteur privé et ses avocats, et qui n'a été découverte qu'à la suite d'une erreur, d'une défaillance de la technologie. C'est ainsi que nous avons su ce qui se passait en coulisses. Dans ce genre de modèles, presque tous les fournisseurs de reconnaissance faciale annoncent qu'ils peuvent aider les organismes du secteur privé à exploiter les données personnelles pour améliorer leur marché, et c'est un problème.

Le président: Merci. Nous avons presque dépassé le temps imparti d'une minute entière. Je serai un peu moins impitoyable que lors de la dernière réunion en raison de la façon dont nous avons structuré celle-ci. Je demande tout de même à tous les membres du Comité d'être conscients du temps lorsqu'ils savent qu'il ne leur reste que quelques secondes et de poser leurs questions en conséquence.

Cela dit, je vous cède la parole, monsieur Fergus.

[*Français*]

L'hon. Greg Fergus (Hull—Aylmer, Lib.): Merci beaucoup, monsieur le président.

En quelque sorte, je comprends la situation de mon collègue M. Kurek. C'est un dossier très épineux et nous avons de nombreuses questions à poser aux témoins. Je dois admettre que je fais de plus en plus de recherches sur ce dossier, et chaque jour mes lectures soulèvent d'autres questions.

Tout d'abord, j'aimerais parler d'un élément que Mme LaPlante a mentionné au début, et je pense que Mme McPhail l'a soulevé aussi. Il semble que la technologie de reconnaissance faciale soit juste une partie de l'usage de l'intelligence artificielle qui nous préoccupe. Certains algorithmes vont analyser non seulement notre visage, mais également nos comportements, les choses que nous disons, notre voix et notre façon de bouger.

Pour ce qui est de la reconnaissance faciale, en tant que Canadien noir, je sais bien que nos appareils photographiques n'offrent pas la même qualité de photographie pour des gens au teint basané, pour des femmes ou pour des jeunes, comparativement aux hommes de race blanche. Il semble donc exister un problème systémique.

Êtes-vous d'accord que l'appareil photographique en soi peut porter un grand préjudice à certaines personnes parce que l'appareil n'a pas été créé pour elles?

Nous pouvons commencer par Mme LaPlante.

[*Traduction*]

Mme Alex LaPlante: Je vous remercie de votre question. C'est très intéressant, et cela met en évidence, je dirais, certains défis liés à d'autres technologies dont nous disposons. Le NIST a réalisé des études très complètes, que je vous encourage à consulter, sur les différents aspects de la performance algorithmique. Certaines de ces études portaient précisément sur les données démographiques. L'une des conclusions, c'est que la qualité des données est un facteur important de la performance algorithmique. Le NIST a également souligné que ces technologies fonctionnent généralement bien pour des choses comme les photos signalétiques. Cela s'explique notamment par le fait que les modèles de photos signalétiques sont souvent conçus de manière à tenir compte des différentes teintes de peau. C'est plus représentatif d'un visage. Si vous avez des photos qui ne saisissent pas nécessairement un individu correctement, cela se reflétera dans la performance de la technologie.

● (1605)

[*Français*]

L'hon. Greg Fergus: Monsieur Labonté, je vous remercie de votre témoignage.

Vous avez parlé de la possibilité d'atteindre un juste équilibre entre les préoccupations que ces technologies soulèvent et les avantages de leur utilisation.

Est-il vraisemblable d'atteindre cet équilibre?

M. Françoys Labonté: Bien entendu, la question du juste équilibre est subjective. Je ne sais pas si je me suis exprimé clairement. Quand je disais que les gens mettaient beaucoup de renseignements personnels dans le domaine public, je faisais allusion à un comportement sociétal. Cela ne justifie pas l'utilisation de ces renseignements à d'autres fins. Comme je l'ai dit, lorsque des applications utilisent des renseignements personnels sans consentement, il est évident que c'est problématique et qu'il ne s'agit pas d'un équilibre.

On a donné l'exemple de l'utilisation de Face ID sur un téléphone. C'est une application très contrôlée que les gens peuvent utiliser et qui comporte certains avantages, par exemple dans les aéroports. Selon mes souvenirs, bien qu'ils datent d'avant la pandémie, les gens peuvent prendre des photos de leur visage afin d'accélérer le contrôle des passeports. Il s'agit d'un contexte très contrôlé où les images sont acquises par le gouvernement dans le cadre d'un processus d'authentification des photos régi par des normes. Cela peut [*difficultés techniques*].

L'hon. Greg Fergus: Monsieur Labonté, nous ne vous entendons plus.

Je vais profiter de cette pause pour poser une dernière question à Mme McPhail.

Madame McPhail, serait-il préférable de repartir à zéro et de bannir toute utilisation de la reconnaissance faciale pour l'instant, le temps qu'on crée un cadre légal définissant pour quels usages et dans quelles circonstances la reconnaissance faciale serait appropriée?

[*Traduction*]

Le président: À titre de précision, monsieur Labonté, nous avons perdu votre audio, et M. Fergus vous a posé une autre question.

[*Français*]

L'hon. Greg Fergus: Je pense que nous avons aussi perdu Mme McPhail.

[*Traduction*]

Le président: Là, je viens aussi de perdre l'audio de l'interprétation.

Nous avons un problème de son généralisé.

Nous allons suspendre la séance en raison de difficultés techniques.

● (1605)

_____(Pause)_____

● (1610)

Le président: Nous reprenons la séance. Espérons que le problème du système Zoom soit résolu.

Je vais demander à M. Fergus de répéter sa question, et nous allons reprendre à partir de là.

[*Français*]

L'hon. Greg Fergus: Merci, monsieur le président.

Ma question s'adresse à Mme McPhail.

Madame McPhail, serait-il préférable pour l'instant de bannir toute utilisation de la reconnaissance faciale, que ce soit dans le secteur privé ou dans le secteur public, jusqu'à ce que nous puissions établir un cadre définissant l'utilisation appropriée de cette technologie? Pensez-vous que ce serait la meilleure façon de procéder?

[*Traduction*]

Mme Brenda McPhail: Oui, tout à fait. L'Association canadienne des libertés civiles a réclamé un moratoire, ce qui est semblable à une interdiction, jusqu'à ce que nous démêlions tout cela et jusqu'à ce que nous ayons justement une conversation de ce genre avec nos représentants démocratiquement élus et avec les gens partout au Canada, afin de bien analyser la situation. Cette technologie peut-elle, oui ou non, être utilisée à bon escient? Dans l'affirmative, quelles sont les mesures de protection qui s'imposent?

Ce sera une conversation longue et difficile, mais elle est absolument nécessaire. Un moratoire sur l'utilisation de cette technologie nous donnerait l'espace et le temps nécessaires pour nous engager dans cette voie de manière judicieuse, prudente et réfléchie.

Le président: Je vous remercie.

Sur ce, monsieur Fergus, votre temps est écoulé.

[*Français*]

Je cède maintenant la parole à M. Garon.

Bienvenue au Comité, monsieur Garon.

Vous disposez de six minutes.

M. Jean-Denis Garon (Mirabel, BQ): Merci beaucoup, monsieur le président.

Je suis très content que la connexion soit rétablie, car je voulais poser l'essentiel de mes questions à M. Labonté.

Monsieur Labonté, nous savons que le fait d'avoir plus d'informations nous permet souvent de prendre de meilleures décisions. Néanmoins, à plusieurs moments de notre histoire, nous avons décidé de restreindre notre capacité à aller chercher de l'information. J'ai en tête, par exemple, la question des perquisitions sans mandat. Nous avons empêché les policiers de faire des perquisitions sans mandat.

