CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

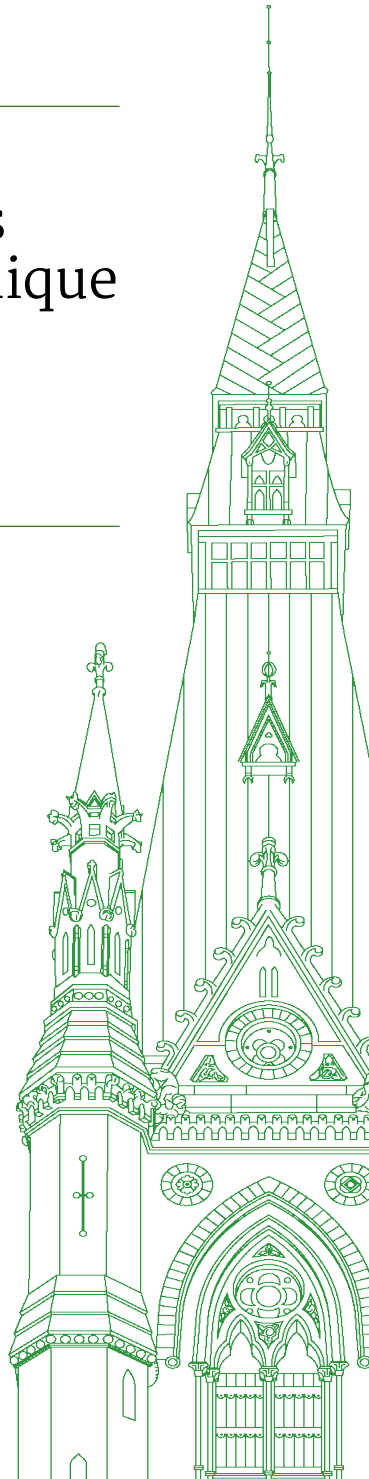
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 011

Le lundi 21 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 lundi 21 mars 2022

● (1100)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): La séance est ouverte.

Bienvenue à la onzième réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

[*Français*]

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

[*Traduction*]

Notre réunion se déroulera selon une formule hybride, conformément à l'ordre pris par la Chambre le 25 novembre 2021. Certains députés sont présents dans la salle de réunion et d'autres siègent virtuellement, par l'intermédiaire de l'application Zoom. Au cours de la webdiffusion, comme vous le savez déjà, c'est toujours la personne qui a la parole qui apparaîtra à l'écran plutôt que 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.

Voilà pour les consignes. Je souhaite maintenant la bienvenue à notre premier groupe de témoins. Nous recevons aujourd'hui Mme Cynthia Khoo, qui est chercheuse universitaire au Citizen Lab de la Munk School of Global Affairs and Public Policy de l'Université de Toronto. Elle témoignera à titre personnel.

Nous accueillons également Mme Carole Piovesan, associée directrice de l'organisme INQ Law.

Madame Khoo, vous pouvez commencer. Vous disposez de cinq minutes pour nous présenter vos remarques liminaires.

Mme Cynthia Khoo (chercheuse universitaire, The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, à titre personnel): Merci. Bonjour à tous.

Je m'appelle Cynthia Khoo. Je suis une associée du Center on Privacy and Technology de l'école Georgetown Law à Washington D.C. et, parallèlement, je mène des recherches au Citizen Lab de l'Université de Toronto.

Je témoigne aujourd'hui à titre professionnel même si j'exprimerai mon point de vue personnel en me fondant sur mes propres travaux de recherche au Citizen Lab, mais aussi sur ceux de mes collègues du Citizen Lab et du Privacy Center.

Je vais centrer mes remarques sur quatre grands sujets de préoccupation concernant la technologie de reconnaissance faciale et proposer une recommandation pour chaque sujet.

Tout d'abord, j'aimerais vous raconter l'histoire de Robert Williams, qui chantait dans sa voiture au moment où un crime avec lequel il n'avait rien à voir a été commis, de Nijeer Parks, qui effectuait une opération de virement de fonds à une succursale de Western Union, et de Michael Oliver, qui se trouvait à son travail.

Ces trois hommes noirs ont été injustement arrêtés par la police à cause de la technologie de reconnaissance faciale. Ces arrestations leur ont fait perdre leur emploi, elles ont traumatisé leurs enfants et elles ont mené à des ruptures, sans parler de l'atteinte à leur dignité personnelle. Ce sont les coûts humains de la confiance aveugle et du recours inconstitutionnel à la technologie de reconnaissance faciale.

Les chercheurs ont constaté que cette même technologie peut entraîner jusqu'à 100 fois plus d'erreurs d'identification pour les personnes noires et asiatiques, et que ce genre d'erreurs se produit plus de 1 fois sur 3 dans le cas des femmes à la peau plus foncée, alors qu'elle fonctionne 99 % du temps pour ce qui est des hommes blancs.

Je vous ai donné des exemples américains, mais ces situations pourraient très bien se produire ici, si ce n'est déjà fait. La discrimination raciale contre les personnes noires et autochtones est flagrante dans l'ensemble du système de justice criminelle canadien, dès les étapes du fichage et de l'arrestation jusqu'à celles de l'enquête sur remise en liberté, de la détermination de la peine et de la libération conditionnelle. L'intégration d'algorithmes de reconnaissance faciale à une structure truffée de préjugés systémiques peut donner un cocktail numérique dangereux qui risque de pérenniser des injustices bien ancrées et de rendre le futur encore plus inéquitable.

Ma première recommandation est donc de mener une enquête judiciaire sur l'utilisation pour le maintien de l'ordre d'ensembles préexistants de données policières de masse comme les photos d'identité judiciaire. Une telle enquête permettrait d'établir s'il est raisonnable de récupérer des données personnelles recueillies pour une autre fin et de les utiliser pour la technologie de reconnaissance faciale et d'autres technologies algorithmiques policières.

J'en arrive au deuxième sujet de préoccupation. Même si on parvient à éliminer tous les préjugés, la technologie de reconnaissance faciale restera aussi menaçante, voire encore plus menaçante pour les droits constitutionnels et les droits de la personne. Parce qu'elle requiert la collecte de données biométriques particulièrement sensibles, l'utilisation de la reconnaissance faciale pour identifier des personnes dans les lieux publics viole le droit à la vie privée qui est garanti par l'anonymat dans la vie courante. Cette technologie risque d'avoir un effet paralysant sur l'exercice de la liberté d'expression dans le cadre de manifestations publiques contre l'injustice, par exemple. Elle risque aussi d'exacerber la violence et l'exploitation fondées sur le genre en facilitant le harcèlement de femmes qui ne demandent rien d'autre que de pouvoir vivre sans peur.

La preuve n'a pas été faite que la reconnaissance faciale est suffisamment nécessaire, proportionnée et fiable pour compenser ces répercussions profondes. Par conséquent, ma deuxième recommandation serait d'imposer un moratoire national sur le recours à la technologie de reconnaissance faciale pour le maintien de l'ordre tant que la preuve n'aura pas été faite que non seulement elle est fiable, mais qu'elle est aussi nécessaire et proportionnée aux objectifs légitimes. Cela pourrait même exiger une interdiction complète dans certains cas, comme plusieurs villes des États-Unis l'ont déjà fait. Le Canada ne devrait pas hésiter à leur emboîter le pas. On ne peut pas demander à un logiciel d'assumer des responsabilités légales et morales que des humains ont par ailleurs abdiquées à l'égard de la vie et de la liberté de personnes vulnérables.

Le troisième sujet de préoccupation a trait au manque de transparence et de responsabilité. C'est un problème évident quand on pense que ce que le public sait au sujet de l'utilisation de la reconnaissance faciale par la police vient principalement des médias, de fuites de renseignements et de demandes d'accès à l'information. Les politiques qui régissent l'utilisation de la reconnaissance faciale par la police peuvent être des boîtes noires encore plus difficiles à comprendre que les algorithmes. Cette opacité engendre de graves manquements à l'équité procédurale dans les affaires criminelles.

Ma troisième recommandation serait d'instaurer des mesures rigoureuses en matière de transparence et de responsabilité si cette technologie est adoptée. Ces mesures devront comprendre l'obligation d'informer le public à l'avance et sans délai, et de lui donner l'occasion de donner son point de vue, d'évaluer les incidences des algorithmes, de consulter les groupes historiquement marginalisés et de mettre en place des mécanismes indépendants de surveillance comme des autorisations judiciaires.

En quatrième et dernier lieu, nous aurons besoin de garanties juridiques strictes pour éviter que les services policiers passent par les sociétés privées pour contourner nos droits constitutionnels à la liberté et à la protection contre les fouilles et les perquisitions abusives. Les logiciels commerciaux comme Clearview AI, Amazon Rekognition et NEC Corporation sont généralement propriétaires, ils sont protégés par les lois sur le secret commercial et sont achetés dans un contexte de lobbying qui se déroule en arrière-scène. Ce contexte est propice à la formation de partenariats secrets de surveillance entre le public et le privé qui privent les accusés dans les affaires criminelles de leur droit à une procédure équitable et qui nous exposent tous à des niveaux impénétrables de surveillance de masse.

Je vais conclure avec ma quatrième recommandation. Si un fournisseur privé de technologie recueille des données personnelles pour le compte d'un organisme policier et lui fournit ces données, il doit être tenu, par contrat ou autrement, de se conformer à des normes d'intérêt public en matière de protection et de communication des renseignements personnels.

Merci. Je répondrai volontiers à vos questions.

● (1105)

Le président: Merci.

Les cinq prochaines minutes seront réservées à Mme Piovesan.

Mme Carole Piovesan (associée directrice, INQ Law): Merci, monsieur le président, et merci, distingués membres du Comité. Bonjour.

Je m'appelle Carole Piovesan. Je suis associée directrice chez INQ Law, et je concentre ma pratique sur les questions de confidentialité et de gestion du risque lié à l'intelligence artificielle, ou IA. Je suis également professeure associée à la Faculté de droit de l'Université de Toronto, où je donne des cours sur la réglementation en matière d'IA. J'ai cosigné un livre sur la législation en matière d'IA qui a été publié chez Thomson Reuters en 2021. Je vous remercie de me donner la possibilité de m'adresser au Comité.

L'utilisation de la technologie de reconnaissance faciale gagne du terrain autant dans le secteur public que dans le secteur privé, comme vient de le dire Mme Khoo. Selon une étude publiée par Grand View Research en 2020, le marché mondial de la technologie de reconnaissance faciale devrait atteindre 12 milliards de dollars américains en 2028, alors qu'il s'établissait à 3,6 milliards de dollars américains environ en 2020. Cette expansion sera favorisée par des investissements majeurs et des avancées marquées dans l'application de cette technologie à l'échelle de la planète, ce qui dénote un environnement concurrentiel très dynamique.

Il est beaucoup question de sécurité et de surveillance quand on parle de la technologie de reconnaissance faciale, mais elle est aussi utilisée dans des secteurs comme le commerce au détail et le commerce électronique, les télécommunications, les technologies de l'information ou les soins de santé. La technologie de reconnaissance faciale devient un débouché économique de plus en plus attrayant pour les concepteurs et les utilisateurs de ces systèmes. Autrement dit, la technologie de reconnaissance faciale gagne en popularité. C'est pourquoi il est impératif d'en comprendre les conséquences profondes pour nos sociétés libres et démocratiques, comme cherche actuellement à le faire votre comité.

À titre informatif, je rappelle que la technologie de reconnaissance faciale utilise des données faciales biométriques extrêmement sensibles pour identifier et vérifier l'identité d'une personne. Il s'agit d'un processus automatisé qui peut être appliqué à grande échelle. Dans ce contexte, il faudra des lois et des politiques contenant des garanties rigoureuses et réfléchies qui nous permettront de tirer profit des avantages de cette technologie, mais aussi d'atténuer et de gérer les risques potentiels.

La technologie de reconnaissance faciale soulève des préoccupations concernant l'exactitude et l'objectivité des résultats des systèmes, les pratiques de surveillance illégales et arbitraires, la technologie de type boîte noire qui échappe aux législateurs et, ultimement, l'entrave à la liberté qui peut en découler. En ce sens, il est clair que la technologie de reconnaissance faciale peut mettre en danger les valeurs fondamentales qui sont consacrées par la Charte canadienne et exprimées dans notre folklore national.

Si l'utilisation de données identifiables extrêmement sensibles peut avoir de graves répercussions pour la réputation et même la liberté d'une personne, comme Mme Khoo l'a expliqué précédemment, elle peut en revanche faciliter et accélérer le paiement en toute sécurité à la caisse d'un magasin, ou sauver la vie d'un patient.

La réglementation de la technologie de reconnaissance faciale doit être façonnée avec un scalpel, pas avec une hache.

Je vais conclure mon exposé en énonçant des questions qu'il faudra se poser et qui seront articulées autour de quatre grands principes qui concordent avec ceux qui régissent la responsabilité en matière d'IA ailleurs dans le monde et qui devront orienter la réglementation axée sur la technologie de reconnaissance faciale. Les principes que je propose sont conformes aux principes en matière d'IA de l'Organisation de coopération et de développement économiques et aux principales orientations qui guident l'utilisation responsable de l'IA dans le monde, et ils englobent les aspects techniques, législatifs, politiques et éthiques dont il faudra tenir compte pour établir un cadre relativement complet de la technologie de reconnaissance faciale. Mon intention n'est pas d'en faire un exposé exhaustif, mais de mettre en lumière les enjeux opérationnels qui conduiront à une analyse approfondie.

Le premier principe est lié à la fiabilité technique. Pour élaborer une réglementation éclairée, il faudra répondre à diverses questions. Notamment, faut-il associer des critères techniques précis aux différentes utilisations possibles de la technologie de reconnaissance faciale et, si oui, lesquels? Des tierces parties indépendantes devraient-elles exercer une surveillance et évaluer la technologie de reconnaissance faciale d'un point de vue technique? Le cas échéant, à qui cette surveillance devrait-elle être confiée?

Le deuxième principe est celui de la responsabilité, et il faudra également répondre à certaines questions pour établir une réglementation éclairée. Par exemple, quels seront les mécanismes de contrôle administratifs exigés pour favoriser la responsabilité en matière de technologie de reconnaissance faciale? Comment faudra-t-il établir ces mécanismes de contrôle et qui devra les établir? Une évaluation des incidences sera-t-elle nécessaire? Le cas échéant, comment cette évaluation devra-t-elle être réalisée? Quand les parties prenantes devront-elles être consultées et à quoi le processus de consultation devra-t-il ressembler?

Le troisième principe concerne la légitimité. Les questions à se poser à des fins de réglementation auront trait aux mécanismes de surveillance requis pour assurer une utilisation de la technologie de reconnaissance faciale respectueuse des valeurs sociales et qui tiendra dûment compte des droits en matière criminelle, civile et constitutionnelle. Il faudra aussi se demander si des applications devront être interdites.

Le dernier principe, mais non le moindre, concerne l'équité, et il faut aussi répondre à certaines questions liées à la réglementation en la matière. Quels pourraient être les effets préjudiciables de la technologie de reconnaissance faciale pour les droits et libertés de chacun? Peut-on atténuer ces incidences? Des mesures seront-elles nécessaires pour éviter que certains groupes soient lésés de manière disproportionnée, même pour ce qui concerne les utilisations à faible risque?

● (1110)

Prises ensemble, les réponses à ces questions permettront au Canada d'élaborer une réglementation qui sera conforme à celle qui émerge un peu partout dans le monde en matière d'intelligence artificielle, en mettant l'accent sur la technologie de reconnaissance faciale afin de prévenir la menace sérieuse qu'elle représente pour nos valeurs et de tirer profit des avantages réels qu'elles ont à offrir.

Je me réjouis de répondre à vos questions. Merci.

Le président: Merci beaucoup.

Nous allons entamer le premier tour de questions.

Monsieur Williams, à vous l'honneur. Vous avez six minutes.

M. Ryan Williams (Baie de Quinte, PCC): Merci, monsieur le président.

Je remercie nos témoins d'être avec nous ce matin.

