CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

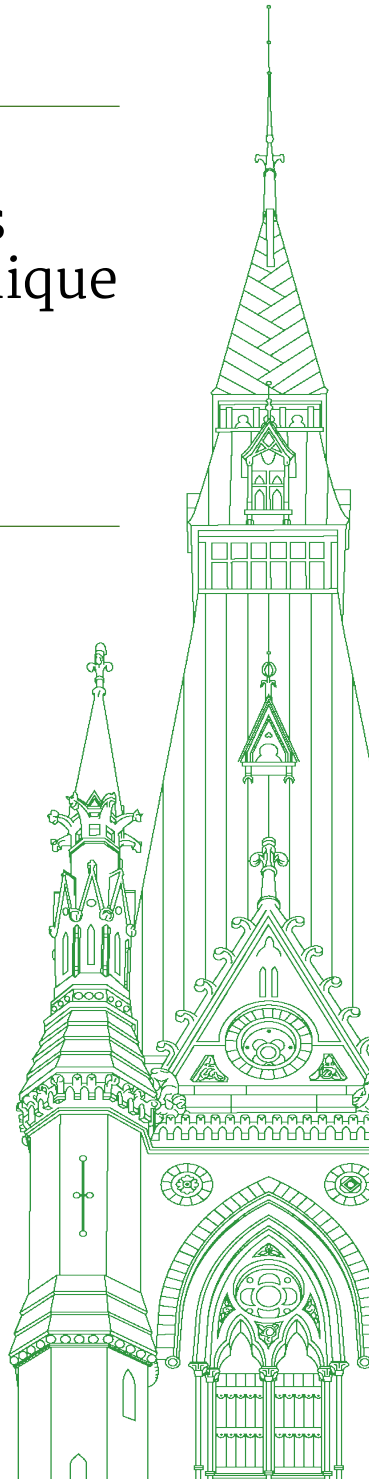
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 027

Le jeudi 16 juin 2022



Président : M. Pat Kelly

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

Le jeudi 16 juin 2022

● (1545)

[*Traduction*]

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

Bienvenue à la 27e 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. Conformément à l'alinéa 108(3)h) du Règlement et à la motion adoptée par le Comité le lundi 13 décembre 2021, le Comité reprend son étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale.

J'aimerais maintenant souhaiter la bienvenue à nos témoins.

Nous accueillons, de l'American Civil Liberties Union, Esha Bhandari; et de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, Tamir Israel, avocat-conseil à l'interne.

Veuillez nous excuser pour ce démarrage tardif. Ce n'est pas rare à cette époque de l'année, mais c'est encore une fois le calendrier des votes à la Chambre des communes qui en est la cause. Nous avions prévu une réunion d'une heure, de 15 h 30 à 16 h 30, et nous allons quand même aller de l'avant pour l'heure complète, à partir de maintenant.

Sur ce, je vais demander à Mme Bhandari de commencer.

Vous avez la parole pour un maximum de cinq minutes.

Mme Esha Bhandari (directrice adjointe, American Civil Liberties Union): Merci beaucoup, monsieur le président.

Je remercie le Comité de m'avoir invitée.

Je m'appelle Esha Bhandari et je suis directrice adjointe du Speech, Privacy, and Technology Project de l'American Civil Liberties Union, à New York. Je suis originaire de Saint John, au Nouveau-Brunswick.

J'aimerais parler au Comité des dangers associés aux identificateurs biométriques, et plus particulièrement de la reconnaissance faciale.

Étant donné que les identificateurs biométriques permettent d'identifier une personne et sont généralement immuables, les technologies biométriques — y compris la reconnaissance faciale — menacent gravement les droits civils et les libertés civiles parce qu'elles permettent les atteintes à la vie privée, notamment la perte de l'anonymat dans des contextes où les gens s'y attendaient traditionnellement, le suivi permanent des mouvements et des activités, et l'usurpation d'identité.

En outre, les failles dans l'utilisation ou le fonctionnement des technologies biométriques peuvent entraîner d'importantes violations des droits civils, notamment des arrestations injustifiées et le refus d'accès aux avantages, aux biens et aux services, ainsi que la discrimination en matière d'emploi. Il a été démontré que tous ces problèmes affectent de manière disproportionnée les communautés racisées.