Je me demande si nous sommes, encore aujourd'hui, dans ce grand type de questionnement sociétal et si les technologies de reconnaissance faciale ont ce potentiel de mettre fin presque complètement à notre liberté réelle et à l'existence de la vie privée.

Qu'est-ce que vous en pensez?

[*Traduction*]

Le président: Monsieur Labonté, vous avez la parole.

[*Français*]

La greffière du Comité (Mme Nancy Vohl): Monsieur Labonté, est-ce que vous nous entendez?

[*Traduction*]

M. Tim McSorley: Excusez-moi. J'ai du mal à entendre les questions sur le canal d'interprétation en anglais. Je ne sais pas si d'autres personnes ont le même problème d'audio.

Le président: Merci.

Je vais demander à la greffière de vérifier rapidement si nous pouvons confirmer que la connexion est adéquate.

La séance est suspendue.

● (1610)

_____(Pause)_____

● (1615)

Le président: Nous reprenons la séance.

Je demande aux députés qui participent en mode virtuel d'indiquer, à tout moment, s'ils perdent le son afin que je sache s'il y a un problème.

Je vais laisser M. Garon recommencer du début, car je crois que personne n'a entendu sa question.

Allez-y. Vous avez six minutes.

[*Français*]

M. Jean-Denis Garon: Merci, monsieur le président.

Monsieur Labonté, je vais répéter la question que j'ai posée tout à l'heure.

Une plus grande collecte d'informations permet de prendre de bonnes décisions. Néanmoins, à certains moments de notre histoire, pour des raisons de vie privée et de droits individuels, nous avons décidé de restreindre cette collecte d'informations. À titre d'exemple, les perquisitions policières sans mandat sont maintenant interdites.

Je me demande si la possibilité est grande qu'un jour les outils de reconnaissance faciale, s'ils sont utilisés à grande échelle et incorrectement, réduisent considérablement notre liberté et notre vie privée, voire qu'ils y mettent fin. C'est une question un peu philosophique, mais j'aimerais entendre votre opinion là-dessus.

M. Françoys Labonté: La réponse est oui, je pense que c'est possible, dans le contexte où la collecte de données se fait sans le consentement des gens, sans qu'ils comprennent tout à fait à quelles fins elles sont utilisées. En fait, c'est même ce qui explique les lois récentes en matière de protection des renseignements personnels. Il s'agit de questions qui sont à l'écran radar des gens du milieu des technologies depuis très longtemps. Des règlements commencent à être mis en place, mais ces questions sont connues depuis longtemps. Effectivement, il doit y avoir des balises claires.

Il y a par contre un élément important à considérer, selon la perspective du CRIM. Le CRIM ne travaille plus sur ces technologies. Les joueurs qui ont des avantages compétitifs en ce moment, ce sont ceux qui ont collecté d'énormes quantités de données afin de procéder à l'entraînement de modèles d'intelligence artificielle. Maintenant, le commun des mortels n'a plus accès à la quantité de données nécessaire pour atteindre de hauts niveaux de performance.

Effectivement, le risque dont vous parlez est réel. C'est pourquoi il est essentiel d'encadrer la collecte de données, afin que les gens comprennent à quelles fins elles sont utilisées et puissent donner un consentement éclairé.

M. Jean-Denis Garon: On connaît des entreprises, comme Palantir, qui utilisent des technologies militaires pour faire ce qu'elles appellent de l'observation de la société.

Que pensez-vous des entreprises et des pratiques de ce genre?

● (1620)

M. Françoys Labonté: Cela revient toujours à la même question. Pour mettre au point de telles technologies, ces entreprises ont collecté plusieurs données, présumément sans le consentement éclairé des gens qui les fournissaient. C'est ce qui s'est produit, c'est une réalité. C'est ce que je disais de façon très pragmatique dans ma présentation. Maintenant, certains de ces joueurs ont des avantages compétitifs importants et non négligeables, et c'est ce qu'on veut encadrer dans l'avenir.

Que peut-on faire à ce sujet? C'est une question assez ouverte, mais très pragmatique. Si on demande à une personne aujourd'hui de redonner toutes les images qu'elle a utilisées pour créer ses modèles, ce sera un défi pour elle, parce qu'on ne peut plus retourner en arrière. C'est un peu cela, le défi. On essaie de moduler l'avenir [*difficultés techniques*].

M. Jean-Denis Garon: Monsieur Labonté, vous avez parlé de gens qui n'ont pas consenti à fournir leurs données. On parle de technologies très complexes dont on ne connaît pas les tenants et aboutissants. On ne connaît pas les algorithmes.

Est-il possible pour un citoyen normal de consentir à fournir, en toute connaissance de cause, ses données à de telles entreprises?

M. Françoys Labonté: Généralement, les gens ne consentent pas à laisser leurs données à une entreprise pour qu'elle en fasse ce que bon lui semblera. Par exemple, s'il est important pour une personne que les gens la suivent dans les réseaux sociaux, elle va consentir à rendre son visage disponible à cette fin uniquement, mais elle ne consentira pas à ce que de tierces parties l'utilisent pour faire du profilage ou concevoir des produits commerciaux.

Ce volet est mis en évidence dans les règlements en cours de préparation ou entrés en vigueur récemment, mais il est encore très difficile de donner un consentement éclairé. Au CRIM, en tant que centre de recherche, quand nous travaillons sur des projets avec un comité d'éthique et que nous demandons un consentement à des sujets, il s'agit d'un consentement très précis, clair, à une fin donnée et souvent pour une période limitée.

Dans le monde dans lequel nous vivons, à la vitesse où vont les choses, il est difficile pour le moment de donner un consentement éclairé. Par exemple, quand les gens téléchargent une application, ils ne lisent même pas le texte de consentement qui l'accompagne ou ne comprennent pas ce que cela implique.

Effectivement, consentir de façon éclairée...

Le président: Merci, monsieur Labonté.

Monsieur Green, je vous cède la parole pour six minutes.

[*Traduction*]

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

Bienvenue à tous les invités.

Monsieur McSorley, dans mes recherches préliminaires sur la fragilité et les incohérences de la technologie de reconnaissance faciale, j'ai constaté qu'on la qualifiait de phrénologie des temps modernes. Luke Stark compare la reconnaissance faciale au plutonium de l'intelligence artificielle. Il affirme que:

> [...] les technologies de reconnaissance faciale, de par leur mode de fonctionnement d'un point de vue technique, ont des défauts insurmontables liés à la façon dont elles schématisent les visages humains. Ces défauts créent et renforcent des catégorisations discréditées fondées sur le sexe et la race, ce qui a des effets toxiques sur le plan social. Le deuxième [point], c'est qu'à la lumière de ces défauts fondamentaux, les risques de ces technologies dépassent largement les avantages, d'une manière qui n'est pas sans nous rappeler le danger des technologies nucléaires.

On utilise cette métaphore pour dire que ces technologies, « par le simple fait de leur conception et de leur construction, sont intrinsèquement toxiques sur le plan social, quelles que soient les intentions de leurs créateurs ».

En juillet 2020, la Coalition pour la surveillance internationale des libertés civiles a cosigné une lettre avec OpenMedia pour demander au gouvernement fédéral d'interdire aux organismes fédéraux de renseignement et d'application de la loi de recourir à la surveillance par reconnaissance faciale.

Par votre entremise, monsieur le président, j'aimerais poser la question suivante à M. McSorley: compte tenu des incohérences, de la fragilité et du capitalisme de surveillance des tiers...

● (1625)

Le président: Je vais vous interrompre un instant.

M. Matthew Green: J'étais sur une lancée.

Le président: Oui.