Madame Khoo, mes premières questions s'adresseront à vous. J'aimerais avoir une précision concernant une de vos recommandations. Vous recommandez d'imposer un moratoire sur les technologies de reconnaissance faciale, n'est-ce pas?

Mme Cynthia Khoo: Plus exactement, je recommande d'imposer un moratoire sur l'utilisation de la technologie de reconnaissance faciale pour le maintien de l'ordre. La raison pour laquelle je propose un moratoire plutôt qu'une interdiction est qu'il nous donnera le temps de pousser les recherches — dans le cadre d'une enquête judiciaire, par exemple — afin de déterminer si c'est une utilisation appropriée. Si la réponse est oui, il faudra ensuite déterminer dans quelles circonstances elle est appropriée et quelles seront les garanties requises. Le moratoire devra inclure la période nécessaire pour mettre ces garanties en place.

M. Ryan Williams: Merci.

En septembre 2020, vous avez écrit ce qui suit:

> Il n'existe pas dans le système juridique canadien de garanties suffisamment précises et efficaces pour assurer le recours à des méthodes de surveillance algorithmique qui respectent les limites constitutionnelles et auxquelles s'appliquent des mécanismes de surveillance réglementaires, judiciaires et législatifs.

Cela m'apparaît très pertinent. Nous savons que des méthodes de surveillance algorithmique sont encore utilisées. Pour la gouverne du Comité, pouvez-vous nous indiquer quel type de garanties seraient nécessaires pour protéger les droits des Canadiens?

Mme Cynthia Khoo: Avec plaisir. D'entrée de jeu, je répondrais qu'il faut assurer la transparence. Une bonne partie de ce que nous savons concernant les activités dans ce domaine nous vient, comme je l'ai dit, des enquêtes réalisées par des journalistes ou de fuites de renseignements. Or, cette information devrait émaner des services policiers ou du gouvernement, idéalement avant l'adoption de ces technologies, et le public devrait avoir la possibilité de donner son point de vue sur les incidences potentielles. C'est la première chose.

Deuxièmement, nous avons besoin de mécanismes de surveillance qui permettront de faire une évaluation... Par exemple, il est essentiel de faire une évaluation des incidences négatives de ces technologies avant leur adoption plutôt qu'après, surtout pour les communautés historiquement marginalisées.

Ces garanties sont fondées sur des principes généraux. Toutefois, dans notre rapport, nous nous sommes concentrés sur le contexte du droit criminel. Un autre exemple de garanties... Pour les accusés dans certaines affaires criminelles, notamment, il faudra prévoir des exigences en matière de divulgation qui leur permettront de savoir si ce type de technologie a été utilisé et de donner leur version des faits.

● (1115)

M. Ryan Williams: Merci.

Dans le cadre d'une autre étude du Comité sur la collecte et l'utilisation des données sur la mobilité, il a été question de l'absence de consentement préalable et éclairé relativement à l'utilisation de données et de renseignements personnels. Dans quelle mesure est-il important d'exiger que les Canadiens puissent donner leur consentement explicite et éclairé avant que leurs renseignements personnels soient recueillis?

Mme Cynthia Khoo: Il est extrêmement important que tous les résidents du Canada puissent donner leur consentement préalable et éclairé avant la collecte de données les concernant. C'est un principe fondamental. Je sais que c'est complexe dans le contexte de la justice criminelle, mais c'est justement le genre de considération qui nous oblige à examiner de près le rôle des fournisseurs commerciaux. Ils recueillent énormément de données qui devraient normalement exiger un consentement préalable et éclairé, mais ce consentement n'est pas demandé. Dans certains cas, il n'existe pas d'obligation et, si elle existe, elle n'est pas appliquée. Ces données se retrouvent ensuite entre les mains des organismes d'application de la loi. Je crois que le Comité devrait examiner cette question de très près.

M. Ryan Williams: Merci.

Madame Piovesan, les lois canadiennes prévoient-elles actuellement des garanties concernant l'utilisation des données de reconnaissance faciale? Plus exactement, existe-t-il des garanties concernant les méthodes, les lieux et les périodes de conservation, ou les modalités d'utilisation et de vente?

Mme Carole Piovesan: Les lois sur la protection des renseignements personnels prévoient certaines garanties. Là encore, tout dépend de qui effectue la collecte. Si c'est un organisme public, diverses mesures réglementaires et la common law encadrent déjà la manière dont certains renseignements peuvent être recueillis, stockés et conservés. La législation fédérale sur la protection des renseignements personnels qui s'applique au secteur privé, y compris la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, obligerait les sociétés à obtenir un consentement pour recueillir les données très sensibles, comme l'a dit Mme Khoo. Au Québec, puisque la technologie de reconnaissance faciale fait appel à des données biométriques, un consentement éclairé serait également exigé. Il existe toutes sortes de mesures qui varient selon qui effectue la collecte.

La réglementation est incomplète, et c'est de là que vient le problème. Je dirais même qu'il nous manque une approche exhaustive pour ce qui concerne chacune des étapes de l'utilisation de la technologie de reconnaissance faciale, c'est-à-dire depuis la collecte des données jusqu'à la conception proprement dite du système et à son utilisation... Il faut bien réfléchir aux garanties qui seront nécessaires relativement à la collecte et au stockage des données, à leur évaluation et aux exigences de divulgation. Elles seront peut-être différentes selon que la divulgation est faite par une partie du secteur public ou privé, mais il faudra des exigences dans tous les cas. Nous avons le droit de savoir si des données sur des parties de notre visage, ou quoi que ce soit qui constitue une donnée immuable et sensible sont recueillies, stockées et potentiellement utilisées d'une manière qui pourrait nous porter préjudice.

Comme je l'ai dit, il existe une panoplie de lois et de règlements qui s'appliquent différemment selon qui effectue la collecte de données mais, pour l'instant, aucune loi suffisamment exhaustive ou ciblée n'encadre la technologie de reconnaissance faciale.

M. Ryan Williams: D'accord. Merci beaucoup.

Le président: M. Fergus maintenant. Vous avez six minutes.

[*Français*]

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

J'aimerais remercier nos deux invités de leurs présentations.

Je le fais rarement, mais aujourd'hui je vais m'exprimer en anglais.

[*Traduction*]

Comme les lectures que j'ai faites sur le sujet étaient surtout en anglais, je vais poser mes questions dans cette langue.

Tout d'abord, je voudrais remercier Mmes Piovesan et Khoo de leur contribution à notre étude, et je les remercie également pour les écrits publiés avant que nous entreprenions cette étude.

Madame Khoo, je vais m'adresser à vous en premier. J'ai lu plusieurs des articles auxquels vous avez participé. Celui que vous avez corédigé dans le rapport du Citizen Lab a particulièrement retenu mon attention. Pour la gouverne du Comité, pourriez-vous nous expliquer brièvement en quoi consistent les technologies algorithmiques? Je vous poserai ensuite quelques questions à ce sujet.

● (1120)

Mme Cynthia Khoo: C'est une excellente question. Les technologies algorithmiques peuvent être très larges. Tout dépend du degré de détail donné à la définition. Notre rapport porte plus particulièrement sur les technologies algorithmiques policières. Toutefois, si on y réfléchit bien, la définition pourrait englober le tableur Excel puisqu'il s'agit d'une technologie fondée sur des algorithmes.

Aux fins de la délimitation de la portée de notre rapport — et je crois que ce serait utile également pour délimiter la portée des travaux du Comité —, nous avons considéré que les technologies algorithmiques policières englobent les technologies nouvelles qui utilisent des formules de calcul automatisées le plus souvent pour appuyer ou compléter le processus décisionnel de la police.

L'hon. Greg Fergus: Selon ce que nous avons compris en les étudiant, ces technologies algorithmiques utilisent des données recueillies par la police — et je retiens ce que vous avez dit concernant l'application possible aux travaux du Comité —, alors que la preuve a été faite que ses méthodes de collecte sont fortement biaisées. Est-ce exact?

Mme Cynthia Khoo: Oui, c'est exact.

L'hon. Greg Fergus: Peu importe l'approche algorithmique adoptée relativement à la collecte de données... En fait, n'importe quelle application de l'intelligence artificielle ne fera qu'exacerber les préjugés.

Mme Cynthia Khoo: Je crois que ce serait le cas dans bien des cas, en effet.

L'hon. Greg Fergus: Dans ce cas, je comprends parfaitement votre deuxième recommandation d'imposer un moratoire national sur l'utilisation de ce type de technologie pour le maintien de l'ordre. Cela dit, et j'ai très hâte d'entendre votre réponse, pourquoi limiter le moratoire à cette utilisation? Pourquoi ne pas imposer également un moratoire sur la collecte de ce type de données par le secteur privé et les organismes non gouvernementaux?

Mme Cynthia Khoo: C'est une excellente question.

J'ai centré mes remarques liminaires et la plupart de mes réponses sur le contexte de la justice criminelle pour la simple et bonne raison que c'est ce sur quoi ont porté mes recherches. Je ne veux pas trop m'éloigner des questions sur lesquelles je me suis directement penchée.

N'empêche, il existe selon moi beaucoup de bonnes raisons de faire des recherches aussi fouillées sur l'utilisation de la reconnaissance faciale non seulement dans le secteur commercial, mais aussi au sein des organismes gouvernementaux qui ne sont pas associés au maintien de l'ordre. Je suis convaincue qu'il serait assez facile de justifier l'imposition d'un moratoire sur le recours à la reconnaissance faciale dans ces secteurs également. Le contexte policier est celui que je connais le mieux et dont je peux parler de manière plus approfondie, mais cela ne m'empêche pas de penser que le moratoire pourrait s'appliquer à d'autres contextes.

L'hon. Greg Fergus: Je le mentionne parce que, comme vous l'avez vous-même souligné, des gens pourraient passer par des moyens détournés pour faire indirectement ce qui est interdit pendant que nous mettons au point le cadre législatif qui régira l'utilisation de cette technologie.

J'ai commencé à m'intéresser à cette technologie il y a trois ans. Un radiodiffuseur public canadien, et plus précisément du Québec, dans la partie francophone du Canada, avait décidé de recourir à la technologie de reconnaissance faciale fondée sur l'IA pour identifier les députés de l'Assemblée nationale du Québec. Comme vous l'avez évoqué et comme plusieurs études l'ont montré, le taux d'erreur augmente énormément pour les personnes de couleur ou non blanches.

Je pense qu'il nous appartient à tous de veiller à ce que des limites soient fixées quant à la manière dont ces données sont recueillies et utilisées dans ce contexte, et pas seulement dans le système de justice criminelle.

Qu'en pensez-vous?

Mme Cynthia Khoo: Je pense que vous avez raison. Nous avons vu tellement d'exemples de nouvelles technologies dans le domaine de la reconnaissance faciale, mais également d'autres types de technologies algorithmiques utilisées pour le maintien de l'ordre... Dans l'intérêt de la société et de nos droits, nous aurions dû privilégier une approche de précaution par rapport à ces technologies plutôt que la fameuse approche qui consiste à faire au plus vite, quitte à tout casser sur notre passage.

Je suis d'accord avec Mme Piovesan concernant l'approche chirurgicale de la réglementation et l'utilisation d'un scalpel plutôt que d'une hache. Mais vous avez tout à fait raison. Nous avons besoin de temps pour réfléchir à ce que sera le contenu précis de cette approche.

Si la prudence et la nécessité de prévenir les dommages nous imposent d'interdire temporairement l'utilisation de cette technologie et de prendre le temps de réfléchir, je crois qu'il faut le faire. C'est certainement l'approche la plus raisonnable.

L'hon. Greg Fergus: Il me reste seulement une vingtaine de secondes. J'espère pouvoir en emprunter cinq à mon collègue.

Très rapidement, savez-vous s'il existe un cadre d'utilisation de la reconnaissance faciale fondée sur l'IA quelque part dans le monde?

● (1125)

Mme Cynthia Khoo: Je sais que l'Union européenne a fait énormément de travail dans ce domaine. Je regarderais de ce côté en premier.

Certaines villes américaines, comme je l'ai mentionné, notamment en Californie et au Massachusetts, ont déjà imposé des interdictions, des moratoires et d'autres cadres de réglementation plus ou moins stricts. C'est un autre modèle qui pourrait être examiné.

L'hon. Greg Fergus: Merci beaucoup.

Le président: Merci. Vous avez utilisé votre temps de manière optimale.

Monsieur Villemure, vous avez la parole.

[*Français*]

Vous disposez de six minutes.

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

Je veux remercier les témoins de leurs formidables présentations.

Je vais poser la même question aux deux témoins. J'aimerais obtenir des réponses très brèves, parce que je passerai à un autre aspect par la suite.

Madame Khoo, la reconnaissance faciale signifie-t-elle la fin de la liberté?

[*Traduction*]

Mme Cynthia Khoo: Il faudrait placer cet énoncé dans un contexte un peu plus précis. C'est peut-être un peu exagéré de dire qu'en elle-même, la technologie de reconnaissance faciale nous fera perdre toute notre liberté.

[*Français*]

M. René Villemure: D'accord, je vous remercie beaucoup.

Madame Piovesan, qu'en pensez-vous?

[*Traduction*]

Mme Carole Piovesan: Je suis plutôt d'accord. Certaines applications de la technologie de reconnaissance faciale peuvent être très bénéfiques. J'ai donné l'exemple des soins de santé. Je ne crois pas qu'il faille autoriser ou interdire complètement la reconnaissance faciale. Elle offre des avantages, mais son utilisation comporte aussi des risques sérieux, et il faut tenir compte de ces deux pôles dans l'élaboration d'une réglementation.

[*Français*]

M. René Villemure: Merci beaucoup.

Je vais retourner vers vous, madame Khoo. La quantité d'images captées à ce jour est presque impossible à évaluer. Cela fait-il en sorte qu'il est déjà trop tard pour agir?

[*Traduction*]

Mme Cynthia Khoo: Je crois que quelques précisions s'imposent. Je pense que vous faites allusion aux trois milliards d'images captées par Clearview AI. À certains égards, on peut penser que c'est trop tard puisque Clearview AI capte déjà ces images. La société fait déjà des affaires, elle a déjà signé des contrats avec de nombreux services policiers, et même si elle n'est plus au Canada, elle poursuit ses activités ailleurs dans le monde. Dans ce cas, on peut penser que les dés sont déjà jetés.

Toutefois, il n'est jamais trop tard pour intervenir. Par exemple, la plateforme Clearview AI a déjà été utilisée au Canada, mais elle ne l'est plus parce que le Commissariat à la protection de la vie privée est intervenu après que le voile a été levé. Il y a eu un tollé public. Quand il est question de technologies, il est vraiment tentant de penser qu'elles sont inévitables et que rien ne peut être fait une fois qu'elles sont implantées. Ce n'est pas toujours vrai, loin de là.

Même quand il est question d'autres types de technologies algorithmiques... La Federal Trade Commission des États-Unis a commencé à introduire des mesures de nettoyage des algorithmes dans certains cas, qui consistent non seulement à supprimer des données recueillies illicitement, mais également à supprimer les modèles algorithmiques conçus à partir de ces données.

[*Français*]

M. René Villemure: Merci beaucoup.

Madame Piovesan, est-il trop tard?

[*Traduction*]

Mme Carole Piovesan: Non. Je suis entièrement d'accord avec Mme Khoo.

Il commence à y avoir des pressions, notamment pour ce qui concerne la technologie de reconnaissance faciale, pour que les algorithmes soient nettoyés et que les données soient supprimées. Les choses bougent et, de plus en plus, on réclame une meilleure réglementation qui forcera les entités qui utilisent la technologie de reconnaissance faciale ou d'autres technologies plus larges d'intelligence artificielle à faire la preuve de leur conformité aux exigences techniques, administratives et autres. On veut qu'il soit imposé aux fournisseurs d'établir que l'utilisation de ces technologies convient au marché, et aux utilisateurs de faire une évaluation des incidences. Tout cela montre l'importance d'une utilisation responsable de l'intelligence artificielle, y compris la technologie de reconnaissance faciale.

Bref, je ne crois pas qu'il est trop tard.