Mais qu'est-ce qu'on entend exactement par biométrie?

Avant l'ère numérique, recueillir quelques données biométriques, comme les empreintes digitales, était laborieux et prenait du temps. Aujourd'hui, nous avons la possibilité de recueillir presque instantanément des données biométriques, y compris les empreintes faciales. Nous disposons de capacités d'apprentissage automatique et de technologies de réseau de l'ère numérique. Toutes ces avancées technologiques combinées rendent la menace de la collecte de données biométriques encore plus grande que par le passé.

La reconnaissance faciale en est un exemple, bien sûr, mais je tiens à souligner que la reconnaissance vocale, la lecture de l'iris ou de la rétine, la collecte d'ADN, la reconnaissance de la démarche et de la frappe au clavier sont également des exemples de technologies biométriques qui ont des effets sur les libertés civiles.

La reconnaissance faciale permet l'identification instantanée à distance, sans que la personne identifiée et suivie le sache ou y consente. Même dans le passé, les éléments d'identification qui devaient être capturés au su de la personne, comme les empreintes digitales, peuvent maintenant être collectés à son insu, et cela inclut l'ADN qu'elle répand dans son quotidien. La numérisation de l'iris peut se faire à distance, tout comme la reconnaissance faciale et la prise d'empreintes faciales, et ce, sans que la personne dont les données biométriques sont collectées le sache ou y consente.

La reconnaissance faciale est particulièrement sujette aux failles de la biométrie, entre autres les défauts de conception et les limitations matérielles. De multiples études ont montré que les algorithmes de reconnaissance faciale présentent des taux d'erreur d'identification nettement plus élevés pour les personnes de couleur, notamment les Noirs, et pour les enfants et les personnes âgées. Il y a de nombreuses raisons à cela. Je n'entrerai pas dans les détails, mais c'est en partie à cause des ensembles de données utilisés, mais aussi des lacunes observées dans des conditions réelles.

Je tiens également à souligner que les taux d'erreur constatés dans des conditions de test sont souvent exacerbés dans des conditions réelles, souvent pires que les conditions de test — par exemple, lorsqu'un outil de reconnaissance faciale est utilisé sur des images de surveillance de mauvaise qualité.

La technologie de reconnaissance faciale présente également d'autres risques lorsqu'elle est combinée à d'autres technologies pour déduire une émotion, un état cognitif ou une intention. Nous constatons que les entreprises privées font de plus en plus la promotion de produits censés détecter les émotions ou les états d'âme, tels que les détecteurs d'agressivité, à partir de tics faciaux ou d'autres mouvements détectés par cette technologie.

Les psychologues qui étudient les émotions s'accordent à dire que ce projet repose sur une science erronée, car il n'existe pas de lien universel entre les états émotionnels et les expressions faciales observables. Néanmoins, ces analyses vidéo se multiplient et prétendent détecter les comportements suspects ou déceler les mensonges. Lorsqu'elles sont déployées dans certains contextes, elles peuvent causer de véritables préjudices, notamment en matière de discrimination à l'embauche, si une entreprise privée utilise ces outils pour analyser le visage d'une personne lors d'un entretien afin de lire ses émotions ou sa sincérité et décide de lui refuser un emploi sur la base de cette technologie.

Bien sûr, je parle des défauts de la technologie et des taux d'erreur qui y sont associés et qui, je le répète, pèsent de manière disproportionnée sur certaines communautés marginalisées, mais il y a, bien sûr, des problèmes même lorsque la technologie de reconnaissance faciale fonctionne et donne des résultats précis.

Par exemple, la capacité des forces de l'ordre de suivre systématiquement les personnes et leurs déplacements dans le temps constitue une menace pour la liberté et les libertés civiles. Il est possible de détecter les allées et venues privées, qu'il s'agisse de personnes se rendant à des manifestations, dans des établissements médicaux ou dans d'autres lieux confidentiels. Sachant les dangers liés à l'utilisation de ces technologies par les forces de l'ordre, au moins 23 administrations aux États-Unis, de Boston à Minneapolis, en passant par San Francisco et Jackson, dans le Mississippi, ont adopté des lois qui interdisent le recours à la technologie de reconnaissance faciale par les forces de l'ordre ou le gouvernement.