Il vous reste 4 minutes et 19 secondes lorsque vous reprendrez la parole, mais ai-je entendu un rappel au Règlement, une question ou une préoccupation concernant l'audio?

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Oui, merci, monsieur le président. Nous avons perdu le son pendant un bout de temps, alors j'ai manqué environ 30 secondes de l'intervention de M. Green.

Je suis désolée, monsieur Green, de vous avoir interrompu.

M. Matthew Green: Je ne vais pas recommencer, mais je demanderai simplement à M. McSorley de me dire, en levant le pouce, s'il m'entend bien maintenant. C'est parfait.

Je voudrais lui demander, par votre entremise, monsieur le président, s'il peut nous en dire plus sur les dangers que présente l'utilisation de technologies d'intelligence artificielle, comme la reconnaissance faciale, par des organismes de renseignement nationaux comme le SCRS et la GRC à des fins de surveillance de masse. Permettez-moi de donner un point de référence précis: en mai 2021, notre propre ministère de la Défense nationale — notre armée — a utilisé des technologies pour surveiller discrètement le mouvement Black Lives Matter.

M. McSorley aimerait peut-être se prononcer sur une telle utilisation et sur les dangers que j'ai mentionnés au début de mon intervention.

M. Tim McSorley: Nous serions tout à fait d'accord avec votre description des dangers que présente la technologie de reconnaissance faciale. Une inquiétude en amène toujours une autre.

Comme d'autres témoins l'ont mentionné aujourd'hui, en particulier Mme McPhail, la précision de la technologie amène un problème après l'autre. En l'absence d'une réglementation appropriée et en ayant autant d'entreprises qui proposent leur technologie aux organismes d'application de la loi, on se demande s'ils utiliseront la technologie la plus précise, ou s'ils utiliseront la plus accessible, celle qui est davantage ciblée et commercialisée pour les organismes d'application de la loi. Il y a en outre toute la question du recours par les organismes d'application de la loi et de renseignement à des entrepreneurs externes et de la manière dont cela se déroule, le manque de transparence à cet égard, et les problèmes de partialité et de précision de la technologie qui peut leur être proposée.

Même si ces problèmes devaient être résolus, comme cela a été mentionné, le ciblage des communautés de couleur est déjà bien connu. Ce problème ne peut pas être résolu simplement en améliorant la technologie, mais plutôt, comme l'a dit Mme McPhail, cela peut même l'exacerber, parce que tout à coup, on dispose de cet outil formidable pour mieux surveiller les populations qui font déjà l'objet d'une surveillance excessive par la police. Il faut être extrêmement...

M. Matthew Green: Si je peux me permettre, monsieur McSorley, par votre entremise, monsieur le président, étant donné que le Comité entend constamment dire, notamment dans le cadre de son étude, que le gouvernement et les services de sécurité et de renseignement ont tendance à faire indirectement ce qu'ils ne peuvent pas faire directement. J'aimerais donc creuser la question, parce que dans la lettre que vous avez cosignée, il y avait un appel à des réformes de la Loi sur la protection des renseignements personnels et des documents électroniques.

D'après vos recherches, quels types de réformes sont nécessaires pour protéger les droits de la personne et la vie privée au Canada et s'assurer que les entrepreneurs externes ne font pas indirectement ce que le gouvernement ne peut pas faire directement?

M. Tim McSorley: Tout d'abord, nous avons besoin de lois sur la protection des renseignements personnels dans le secteur privé qui sont basées sur les droits de la personne, qui sont basées clairement sur la proportionnalité et la nécessité, qui contiennent des règles claires sur le consentement, qui prévoient la surveillance et la réglementation de l'intelligence artificielle utilisée par le secteur privé, et qui prévoient également des règlements rigoureux, sinon des interdictions — cela doit être étudié plus à fond — sur l'utilisation par les organismes d'application de la loi et de sécurité nationale de tiers externes et d'entrepreneurs privés pour mener les activités qu'ils ne peuvent pas faire eux-mêmes.

Par exemple, comme je l'ai mentionné plus tôt, la GRC a contesté le fait d'avoir à vérifier la légalité des services fournis par des entrepreneurs externes. Si le principal organisme fédéral d'application de la loi du pays dit qu'il peut utiliser une technologie jugée illégale et que ce n'est pas son problème, en autant de mots, nous avons un sérieux problème. Il faut que cela soit réglé dans les lois du secteur privé tout comme dans celles du secteur public, car les lois du secteur privé actuelles permettent la communication de renseignements du secteur privé au secteur public dans l'application de la loi en raison d'exceptions relatives à la sécurité nationale.

Il faut que cela soit au cœur de la réforme des lois canadiennes sur la protection des renseignements personnels dans le secteur privé.

● (1630)

M. Matthew Green: Je vous remercie.

Le président: Monsieur Williams, vous avez cinq minutes.

M. Ryan Williams (Baie de Quinte, PCC): Je vous remercie beaucoup, monsieur le président.

Je remercie aussi tous les témoins.

Je vais poursuivre avec M. McSorley.

En juin 2021, vous avez demandé au ministre de la Sécurité publique de préparer une proposition claire pour assurer une surveillance indépendante des outils de reconnaissance faciale et d'intelligence artificielle utilisés par les services de police. D'après vous, quelle forme devrait prendre cette surveillance indépendante?

M. Tim McSorley: Tout d'abord, nous pensons que nous avons besoin d'une consultation plus large pour décider quelles sont les utilisations interdites. Comme nous l'avons dit, nous pensons que l'utilisation de la reconnaissance faciale pour la surveillance de masse en ferait clairement partie. Outre cela, il faut une surveillance pour s'assurer que lorsque les organismes d'application de la loi et les services de renseignement adoptent de nouvelles technologies, elles sont examinées au préalable, avant d'être mises en place, afin de s'assurer qu'elles respectent les normes établies par les lois canadiennes en matière de protection des renseignements personnels.

À l'heure actuelle, il revient essentiellement aux organismes d'application de la loi eux-mêmes, comme nous l'avons vu pour le choix de Clearview AI, de prendre ces décisions. Il n'était pas clair si le ministre savait dans quelle mesure la GRC utilisait la technologie de reconnaissance faciale de Clearview AI. Ce qui est inquiétant, c'est que cette technologie est adoptée sans aucune forme de surveillance politique ou autre.

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement entreprend actuellement un examen de l'utilisation de la surveillance biométrique par les organismes de sécurité nationale du Canada, mais cela pourrait prendre, encore une fois, quelques années avant que le tout soit rendu public. Nous avons besoin que le ministre agisse dès maintenant afin de s'assurer que les organismes d'application de la loi n'adoptent pas ces technologies en secret et qu'ils disent publiquement, dans le cadre des évaluations des facteurs relatifs à la vie privée, quelles seront, selon eux, les répercussions sur la vie privée, et il faut qu'il y ait un débat clair et approfondi sur la question.

M. Ryan Williams: Votre organisme a fait parvenir une lettre ouverte au ministre en 2020. Avez-vous reçu une réponse de sa part?

M. Tim McSorley: Nous avons eu une conversation de suivi avec le directeur des politiques du cabinet du ministre, mais il s'agissait davantage d'une séance d'écoute que d'une déclaration claire sur les mesures que prendrait le ministre. La seule nouvelle information que nous avons obtenue est que l'Agence des services frontaliers du Canada n'utilisait pas la reconnaissance faciale en temps réel à ce moment-là. On n'a rien pu nous dire sur l'utilisation de cette technologie par le SCRS, et il n'y a pas eu d'engagement clair de la part du cabinet du ministre à propos d'autres mesures à venir.