[*Français*]

M. René Villemure: Merci, madame Piovesan. Je vais poursuivre avec vous, si vous me le permettez.

Il y a environ deux mois, la Cour supérieure du Québec a rendu un jugement au sujet de Clearview AI, demandant à cette entreprise de restituer les données qu'elle détient ou de les détruire. Clearview AI a simplement refusé, ajoutant qu'elle n'est pas au Canada et que nous n'avons pas autorité sur elle.

Que fait-on dans de tels cas?

[*Traduction*]

Mme Carole Piovesan: L'application de ce type de décisions à l'extérieur de nos frontières est très difficile. Les tribunaux ont déjà soulevé ce problème. Nous nous inspirons du Règlement général sur la protection des données de l'Union européenne, au titre duquel des amendes assez élevées commencent à être distribuées non pas pour des activités menées en territoire européen, mais pour l'utilisation des données des personnes concernées, soit des résidents de pays européens...

Beaucoup d'études sont menées actuellement sur les possibilités d'élargir la zone de compétence et d'application. Nous l'avons constaté au Québec, après l'adoption d'une réforme du régime législatif en matière de protection des renseignements personnels dans le secteur privé. C'est aussi une réflexion qui a eu lieu au cours des travaux entourant l'ancien projet de loi C-11, qui visait à modifier certaines parties de la LPRPDE. Nous attendons de voir les répercussions de la réforme, si elle est adoptée.

● (1130)

[*Français*]

M. René Villemure: Merci beaucoup.

Vous avez parlé d'une approche holistique dans une entrevue récente. J'aimerais que vous en parliez un peu plus.

[*Traduction*]

Mme Carole Piovesan: Volontiers.

L'examen visant à assurer une réglementation adéquate en matière d'intelligence artificielle doit englober certains aspects des données ainsi que l'utilisation et la conception de la technologie. Ailleurs dans le monde, et notamment aux États-Unis et dans l'Union européenne, la tendance est d'aborder la réglementation dans le domaine de l'intelligence artificielle, y compris la reconnaissance faciale, selon une approche axée sur le risque.

Par exemple, dans le projet de loi de l'Union européenne sur l'intelligence artificielle, le caractère critique du risque est prévu d'emblée, ce qui signifie que certaines utilisations sont carrément interdites ou considérées comme étant à risque. Le degré de risque peut baisser pour certaines catégories pour lesquelles il a été considéré comme étant élevé dans la réglementation.

Les catégories à risque font l'objet d'une réglementation plus prescriptive. Cette réglementation impose des exigences claires aux fournisseurs et aux utilisateurs des systèmes visés, des mécanismes de vérification et de validation du système et des données, de même que des contrôles continus pour assurer que le système est utilisé comme prévu.

C'est un point très important parce que quand un système d'IA considéré à risque est utilisé, et sachant que l'intelligence artificielle est très évoluée et unique pour ce qui est de ses capacités d'autoapprentissage et d'autoapplication, il est primordial de faire des contrôles après-coup pour assurer une utilisation continue.

Le président: Merci.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Nous avons pris un peu de retard.

Je vais maintenant donner la parole à M. Green. Vous avez six minutes.

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

Je voudrais commencer par souligner que nous sommes le 21 mars, et que c'est aujourd'hui la Journée internationale pour l'élimination de la discrimination raciale. Cette date a été retenue parce qu'il y a une soixantaine d'années, et plus exactement en 1960, se produisait le massacre des travailleurs par la police de Sharpeville, en Afrique du Sud.

J'aimerais prendre un peu de recul par rapport à la question plus pointue des outils et aborder un petit moment celle des systèmes. Il existe selon moi un lien direct entre ce qui s'est produit lors de l'élaboration du projet de loi C-51 et la mise en place de protocoles de lutte au terrorisme dans les provinces, qui étaient ni plus ni moins des techniques analogiques de reconnaissance faciale. Je parle en fait des contrôles de routine dans les rues et du profilage racial, que l'on appelle aussi le « fichage », par les services de police locaux. Je vais reprendre de là parce que, à mon avis, le profilage racial, qui est une technique analogique, a été très subtilement aboli puis rétabli, comme on a pu le constater ici dans les contrats signés dans le secteur privé qui permettent à des sociétés comme Clearview de faire indirectement ce que les services policiers faisaient directement.

J'aimerais également recadrer la discussion pour parler du système... Je vais axer mes questions sur le principe du maintien de l'ordre prédictif, parce que la reconnaissance faciale me semble un sujet trop large pour que nous puissions en faire le tour.

Mes questions s'adressent à Mme Khoo, qui dans son rapport très complet a posé les bases de certaines des recommandations qui pourront être faites. J'aimerais que Mme Khoo nous fasse un état des lieux pour ce qui a trait au maintien de l'ordre prédictif, aux préjugés raciaux qui en font partie prenante et à l'idée de créer des prisons *de facto* panoptiques dans des communautés où la surveillance et les contrôles policiers sont souvent excessifs, mais les services souvent insuffisants.

Madame Khoo, j'aimerais vous entendre à ce sujet. Si possible, j'aimerais aussi savoir si, selon ce que vous avez pu observer, les contrôles de routine dans les rues et le fichage ont déjà servi de sources de données pour alimenter des outils comme ceux du Centre d'information de la police canadienne, qui seront de toute évidence remplacés par des outils plus évolués comme l'IA et la reconnaissance faciale.

● (1135)

Mme Cynthia Khoo: Merci beaucoup de cette question. J'essaie de rassembler mes idées pour répondre aux nombreuses questions que vous venez de formuler.

Tout d'abord, vous avez tout à fait raison de faire ce lien. C'est quelque chose que nous avons abondamment entendu de la part des militants pour la justice raciale que nous avons rencontrés dans le cadre des recherches que nous avons menées pour notre rapport. Il est clair pour eux qu'il s'agit de violence étatique version XXI^{e} siècle. Avant, on utilisait des stylos et du papier, alors que maintenant, on utilise des ordinateurs et des algorithmes.

Nous essayons de nous dissocier de la notion de « maintien de l'ordre prédictif » tout simplement parce que c'est devenu un terme de marketing qui promet beaucoup plus que ce que la technologie permet d'accomplir. Ce terme a été popularisé et c'est celui que les gens connaissent. Pour mettre en lumière les enseignements de l'histoire de la justice raciale, on peut se demander si le problème perdurerait si la technologie fonctionnait à la perfection. Pour répondre à cette question, il faut réfléchir aux utilisations qu'on en fait. On l'utilise pour les introductions par effraction et la soi-disant criminalité de rue ou contre la propriété. Il est clair qu'on arrêtera un certain type de personnes si on se borne à un certain type d'infractions.

Un projet satyrique très intéressant donne une perspective très éloquente de la situation à New York. Une carte de densité des clics a été publiée pour répertorier ce qu'on a appelé la criminalité des cols blancs. En fait, la carte représente la criminalité dans le quartier des finances du centre-ville de Manhattan. Pourquoi les investisseurs en capital de risque ne se bousculent-ils pas au portillon pour financer le démarrage d'entreprises spécialisées dans le maintien de l'ordre prédictif? Parce que, même si tout fonctionnait à merveille, l'application se ferait encore au profit de certains et au détriment des groupes sociaux historiquement victimes de l'oppression systémique.

Je suis ravie que vous ayez fait un « zoom arrière » sur le contexte de ces technologies. Le prochain groupe de témoins vous permettra de discuter avec la professeure Kristen Thomasen, qui est une de mes collègues. Je vous invite à bien écouter ce qu'elle a à vous dire, car son principal champ d'intérêt englobe le contexte élargi de ces technologies, qui sont en fait des systèmes sociotechniques qui ne peuvent pas être dissociés de leur contexte historique. Au Brésil, un nouveau champ de recherche s'intéresse à la responsabilité algorithmique critique, ou IA critique. Les chercheurs ont voulu savoir ce qui se produirait si les études en matière d'intelligence artificielle étaient décolonisées, ou si on mettait les groupes historiquement marginalisés au centre des travaux des équipes d'experts en science des données ou des personnes qui étudient ces questions.

J'aurais une ou deux autres remarques à formuler, mais je crois que je vais m'arrêter ici.

M. Matthew Green: Il me reste une minute... Je me souviens, quand j'étais conseiller municipal, de m'être intéressé aux questions des contrôles de routine dans les rues et de profilage racial. J'ai soumis des demandes d'accès à l'information et j'ai obtenu une note de service interne du ministère du Procureur général de l'Ontario dans laquelle il était énoncé que le protocole de lutte au terrorisme offrait une occasion unique de faire une collecte massive de données dans le cadre des contrôles de routine dans les rues.

Je pense notamment à l'utilisation de Clearview par le Service de police d'Hamilton. J'y fais souvent référence quand il est question de vols d'identité et des poursuites judiciaires qui suivent. Je repense souvent à ce qui était constamment répété concernant le maintien de l'ordre prédictif.

J'en ai entendu parler pour la première fois lors d'une séance de planification des activités du Service de police d'Hamilton. Je ne pouvais pas m'empêcher de penser au film *Rapport minoritaire* et à la terreur que nous inspirait ce commentaire social dystopique il y a 20 ans. Aujourd'hui, ce n'est plus de la science-fiction.

Merci.

Le président: Nous allons passer à la prochaine série de questions de cinq minutes en commençant par M. Kurek.

Vous avez la parole, monsieur Kurek.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup. J'ai bien aimé les témoignages et les questions qui ont été posées.

Toute cette discussion, qu'il s'agisse de la reconnaissance faciale ou de l'intelligence artificielle, concerne ce qui est en fait une boîte de Pandore ayant d'énormes conséquences sur notre société, l'application de la loi et la technologie. En lisant à ce sujet, nous voyons que cela touche tout, de la façon dont nous utilisons nos téléphones à des preuves recueillies sans consentement à des fins de poursuites criminelles.

J'espère que vous pourrez toutes les deux répondre à quelques questions. Ma première porte sur l'interaction entre l'État et les sociétés privées et, parfois, les contrats par lesquels des acteurs étatiques — qu'il s'agisse de services de police ou autres — collaborent avec des sociétés privées.

Mme Khoo peut répondre en premier. Avez-vous des recommandations précises sur la forme que devrait prendre la réglementation pour assurer la protection de la vie privée des Canadiens dans ces cas?

● (1140)

Mme Cynthia Khoo: Je vais d'abord présenter trois recommandations.

Premièrement, si les autorités chargées de l'application de la loi envisagent d'adopter une technologie de reconnaissance faciale ou une technologie algorithmique policière, elles peuvent vraiment le faire sans collaborer avec un fournisseur commercial. Par exemple, le Saskatchewan Police Predictive Analytics Lab a développé lui-même toute sa technologie, précisément pour éviter ce genre de problèmes et d'être redevable à des intérêts privés. C'est une technologie financée par l'État. Tout est géré par la province, l'Université de la Saskatchewan et le service de police municipal. Cela ne signifie pas qu'il n'y a aucun problème, mais cela élimine au moins les problèmes qui découleraient d'une association avec un fournisseur commercial.

Deuxièmement, si vous avez décidé de vous approvisionner auprès d'un fournisseur commercial, notre suggestion est de prévoir plusieurs conditions d'achat très sévères. Un exemple serait de ne pas faire affaire avec une entreprise qui refuse de renoncer à ses secrets commerciaux aux fins de vérifications indépendantes, et de veiller à ce que le respect des normes d'intérêt public en matière de protection des renseignements personnels soit une obligation contractuelle.

La troisième façon de protéger la vie privée et d'assurer la reddition de comptes est de réduire le secret entourant ces contrats. Nous ne devrions pas apprendre que ces contrats existent après coup, à la suite de divulgations, de demandes répétées d'accès à l'information ou d'enquêtes journalistiques. Nous devrions être informés avant qu'ils ne soient conclus, alors qu'ils en sont encore à l'étape de l'appel d'offres, et nous devrions avoir l'occasion de les commenter.

M. Damien Kurek: Je vous remercie beaucoup.

Madame Piovesan, aimeriez-vous ajouter quelque chose?

Mme Carole Piovesan: Je suis tout à fait d'accord avec Mme Khoo.

J'ajouterais qu'il y a aussi un aspect concernant la mobilisation des intervenants. Nous devons avoir la possibilité de communiquer avec la communauté, notamment avec les personnes touchées, et d'avoir une discussion sérieuse sur l'utilisation de ces technologies et leurs incidences avant qu'elles ne soient déployées.

Nous avons beaucoup entendu parler de la transparence radicale. Lorsque nous parlons d'une chose aussi importante que la technologie de reconnaissance faciale, l'application et l'adoption d'un concept de transparence radicale peuvent se révéler très utiles.

De plus, pour ce qui est de la capacité d'expliquer, serons-nous capables de comprendre comment ces algorithmes fonctionnent? Pourrons-nous comprendre les résultats qu'ils fournissent et obtenir une vérification indépendante qui nous assurera qu'ils sont exacts et fiables?

M. Damien Kurek: Je vous remercie de votre réponse.

C'est intéressant. J'ai devant moi un article dont le titre est « La police de Toronto a utilisé le logiciel de reconnaissance faciale Clearview AI dans 84 enquêtes » et dans lequel il est écrit qu'au moins deux affaires ont été portées devant les tribunaux. Ce n'est pas seulement théorique; c'est quelque chose qui se passe en ce moment.

Particulièrement dans un contexte d'une guerre en Europe et de quelques discussions sur la reconnaissance faciale et l'intelligence artificielle dans un contexte militaire, lorsque l'on pense à la Convention de Genève, il est question de bombes larguées par les avions. Il s'agit cependant d'un tout nouveau domaine dont les conséquences sont énormes.

Beaucoup de mes électeurs m'ont fait part de leurs préoccupations au sujet de l'identification numérique, du système de crédit social et de certains enjeux associés au fait que l'État établit des liens entre vos renseignements et certains volets de votre interaction avec le gouvernement. Je me demande si vous deux, j'espère...

Mon temps est écoulé.

Le président: Vous allez devoir accorder aux témoins environ 15 secondes pour répondre. Nous devrons ensuite reprendre la discussion au prochain tour.

Je ne sais pas qui souhaite intervenir brièvement pour répondre aux questions de M. Kurek.

Mme Cynthia Khoo: Je crois que nous pensions qu'il avait terminé. Nous essaierons peut-être de nouveau au prochain tour.

Le président: Nous allons garder cela en mémoire.

La parole est maintenant à Mme Hepfner.

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

Je remercie les témoins de leur participation ce matin. C'est très intéressant et aussi, je pense, très technique. Je vais peut-être paraître un peu répétitive, mais je veux m'assurer de bien comprendre vos opinions.

J'aimerais commencer par la LPRPDE. Nous savons que le gouvernement examine actuellement ce cadre stratégique numérique et qu'il essaie de l'adapter. Ce cadre a été élaboré avant l'existence des logiciels de reconnaissance faciale. Pourriez-vous nous dire exactement quel genre d'améliorations vous aimeriez voir dans ce projet de loi. Que pouvons-nous faire pour rendre cette loi plus appropriée à ces technologies? Ce ne sera pas la dernière nouvelle technologie à laquelle nous devrons réagir. Il y en a sans cesse de nouvelles, et la loi n'évolue pas au même rythme. J'aimerais savoir si vous avez des idées sur ce qui nous donnerait plus de souplesse afin que nous puissions mieux répondre aux enjeux liés à la protection de la vie privée à mesure que de nouvelles technologies comme celle-ci apparaissent dans notre société.

Nous pourrions peut-être entendre d'abord Mme Khoo.

● (1145)

Mme Cynthia Khoo: Je crois que pour améliorer la LPRPDE, la première chose, la chose la plus importante — réclamée, je crois, par beaucoup de défenseurs de la protection de la vie privée depuis l'élaboration de cette loi — est de régler le problème de son application. Il y a beaucoup de cas où la LPRPDE, sur le plan de son contenu juridique et de ce qu'elle permet et ne permet pas, interdirait en fait l'activité réalisée.