● (1550)

Je tiens également à souligner l'utilisation de cette technologie par le secteur privé. Là encore, on observe désormais, par exemple, que les propriétaires utilisent la technologie de reconnaissance faciale dans les immeubles, ce qui leur permet de suivre les allées et venues de leurs locataires, mais aussi de leurs invités — partenaires romantiques et autres — dans l'immeuble. Nous voyons également cette utilisation dans les centres commerciaux privés et dans d'autres contextes...

Le président: Madame Bhandari, je suis désolé de devoir vous interrompre, mais je vais vous demander de conclure dans les deux prochaines secondes pour que nous puissions continuer. Vous avez un peu dépassé le temps qui vous était imparti.

Mme Esha Bhandari: Oui, absolument.

Je voudrais juste conclure par quelques recommandations stratégiques.

La première est d'interdire le recours à la technologie de reconnaissance faciale au gouvernement et aux forces de l'ordre. Il faut au moins prendre des règlements pour en restreindre l'usage et protéger les individus des préjudices qui peuvent en résulter.

La deuxième est d'appliquer cette réglementation aux entités privées qui utilisent la technologie de reconnaissance faciale.

Merci beaucoup.

Le président: Merci.

Nous allons maintenant entendre M. Israel, qui dispose d'un maximum de cinq minutes.

M. Tamir Israel (avocat-conseil à l'interne, Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko): Bonjour, monsieur le président, mesdames et messieurs les membres du Comité.

Je m'appelle Tamir Israel et je suis avocat à la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko de l'Université d'Ottawa, qui se trouve sur le territoire traditionnel non cédé des Algonquins Anishinaabe.

Je tiens à vous remercier de m'avoir invité à participer à cette importante étude sur les systèmes de reconnaissance faciale.

Comme le Comité l'a entendu, la technologie de reconnaissance faciale est polyvalente et constitue une menace insidieuse pour la vie privée et l'anonymat, en plus de miner l'égalité réelle. Elle exige une réponse sociétale différente, plus proactive, que pour les autres formes de technologie de surveillance.

Actuellement, la reconnaissance faciale se distingue par sa capacité de fonctionner discrètement et à distance. Des bases de données d'images préalablement authentifiées peuvent également être compilées sans la participation d'individus, ce qui a fait de la reconnaissance faciale la biométrie de choix pour accomplir toute une série de tâches. Dans son état actuel de développement, la technologie est suffisamment précise pour inspirer confiance à ses utilisateurs, mais suffisamment sujette à l'erreur pour avoir des conséquences potentiellement dévastatrices.

Nous reconnaissons depuis longtemps, par exemple, que les étalements de photos peuvent amener la police à concentrer à tort son attention sur certains suspects. Le biais de l'automatisation aggrave ce problème de manière exponentielle. Lorsque des agents qui utilisent une application telle que celle de Clearview AI ou qui effectuent des recherches dans une base de données de photos d'identité judiciaire se font présenter une galerie générée par un algorithme de 25 suspects potentiels correspondant à une image granuleuse prise par une caméra de vidéosurveillance, la tendance est de s'en remettre à la technologie et de présumer qu'ils ont trouvé la bonne personne. Inclure simplement une supervision humaine ne suffira donc jamais à atténuer pleinement les méfaits de cette technologie.

Bien entendu, les préjugés raciaux restent un problème important pour les systèmes de reconnaissance faciale. Même pour les algorithmes les mieux notés, les fausses correspondances peuvent être 20 fois plus élevées pour les femmes noires, 50 fois plus élevées pour les Autochtones de sexe masculin et 120 fois plus élevées pour les Autochtones de sexe féminin, par rapport aux hommes blancs.