M. Ryan Williams: Est-il vrai qu'en réponse à certaines des conclusions du commissaire à la protection de la vie privée, la GRC a accepté de procéder à des évaluations des facteurs relatifs à la vie privée pour les outils provenant de tiers qui établiraient une nouvelle fonction de surveillance de la nouvelle technologie; et si c'est le cas, a-t-elle été mise en place de manière à pouvoir protéger les droits des Canadiens?

M. Tim McSorley: C'est une bonne question.

Nous savons que la GRC s'est engagée à apporter des améliorations à ses politiques, même si elle a rejeté la conclusion générale selon laquelle elle est responsable de la légalité de la technologie d'un tiers. Nous n'avons encore rien vu de publié à ce sujet et, en fait, cela illustre l'un des problèmes que nous constatons actuellement: en théorie, les organismes fédéraux doivent procéder à des évaluations des facteurs relatifs à la vie privée avant de mettre en place de nouvelles technologies ou de nouveaux projets ayant une incidence sur la vie privée, mais ces évaluations ne sont souvent pas effectuées du tout. Si elles sont faites, elles peuvent être tenues secrètes. Un résumé est censé être présenté, mais souvent, surtout dans le cas des organismes chargés de l'application de la loi et du renseignement, ces évaluations ne sont pas présentées, parce qu'elles pourraient avoir des répercussions sur leurs activités. Nous pensons toutefois qu'il faut exercer des pressions pour obtenir un plus grand degré de transparence et de responsabilisation.

M. Ryan Williams: D'accord.

Vous avez déjà répondu en bonne partie à ma prochaine question, mais je veux vous donner l'occasion d'étoffer votre réponse, si vous le souhaitez. Votre troisième recommandation dans la lettre était l'établissement de politiques et de lois claires et transparentes concernant l'utilisation de la reconnaissance faciale.

À quoi ressembleraient ces politiques et ces lois, et quelles réformes, selon vous, serait-il nécessaire d'apporter à la Loi sur la protection des renseignements personnels et à la Loi sur la protection des renseignements personnels et les documents électroniques?

M. Tim McSorley: Notre expertise se situe principalement du côté du secteur public, alors je vais me concentrer sur ce secteur.

Encore une fois, il convient d'établir clairement les utilisations interdites, par exemple, en ce qui concerne la surveillance de masse des lieux publics. Il faut aussi qu'il y ait des règles claires concernant la publication des évaluations des facteurs relatifs à la vie privée.

Nous pensons qu'il serait utile de prévoir un examen obligatoire par un tiers indépendant des outils algorithmiques de surveillance et des outils de surveillance biométrique utilisés par les forces de l'ordre, afin qu'ils soient évalués du point de vue de leurs répercussions sur les droits de la personne, de leur précision et de leur partialité.

Nous pensons qu'il serait également utile qu'une agence gouvernementale soit chargée expressément d'examiner l'utilisation, par les agences fédérales, des outils algorithmiques et biométriques en général, mais surtout en matière de surveillance, ainsi que d'effectuer un suivi et de créer un répertoire à cette fin.

● (1635)

M. Ryan Williams: Je vous remercie, monsieur.

Le président: Nous passons maintenant à M. Bains pendant cinq minutes.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Je vous remercie, monsieur le président, et je remercie tous nos invités d'être avec nous aujourd'hui.

Mes questions émanent de Richmond, en Colombie-Britannique. L'utilisation de l'intelligence artificielle m'inquiète. Comme vous le savez, en Colombie-Britannique, nous avons une grande communauté autochtone, noire et de couleur, principalement asiatique et sud-asiatique. Un témoin nous a signalé l'autre jour que le service de police de Vancouver utilise l'intelligence artificielle.

Ma question s'adresse à Mme McPhail. Le chef de la police de Vancouver, Adam Palmer, a assuré à la commission de police en avril 2021 que ses agents n'utiliseront pas la technologie de reconnaissance faciale pour les enquêtes tant qu'une politique n'aura pas été mise en place.

Savez-vous si une politique a été présentée à la commission de police à ce sujet?

Mme Brenda McPhail: Je ne sais pas si une telle politique a été présentée à Vancouver.

Je sais qu'à Toronto, ce que nous croyons être la première politique de ce genre a été adoptée récemment, et le bruit court que de nombreux autres services de police au Canada attendaient que cela se produise pour y jeter un coup d'œil et élaborer leurs propres politiques en ce sens. Je m'excuse toutefois de ne pas avoir d'information en ce qui concerne Vancouver.

M. Parm Bains: Avez-vous été informée de ce qu'un précédent témoin nous a signalé, à savoir que l'intelligence artificielle est déjà utilisée?

Mme Brenda McPhail: Oui, je crois que c'est une information qui provient des recherches approfondies menées par le Citizen Lab et qui se trouve dans son rapport sur l'utilisation d'algorithmes par les services de police au Canada.

Un certain nombre de forces de police au Canada, y compris celle de Vancouver, ont commencé à utiliser ce genre d'outils. Cela se passe discrètement, sous le radar, généralement sans aucune mention publique au moment de l'acquisition, de l'élaboration de la politique ou de la mise en œuvre. Nous avons une véritable crise de responsabilisation dans l'utilisation de ces technologies par la police.

M. Parm Bains: Et cela se fait sans qu'il y ait une politique en place. Est-ce bien cela?

Mme Brenda McPhail: Soit il n'y a pas de politique en place, soit il n'y a pas de politique accessible au public. J'ai fait de nombreuses demandes d'accès à l'information sur des sujets similaires, plus particulièrement sur la technologie de reconnaissance faciale, et c'est extrêmement ardu d'obtenir l'information d'une façon raisonnable.

M. Parm Bains: En décembre 2021, l'Association canadienne des libertés civiles a appuyé les décisions des commissaires de la Colombie-Britannique, de l'Alberta et du Québec, ordonnant notamment à Clearview AI de cesser de recueillir des renseignements personnels dans ces provinces et de supprimer tous les renseignements personnels déjà recueillis sans consentement. Savez-vous si Clearview AI a donné suite à ces ordonnances?

Mme Brenda McPhail: En effet, Clearview AI a déposé des demandes juridiques, des poursuites, contre les commissaires en Colombie-Britannique, en Alberta, au Québec et au niveau fédéral, pour contester ces ordonnances à partir d'une série de motifs qui vont de la difficulté ou de l'impossibilité de se conformer à ces ordonnances, à la contestation de la constitutionnalité des lois canadiennes sur la protection de la vie privée, en passant par l'argument selon lequel ils ont une liberté d'expression concernant les données recueillies sur Internet.

Il s'agit d'un litige en cours qui mérite grandement l'attention du Comité.

● (1640)

M. Parm Bains: Je vous remercie.

S'il me reste du temps, j'aimerais poser une question à Mme LaPlante.

En janvier 2021, vous avez cosigné un article sur le site de RBC Capital Markets intitulé « Ensuring AI Remains a Force for Good ». Vous y parlez du programme Respect AI comme d'un moyen de renforcer la confiance du public. L'une des façons pour y arriver serait d'utiliser la technologie pour exposer les préjugés.

Pour revenir à la question de mon collègue M. Fergus sur la technologie qui capture des images, pouvez-vous donner au Comité une idée ou des exemples de la façon dont la technologie peut être utilisée pour éliminer les préjugés?

Le président: Soyez brève, s'il vous plaît.

Mme Alex LaPlante: Je pense qu'il sera très difficile de vous donner une réponse brève, mais je vous suggérerais de vous pencher sur le concept de l'éthique dès la conception, qui consiste essentiellement à prendre en compte les considérations éthiques tout au long du cycle de développement, de la collecte initiale des données à l'élaboration des algorithmes, en passant par les questions que vous devez vous poser au sujet de la mise en production et de la surveillance de ces systèmes. Il y a beaucoup de détails que vous pouvez rassembler à ce sujet. Il y a un certain nombre d'organismes qui mettent cela en pratique, comme Borealis.