Dans le cas de Facebook et de Cambridge Analytica, par exemple, l'activité a été jugée illégale en vertu de la LPRPDE. Dans le cas de Clearview AI, ils ont réussi... La LPRPDE englobait l'activité, mais le Commissariat à la protection de la vie privée n'avait pas le pouvoir de rendre des ordonnances. Il aurait été obligé de poursuivre l'entreprise devant les tribunaux. Il n'avait pas le pouvoir d'imposer des amendes, encore moins des amendes en vertu du Règlement général sur la protection des données, ou RGPD.

Je pense que le changement le plus percutant qui pourrait être fait serait de donner plus de mordant au Commissariat à la protection de la vie privée pour assurer le respect des ordonnances rendues contre les entreprises déjà reconnues coupables d'activités illégales en vertu de la LPRPDE, ou de ce qui suivra la LPRPDE.

Mme Carole Piovesan: Je suis d'accord sur l'enjeu de l'application de la loi. Je pense qu'un aspect intéressant du projet de loi C-11 est qu'il envisageait de créer un tribunal qui surveillerait des violations bien précises à la loi et pourrait imposer des sanctions plus sévères. J'espère que c'est quelque chose que nous verrons encore à la prochaine étape.

Nous avons également constaté que, dans une certaine mesure, le projet de loi C-11 élargissait les divers aspects du consentement à la collecte, à l'utilisation et à la communication de renseignements personnels. Encore une fois, il ne faut pas oublier que la LPRPDE est une loi sur la protection des renseignements personnels dans le secteur privé. Nous devons tenir compte de certaines des utilisations positives de la technologie de reconnaissance faciale, et c'est pourquoi je dis qu'elle doit être réglementée à l'aide d'un scalpel et non d'une hache. Il y a des utilisations très intéressantes, mais nous avons besoin de mesures de protection appropriées pour veiller à ce que ces utilisations soient bien contrôlées et encadrées, et qu'elles servent l'intérêt public sans aller contre nos valeurs. Il est très important de voir cela dans la nouvelle LPRPDE, peu importe ce que sera le résultat final de la réforme.

Mme Lisa Hepfner: Je vous remercie beaucoup.

Cela cadre parfaitement avec ma prochaine question, à savoir quels sont les avantages sociétaux que nous pouvons tirer de cette technologie? Nous avons beaucoup entendu parler des enjeux liés à la protection de la vie privée et à la discrimination. Mis à part les avantages commerciaux évidents pour les entreprises qui possèdent un logiciel de ce genre, quels sont les avantages pour la société?

Mme Carole Piovesan: Cela me fait plaisir de répondre en premier. J'ai parlé de l'utilisation de la reconnaissance faciale dans le domaine de la santé, où nous avons vu des exemples dans lesquels les TRF aident à surveiller les patients et à s'assurer que leur condition ne change pas, surtout s'ils sont alités et peut-être incapables de parler. Nous avons appris qu'il y avait de très bonnes utilisations des TRF dans le domaine des soins de santé. La prudence est évidemment de mise à l'égard de la collecte des données et de l'utilisation de cette technologie. La conservation des données est très importante. La divulgation restreinte de ces données est extrêmement importante. Mais nous constatons d'importantes retombées positives dans le secteur de la santé.

Personnellement, je me sers de la reconnaissance faciale pour prouver mon identité et utiliser les services bancaires et mon téléphone. Je le répète, nous voulons qu'il y ait des contrôles très sévères. Nous considérons qu'elle est utile. Est-ce quelque chose d'absolument nécessaire? Non, mais cela peut être une façon très sûre de faire un paiement dans un aéroport ou d'effectuer une transaction financière.

Il peut y avoir des avantages pour la société. L'enjeu est donc d'établir s'il y a un avis de divulgation approprié concernant la collecte de ces données et sur la façon dont elles seront utilisées. Y a-t-il une période de conservation appropriée qui, au bout du compte, relève de l'utilisateur? C'est exactement l'objectif de la LPRPDE: redonner aux utilisateurs certains pouvoirs à l'égard de la protection des renseignements personnels, avec...

Le président: Je vais devoir passer à un autre intervenant. Il ne nous reste plus beaucoup de temps. Je vous remercie de votre réponse.

La parole est maintenant à M. Villemure.

[*Français*]

Vous avez deux minutes et demie.

M. René Villemure: Merci, monsieur le président. Deux minutes et demie, cela passe très vite.

Madame Piovesan, je vais encore m'adresser à vous.

Vous avez fait allusion au Règlement général sur la protection des données, ou RGPD. J'aimerais savoir quelles seraient les meilleures pratiques du RGPD dont on pourrait s'inspirer.

En même temps, on a parlé du consentement qui était difficile à obtenir, mais, au bout du compte, est-il impossible de l'obtenir?

● (1150)

[*Traduction*]

Mme Carole Piovesan: Vous savez, le consentement peut être très difficile selon le scénario d'utilisation, particulièrement en ce qui a trait à l'évolutivité de la technologie de reconnaissance faciale, mais il ne devrait pas être écarté à titre d'exigence. Nous devons inclure le consentement et en faire une exigence clé. Nous parlons d'un point de données biométriques immuable sur une personne. Avoir un avis approprié, et accorder un certain contrôle à la personne sur les décisions relatives au partage des données ou à la façon dont elles sont recueillies est absolument essentiel. Je ne veux pas laisser entendre que le consentement ne devrait jamais être un facteur dans le cas des technologies de reconnaissance faciale. Ce n'est absolument pas le cas.

Lorsque nous examinons le RGPD, nous pouvons certainement nous inspirer des exigences en matière de profilage dont il a été question au Québec, je le sais, concernant un droit de recours et un droit d'opposition au profilage réalisé uniquement par des moyens automatiques. C'est quelque chose dont nous devrions tenir compte, et j'encourage de nouveau fortement le Comité à examiner la législation sur l'intelligence artificielle de l'Union européenne. Elle n'est pas encore finale, mais elle peut être une véritable source d'inspiration. Le projet de loi américain sur la responsabilité algorithmique mérite aussi d'être examiné.

[*Français*]

M. René Villemure: D'accord.

Parlez-moi un peu encore de la transparence radicale.

[*Traduction*]

Mme Carole Piovesan: La transparence radicale concerne l'ensemble du processus de divulgation, c'est-à-dire de permettre, d'être ouvert, de dire aux gens qui sont vos fournisseurs, quelles sont vos utilisations, où vous recueillez ces données et pourquoi vous le faites. Il s'agit surtout de faire participer le public plutôt que, comme Mme Khoo l'a mentionné à plusieurs reprises, de favoriser ce contexte de secret qui mine notre confiance et qui commence aussi à compromettre certaines valeurs qui sont très importantes pour les Canadiens.

La transparence radicale repose sur le principe que nous allons informer nos électeurs sur ce que nous faisons avec la reconnaissance faciale — ou avec toute autre technologie vraiment avancée susceptible d'avoir une incidence sur leurs droits —, les inviter à participer de façon significative à la discussion, et présenter des rapports sur certains des extrants obtenus, y compris des rapports sur les relations avec les fournisseurs.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Il nous reste deux minutes et demie pour entendre M. Green.

M. Matthew Green: Merci.

J'aimerais revenir sur un sujet qui a été soulevé à l'occasion que mon collègue du Bloc, et qui m'intéresse également, à savoir le capitalisme de surveillance. Mes questions s'adressent à Mme Khoo et portent sur la relation avec les entreprises privées. Nous avons parlé de Clearview. Nous connaissons d'autres cas, notamment celui d'Amazon. Nous savons aussi que la technologie Ring pour les sonnettes de porte permet de privatiser et d'exploiter l'espace public subrepticement, à l'insu des gens.

J'aimerais savoir ce que vous en pensez, et que vous nous parliez ensuite des risques d'utilisations abusives de la part du secteur privé et du gouvernement. Je pense aux façons dont il est utilisé pour observer les autres. Vous avez parlé d'une analyse comparative entre les sexes.

Je me demande si vous auriez quelques observations sur ces deux sujets.

Mme Cynthia Khoo: Absolument. Merci.

Pour ce qui est d'exploiter l'espace public, c'est certainement quelque chose qui nous préoccupe, et Amazon Ring en est l'exemple parfait. À ma connaissance, ces situations ne se sont pas encore produites ici. Encore une fois, Mme Thomasen pourra vous donner plus de détails à ce sujet. Je crois qu'Amazon Ring s'est intéressée à Windsor à un moment donné.

Nous savons qu'il existe des partenariats ouverts — bien, nous savons qu'il y en a maintenant — entre Amazon et des services de police. Les services de police sont pratiquement devenus responsables du marketing d'Amazon Ring, ce qui soulève de nombreuses préoccupations tant du point de vue du secteur privé que du secteur public, mais surtout sous l'angle du secteur public.

Le capitalisme de surveillance est un volet de cet écosystème de surveillance public-privé, car il est lié aux structures incitatives. Il y a les entreprises privées qui ont leurs propres motivations pour recueillir le plus de données possible afin d'en tirer profit et dont une grande partie du financement provient alors de subventions gouvernementales. Que ce soit sous le couvert de l'innovation ou parce qu'elles ont fait pression sur le gouvernement en coulisses pour obtenir ces subventions précises, elles sont financées par le gouvernement. Dans une certaine mesure, c'est parce que le gouvernement accepte cette histoire d'innovation ou qu'il se dit simplement que si l'entreprise recueille toutes ces données, il y aura peut-être accès lui-même un jour. C'est essentiellement le gouvernement et les entreprises privées qui travaillent main dans la main au développement de ce réseau de surveillance.

Vous avez aussi parlé des utilisations abusives. Nous en avons énormément d'exemples. En fait, en répondant à la question précédente sur les utilisations possiblement positives de la technologie de reconnaissance faciale, j'ai pensé...

● (1155)

Le président: Je suis vraiment désolé, mais je dois vous interrompre afin que nous puissions passer aux deux dernières séries de questions. Vous pourrez peut-être reprendre au même endroit.

Je dois abréger les deux derniers tours. M. Bezan et Mme Khalid auront chacun trois minutes.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président. C'est dommage parce que j'ai plusieurs questions.

Je remercie nos deux témoins de leurs excellentes observations.

Commençons par Mme Khoo. Vous et Mme Kate Robertson avez envoyé une lettre au commissaire à la protection de la vie privée du Canada le 22 octobre 2021. Avez-vous reçu une réponse à cette lettre et, dans l'affirmative, pouvez-vous la transmettre au Comité?

Mme Cynthia Khoo: À ce que je sache, nous n'avons pas obtenu de réponse, mais je vais vérifier auprès de ma collègue Kate Robertson et nous pourrons assurer un suivi si vous le désirez.

M. James Bezan: D'accord, veuillez le faire, car je crois vraiment ce que vous avez écrit dans cette lettre, lorsque vous dites qu'il y a trois volets aux technologies algorithmiques policières. Vous parlez de moratoires, vous demandez au gouvernement fédéral de mener une enquête judiciaire, que les gouvernements prennent des mesures pour que la fiabilité, la nécessité et la proportionnalité, ainsi que la transparence, soient des conditions préalables, et qu'il y ait des directives plus précises sur les technologies algorithmiques policières, ou les services de police prédictifs — ce qui est encore plus inquiétant —, etc.

Dans votre lettre, vous parlez des « pires cas de violation des droits de la personne et de la Charte qui pourraient survenir si le gouvernement canadien et les autorités chargées de l'application de la loi utilisaient des technologies algorithmiques policières ». Vous devriez atténuer cela.

Comment pouvons-nous, en tant que parlementaires, faire cela alors que nous cherchons à élaborer des règlements qui respectent nos droits en vertu de la Charte et, au bout du compte, établir un équilibre entre la transparence, la capacité des gens d'accepter ou de refuser, et l'optimisation de la technologie qui s'en vient?

Mme Cynthia Khoo: En tant que parlementaires, la première chose que vous pourriez faire et notre première recommandation serait de lancer une enquête, essentiellement, ou une commission nationale sur ces technologies.

Dans le contexte des travaux du Comité, je recommandais de décréter un moratoire sur la reconnaissance faciale. Cependant, dans ce rapport, nous demandons en fait un moratoire sur toutes les technologies algorithmiques policières en attendant de mener, à la lumière des résultats de cette enquête — qu'il s'agisse d'une commission nationale ou d'une enquête judiciaire —, une analyse constitutionnelle et des droits de la personne beaucoup plus approfondie que ce que nous avons pu faire, afin que vous puissiez définir ce qui est approprié et ce qui ne l'est pas, établir les mesures de protection requises, et assurer ensuite la mise en œuvre de ces mesures.

Autrement, ce train continue d'avancer. Une pause nationale est nécessaire pour nous donner le temps de décider ce qu'il faut faire avec cette technologie et éviter de nous retrouver devant des faits accomplis longtemps après.

M. James Bezan: Le commissaire à la protection de la vie privée aurait le pouvoir de décréter cette pause si nous croyons qu'il y aura des violations aux droits à la vie privée des Canadiens, et nous aurions ainsi le temps de faire l'évaluation.

Combien de services de police canadiens utilisent la technologie de reconnaissance faciale?

Mme Cynthia Khoo: C'est une excellente question.

Si nous parlons de Clearview AI, je crois que plusieurs dizaines en faisaient l'essai. Cependant, aux fins de notre rapport, pour ce qui est de savoir qui l'utilisait vraiment, nous avons constaté que c'était le service de police de Toronto et le service de police de Calgary.

J'ai appris le mois dernier que le service de police d'Edmonton avait signé un contrat, mais pas avec Clearview AI; c'est avec NEC Corporation, et il s'agit donc d'une autre technologie de reconnaissance faciale.

Dans notre rapport, nous avons indiqué que York et Peel avaient annoncé qu'elles envisageaient elles aussi conclure des contrats.

Le président: Je vais devoir passer à un autre intervenant, mais c'est une excellente question et si vous avez d'autres renseignements précis à ce sujet, ils nous seraient probablement très utiles dans la préparation de notre rapport.

Sur ce, nous allons terminer avec Mme Khalid qui dispose de trois minutes.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Merci beaucoup, monsieur le président, et merci à nos témoins qui ont été très convaincantes aujourd'hui.

Pour gagner du temps, je vais poser cette question à Mme Piovesan. C'est quelque chose que nous voyons dans Facebook lorsque nous publions une photo de nous et de nos amis. Soudainement, au moment de faire les identifications, une liste de personnes dont il pourrait s'agir s'affiche, et neuf fois sur dix, c'est exact. Nous avons ces plateformes de médias sociaux qui utilisent la reconnaissance faciale et leurs algorithmes. Elles produisent ces cercles ou bulles de relations, et nous avons vu comment l'aspect commercial de cette activité influence la discrimination, l'émergence de points de vue extrêmes, etc.

Pourriez-vous nous parler de cet aspect commercial? Comment pouvons-nous en restreindre la portée pour nous assurer que les entreprises puissent offrir efficacement des services aux consommateurs sans que ceux-ci deviennent des moutons poussés dans une certaine direction, non seulement sur le plan des produits, mais aussi des idéologies?

● (1200)

Mme Carole Piovesan: J'ai quatre propositions rapides.

La première est que nous devons mener une évaluation de l'incidence des systèmes afin de comprendre où se trouvent les risques, les conséquences imprévues possibles et les préjudices prévisibles.

Cela mène ensuite à une évaluation de l'incidence dans laquelle les répercussions possibles de ce système sur les personnes, la propriété et les droits sont examinées en détail. Cette évaluation doit être approfondie, comme ce qui se fait déjà dans le domaine de la protection des renseignements personnels et ce que Mme Khoo a décrit comme étant l'évaluation de l'incidence algorithmique déjà adoptée par le gouvernement fédéral.

De plus, il doit y avoir une divulgation claire et simple qui aidera les personnes à prendre des décisions dans un contexte commercial précis. Souvent, il ne s'agit pas de quelque chose d'essentiel, c'est simplement quelque chose d'agréable. Les gens doivent avoir la possibilité de comprendre comment leurs renseignements seront utilisés, non pas au moyen de politiques de protection des renseignements personnels de 20 pages — ce que je rédige moi-même tout le temps —, mais par le biais d'information claire, simple et fournie en temps opportun qui leur permettra de décider de donner ou non leur consentement, et de le modifier s'ils changent d'idée. S'ils acceptent au départ que leur visage soit utilisé, ils ont le droit de modifier leur décision plus tard.