À cause des préjugés raciaux persistants, même les utilisations les plus banales de la reconnaissance faciale peuvent devenir très problématiques. Par exemple, un site Web du gouvernement britannique utilise la détection du visage pour vérifier la qualité des photos de passeport, ce qui constitue un mécanisme efficace pour le renouvellement des passeports en ligne. Cependant, l'algorithme de détection du visage échoue souvent pour les personnes de couleur, ce qui aliène des individus déjà marginalisés en les privant de certaines commodités accessibles à d'autres.

Comme l'a dit mon amie, Mme Bhandari, la reconnaissance faciale reste profondément problématique, même si elle est débarrassée de ses préjugés et de ses erreurs. Les systèmes de reconnaissance faciale utilisent des renseignements biométriques très critiques et fournissent une puissante capacité d'identification qui, comme nous l'avons vu avec d'autres outils d'enquête tels que les contrôles de routine, sera utilisée de manière disproportionnée contre les communautés marginalisées, notamment les communautés autochtones et noires.

Jusqu'à présent, la police canadienne utilise, parce qu'elle le peut, des systèmes de reconnaissance faciale sur l'appareil mobile d'un suspect arrêté, sur l'album photo d'un appareil, sur des images de télévision en circuit fermé dans le voisinage général des crimes et sur des photos de surveillance prises par la police dans des lieux publics.

À nos frontières, la reconnaissance faciale est au cœur d'un effort visant à créer des identités numériques sophistiquées. Nous entendons trop souvent le refrain « Votre visage sera votre passeport ». La technologie permet également d'associer ces identités établies par des moyens sophistiqués et d'autres profils numériques aux individus, ce qui engendre un degré d'automatisation sans précédent.

À toutes les étapes, la transparence pose problème, car les agences gouvernementales en particulier sont en mesure d'adopter subrepticement des systèmes de reconnaissance faciale et d'en faire un usage nouveau. Elles misent à cette fin sur des pouvoirs légaux douteux et ne disposent d'aucune autorisation publique préalable.

Nous joignons nos voix à celles de nombreux collègues qui demandent un moratoire sur les utilisations de la reconnaissance faciale liées à la sécurité publique et nationale et sur les nouvelles utilisations à nos frontières. En l'absence d'un moratoire, nous recommandons de modifier le Code criminel pour limiter l'utilisation de cette technologie par les forces de l'ordre dans le cadre d'enquêtes sur des crimes graves et en l'absence de motifs raisonnables de croire à une infraction. Il serait aussi bon d'interdire de façon permanente l'utilisation de la reconnaissance biométrique automatisée en direct par la police dans les lieux publics, et nous recommandons également d'explorer une interdiction plus générale de l'adoption de nouvelles capacités de reconnaissance faciale par les organismes fédéraux en l'absence d'une forme d'approbation législative ou réglementaire explicite.

Une réforme en profondeur de nos deux principales lois fédérales sur la protection de la vie privée est également nécessaire. Le projet de loi C-27a été déposé ce matin. Il s'agit d'une loi édictant entre autres la Loi sur l'intelligence artificielle et les données et réformant les dispositions relatives au secteur privé, et la LPRPDE fédérale. Ces réformes sont en cours et feront l'objet de discussions, mais outre les modifications prévues par le projet de loi C-27, il faut modifier la LPRPDE et la Loi sur la protection des renseignements personnels afin que les renseignements biométriques soient explicitement codés comme critiques, qu'ils nécessitent une plus grande protection dans tous les contextes et, en vertu de la LPRPDE, qu'ils nécessitent un consentement explicite dans tous les contextes.

● (1555)

La LPRPDE et la Loi sur la protection des renseignements personnels devraient également être modifiées de sorte que les entreprises et les organismes gouvernementaux soient légalement tenus de déposer des évaluations des répercussions auprès du commissaire à la protection de la vie privée avant d'adopter des technologies intrusives. Enfin, le commissaire devrait être habilité à examiner les technologies intrusives dans le cadre d'un processus réglementaire public et à mettre en place des restrictions d'utilisation, voire des moratoires, au besoin.

C'est tout pour ma déclaration liminaire. Je remercie le Comité de m'avoir accordé ce temps, et je me ferai un plaisir de répondre à vos questions.

Le président: Merci.