Le président: Monsieur Bains et madame Saks, je vous ai donné la parole dans le mauvais ordre en ne suivant pas ce qui m'avait été fourni. J'ai interverti vos noms, et je m'en excuse. Si je ne donne pas la parole à la personne prévue, corrigez-moi rapidement et je vais la donner à la bonne personne.

[*Français*]

Sur ce, je cède la parole à M. Garon pour deux minutes et demie.

M. Jean-Denis Garon: Merci, monsieur le président.

Je vais poursuivre avec M. Labonté.

Je vais reprendre la question de mon collègue M. Fergus. Tout à l'heure, il demandait s'il fallait repartir à zéro, le temps d'établir une réglementation adéquate. Or, des entreprises comme Clearview AI ont déjà récolté et emmagasiné une quantité phénoménale de photos.

A-t-on déjà trop attendu avant d'établir une réglementation?

M. Françoys Labonté: Il est trop tard pour réglementer la collecte des données, car on ne peut pas reculer dans le temps. Par contre, on peut réglementer l'utilisation des technologies.

Ce que les gens ne comprennent pas toujours très clairement, c'est que l'idée derrière les nouvelles approches d'intelligence artificielle qui donnent lieu aux technologies dont nous parlons, c'est d'obtenir un nombre considérable de données et de les utiliser pour faire l'entraînement des systèmes. Le résultat attendu, c'est la reconnaissance faciale, c'est-à-dire la capacité d'identifier s'il s'agit de tel ou tel individu. Ce qui se crée, c'est un modèle explicite. Dans le domaine des technologies ou de l'ingénierie, on a habituellement des entrées de données dont on procède au traitement pour avoir des résultats. Or, on n'est plus dans ces modèles. Maintenant, on crée des modèles implicites qui, à partir de l'observation, du traitement et de l'analyse de plusieurs jeux de données, vont fournir les résultats auxquels on s'attend. Les joueurs qui ont réussi à faire cela, en collectant plein de données au cours des 10 dernières années, ont maintenant un avantage compétitif, comparativement à ces modèles. C'est quelque chose de très difficile à reproduire. Ce sont des boîtes noires opaques.

À mon avis, ce sera extrêmement difficile, puisque l'on ne peut pas reculer dans le temps.

M. Jean-Denis Garon: Il ne me reste que 30 secondes, alors je vous pose rapidement une question.

Étant donné que les données circulent énormément, la réglementation de l'utilisation de ces données s'apparente-t-elle à la réglementation de l'évasion fiscale, en ce sens qu'il faut que les pays se coordonnent afin de correctement l'encadrer?

M. Françoys Labonté: Ce sera fort probablement nécessaire.

Comme on le dit souvent, le nerf de la guerre, ce sont les données. Quand on regarde les chiffres qui montrent l'évolution de la situation, on voit que la quantité de données stockées dans les plateformes infonuagiques est exponentielle. Une fois que la roue est lancée, c'est très difficile de reculer.

● (1645)

[*Traduction*]

Le président: Je vous remercie, monsieur Labonté.

Nous passons à M. Green pendant deux minutes et demie.

M. Matthew Green: Je vous remercie.

Je vais commencer par Mme LaPlante. Dans son témoignage, je crois qu'elle a parlé de la nécessité de responsabiliser le secteur privé. Je me demande si elle a en tête des cadres législatifs qui permettraient une véritable responsabilisation dans le cas où des sociétés indépendantes utiliseraient cette technologie de mauvaise foi ou d'une manière qui constitue une violation flagrante de la vie privée.

Mme Alex LaPlante: Je vais concentrer mes commentaires sur la réglementation de l'intelligence artificielle en général. À l'heure actuelle, au Canada, nous n'avons pas de réglementation de bout en bout, et plusieurs changements s'imposent. Je vais vous mentionner à cette fin un cadre récemment publié par la Commission européenne — il s'agit d'un projet de cadre, mais il est très probable qu'il entrera en vigueur en 2022 — qui porte sur les questions liées à l'intelligence artificielle et aux risques qui y sont associés, qu'il s'agisse de la vie privée et des droits de la personne ou de concepts très techniques liés à la robustesse et à la stabilité.

En définitive, chaque fois que nous concevons l'un de ces systèmes, nous devrions procéder à une évaluation des répercussions. Comme je l'ai indiqué dans mes remarques, la surveillance de ces systèmes devrait être basée sur la matérialité des risques, soit les systèmes à très haut risque. Il devrait y avoir un certain niveau d'examen des exigences relatives à leur utilisation et aux tests. Les tests couvrent un très large éventail de concepts techniques, comme la robustesse, la stabilité, la partialité et l'équité, et des seuils doivent être établis. Il est vrai que ces derniers dépendent du contexte et qu'ils doivent être mis en place par les développeurs pour que nous puissions garantir la responsabilisation.

Je noterai également — et je pense que c'est quelque chose qui est souvent oublié — que ces systèmes sont stochastiques. Cela signifie que lorsque nous les mettons en production, nous pouvons avoir une très bonne idée de la façon dont ils se comporteront aujourd'hui, mais qu'au fur et à mesure que nos données changent, nous devons nous assurer de les surveiller continuellement pour garantir qu'ils fonctionnent comme nous l'avions initialement prévu. S'ils ne fonctionnent plus de cette manière, ils doivent être retirés de la production et réévalués avant d'être remis en service. Cela est particulièrement vrai dans les cas d'utilisation à haut risque comme l'identification des criminels.

M. Matthew Green: Ma dernière question s'adresse à Mme McPhail. D'après votre expérience, dans les cas où les forces de l'ordre ont utilisé cette technologie, y a-t-il eu des situations dans lesquelles des faux positifs ont causé un préjudice matériel aux personnes innocentes qui avaient été identifiées?

Le président: Veuillez fournir une réponse très brève. Merci.

Mme Brenda McPhail: Au Canada, en partie parce que les forces de police se sont montrées prudentes et modérées dans l'adoption de cette technologie et l'utilisent de façon relativement limitée, je n'ai pas connaissance que de tels cas se soient produits.

Aux États-Unis, où l'adoption a été plus rapide et moins prudente, notre organisation sœur, la American Civil Liberties Union, a entamé des poursuites dans plusieurs États pour défendre des hommes — tous noirs — qui ont été mal identifiés par cette technologie. L'un d'entre eux en particulier, M. Williams, a vu la police venir chez lui, le menotter et le traîner hors de chez lui devant ses enfants mineurs.

Le président: Merci, madame McPhail.

Nous passons maintenant à M. Bezan.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Je tiens à remercier les témoins. Vos interventions sont très instructives et révélatrices pour nous tous, compte tenu de ce qui est en jeu.

Je vais revenir sur la première question de M. Green.

Avec mes antécédents dans le domaine de la défense et de la sécurité nationales, je n'avais même pas pensé à la façon dont la technologie de reconnaissance faciale est utilisée pour porter atteinte aux droits garantis par la Charte, et même enfreindre le Code criminel et la Loi sur la défense nationale, qui stipulent que l'on ne peut pas espionner quelqu'un, directement ou indirectement, à moins qu'un mandat n'ait été lancé ou que, dans le cas d'une menace imminente, une autorisation ministérielle n'ait été donnée. Il existe des freins et des contrepoids dans l'ensemble de ce processus.