Mme Iqra Khalid: Merci. Je comprends.

Je vois qu'il me reste 20 secondes, mais madame Khoo, auriez-vous quelque chose à ajouter à ce sujet?

Mme Cynthia Khoo: Je n'ai rien à ajouter, mais je vais profiter de l'occasion pour revenir aux commentaires formulés par M. Green sur la justice raciale et recommander la lecture du livre de Simone Browne, intitulé *Dark Matters*, qui retrace les origines de la surveillance biométrique jusqu'à l'esclavage transatlantique et au marquage des esclaves. Elle soutient que c'est l'origine de la surveillance biométrique.

Le président: Je remercie beaucoup nos témoins.

Sur ce, nous allons suspendre brièvement la séance.

M. Matthew Green: Monsieur le président, avant de suspendre la séance, pourrais-je par votre intermédiaire inviter les témoins à fournir au Comité une réponse écrite dont nous pourrons tenir compte dans nos rapports s'ils ont l'impression de ne pas avoir eu chance de donner des réponses complètes?

Je m'en voudrais de ne pas partager les préoccupations [*inaudible*].

Le président: Oui, vous pouvez le faire et c'est maintenant fait.

Merci, monsieur Green.

J'aimerais faire un commentaire général à l'intention des membres du Comité. Lorsque vous posez une question élaborée et ne vous laissez que 10 secondes pour obtenir une réponse, vous me placez dans l'inconfortable position d'avoir à interrompre notre témoin. Il faudrait gérer votre temps de façon à pouvoir obtenir des réponses et non seulement à poser vos questions.

Sur ce, nous allons suspendre...

M. Matthew Green: Monsieur le président, les sujets compliqués soulèvent des questions complexes.

Si les témoins peuvent fournir des réponses plus étoffées, ce serait bien de pouvoir en tenir compte.

● (1205)

Le président: Je suis tout à fait d'accord.

Sur ce, nous allons suspendre brièvement la séance pendant que les prochains témoins prennent place.

● (1205)

_____(Pause)_____

● (1205)

Le président: Nous reprenons la séance.

J'invite toutes les personnes présentes à s'asseoir et à éviter les discussions en aparté afin que nous puissions commencer. Merci.

Nous sommes déjà pressés par le temps. Nous allons d'abord entendre les déclarations préliminaires. Je vais demander à nos témoins de respecter un maximum absolu de cinq minutes. Je vais devoir les interrompre dès que ce temps sera écoulé.

Aujourd'hui, nous entendrons à titre personnel Mme Ana Brandusescu, experte en gouvernance de l'intelligence artificielle, Mme Kristen Thomasen, professeure à la Peter A. Allard School of Law de l'Université de la Colombie-Britannique, et Mme Petra Molnar, directrice associée du Refugee Law Lab.

Nous entendrons d'abord Mme Brandusescu.

Vous avez une durée maximale absolue de cinq minutes, madame Brandusescu.

Mme Ana Brandusescu (experte en gouvernance de l'intelligence artificielle, à titre personnel): Bonjour, monsieur le président et membres du Comité. Je vous remercie de m'accueillir ici aujourd'hui.

Je m'appelle Ana Brandusescu et je fais de la recherche sur la gouvernance et l'approvisionnement en technologies de l'intelligence artificielle, en particulier par le gouvernement. Cela comprend la technologie de reconnaissance faciale, ou TRF.

Aujourd'hui, je voudrais vous présenter deux enjeux et trois solutions. Le premier enjeu est la discrimination. La TRF distingue mieux les visages des hommes blancs que les visages noirs, bruns, autochtones et transgenres. Nous le savons grâce aux travaux révolutionnaires d'universitaires comme Joy Buolamwini et Timnit Gebru. Leur étude a révélé que:

> [...] les femmes à la peau plus foncée constituent le groupe le plus incorrectement classé (avec des taux d'erreur allant jusqu'à 34,7 %). Le taux d'erreur maximal pour les hommes à la peau claire est de 0,8 %.

La TRF génère beaucoup de faux positifs. Cela signifie que l'on pense que vous êtes quelqu'un d'autre, et cela amène les autorités à arrêter des personnes innocentes. La journaliste Khari Johnson a récemment relaté dans Wired que trois Noirs avaient été arrêtés à tort aux États-Unis après avoir été mal identifiés par la TRF.

En outre, les RH pourraient refuser d'embaucher quelqu'un en raison d'une erreur de la TRF ou permettre à une compagnie d'assurance de refuser de couvrir une personne. La TRF est plus que problématique.

Dans un rapport de 2021, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a dit qu'il y avait du racisme systémique dans les services de police du Canada. La TRF exacerbe le racisme systémique.

Le deuxième enjeu est l'absence de mécanismes de réglementation. Dans un rapport que j'ai rédigé en collaboration avec Yuan Stevens, un spécialiste de la cybersécurité et de la protection des renseignements personnels, pour le Centre for Media, Technology and Democracy, nous avons écrit qu'en tant que contribuables, nous payons essentiellement pour être surveillés, alors que des entreprises comme Clearview AI peuvent tire profit des processus d'approvisionnement en technologie du secteur public.

La réglementation est difficile. Pourquoi? Comme la plupart des grandes technologies, l'IA transcende les frontières politiques. Elle peut aussi échapper aux politiques d'approvisionnement, comme lorsque Clearview offre des essais gratuits de logiciels. Puisque la TRF est intégrée à des systèmes complexes et opaques, il est parfois difficile pour un gouvernement de savoir que la TRF fait partie d'un progiciel.

En juin 2021, le Commissariat à la protection de la vie privée du Canada a clairement dit que des contrôles étaient nécessaires pour s'assurer que la GRC respecte la loi lorsqu'elle utilise de nouvelles technologies. Cependant, dans sa réponse au commissaire, la GRC se montrait favorable à l'autoréglementation de l'industrie. L'autoréglementation — par exemple, sous la forme d'évaluations de l'incidence algorithmique — peut s'avérer insuffisante. Une grande partie de la réglementation relative à l'IA est essentiellement une activité volontaire.

Quelle est la voie à suivre? Des entités gouvernementales, grandes et petites, ont demandé une interdiction de l'utilisation des TRF, et certaines l'ont déjà fait. Ce devrait être l'objectif final.

La Montréal Society and Artificial Intelligence Collective, à laquelle je collabore, a participé à la consultation publique tenue en 2021 sur le projet de politique sur l'IA de la Commission de services policiers de Toronto. Je vais partager certaines des recommandations présentées, ainsi que les miennes. Je propose trois solutions.

La première solution est d'améliorer les marchés publics. Dans le cas de Clearview AI, l'entreprise s'en est tirée impunément avec ce qu'elle a fait dans de multiples administrations au Canada parce qu'il n'y avait eu aucun processus contractuel ou d'approvisionnement. Pour éviter cela, le Commissariat à la protection de la vie privée devrait adopter une politique de divulgation proactive des essais gratuits de logiciels réalisés par les autorités responsables de l'application de la loi et l'ensemble du gouvernement, et mettre sur pied un registre public de ces essais. Cette boîte noire doit devenir une boîte de verre. Nous devons savoir ce que l'on nous vend. Nous devons accroître notre expertise interne en matière d'intelligence artificielle, sans quoi nous ne pouvons être certains que les organismes comprennent vraiment ce qu'ils achètent. De plus, les entreprises liées à des violations des droits de la personne, notamment Palantir, devraient être retirées de la liste des fournisseurs d'IA préqualifiés du Canada.

La deuxième solution est d'accroître la transparence. Le Commissariat à la protection de la vie privée devrait collaborer avec le Conseil du Trésor pour créer un autre registre, cette fois pour l'IA, et plus particulièrement l'IA utilisée à des fins d'application de la loi et de sécurité nationale, et pour les organismes qui envisagent d'utiliser la reconnaissance faciale pour les services d'aide sociale tels que l'assurance-emploi. Un registre de l'IA sera utile aux chercheurs, aux universitaires et aux journalistes d'enquête qui informent le public. Nous devons également améliorer nos évaluations de l'incidence algorithmique, aussi appelées EIA.

Les EIA devraient véritablement mobiliser la société civile. Pourtant, les seuls intervenants non gouvernementaux externes consultés dans les trois EIA publiées au Canada étaient des entreprises. En collaboration avec le Conseil du Trésor, le Commissariat à la protection de la vie privée devrait élaborer des exigences plus précises à l'égard de la surveillance continue et de la production de rapports afin que le public puisse savoir si l'utilisation ou l'incidence d'un système a changé depuis la première EIA.

La troisième solution est de faire de l'imputabilité une priorité. À l'intérieur, le Commissariat devrait assurer le suivi des engagements de la GRC envers la protection des renseignements personnels et exiger un rapport public expliquant en détail comment elle utilise la TRF. Cette pratique pourrait s'appliquer à tous les ministères et organismes à l'avenir. À l'extérieur, le Commissariat et le Conseil du Trésor devraient financer et écouter la société civile et les groupes communautaires qui travaillent sur des enjeux sociaux, pas seulement sur les enjeux liés à la technologie.

Merci.

● (1210)

Le président: Merci beaucoup.

Nous allons maintenant passer la parole à Mme Thomasen pour cinq minutes.

Mme Kristen Thomasen (professeure, Peter A. Allard School of Law, University of British Columbia, à titre personnel): Merci, monsieur le président, et merci aux membres du Comité.

Je vous parle depuis le territoire non cédé des nations Squamish, Tsleil-Waututh et Musqueam.

Comme vous l'avez entendu, je suis professeure de droit et je mène des recherches sur la réglementation nationale de l'intelligence artificielle et la robotique, et en particulier sur les aspects touchant les espaces publics et la protection de la vie privée. Je témoigne aujourd'hui à titre personnel.

Je suis très reconnaissante d'avoir été invitée par le Comité à contribuer à cette importante étude. Je vous encourage fortement à intégrer une véritable optique d'égalité dans votre rapport et les recommandations qui seront soumises au gouvernement.

De nombreuses recherches ont déjà montré à quel point les diverses formes de surveillance faciale peuvent être inéquitables, particulièrement dans les cas d'identifications erronées en raison de la race, du sexe et de l'âge, ainsi que de la qualité et de la source des données utilisées pour développer ces systèmes. Cependant, même les systèmes de surveillance faciale extrêmement précis reposant sur des données réputées provenir de sources légales peuvent, pour diverses raisons, refléter et aggraver les inégalités sociales. Je vais aborder certains éléments clés et je répondrai ensuite avec plaisir à d'autres questions, notamment sur les cas manifestement limités d'utilisation utile.

Premièrement, les systèmes de surveillance faciale sont des systèmes sociotechniques, ce qui signifie que l'on ne peut pas comprendre ces technologies en examinant simplement la conception d'un système. Il faut aussi considérer la manière dont le système interagira avec les utilisateurs, les personnes visées et les milieux sociaux dans lesquels le système est déployé.

La reconnaissance faciale renforce et perfectionne la surveillance. Elle est utilisée à des endroits où, par exemple, la Cour suprême du Canada — entre autres — a déjà reconnu que les communautés sont trop surveillées pour des motifs liés à la protection de l'identité. Les groupes qui luttent pour l'égalité font l'objet d'une surveillance des relations interpersonnelles, étatiques et commerciales accrue, et peuvent subir des préjudices qualitativement plus importants en raison de cette surveillance. Une surveillance plus perfectionnée signifie plus de préjudices à la vie privée et plus d'inégalité.

J'exhorte le Comité à tenir compte du contexte social dans son rapport et ses recommandations, y compris du fait que la surveillance biométrique n'est pas une nouveauté. Je vous encourage à examiner la surveillance faciale à la lumière de son évolution historique, qui émane des idéologies eugéniques et de suprématie blanche.

Dans une partie du contexte sociotechnique dans lequel la surveillance faciale est implantée, les lois d'application générale et leurs théories sous-jacentes comportent des lacunes. Autrement dit, nos lois ne nous protègent pas adéquatement contre l'utilisation abusive de cette technologie. Plus précisément, et selon mes propres recherches, je voudrais signaler que les utilisations des relations interpersonnelles de la surveillance faciale ne seront pas suffisamment réglementées.

Je suis très contente de voir que le Comité examine l'utilisation des relations interpersonnelles dans le cadre de son étude et je l'encourage fortement à étudier les liens entre la surveillance des relations interpersonnelles et les entités commerciales et étatiques. Par exemple, bien que cela ne soit pas propre à la surveillance faciale, l'émergence de partenariats entre Amazon Ring et les services de police aux États-Unis met en lumière l'Interweb possible de la surveillance personnelle, de l'infrastructure de surveillance commerciale et de la police d'État, ce qui posera — à tout le moins —, des défis aux lois actuelles sur la responsabilité délictuelle et aux lois constitutionnelles au fur et à mesure que des interrelations de ce genre apparaîtront au Canada.

La surveillance faciale à des fins personnelles s'est déjà révélée très préjudiciable dans plusieurs cas, notamment en ce qui concerne le harcèlement, l'extorsion et d'autres formes de violence facilitées par la technologie. Ces utilisations demeurent sous-réglementées parce que la surveillance des relations interpersonnelles dans l'espace et l'information publics est insuffisamment réglementée. Bien que la gouvernance de la protection des relations interpersonnelles ne relève peut-être pas entièrement de la compétence fédérale, je crois qu'il s'agit d'un élément fondamental pour comprendre la surveillance faciale en tant que système sociotechnique et qu'il faut en compte dans la gouvernance d'une telle technologie. Je ne crois pas que la solution soit de criminaliser l'utilisation personnelle des systèmes de surveillance faciale, mais plutôt de renforcer la reconnaissance normative et juridique des droits interpersonnels et de réglementer la conception et la disponibilité des technologies de surveillance faciale.

Les lois et les politiques régissant la technologie peuvent avoir au moins trois objectifs, soit réglementer l'utilisation de la technologie, réglementer l'utilisateur ou réglementer la conception et la disponibilité de la technologie. La réglementation de la conception et de la disponibilité pourrait relever plus directement de la compétence du gouvernement fédéral et viser davantage les responsables de la création d'un préjudice possible plutôt que de se concentrer uniquement sur la punition réactive d'actes répréhensibles ou l'indemnisation de préjudices qui se sont déjà produits.

De plus, pour ce qui est de la réglementation de l'utilisation de la surveillance faciale, j'exhorte le Comité à examiner des cas observés dans d'autres pays où des gouvernements ont imposé un moratoire, comme d'autres témoins l'ont mentionné, et je recommande que le Canada fasse de même. Bien entendu, il faudra en faire plus à long terme, notamment en élargissant la portée de la gouvernance pour y inclure toutes les formes de surveillance biométrique automatisée, et non seulement la surveillance faciale. De plus, le Comité pourrait envisager de recommander la formation d'un groupe national d'experts indépendants qui mènerait des consultations sur l'amélioration des lois d'application générale, l'utilisation de la conception et les restrictions imposées aux utilisateurs à l'avenir, peut-être pour les lignes directrices fédérales et provinciales.

● (1215)

Parmi les experts, il faut des personnes qui...

Le président: Je vous remercie.

Mme Kristen Thomasen: ... font partie des communautés touchées.

Merci.

Le président: Madame Thomasen, je suis vraiment désolé de devoir vous interrompre. Nous devons passer à notre troisième témoin.

Madame Molnar, vous disposez de cinq minutes.

Mme Petra Molnar (avocate, York University, Refugee Law Lab): Merci beaucoup.

Je m'appelle Petra Molnar. Je suis avocate et anthropologue. Aujourd'hui, j'aimerais vous faire part de quelques réflexions issues de mon travail sur les répercussions pour les droits de l'homme de technologies telles que la reconnaissance faciale utilisée en matière d'immigration et de gestion des frontières.

La technologie de reconnaissance faciale est à la base de nombreux types d'expériences technologiques qui ont cours dans le domaine des migrations et des frontières, des technologies qui mettent en oeuvre une surveillance biométrique généralisée dans les camps de réfugiés, les procédures de détention des immigrants et les aéroports. Cependant, lorsque nous tentons de saisir les répercussions des différentes technologies de gestion des migrations et des frontières — par exemple, les détecteurs de mensonges à intelligence artificielle, la surveillance biométrique généralisée et les différents outils de prise de décision automatisée —, il est important de prendre en compte l'écosystème plus vaste dans lequel ces technologies se développent. Nous y trouvons de plus en plus de criminalisation de la migration, de sentiments anti-migrants et de pratiques frontalières engendrant des milliers de décès, que nous voyons non seulement en Europe, mais aussi à la frontière entre les États-Unis et le Mexique, et plus récemment à la frontière entre les États-Unis et le Canada, lorsqu'une famille est morte de froid au Manitoba.

Depuis 2018, j'ai suivi et visité des frontières dans le monde entier, plus récemment la frontière entre les États-Unis et le Mexique et la frontière ukrainienne pendant l'occupation en cours. Les frontières deviennent facilement des terrains d'essai pour les nouvelles technologies, car la migration et l'application des lois à la frontière constituent déjà un espace décisionnel opaque et discrétionnaire, où des décisions qui changent le cours d'une vie sont rendues par des décideurs soumis à peu de surveillance et de responsabilisation dans un système de vastes déséquilibres de pouvoir entre ceux qui sont touchés par la technologie et ceux qui la manient.

Un exemple concret pourrait peut-être illustrer à quel point les répercussions des technologies utilisées pour la gestion des migrations peuvent être profondes. Il y a quelques semaines, je me trouvais dans le désert de Sonoran, à la frontière entre les États-Unis et le Mexique, pour constater de visu les effets des technologies mises à l'essai. Ces expériences technologiques comprennent différentes tours de surveillance automatisées et alimentées par l'intelligence artificielle qui balaient le désert. La reconnaissance faciale et la surveillance biométrique généralisée, et même les « chiens robots » récemment annoncés — comme mon chien qui aboie en arrière-plan — rejoignent maintenant l'arsenal mondial des technologies d'application de la loi aux frontières.

Toutefois, l'avenir n'est pas seulement fait de technologies, mais aussi de morts. Des milliers de personnes ont déjà péri en tentant des traversées dangereuses. Ce sont des personnes comme M. Alvarado, un jeune mari et père de famille d'Amérique centrale dont nous avons visité le site commémoratif. En effet, il a été prouvé que les technologies de surveillance et les technologies frontalières intelligentes ne dissuadent pas les gens de tenter des traversées dangereuses. Au contraire, les gens ont été contraints de modifier leurs itinéraires vers des terrains moins habités, ce qui a entraîné des pertes humaines.

Encore une fois, dans le monde opaque et discrétionnaire de l'application de la loi aux frontières et de la prise de décisions en matière d'immigration, de structures qui sont fondées sur l'intersection entre un racisme systémique et une discrimination historique à l'endroit des migrants, les répercussions de la technologie sur les droits de la personne sont bien réelles. Comme d'autres témoins l'ont dit, nous savons déjà que la reconnaissance faciale est hautement discriminatoire à l'égard des visages noirs et bruns et que les décisions algorithmiques reposent souvent sur des ensembles de données biaisés qui donnent des résultats biaisés.

Pour ma part, un des exemples les plus viscéraux des répercussions profondes de la reconnaissance faciale est l'appétit croissant pour les polygraphes à intelligence artificielle, ou les détecteurs de mensonges, utilisés à la frontière. L'Union européenne a expérimenté un système aujourd'hui tourné en dérision, l'iBorderCtrl. Le Canada a mis à l'épreuve un système similaire appelé AVATAR. Ces polygraphes utilisent des technologies de reconnaissance faciale et émotionnelle pour détecter si une personne ment lorsqu'on lui pose une série de questions à un passage frontalier. Cependant, comment un détecteur de mensonges à intelligence artificielle peut-il composer avec les différences de communication interculturelle lorsqu'une personne, en raison de différences religieuses ou ethniques, peut être réticente à établir un contact visuel, ou peut simplement être nerveuse? Qu'en est-il de l'effet des traumatismes sur la mémoire, ou du fait que nous savons que notre rappel d'information n'est pas linéaire? Les décideurs humains éprouvent déjà des problèmes avec ces facteurs complexes.

Au bout du compte, cette conversation ne porte pas seulement sur la technologie, mais sur des questions plus vastes. Il s'agit de savoir quelles communautés peuvent participer aux conversations sur les innovations proposées, et quels groupes de personnes deviennent des terrains d'essai pour les technologies frontalières. Pourquoi le secteur privé détermine-t-il, encore et encore, l'objet et l'objectif de nos innovations dans le cadre de partenariats public et privé souvent problématiques que des États sont de plus en plus enclins à conclure dans la course mondiale aux armements à intelligence artificielle qui est en cours? Quelles priorités comptent vraiment lorsque nous choisissons de créer des détecteurs de mensonges alimentés par l'intelligence artificielle à la frontière au lieu d'utiliser l'intelligence artificielle pour reconnaître les gardes-frontières racistes?

Dans mon travail, basé sur des années de recherche sur le terrain et des centaines de conversations avec des personnes qui sont elles-mêmes aux limites les plus pointues de l'expérimentation technologique à la frontière, il est clair que le manque actuel de gouvernance mondiale autour des technologies à haut risque crée un laboratoire parfait pour des expériences à haut risque, faisant des personnes déplacées, des migrants et des réfugiés un terrain d'essai.

À l'heure actuelle, il existe très peu de réglementation sur les TRF au Canada et à l'échelle internationale. Cependant, le récent projet de règlement sur l'intelligence artificielle de l'Union européenne montre une reconnaissance régionale de la nécessité que les technologies employées pour la gestion des migrations soient strictement réglementées, avec des discussions en cours autour d'une interdiction totale de la surveillance biométrique généralisée, de la reconnaissance faciale à haut risque et des détecteurs de mensonges de type IA. Le Canada devrait lui aussi jouer un rôle de premier plan à l'échelle mondiale. Nous devrions instaurer des mécanismes de gouvernance similaires qui reconnaissent les répercussions considérables sur les droits de la personne des technologies à haut risque et interdire l'utilisation à haut risque des TRF dans la migration et à la frontière.

● (1220)

Nous avons désespérément besoin de plus de réglementation, de surveillance et de mécanismes de responsabilisation pour les technologies frontalières utilisées par des États comme le Canada.

Le président: Merci, madame Molnar.

Je vais devoir commencer les questions. Il est 12 h 25. Je vais réduire les tours de six et cinq minutes à quatre minutes. Ainsi, nous devrions peut-être terminer quelques minutes après 13 heures.

Je vais donner la parole à M. Williams pour quatre minutes.

M. Ryan Williams: Merci beaucoup à nos témoins.

Je vais m'adresser d'abord à Mme Brandusescu.

Le mois dernier, vous avez participé à une réponse au projet de politique du Service de police de Toronto sur l'utilisation des technologies à intelligence artificielle, qui incluait la reconnaissance faciale. Le deuxième article traitait de l'« explicabilité », qui était qualifiée d'étape importante pour garantir que la responsabilisation des technologies à intelligence artificielle envers les utilisateurs et les populations touchées. J'ai également adoré votre définition de la boîte de verre contenant la boîte noire. C'est très important.

Devons-nous définir l'« explicabilité » dans le cadre législatif fédéral pour assurer une application et une compréhension universelles du terme? Si oui, comment la définiriez-vous?

Mme Ana Brandusescu: Merci beaucoup.

On nous dira que l'IA explicable est une solution computationnelle que nous devrons mettre en place pour que la TRF puisse aller de l'avant.

Je tiens à faire valoir que même si l'IA explicable est un domaine en plein essor, elle la complexifie en fait au lieu de la simplifier. La raison en est que l'explication dépend entièrement du public. Ce public est généralement composé d'informaticiens, non de politiciens.

Il est très important de déterminer qui peut participer à cette conversation et qui en est exclu. Il ne suffit pas d'avoir une IA explicable, en raison même du type d'IA à réseau neuronal sur lesquelles la TRF repose. On ne peut jamais entièrement l'expliquer.

Cela fait également partie de notre recommandation. En bref, il faut vraiment tenter d'aller au coeur de la technologie et de comprendre la boîte noire. La disponibilité d'une solution technique à une technologie très problématique ne signifie pas que nous devrions l'utiliser à l'avenir et ne pas envisager son interdiction.

● (1225)

M. Ryan Williams: Merci.

Vous avez publié en 2021 un article intitulé « Weak privacy, weak procurement: The state of facial recognition in Canada ». Vous avez parlé de la protection des données biométriques et de la façon dont les lois canadiennes sur la protection de la vie privée sont défaillantes par rapport au reste du monde.

Dans une séance précédente, un témoin nous a parlé des bienfaits du Règlement général sur la protection des données, le RGPD. L'adoption d'une protection de cette nature serait-elle préférable pour le droit à la vie privée au Canada?

Mme Ana Brandusescu: C'était la piste de mon coauteur, Yuan Stevens, qui se spécialise dans la protection de la vie privée. Je me contenterai de dire que le RGPD est une bonne référence à avoir en matière de pratiques exemplaires à ce jour.

Je dirais simplement que l'enjeu dépasse la protection des données ou de la vie privée. Il s'agit aussi d'une conversation sur le secteur privé et sa participation à la gouvernance publique. Actuellement, notre réglementation n'est qu'une réglementation privée.

Je pourrais aborder plus en profondeur l'évaluation de l'impact des algorithmes et notre propre prise de décision automatisée fondée sur des directives dans une prochaine question.

M. Ryan Williams: Merci.

Madame Thomasen, dans un article que la CBC a publié en mars 2020, vous parliez de l'utilisation par la police de Windsor de l'outil de reconnaissance faciale de Clearview AI. Vous vous demandiez comment nous savons que, si la victime est même identifiée, ses renseignements seront protégés. Je pense que c'est un élément clé alors que la reconnaissance faciale se répand de plus en plus.

La question que je vous pose vise essentiellement à aider à répondre à la question que vous posiez dans le reportage de la CBC. Comment pouvons-nous garantir que les Canadiens savent que leurs renseignements sont protégés?

Mme Kristen Thomasen: Pour situer un peu cette question dans son contexte, il était question d'un fil narratif qui surgit souvent par rapport à l'utilisation de la surveillance faciale par la police, à savoir que nous l'utilisons pour protéger... en l'occurrence, il s'agissait d'enfants. Nous devons nous inquiéter des effets plus profonds sur la vie privée en tant que bien social.

Ce que je voulais dire, c'est que...

Le président: Je crains qu'on ne vous ait pas laissé assez de temps pour répondre à cette question. Je vais devoir vous interrompre et donner la parole à Mme Saks.

Mme Kristen Thomasen: Je serais heureuse de vous soumettre une explication supplémentaire.

Le président: Bien sûr, veuillez nous soumettre une explication écrite si vous en avez une sous la main ou si vous souhaitez en fournir une.

Allez-y, madame Saks, pour quatre minutes, je vous en prie.

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

M. Williams sera peut-être heureux de voir que je vais m'écarter un peu de sa question.

Je pense que nous convenons tous qu'il faut faire davantage pour comprendre l'utilisation de cette technologie et nous assurer qu'il y a une consultation solide avec tous ceux dont la vie privée est touchée et la façon dont elle est utilisée. Selon la description qu'un témoin précédent en a donnée, nous devons procéder avec un scalpel et non avec une hache. J'apprécie les appels à un moratoire pour que nous puissions utiliser ce scalpel. C'est une métaphore importante.

Madame Thomasen, en parlant des victimes, j'ai entendu beaucoup d'effets négatifs. Je ne les conteste pas. Je suis moi-même engagée dans la lutte contre la traite des personnes depuis de nombreuses années. Je comprends les effets de la migration et des frontières, ainsi que l'incidence de la traite de personnes sur les femmes et les enfants, dont beaucoup appartiennent à des minorités racialisées.

N'y a-t-il pas une certaine sagesse à utiliser le scalpel dans cette technologie afin que nous puissions protéger efficacement les victimes de la traite de personnes ou les enfants victimes d'agressions ou de pornographie infantile? Existe-t-il d'autres outils dont nous avons besoin pour trouver des moyens de les protéger?

N'est-ce pas un élément qui doit faire partie de cette discussion?

● (1230)

Mme Kristen Thomasen: Oui. La vie privée est un bien social qui profite à tous, y compris aux femmes et aux enfants qui sont souvent au coeur du fil narratif selon lequel l'une des utilisations bénéfiques de la reconnaissance faciale est de protéger les groupes marginalisés ou victimisés. Il est très important de reconnaître ces utilisations bénéfiques potentielles de la reconnaissance faciale tout en nuançant considérablement ce fil narratif. En particulier, nous devons reconnaître comment l'érosion potentielle de la vie privée en tant que bien social causera également un préjudice aux femmes et aux enfants.

D'après ce que je comprends, il y a un exemple d'utilisation bénéfique de la surveillance faciale au Canada, soit le Projet Arachnid. Vous pourriez trouver utile de parler à une personne qui y participe. Il s'agit d'un cas d'utilisation très précis de la surveillance faciale, ou plus précisément de la technologie de reconnaissance faciale. Je serais heureuse de parler davantage des définitions dans une autre question.

Les buts et les objectifs précis de la création d'un système interne de reconnaissance faciale ont été établis de façon très étroite. C'est tout à fait différent des arguments ou des fils narratifs plus larges selon lesquels la reconnaissance faciale ne devrait pas être interdite ou limitée de différentes façons parce qu'en général, des cas d'utilisation potentiellement positive sont possibles. Dans ce type de discussions, il est beaucoup plus important de peser le bien social positif de la protection de la vie privée.

J'ai l'impression que le temps me manque. Je serais plus qu'heureuse d'en parler davantage.

Mme Ya'ara Saks: J'aimerais essayer de poser une dernière question, si vous le permettez.

Le président: Vous pouvez en poser une seule.

Mme Ya'ara Saks: En décembre 2021, vous avez présenté un mémoire au Service de police de Toronto dans le cadre de ses consultations sur l'utilisation de la technologie à intelligence artificielle. Vous avez formulé plusieurs recommandations. Si vous le souhaitez, vous pourriez souligner une recommandation clé ici, mais je vous invite à nous fournir ensuite des observations par écrit afin que nous puissions les examiner.

Mme Kristen Thomasen: Je le ferai volontiers.

Il s'agissait d'un mémoire cosigné.

Une recommandation clé que j'aimerais souligner dès maintenant est que cette technologie n'est pas inévitable. Le fait qu'elle existe ne signifie pas qu'elle devrait exister ou que nous devrions l'utiliser. Cela ne signifie pas non plus que nous ne devons pas la limiter.

La mise en évidence de certains cas d'utilisation bénéfique ne devrait pas être suffisante pour limiter notre réflexion sur les inconvénients potentiels d'une utilisation plus répandue de cette technologie. En particulier, nous devrions réfléchir davantage aux interrelations entre la façon dont les services de police, les organismes commerciaux et les particuliers pourraient collaborer à la collecte d'informations à des fins carcérales.

Le président: Je vous remercie.

[*Français*]

Monsieur Villemure, vous disposez de quatre minutes.

M. René Villemure: J'aimerais poser une brève question à chacune des trois témoins, dans leur ordre de comparution.

Madame Brandusescu, la technologie de reconnaissance faciale signifie-t-elle la fin de la liberté?

[*Traduction*]

Mme Ana Brandusescu: Je dirais que non, car nous pouvons interdire la reconnaissance faciale. La fin de la liberté est une question et une affirmation très complexes et terribles. Je dirais que, encore une fois, il ne s'agit pas seulement de surveillance généralisée; il s'agit de la façon dont nos gouvernements interagissent avec le secteur privé, comment ils achètent différents logiciels sans avoir la moindre idée de ce qu'ils achètent...