Lorsque l'on commence à étudier la collecte et la surveillance de masse à l'aide de la technologie de reconnaissance faciale, comment peut-on même déterminer que l'utilisation de cette technologie est possible quand on sait que le Code criminel, la Charte et la Loi sur la défense nationale telle qu'elle s'applique au CST sont censés imposer tous ces freins et contrepoids ? Il suffit de penser au SCRS et à l'Agence des services frontaliers du Canada, sans parler de la GRC, de la Police provinciale de l'Ontario et de toutes les autres organisations policières qui existent.

J'aimerais que M. McSorley et Mme McPhail s'expriment brièvement à ce sujet.

M. Tim McSorley: S'il est vrai que des règles ont été mises en place pour limiter la surveillance de masse exercée par ces organismes, comme cela a été mentionné, dans l'ébauche récente d'un projet d'orientation destiné aux organismes d'application de la loi, le commissaire à la protection de la vie privée s'est dit préoccupé par le fait qu'étant donné qu'il existe un ensemble disparate de lois en la matière, il existe des failles et que les organismes fédéraux et les organismes d'application de la loi puissent se livrer à une surveillance de masse qui serait autrement jugée illégale.

Il existe actuellement un manque de clarté à ce sujet. L'absence de discussion et le manque de volonté des organismes fédéraux de discuter de l'utilisation qu'ils font de la technologie de reconnaissance faciale suscitent de profondes inquiétudes quant au fait qu'ils pourraient se livrer à des formes de surveillance illégales ou qui seraient autrement jugées illégales, permises par cet ensemble disparate de lois.

Des débats sont également en cours quant à ce qui constitue une surveillance de masse. Par exemple, la GRC recueille des renseignements sur les personnes en ligne et les conserve dans des bases de données. Nous le savons. Cette pratique va au-delà de la reconnaissance faciale, mais elle soutient qu'elle a le droit de recueillir ces renseignements, alors que d'autres personnes, comme nous, l'ont contesté, affirmant qu'il s'agit d'une forme de surveillance de masse qui doit être réglementée.

● (1650)

M. James Bezan: Vous dites donc, M. McSorley — je vais laisser Mme McPhail intervenir sur ce point — que la capture d'images sur les médias sociaux de personnes, qui participent à des manifestations de masse comme celles que nous avons connues récemment ici au Canada, ainsi que la surveillance de masse et la technologie de reconnaissance faciale constituent selon vous deux des violations de leurs libertés civiles?

Madame McPhail, vous avez la parole.

Mme Brenda McPhail: Oui, monsieur le président, je le crois.

Notre régime législatif actuel présente des lacunes importantes qui semblent être exploitées, à l'heure actuelle, pour permettre des utilisations de cette technologie qui n'ont pas encore été évaluées ou examinées devant un juge. Cela se produira probablement dans un avenir proche ici au Canada, mais nous pouvons agir de façon préventive si nous nous asseyons et réfléchissons très attentivement à la question de savoir s'il existe des moyens d'utiliser cette technologie en toute sécurité.

Dans certains cas, la réponse sera négative. L'Association canadienne des libertés civiles soutient une interdiction complète de l'utilisation de cette technologie pour la surveillance de masse.

Dans certains cas, comme pour ce qui est de l'utilisation actuellement faite par la police de la technologie de reconnaissance faciale en conjonction avec les bases de données de photos signalétiques, par exemple, même ces utilisations peuvent prêter à controverse. Nous n'y avons tout simplement pas pensé. L'utilisation par la police de la technologie de reconnaissance faciale dans les bases de données de photos signalétiques est effectuée sur des bases de données existantes qui présentent leurs propres problèmes de partialité et de discrimination, que nous connaissons depuis très longtemps.

Je pense qu'il ne s'agit pas seulement des aspects liés à la surveillance de masse, mais aussi des aspects plus ciblés auxquels nous n'avons pas encore réfléchi.

M. James Bezan: Si nous commençons à parler des aspects ciblés, nous avons avec nous Mme LaPlante, de Borealis AI, qui travaille avec RBC. Nous savons que la GRC et le gouvernement voulaient geler les comptes bancaires des personnes qui ont participé à la manifestation qui a eu lieu récemment.

Par où devons-nous commencer...?

Une partie de la technologie dont dispose Borealis AI serait-elle utilisée pour permettre au gouvernement de geler les comptes bancaires de certaines personnes dont les visages ont été extraits des médias sociaux ou de la surveillance de masse par d'autres moyens, comme des drones et des caméras?

Le président: Je vous demanderai d'être brève. M. Bezan a utilisé tout son temps pour poser sa question, alors veuillez donner une réponse très brève.

Mme Alex LaPlante: C'est un non catégorique.

Comme je l'ai mentionné, nous prenons l'éthique très au sérieux dans le cadre de la conception de tous nos systèmes algorithmiques. Il ne s'agit certainement pas d'un cas d'utilisation qui aurait atterri sur notre bureau à RBC.

Le président: Merci de votre réponse.

Madame Saks, allez-y. Vous avez cinq minutes.

Mme Ya'ara Saks (York-Centre, Lib.): Merci, monsieur le président.

Merci à tous les témoins présents aujourd'hui.

Par votre entremise, monsieur le président, j'aimerais d'abord poser une question à Mme McPhail.

De toute évidence, nous avons affaire à des quantités massives de données et à une prolifération massive de l'utilisation de la technologie de reconnaissance faciale et de l'intelligence artificielle. Comme M. Labonté l'a mentionné plus tôt, il existe des zones floues pour ce qui est de son utilisation dans le secteur du commerce de détail. D'autres témoins ont parlé des soins de santé et d'autres utilisations bénéfiques, et nous savons que ce débat est en cours.

Pour ce qui est de la demande de moratoire, ma question est de savoir par où nous devons commencer.

Il existe actuellement des lacunes dans les lois, qui ne visent pas le secteur privé, alors que c'est ce dernier qui fabrique cette technologie. À qui exactement imposons-nous donc un moratoire?

● (1655)

Mme Brenda McPhail: L'Association canadienne des libertés civiles soutient en particulier l'imposition d'un moratoire sur les utilisations de cette technologie par la police et la sécurité nationale, car il s'agit de situations dans lesquelles les conséquences, si nous nous trompons, peuvent changer la vie des personnes concernées.

Cela dit, il serait bénéfique d'imposer un moratoire général, car nous savons que des fournisseurs du secteur privé vendent des technologies à des intervenants du secteur public, notamment à des organismes chargés de l'application de la loi et de la sécurité nationale. Le fonctionnement de notre régime juridique actuel en matière de protection de la vie privée est tel que ces deux parties, publique et privée, sont régies d'une certaine manière par des réglementations différentes, ce qui ne fait qu'accroître la difficulté de réglementer efficacement ce domaine.

Nous devons absolument adopter une approche cohérente pour réfléchir à la manière de développer les protections à cet égard.

Mme Ya'ara Saks: Merci. J'aimerais approfondir un peu plus cette question, car en vérité, si nous posons la question... Quand j'étais enfant, mon père me disait toujours de poser la question *quanto uno*: qui en profite?

Étant donné que des entreprises du secteur privé offrent cette technologie pour la surveillance à des fins de sécurité, qu'il s'agisse des forces de police ou de la GRC, nous pénétrons dans cette zone floue. Dans vos recommandations au commissaire à la protection de la vie privée, avez-vous abordé cette zone floue des échappatoires, en mettant en place un...?

La question est la suivante: si vous demandez un moratoire, comment peut-on en assurer l'efficacité? Le phénomène est tellement répandu à ce stade que pour le rendre efficace... Je demande quelle en serait l'efficacité.

Mme Brenda McPhail: C'est une bonne question. L'une des principales lacunes de notre régime de protection de la vie privée est que notre commissaire fédéral n'a pas de pouvoirs d'exécution et ne peut pas émettre d'ordonnances exécutoires. L'un des buts du moratoire serait de donner au gouvernement la possibilité de combler cette lacune, s'il décide de le faire.

Quand on crée une loi, on se demande toujours si les personnes vont la respecter. Si vous émettez une ordonnance, les personnes vont-elles s'y conformer? Je pense que nous sommes tous très conscients des risques que présente ce genre d'équation après avoir vécu toutes ces années de pandémie. Le fait qu'elle puisse ou non être efficace à 100 % à tous les égards ne signifie pas qu'elle n'est pas nécessaire et que nous ne devrions pas essayer, car les enjeux sont très élevés. Nous parlons des droits garantis par la Charte des personnes de tout le Canada qui sont en danger chaque jour où nous permettons que ces technologies continuent d'être utilisées sans que des garanties juridiques soient mises en place pour les protéger.

Mme Ya'ara Saks: Ma question s'adresse maintenant à M. Labonté. Nous savons qu'une grande partie de la technologie de l'intelligence artificielle présente des problèmes de discrimination à l'égard des personnes de couleur. Steve Lohr, du New York Times, a déclaré à un moment donné — et je pense en fait que ce chiffre est faible — que le taux d'inexactitude était de 35 % lorsqu'il s'agissait de discriminer les personnes de couleur, les femmes et les enfants. Je suppose que ce taux pourrait être plus élevé, surtout à la lumière du rapport du NIST de 2019.

Qui conçoit cette technologie? Nous posons-nous ces questions et veillons-nous à ce que ces algorithmes et la conception de cette technologie tiennent compte de la perspective des minorités visibles et des groupes racisés, du point de vue du CRI?

M. Françoys Labonté: Nous n'avons pas beaucoup de temps, mais si nous retournons de nombreuses années en arrière, à l'époque où nous compilions des statistiques, nous concevions généralement des expériences pour veiller à ce que nos échantillons soient représentatifs et obtenir des résultats significatifs sur le plan statistique.

Nous vivons maintenant dans un monde qui compte une abondance de données, et où l'on utilise ce que l'on a et on obtient ce que l'on obtient.

La conception de systèmes basés sur la représentativité des données est une question essentielle. Très souvent, lorsque nous disons que les systèmes sont biaisés, cela signifie simplement que les échantillons de données initiaux ne sont pas égaux ou que leur représentativité n'est pas égale. Voilà la difficulté qui se pose habituellement. Le problème n'est pas la technologie en soi, mais les données qui ont été fournies au système.

Mme LaPlante a mentionné tous les problèmes liés à l'intelligence artificielle. Ceux-ci indiquent que notre système d'intelligence artificielle pourrait devenir un système essentiel qui devrait être réglementé. Il en va de même lorsque vous concevez des voitures ou des avions; vous devez démontrer toutes ces questions de fiabilité, de reproductibilité et tous ces éléments. Beaucoup de ces questions vont en fait dans ce sens.

L'intelligence artificielle est encore la nouvelle génération...

● (1700)

Le président: Je suis vraiment désolé de vous interrompre, mais nous avons largement dépassé le temps imparti, et je vais devoir conclure cette série de questions.

Nous avons terminé les deux premières séries. Il nous reste une demi-heure. Nous nous attendons à ce que la sonnerie retentisse dans environ 15 minutes, mais nous allons entendre d'autres questions.

Nous allons passer à M. Kurek, qui aura cinq minutes, puis ce sera au tour de Mme Kayabaga.

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

Tout d'abord, j'aimerais profiter de cette occasion pour remercier tous les témoins, car cette conversation est très instructive et, je pense, très significative. Je crois que toutes les parties conviendront que le sujet et la substance réelle de ce que nous abordons ici sont très précieux pour notre pays.

Monsieur le président, si vous me le permettez, je vais utiliser ces quelques minutes de mon temps pour présenter la motion pour laquelle j'ai donné un préavis verbal le 3 mars de cette année. Je vais la lire une fois de plus pour qu'elle figure au compte rendu:

> Que, conformément à l'article 108(3)h) du Règlement, le Comité entreprenne une étude sur les questions de conflit d'intérêts et la Loi sur le lobbying en ce qui concerne les dépenses liées à la pandémie, à condition que: a) les témoignages et la documentation reçus par le Comité au cours des deux sessions de la 43e législature sur le sujet soient pris en considération par le Comité au cours de la présente session; b) le Comité adopte le rapport intitulé Questions de conflits d'intérêts et de lobbying en relation avec les dépenses liées à la pandémie, initialement adopté comme deuxième rapport du Comité lors de la deuxième session de la 43e législature; c) les opinions dissidentes ou supplémentaires soient soumises par voie électronique dans les deux langues officielles au greffier du comité dans les 48 heures suivant l'adoption de la présente motion; d) le président dépose ce rapport à la Chambre au plus tard le 31 mars 2022.

Monsieur le président, je vais être très bref, car j'espère que les membres du Comité consentiront à ce que nous ne rouvrions pas ce dossier, mais que nous reconnaissions plutôt le travail acharné accompli par les membres du Comité avant l'élection déclenchée l'été dernier, et que nous veillions à ce que les Canadiens aient la possibilité de voir le rapport sur lequel tous les membres de ce comité ont travaillé. Je crois qu'il y a des membres de la plupart des partis qui siègent encore à ce comité depuis la dernière législature.

Sur ce, monsieur le président, je propose cette motion.

Le président: Très bien, monsieur Kurek, vous avez proposé cette motion.

Souhaitez-vous continuer d'en parler, car d'autres personnes vont intervenir? Si vous avez terminé, je vais passer au débat sur la motion.

M. Damien Kurek: Monsieur le président, je voudrais simplement dire que je me suis efforcé autant que possible de ne pas donner lieu à controverse. Je m'en tiendrai là.

Le président: Merci.

La motion est proposée. Elle a fait l'objet d'un préavis et, compte tenu de la date, il n'est pas surprenant que nous devions l'examiner aujourd'hui.

J'ai d'abord M. Fergus. Je vais vous mettre sur la liste. J'ai plusieurs personnes.

Allez-y, monsieur Fergus.

[*Français*]

L'hon. Greg Fergus: Je suis un peu bouche bée.

[*Traduction*]

Je suis étonné qu'au cours d'une discussion particulièrement importante sur la reconnaissance faciale, où tous les partis semblent exprimer de graves inquiétudes quant à cette technologie et quant à la manière dont elle nuit en particulier aux personnes de couleur, aux femmes et aux jeunes, nous jouions à ce jeu et qu'il s'agisse un peu d'un jeu.

Monsieur le président, contrairement à ce qu'a déclaré mon respecté collègue, pour autant que je sache, je suis le seul à avoir siégé au sein du Comité l'année dernière, à l'époque où nous avons mené ce très long débat, puis examiné, je crois, un rapport très substantiel.

Puis-je ajouter, monsieur le président, au profit de tous les autres députés qui ne faisaient pas partie du Comité à l'époque, que chacune des recommandations demandées par le parti du député d'en face a été adoptée dans ce rapport? Le rapport a été présenté à la Chambre, alors j'essaie de comprendre pourquoi, près d'un an plus tard, nous réexaminons cette question.

Nous, les parlementaires, avons fait un excellent travail. Je siège au sein de notre comité et du Comité de la procédure et des affaires de la Chambre. J'ai été impressionné par la bonne volonté des députés qui s'efforcent de mettre de côté leurs intérêts partisans étroits dans l'intérêt des Canadiens et de prendre de très bonnes initiatives.