[*Français*]

M. René Villemure: Je suis désolé de vous interrompre, mais mon temps de parole est limité. Nous allons y revenir.

Madame Thomasen, je vous pose la même question.

[*Traduction*]

Mme Kristen Thomasen: Je suis d'accord avec les témoins précédents: c'est une question complexe à laquelle il est difficile de répondre très simplement.

Je vous encourage également à ne pas vous limiter à la reconnaissance faciale. Il y a toutes les différentes formes de reconnaissance biométrique qui font partie de la conversation que nous avons aujourd'hui.

[*Français*]

M. René Villemure: Merci beaucoup.

Madame Molnar, qu'en pensez-vous?

[*Traduction*]

Mme Petra Molnar: Je préconiserais simplement une spécificité contextuelle par rapport à cette question, en particulier lorsque nous parlons de libertés: pour qui?

En matière d'immigration, bien sûr, nous parlons d'un domaine opaque et discrétionnaire qui présente déjà un risque très élevé. Dans ce cas, oui, cela peut certainement être très contraignant.

[*Français*]

M. René Villemure: Je vous remercie.

Madame Brandusescu, la technologie de reconnaissance faciale en vient-elle à transformer l'espace public sur le plan de la surveillance, au sens où l'entend M. Jürgen Habermas?

[*Traduction*]

Mme Ana Brandusescu: Oui, je dirais qu'il y a une surveillance généralisée, mais aussi une surveillance raciste et sexiste discriminatoire, comme nous le savons, parce que cette technologie est très discriminatoire dans la façon dont elle se situe à un niveau très informatique. Plus nous l'acceptons dans la société, plus nous nous y habituerons. Je ne tiens pas à avoir cette commodité.

On a parlé de commodité tout à l'heure. Je dis parfois que la commodité aura raison de nous lorsque nous l'utiliserons pour ouvrir nos téléphones. Plus elle fait partie de notre vie quotidienne, plus nous pensons qu'il est normal de l'avoir, mais en fait, ce n'est pas le cas, car elle peut vraiment nuire à certaines personnes et à certains groupes. Il est parfois préférable de ne pas avoir cette technologie du tout.

C'est une question plus vaste à se poser. C'est une question de culture numérique. Nous devons tenir ces discussions, et en fait, nous devons posséder la culture numérique essentielle pour poser les bonnes questions.

● (1235)

[*Français*]

M. René Villemure: Merci beaucoup.

Au-delà des biais identifiés, comme ceux en lien avec la race ou l'âge, le citoyen qui n'est pas visé par ces biais entre néanmoins dans un monde de surveillance, n'est-ce pas?

[*Traduction*]

Mme Ana Brandusescu: Nous pouvons aller plus loin et parler d'entreprises d'analyse de données, de Palantir et d'autres qui ne sont même pas des TRF. Le monde de la surveillance dépasse largement celui des TRF, et il y a une question plus vaste à se poser sur le complexe militaro-industriel de notre pays et sur l'origine de ces technologies.

Nous devons à nouveau prendre du recul et examiner la façon dont la technologie a pris le dessus. Nous devons réfléchir à ce que signifie le solutionnisme technologique, à la raison pour laquelle nous investissons autant d'argent dans l'innovation technologique en particulier, et pourquoi nous considérons l'innovation comme une simple prédilection pour la technologie, sans financer des groupes qui travaillent très fort sur des questions sociales pour comprendre cette technologie, pour sensibiliser et éduquer le public à ce sujet.

J'ai une vision optimiste de l'avenir, même si je suis très critique vis-à-vis de cette technologie. Nous devons imaginer, réfléchir à la façon dont nous pouvons vivre sans certaines de ces technologies, et tout ira bien.

Le président: Merci. Je vais devoir passer à M. Green qui disposera de quatre minutes. Je vous en prie.

M. Matthew Green: Merci.

Je vais m'adresser d'abord à Mme Brandusescu. Dans votre rapport intitulé *Artificial Intelligence Policy and Funding in Canada: Public Investments, Private Interests*, l'une de vos principales conclusions est que la politique gouvernementale actuelle permet aux entreprises impliquées dans des violations des droits de la personne de se préqualifier comme fournisseurs d'IA du gouvernement.

Dans votre réponse précédente, vous avez évoqué le complexe militaro-industriel. Nous avons entendu des histoires d'entreprises qui vantent leurs technologies en disant qu'elles ont été testées au combat.

Connaissez-vous des entreprises qui ont été préqualifiées en tant que fournisseurs, pas seulement pour la reconnaissance faciale, mais pour l'ensemble de l'IA et toute cette gamme de choses, et qui ont déjà été mêlées à des violations des droits de la personne?

Mme Ana Brandusescu: Merci pour cette excellente question.

Oui, j'en connais. L'un de ces fournisseurs est Palantir Technologies Inc., une entreprise d'analyse de données qui a travaillé avec le gouvernement américain pour planifier des arrestations massives de près de 700 personnes et la séparation d'enfants de leurs parents, causant ainsi un préjudice irréparable. Vous pouvez consulter le rapport de 2020 d'Amnesty U.S.A. à ce sujet. Pourtant, comme je l'ai mentionné dans ma déclaration liminaire, Palantir s'est engagée à se soumettre à l'évaluation de l'incidence algorithmique du Canada et figure sur cette liste de fournisseurs préqualifiés. L'évaluation est vue comme une mesure éthique qui favorise une IA responsable. S'engager à se soumettre à une évaluation de l'incidence algorithmique censée être éthique, puis s'engager avec un autre gouvernement dans ces violations des droits de la personne est très paradoxal et contradictoire.

Je demande à notre gouvernement, en particulier au Conseil du Trésor, qui gère cette liste, de reconsidérer, comme je l'ai dit, de les rayer de la liste — et pas seulement eux, mais d'autres que je n'ai pas examinés en profondeur en ce qui concerne les violations potentielles des droits de la personne.

M. Matthew Green: Selon vous, quelles modifications devrions-nous apporter à notre politique pour que notre processus d'approvisionnement tienne compte des droits de la personne?

Mme Ana Brandusescu: Je crois qu'une modification serait que lorsque nous écrivons, nous les chercheurs, journalistes d'enquête, ou qui que ce soit, il faut que vous nous entendiez, parce que nous sommes au point où notre gouvernement ouvert n'est pas vraiment ouvert, où nous devons encore présenter une demande d'accès à l'information et trouver tous ces renseignements. Le gouvernement sait donc maintenant que Palantir a porté atteinte à des droits de la personne ou est liée à ces atteintes. La liste s'allonge, elle compte maintenant environ 105 entreprises, et le gouvernement devrait rayer Palantir de la liste. C'est une étape simple, mais il faut aussi réfléchir à qui peut s'engager dans un processus d'évaluation de l'incidence algorithmique et qui peut y contribuer. Si on ne fait que retenir d'autres entreprises lorsqu'une évaluation de l'incidence algorithmique est publiée, qu'en est-il du reste du Canada, pas seulement de la population canadienne, mais des groupes concernés, des organisations de défense des droits numériques, des organismes de la société civile? Quel rôle jouons-nous dans la conversation?

● (1240)

M. Matthew Green: C'est un travail important.

Monsieur le président, par votre entremise, je demanderais à Mme Brandusescu à quel point nous devrions nous inquiéter de la mainmise des entreprises sur l'élaboration de la politique gouvernementale visant à réglementer l'IA et la reconnaissance faciale au Canada? Dans cette optique, pouvez-vous préciser qui établit le cadre stratégique canadien en matière d'IA et quelles en sont les conséquences?

Mme Ana Brandusescu: Nous devrions être très inquiets.

Au cours des quatre prochaines années, ma recherche en tant qu'étudiante au doctorat portera sur la privatisation des États, en particulier en ce qui concerne ces technologies. Je pense que le phénomène ne fera que s'amplifier. Comme Mme Molnar l'a dit, les partenariats public-privé sont un élément clé de l'acquisition, de la mise en oeuvre, du développement et l'utilisation de ces technologies. Nous devons nous assurer que nous sommes en phase avec le Conseil du Trésor, qui héberge toutes les suites d'IA concernées, mais aussi avec d'autres organismes, comme Services publics et Approvisionnement Canada qui détient vraiment beaucoup de cartes dans ce domaine, mais qui participe rarement à ces discussions. C'est toujours soit le Conseil du Trésor, soit le Commissariat à la protection de la vie privée qui participe à la conversation. Je ne vois jamais les responsables de l'approvisionnement, mais ils sont vraiment un élément clé de cette conversation.

Le président: Merci.

Sur ce, nous passons à M. Kurek pour quatre minutes.

M. Damien Kurek: Merci beaucoup.

Avant de poser mes questions, sachant que le temps nous manque, j'invite toutes les témoins ici présentes à ne pas hésiter à nous faire parvenir des renseignements s'il y a des choses que vous n'avez pas eu l'occasion d'aborder. Il s'agit de questions importantes et de réponses techniques. Deux, trois ou quatre minutes ne sont certainement pas suffisantes pour y répondre de façon appropriée.

Je pense que l'un des plus grands défis à relever est simplement lié à l'évolution du domaine de l'intelligence artificielle et de la reconnaissance faciale. Au tour précédent, par rapport au conflit en cours en Europe, j'ai parlé des implications de la façon dont les militaires utilisent certaines de ces technologies et du fait que la Convention de Genève, par exemple, traite des bombes qui sont larguées des avions, mais un tout nouveau domaine s'est ouvert.

Madame Brandusescu, à mesure que cette technologie se développe, par rapport à la recherche, au gouvernement, aux sociétés privées, aux essais et à la compréhension des répercussions de cette technologie et de ses effets sur la société, avez-vous des suggestions à nous faire sur la marche à suivre pour garantir qu'il y a une compréhension appropriée de ce que cela signifie pour les citoyens canadiens, et du fait que nous sommes confrontés à un monde où l'IA et la reconnaissance faciale font de plus en plus partie de notre vie quotidienne?

Mme Ana Brandusescu: Je le répète, je pense que nous pouvons contester l'inévitabilité de la technologie et nous pouvons dire non à certaines de ces technologies, mais cela nécessite aussi des fonds et des ressources pour la sensibilisation à ces technologies. Bon nombre de ces contrats sont conclus à huis clos. Dans les relations entre l'industrie et le gouvernement, les partenariats public-privé font parfois intervenir des universités et des laboratoires, mais c'est toujours dans un intérêt privé. Vous voulez financer ces technologies, les développer, puis les utiliser. Vous ne pensez pas aux conséquences. Très peu d'argent, de temps et de ressources sont consacrés à la gestion du désordre que ces technologies causent et des dommages qu'elles occasionnent.

Nous devons nous assurer qu'il y a un équilibre dans tout cela, prendre un peu de recul et revoir comment nous envisageons l'innovation lorsque nous finançons ces technologies, surtout en tant que contribuables. Nous devons vraiment diversifier notre examen. Pour l'instant, je dirais que le travail d'innovation a été capturé par des innovations explicitement technologiques qui sont conçues pour développer et déployer d'abord ces technologies et poser des questions ensuite. Nous pouvons voir tout le mal qu'elles ont causé et pourtant, nous sommes encore en train d'en débattre.

Je ne tiens pas à ce que nous ayons un cas comme Clearview AI, alors que devons nous faire? La transparence à l'égard des logiciels d'essai gratuits est vraiment importante, parce que cela va au-delà des TRF. Cela se rapporte à l'ensemble des systèmes et technologies d'IA que le gouvernement utilise. Personne ne voit cette information nulle part. Si nous pouvons obtenir cette information, en particulier pour les forces de l'ordre et la sécurité nationale qui n'invoqueront pas ces excuses pour dire qu'ils couvrent des secrets commerciaux...

Nous devons pousser plus loin notre examen. Encore une fois, si nous voulons établir la confiance avec le gouvernement, nous devons avoir ce niveau de transparence pour savoir même ce qu'ils achètent et utilisent afin que nous puissions poser de questions plus pertinentes.

● (1245)

Le président: Merci.

Sur ce, nous passons à M. Bains pour quatre minutes.

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

Merci à nos témoins de leur présence. Vous toutes, ainsi que nos témoins précédentes, avez mis en évidence les défis considérables auxquels nous sommes confrontés.

Madame Thomasen, vous avez récemment participé à la rédaction de certains commentaires sur le projet de politique de la commission des services de police de Toronto, la TPSB, concernant les technologies d'intelligence artificielle. Voici la version traduite de la première recommandation:

> Toute mise en oeuvre de technologies d'IA par les forces de l'ordre doit partir de l'hypothèse qu'elles ne peuvent pas anticiper avec assurance tous les effets de ces technologies sur le maintien de l'ordre ou sur les communautés contrôlées et agir en conséquence à la lumière de ces incidences.

J'aimerais savoir à quelle fréquence, selon vous, les gouvernements devraient examiner les effets des technologies d'IA utilisées dans le maintien de l'ordre.

Mme Kristen Thomasen: Souvent. Je sais que dans le projet de politique que la TPSB a finalement adopté, les examens auront lieu chaque année, ce qui me semble positif. Je pense en fait qu'en raison de la façon dont la technologie évolue et de la quantité de données qui peuvent être recueillies et utilisées, même au cours d'une année, cela ne serait pas suffisant en pratique, dans un monde parfait. Bien sûr, les examens et les vérifications prennent du temps et des ressources. Je reconnais que des limites concrètes entrent en jeu.

Il s'agit cependant d'un seul service de police au Canada. Nous savons déjà que d'autres services de police utilisent des technologies algorithmiques de maintien de l'ordre et qu'ils ne procèdent pas à ces examens, du moins pas dans la mesure où nous en avons connaissance publiquement. Il n'y a pas nécessairement de surveillance publique ou de transparence.

Je pense donc que la politique de la TPSB est un pas dans la bonne direction. C'est un pas positif, mais même là, je pense que c'est insuffisant. Il y a encore beaucoup à faire. Je pense que dans la mesure où le gouvernement fédéral pourrait s'engager dans l'établissement d'une certaine forme de lignes directrices, puis bien sûr dans la surveillance des forces de police à l'échelle fédérale, ce serait un pas positif.

M. Parm Bains: Vos recommandations ont-elles été incorporées de manière satisfaisante dans la version définitive de la politique par le service de police de Toronto?

Mme Kristen Thomasen: Je pense que la version définitive de la politique a incorporé un certain nombre de recommandations — plusieurs parties ont fait des recommandations dans ce processus — mais la politique présente encore certaines faiblesses. À mon avis, la politique traite encore beaucoup les technologies algorithmiques de maintien de l'ordre comme si elles étaient inévitables, comme un avantage net tant que nous pouvons atténuer certains risques. Je pense que ce que vous avez entendu de la part des témoins aujourd'hui, moi y compris, c'est que ce n'est pas le bon cadre pour aborder cette technologie, étant donné les préjudices considérables qu'elles peuvent causer et le contexte social dans lequel elles sont introduites.

La formation d'un groupe d'experts indépendants comprenant des spécialistes de différents domaines, pas seulement des experts techniques, est un aspect de ce processus politique qui n'a pas été officialisé, mais dont il a été question. Cela ne s'est pas concrétisé. Il y a encore des discussions à ce sujet. Je pense que c'est une étape qui pourrait être utile à l'échelle fédérale pour fournir une sorte d'orientation et de gouvernance supplémentaires autour non seulement de la reconnaissance faciale, mais de toutes les formes de technologies algorithmiques de maintien de l'ordre.

M. Parm Bains: Je viens aussi de la Colombie-Britannique, alors mes questions vous proviennent de Richmond, en Colombie-Britannique. Je veux savoir si vous avez examiné et étudié certains éléments en ce qui concerne des organismes d'application de la loi de cette province.

Mme Kristen Thomasen: Eh bien, je vous signale que le service de police de Vancouver utilise des technologies algorithmiques de maintien de l'ordre et qu'il aurait avantage à examiner certains processus que la commission des services de police de Toronto a mis en oeuvre. S'engager dans ce processus à l'échelle fédérale et provinciale serait beaucoup plus utile, je pense, que simplement au niveau de la ville ou du service de police municipal, parce que la TPSB reconnaît en fait...

Le président: Madame Thomasen, je suis désolé. Je vais devoir passer au tour suivant.

Mme Kristen Thomasen: Pas de problème. C'est avec plaisir que je vous ferai parvenir quelques observations.

● (1250)

Le président: Merci beaucoup.

Nous allons passer à M. Villemure.

[*Français*]

M. René Villemure: Monsieur le président, combien de temps me reste-t-il?

[*Traduction*]

Le président: Vous avez deux minutes et demie.

[*Français*]

M. René Villemure: D'accord, je vous remercie beaucoup.

Madame Brandusescu, je me tourne de nouveau vers vous.

Lors de votre première intervention, dès le départ, vous avez parlé de la compagnie Palantir. Je ne sais pas si mes collègues le savent, mais, sur les médias sociaux, Palantir se présente comme une entreprise très sympa et se donne une image très positive.

En même temps, on sait que les projets comme Gotham et Apollo sont en quelque sorte des projets de guerre. Palantir est une compagnie qui sert essentiellement le secteur militaire; elle se sert des technologies militaires pour observer la société. J'en conclus donc que les mots « éthique » et « Palantir » ne doivent pas être utilisés dans la même phrase.

J'aimerais que vous précisiez votre pensée relativement à Palantir. J'aimerais aussi que vous nous fournissiez la liste des 105 compagnies que vous avez évoquées un peu plus tôt en nous indiquant les éléments sur lesquels nous devrions nous concentrer pour mieux comprendre le problème.

Pour l'instant, je vous laisse parler de Palantir.

[*Traduction*]

Mme Ana Brandusescu: Je vous remercie pour votre question à laquelle j'y répondrai avec plaisir. J'aime que vous ayez dit que les mots « éthique » et « Palantir » ne sont pas synonymes, car c'est exact.

Comme je l'ai dit, Palantir est une société technologique d'analyse de données et c'est donc là le problème avec la façon dont le gouvernement fédéral définit l'« IA ». La définition est vraiment large et je pense qu'il est simplement important que je dise ici en quoi elle consiste. Le Conseil du Trésor définit l'expression « intelligence artificielle » comme toute « technologie de l'information », autrement dit les TI, « qui exécute des tâches pour lesquelles il faut habituellement faire appel à l'intelligence biologique, comme comprendre le langage parlé, apprendre des comportements ou résoudre des problèmes ».

Voilà comment Palantir a réussi à figurer sur cette liste, que je vous ferai parvenir avec plaisir. Le problème avec Palantir, c'est qu'elle est en fait très appréciée par les gouvernements du monde entier, mais elle fait l'objet d'une certaine réticence de la part de l'UE, bien qu'elle participe au projet GAIA-X.

La société a été largement financée et créée par Peter Thiel et d'autres, et il y a de nombreux cas de conflits d'intérêts même au sein de cette gouvernance.

Le problème tient au fait qu'elle est toujours là. Clearview AI est elle aussi toujours là, bien que le Canada ait clairement déclaré au Commissariat à la protection de la vie privée qu'il l'expulserait du pays, pour ainsi dire, bien que cela soit douteux. Elle est toujours en train de fouiller le Web.

Avec Palantir, ils font vraiment de la gouvernance de données dans le monde entier. Ils sont dangereux parce que, même si tout le monde sait qu'ils ne sont pas éthiques et que certaines personnes pensent qu'ils sont cool, ils sont toujours embauchés par les forces de l'ordre et...

Le président: Merci, madame Brandusescu. Je vais devoir céder la parole à M. Green. Nous avons un peu dépassé le temps imparti, mais ce sont d'excellents renseignements.

Nous passons maintenant à M. Green pour deux minutes et demie.

M. Matthew Green: Merci, monsieur le président. Par votre entremise, ma dernière série de questions s'adressera à Mme Molnar, qui a fait allusion à ce qui m'apparaît comme des perspectives dystopiques de « chiens robots » et de drones de plus en plus utilisés en conjonction avec l'IA et la reconnaissance faciale aux passages frontaliers.

Pouvez-vous nous expliquer comment les déséquilibres de pouvoir actuels entre l'État et les personnes qui traversent les frontières, en particulier les réfugiés, peuvent être exploités davantage par l'utilisation de l'IA et de la reconnaissance faciale?

Mme Petra Molnar: Merci beaucoup. Au bout du compte, cela se résume aux déséquilibres de pouvoir, comme vous le dites, dans ce contexte. Nous avons déjà affaire à un système décisionnel opaque et discrétionnaire dans lequel, lorsque des humains prennent des décisions vraiment complexes, il est souvent très difficile de savoir pourquoi certaines décisions sont prises et ce que nous pouvons faire si des erreurs sont commises. Imaginez maintenant que nous commencions à augmenter ou à remplacer les décideurs humains par des décisions automatisées et une surveillance accrue. Cela ne fait que brouiller le domaine déjà très discrétionnaire du traitement et de la prise de décision en matière d'immigration et de réfugiés.

Encore une fois, tout est lié à un long passé de pouvoir et de privilège, et souvent, je le répète, nous parlons de communautés qui ont déjà moins d'accès à la justice et une incapacité, par exemple, à contester des erreurs dont les répercussions sont vraiment profondes.

M. Matthew Green: Je voudrais être un peu plus précis. Dans votre rapport intitulé *Bots at the Gate*, vous déclariez que, je traduis:

> Pour les personnes ayant besoin de protection conformément au paragraphe 97(1) de la Loi sur l'immigration et la protection des réfugiés, une erreur ou un préjugé dans la détermination de leur demande peut les exposer à une menace de torture, de traitement ou de châtiment cruels et inusités, ou à une menace pour leur vie.

Avons-nous une obligation légale ou morale de veiller à ce que le processus d'octroi de l'asile donne la priorité à la sûreté et à la sécurité de la personne, et de supprimer toute technologie ou pratique qui augmente le risque d'erreur?

● (1255)

Mme Petra Molnar: Oui, absolument. Lorsque nous parlons de la détermination de l'asile en particulier, nous parlons d'une application de la technologie à très haut risque. Comme vous le dites à juste titre, et comme notre rapport l'a fait en 2018, si des erreurs sont commises et une personne est, par exemple, expulsée à tort vers un pays qu'elle fuit, les ramifications peuvent être assez terribles.

Il est très inquiétant que nous fassions des essais et des expériences dans ce domaine opaque et discrétionnaire sans les contrôles et les sauvegardes appropriés. Cela doit changer, parce que cela a des répercussions réelles sur la vie de vraies personnes.

Le président: Merci beaucoup.

Sur ce, nous allons passer aux deux derniers tours.

Nous avons M. Bezan, pour quatre minutes, puis nous donnerons la parole à Mmes Hepfner et Khalid.

Allez-y, monsieur Bezan.

M. James Bezan: Merci, monsieur le président.

Je remercie beaucoup nos témoins.

Je vais adresser mes questions à Mme Brandusescu. Vous êtes prolifique. J'ai parcouru au moins trois rapports que vous avez publiés, de *AI for the Rest of Us* et *Weak privacy, weak procurement: The state of facial recognition in Canada* à *Artificial intelligence policy and funding in Canada: Public Investments, Private Interests*. Je crois que vous suggérez suivre l'argent pour voir où se trouvent les intérêts privés.

Les gouvernements fédéral et provinciaux devraient-ils financer ce type de technologie d'intelligence artificielle et de reconnaissance faciale?

Mme Ana Brandusescu: J'ai une brève question à vous poser. Quand vous dites « financer ce type de technologie », est-ce que les gouvernements devraient financer les TRF?

M. James Bezan: C'est la question que je vous pose.

Mme Ana Brandusescu: D'accord. Non, ils ne devraient pas le faire.

Nous en sommes au point où nous finançons beaucoup de R-D, dont une partie peut devenir des TRF. Je le répète, l'objectif ultime devrait être une interdiction.

Nous voyons déjà le Parlement européen réclamer une interdiction. C'est la dernière interdiction en date qui a été demandée. Il est possible de passer d'un moratoire à une interdiction et c'est ce que nous devrions faire. Nous n'en sommes même pas à un moratoire. Nous pouvons commencer par appliquer la loi, mais comme d'autres témoins l'ont dit, les TRF posent un problème dans l'ensemble du gouvernement. Il ne s'agit pas que d'un problème d'application de la loi, bien que l'application de la loi soit le pire problème que les TRF [*inaudible*].

Les gouvernements ne devraient pas les financer. Ils devraient financer la société civile, les groupes de défense des droits numériques et les groupes communautaires qui font ce travail pour montrer tout le mal qui découle des TRF. Ils connaissent les problèmes sociaux et les communautés dans lesquelles ils travaillent. Ils sont les experts et ils devraient aussi participer à la conversation sur ce que le gouvernement décide de financer.

M. James Bezan: Comment pouvons-nous examiner à la fois les directives stratégiques et le financement de l'intelligence artificielle et du TRF? Que devons-nous faire en ce qui concerne les dispositions législatives sur la protection de la vie privée, qu'il s'agisse de la Loi sur la protection des renseignements personnels ou de la LPRPDE? Quelles garanties devons-nous y incorporer pour assurer la protection des données biométriques?

Mme Ana Brandusescu: Cela fait beaucoup de questions. J'en aborderai une, à savoir que nous devrions transformer la directive sur la prise de décisions automatisée...

M. James Bezan: Vous pouvez aussi nous fournir vos réponses plus tard. Vous pourriez répondre par écrit après notre séance, mais si vous pouviez nous faire un résumé rapide, ce serait formidable.

Mme Ana Brandusescu: Oui. Un résumé rapide serait d'améliorer la directive sur la prise de décisions automatisée. S'assurer que les examens internes rédigés tous les six mois soient effectivement rendus publics. Nous attendons toujours celui qui était censé être publié l'an dernier. Il semblerait qu'il sera publié en avril. Nous l'attendons toujours.

D'autres ont mentionné que nous ne devrions pas compter sur les journalistes d'enquête pour continuer à faire ce travail. Le public devrait disposer de ces informations. Nous devrions obtenir des mises à jour. Nous devrions avoir des pages d'accueil sur les sites Web du CPVP et du Conseil du Trésor et dans d'autres endroits pour montrer les plus récentes interventions, comme l'acquisition de ces technologies, dont les TRF, jusqu'à ce qu'elles soient interdites.

Il faut améliorer la directive elle-même. Je présenterai ces améliorations et ces recommandations par écrit plus tard. Nous devrions suivre l'exemple de l'UE et des États-Unis en élaborant une loi qui couvre la transparence de l'application de la loi, laquelle n'est actuellement pas couverte par d'autres registres publics de l'intelligence artificielle dans le monde. Je mettrai également cela par écrit.

● (1300)

M. James Bezan: La mise en oeuvre de cette reddition de comptes ou les pouvoirs de contrôle qu'exercent les services de police du pays nécessiteraient-ils des modifications de notre Code criminel? Comment pouvons-nous ensuite lier cela au secteur privé qui...

Le président: Je suis désolé, monsieur Bezan. Vous n'avez laissé du temps que pour une réponse par oui ou par non à cette question, puis nous devrons poursuivre.

Mme Ana Brandusescu: Je vais juste vous donner un « peut-être ». Ce n'est pas mon domaine de spécialisation.

Le président: D'accord. Merci.

Sur ce, nous allons terminer avec Mme Khalid qui dispose de quatre minutes.

Mme Iqra Khalid: Merci beaucoup, monsieur le président, et merci à nos témoins.

Je vais m'adresser d'abord à Mme Molnar.

Les États-Unis se sont engagés à ce que, d'ici 2023, 97 % de toutes les personnes qui passent par leurs aéroports soient contrôlées par un quelconque système de reconnaissance faciale. Au Canada, nos processus d'évaluation des demandes d'immigration d'IRCC — non seulement pour les réfugiés, mais aussi pour tous les visiteurs et les immigrants qui cherchent à immigrer au Canada — sont en train de passer à un modèle d'évaluation des demandes par intelligence artificielle.

Pouvez-vous nous parler un peu du profilage et de la façon dont il pourrait avoir une incidence directe ou indirecte sur la discrimination institutionnelle?

Mme Petra Molnar: Il pourrait être instructif de comparer ce que le Canada pourrait faire et ce que l'Union européenne envisage de faire en vertu de son projet de règlement sur l'intelligence artificielle. L'Union européenne reconnaît clairement que les évaluations individuelles des risques aux fins du traitement des demandes d'immigration et d'asile sont à haut risque. On évoque l'interdiction pure et simple de l'évaluation individuelle des risques susceptible d'être utilisée aux fins de profilage et pour renforcer la discrimination systémique, ce qu'on retrouve déjà abondamment dans notre système d'immigration.

Je pense que le gouvernement canadien a l'occasion de réfléchir à la meilleure façon de réglementer l'utilisation des technologies de reconnaissance faciale aux fins d'immigration. Vous avez tout à fait raison. Elle est déjà utilisée, tant au Canada que chez ses partenaires régionaux, comme les États-Unis, avec lesquels il échange également une grande partie des données.

L'échange de données est un élément que nous n'avons pas vraiment abordé aujourd'hui, mais c'est un élément auquel nous devons tous prêter davantage attention.

Mme Iqra Khalid: Merci.

Madame Brandusescu, voulez-vous nous dire aussi ce que vous en pensez?

Mme Ana Brandusescu: Oui, je suis tout à fait d'accord avec Mme Molnar.

Mme Iqra Khalid: Très bien. Merci.

Enfin, nous avons entendu certains des avantages de la reconnaissance faciale pour retrouver des enfants disparus et démanteler des réseaux de pornographie juvénile, par exemple. Nous renonçons à une petite partie de notre vie privée pour assurer la sécurité et le bien-être de nos communautés.

Où se situe l'aspect commercial à cet égard? L'une d'entre vous souhaite-t-elle faire un commentaire à ce sujet?

Mme Petra Molnar: Je répéterai peut-être que lorsque nous parlons d'intérêts commerciaux et du genre d'attention portée au bilan que le secteur privé fait souvent entrer dans l'équation, il s'agit d'un cadre de responsabilisation très différent en ce qui concerne l'utilisation à haut risque de la technologie, en particulier à la frontière, ou comme vous le mentionnez, de la traite de personnes.

Encore une fois, nous devons accorder une attention particulière aux acteurs de l'écosystème dans lequel ces technologies se développent et sont mises en oeuvre. Rien de tout cela n'est neutre. Tout cela est un exercice politique.

Mme Kristen Thomasen: Je peux aussi intervenir.

Je pense qu'en abordant la réflexion sur la réglementation et les limites de la surveillance faciale sous l'angle de la réglementation de l'utilisation, des utilisateurs ou de la disponibilité de la technologie, nous pouvons commencer à réfléchir à des choses comme les contraintes ou les restrictions touchant l'utilisation des systèmes commerciaux de surveillance faciale. Il conviendrait plutôt de financer ou de mettre au point des systèmes internes utilisant des données qui ne sont pas seulement obtenues légalement, mais dans le cadre d'un consentement pleinement éclairé et de processus qui garantissent la dignité des personnes dont les données sont traitées. Ces systèmes seraient conçus et utilisés exclusivement pour des cas d'utilisation très précis, contrairement aux systèmes commerciaux comme Clearview AI, par exemple, qui sont employés dans une vaste gamme de scénarios différents, dont aucun ne tient compte du contexte social particulier et des implications pour les personnes dont les données sont traitées ou qui sont touchées par l'utilisation de ce système.

J'estime que des moyens nous permettent de distinguer des cas d'utilisation très circonscrits et de ne pas acheter un discours qui dit que nous avons besoin de la reconnaissance faciale parce qu'elle peut être utilisée pour protéger des gens d'un préjudice potentiel.

● (1305)

Le président: Merci beaucoup.

Voilà qui met fin à cette série de questions.

Sur ce, je remercie beaucoup nos témoins. Nous avons entendu des témoignages très importants et intéressants aujourd'hui, alors merci à vous.

La séance est levée.