Cette discussion sur la reconnaissance faciale est en suspens depuis non pas un an, ni deux ans, mais trois ans. Trois années se sont écoulées alors que nous aurions pu prendre des mesures à ce sujet. Au cours de ces trois années, il y a eu encore plus de visages qui ont été extraits du Web et encore plus de personnes qui ont été injustement ciblées par l'utilisation de cette technologie. Et, maintenant, nous allons aborder une question que nous avons passé d'innombrables heures non seulement à débattre, mais aussi à présenter dans un rapport. Le parti de mon collègue a obtenu que toutes ses recommandations figurent dans le rapport sans modification. Allons-nous revenir sur ce sujet? C'est un gaspillage de temps et une déception. Franchement, je dois dire que cela me met très en colère.

Nous avons essayé d'entreprendre cette étude pendant trois ans. Nous avons finalement réussi, et chaque question posée aujourd'hui...

● (1705)

[*Français*]

Chapeau à tous mes amis ici, autour de la table, pour le sérieux de leurs questions.

Maintenant, on va faire de la politicaillerie au sujet d'un dossier que nous avons réglé il y a un an et qui a déjà été soumis à la Chambre des communes?

Monsieur le président, c'est ridicule et c'est insultant. Cela me dépasse.

[*Traduction*]

C'est vraiment très décevant.

Merci, monsieur le président.

Le président: Merci, monsieur Fergus.

J'ai maintenant une longue liste d'intervenants.

Mme Khalid est notre prochaine intervenante.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Je me fais l'écho des sentiments de mon collègue. Je remercie les témoins d'être venus aujourd'hui et de nous aider à étudier ce projet de loi très important.

Pendant que M. Kurek lisait le contenu de sa motion, j'avais en fait devant moi une copie d'une motion présentée le 13 décembre par M. Brassard au même comité. Cette motion était exactement la même, mot pour mot.

Je sais qu'au chapitre 20 de l'ouvrage intitulé « La procédure et les usages de la Chambre des communes », sous la rubrique « Format et recevabilité » des motions, il est écrit ce qui suit:

> Une motion au contenu identique à une motion qui a déjà fait l'objet d'une décision au cours de la même session est irrecevable; toutefois, un député peut présenter une motion qui, quoique semblable, s'en distingue suffisamment pour constituer une nouvelle question.

Je remarque effectivement que la seule différence entre la motion que M. Kurek a présentée aujourd'hui et celle que M. Brassard a présentée auparavant, c'est une nouvelle section, notamment le paragraphe d), qui ajoute simplement une échéance à un contenu tout à fait identique.

Puis-je humblement vous demander de rendre une décision à ce sujet, à savoir si cette motion est recevable ou non?

● (1710)

Le président: J'ai accepté cette motion lorsqu'elle a été présentée. Elle contient quelques différences, et je l'ai jugée recevable. C'est là ma décision.

Mme Iqra Khalid: Dans ce cas, monsieur le président, après avoir écouté les propos de M. Kurek et les avoir comparés à la motion identique qui a fait l'objet d'un vote et qui a été rejetée par le Comité le 13 décembre, je ferais appel de votre décision.

Le président: Mme Khalid conteste ma décision, selon laquelle la motion est recevable. Je demanderais à la greffière de procéder au vote.

M. James Bezan: Soyons clairs. Nous votons pour ou contre le maintien de la décision de la présidence, n'est-ce pas?

La greffière: Exactement. J'aillais en fait expliquer la situation.

Une motion a fait l'objet d'un débat. Le président a jugé la motion recevable, et Mme Khalid conteste la décision de la présidence.

La question est de savoir si la décision que le président a rendue au sujet de la motion de M. Kurek est maintenue.

Si vous pensez que la décision de la présidence, selon laquelle la motion est recevable, est correcte, vous votez oui.

Si vous pensez que la décision de la présidence est incorrecte et que la motion doit être considérée comme irrecevable, vous votez non.

(La décision de la présidence est maintenue par 6 voix contre 5.)

Le président: Madame Khalid, vous aviez la parole et vous l'avez toujours si vous souhaitez ajouter quelque chose. Sinon, je vais passer à l'intervenant suivant.

Mme Iqra Khalid: Oui, monsieur le président.

Dans ce cas, je commencerai par présenter mes excuses à nos témoins d'aujourd'hui qui ont eu moins de temps pour nous faire part de l'important témoignage qu'ils voulaient apporter au sujet du travail très important que nous réalisons.

Monsieur le président, par votre entremise, je leur demanderais s'il y a d'autres points qu'ils aimeraient voir soulignés compte tenu des questions qui ont été posées aujourd'hui et des propos qu'ils ont entendus les autres intervenants et les députés prononcés aujourd'hui. Le cas échéant, ils pourraient peut-être le faire par écrit. Nous leur serions grandement reconnaissants de ces mémoires. Nous espérons que nous pourrons reprendre cette étude assez rapidement.

Je dirai également, monsieur le président, que je suis très déçue. Comme je l'ai indiqué, la motion contenait littéralement les mêmes mots qui ont déjà fait l'objet d'un vote et qui ont été rejetés le 13 décembre. Comme M. Fergus l'a très clairement souligné, nous avons par la suite étudié des questions beaucoup plus importantes. Cependant, nous sommes désormais de retour à la case départ. Nous allons maintenant passer beaucoup de temps, je pense, à débattre du bien-fondé d'une motion dont nous avons déjà débattu longuement.

J'espérais que le Comité comprendrait l'importance de la raison pour laquelle nous devons passer à cette étude sur la reconnaissance faciale. Notre pays a vraiment besoin de renforcer ses lois sur la protection des renseignements personnels et les lois qui régissent l'industrie qui tire parti des renseignements personnels des Canadiens. Nous avons vraiment besoin de réformer la LPRPDE. Elle a été mise en place bien avant que la reconnaissance faciale et l'intelligence artificielle n'entrent en jeu.

J'espère que nous nous y remettrons et que nous étudierons des questions plus pertinentes que nous n'avons pas déjà rabâchées. Comme l'a dit M. Fergus, cela fait trois ans que nous attendons d'amorcer cette étude. Je ne peux pas souligner à quel point il est important que nous continuions de faire avancer cette étude et que nous proposions des recommandations sérieuses et robustes pour réformer la façon dont l'industrie et les technologies comme l'intelligence artificielle et la reconnaissance faciale doivent être freinées pour faire en sorte que nous trouvions cet équilibre. L'un de nos témoins — je crois que c'était M. Labonté — a parlé de l'équilibre entre la protection des renseignements personnels, l'acceptation sociale et les avantages sociétaux...

● (1715)

M. James Bezan: J'invoque le Règlement.

Le président: Il y a un rappel au Règlement.

Monsieur Bezan, veuillez faire valoir votre argument qui est...

M. James Bezan: Mon rappel au Règlement est lié à la pertinence. Les commentaires de Mme Khalid n'ont rien à voir avec la motion. Elle parle de l'étude dont nous avons parlé plus tôt. Nous devrions revenir à nos moutons.

Nous disposons de beaucoup de temps en ce moment. Nous pourrions revenir à l'étude si nous procédions au vote.

Le président: Merci, monsieur Bezan.

J'accordais à Mme Khalid une certaine marge de manoeuvre dans la formulation de ses observations, qui s'écartaient un peu de la motion elle-même.

Il a été porté à mon attention que la sonnerie retentit en ce moment. À ce stade, je vais avoir besoin du consentement unanime des membres du Comité pour poursuivre la séance.

Je vois des gens hocher la tête.

Sur ce, la séance est levée.