Le premier intervenant pour ce tour de six minutes au maximum est M. Kurek.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup. J'aimerais remercier nos témoins de leur présence aujourd'hui. Comme je le dis souvent au début, n'hésitez pas à formuler des recommandations précises. Cela sera certainement très utile au Comité lorsqu'il en sera à rédiger son rapport.

Je suis sensible à la teneur de vos déclarations liminaires. Je pense que l'un des grands défis que doivent relever les législateurs et les responsables des politiques publiques dans ce domaine est d'essayer de trouver un juste équilibre. Il y a les forces de l'ordre qui disent avoir besoin de tous les outils disponibles pour lutter contre la criminalité, pour protéger les victimes, et ainsi de suite. De l'autre côté, nous avons l'argument valable selon lequel nous devons assurer la protection des personnes et des groupes vulnérables et le respect des droits des Canadiens, dans le cas du Canada.

Je vous pose à tous les deux la question suivante. Avez-vous des recommandations à faire au Comité sur la façon de trouver ce juste équilibre? Je vais commencer par M. Israel.

M. Tamir Israel: Lorsqu'il s'agit d'une technologie intrusive comme celle-ci, il incombe au gouvernement de justifier l'utilisation de cette technologie. L'un des grands problèmes — comme le Comité l'a entendu — est que cette technologie est en ce moment utilisée sur le terrain et que toute réaction d'ordre législatif découle de cette situation.

L'adoption de certaines de nos recommandations permettrait de renverser la situation. Il s'agirait de créer une obligation législative de saisir le législateur et de justifier à l'avance l'utilisation de certaines de ces techniques, ou encore d'habiliter l'organisme de réglementation, le commissaire indépendant à la protection de la vie privée du Canada, à jouer un rôle proactif dans l'évaluation et l'approbation ou le rejet de certains éléments de ces technologies. Je pense que cela pourrait être une métaétude de la façon de relever certains de ces défis de façon plus générale.

M. Damien Kurek: Merci.

Madame Bhandari, nous vous écoutons.

Mme Esha Bhandari: Pour faire suite aux propos de M. Israel, je dirais que je suis d'accord pour dire que, lorsque nous parlons d'une nouvelle technologie, en particulier d'une technologie comportant autant de failles que la reconnaissance faciale, la responsabilité doit incomber aux forces de l'ordre. Dans ce cas, nous connaissons les failles. De multiples études ont montré les taux d'erreur disproportionnés et les conséquences sur la vie des gens. Il y a eu quelques cas très médiatisés aux États-Unis d'hommes noirs arrêtés à tort à cause de la reconnaissance faciale, avec les conséquences dévastatrices que cela implique pour les gens.

Il faut au moins faire une étude approfondie pour montrer que les failles et les taux d'erreur ont été éliminés et qu'il n'y a pas de répercussions disproportionnées sur les personnes en fonction de la démographie. Ce n'est tout simplement pas le cas actuellement. En l'absence de cela, utiliser largement la technologie de reconnaissance faciale dans ces contextes particuliers revient à soumettre la population dans son ensemble à une expérience.

Nous n'en sommes pas encore là, mais je serais certainement d'accord pour dire que les inquiétudes concernant le suivi permanent et le vol d'identité sont bien fondées. Tout compromis recommandé par le Comité doit tenir compte des préjudices qui en résulteront même si la technologie fonctionne comme elle est censée le faire.

● (1600)

M. Damien Kurek: Je vous remercie.

Madame Bhandari, toujours dans la même veine, le Comité a étudié l'utilisation des données sur la mobilité dans le cadre de la réponse du Canada en matière de santé publique à la COVID-19. C'était intéressant. Dans une certaine mesure, votre déclaration liminaire correspondait à certaines des préoccupations entendues par le Comité au cours de cette étude antérieure. Je me demande si vous avez des observations à faire, si vous avez eu l'occasion de voir le travail de ce comité. Y a-t-il quelque chose que vous aimeriez ajouter à cela?

Mme Esha Bhandari: Il y a certainement, je pense, un lien avec ces préoccupations, parce que la localisation est l'un des inconvénients de la reconnaissance faciale, même quand elle fonctionne correctement. C'est une société dans laquelle chacun de nos mouvements est enregistré dans une base de données pour être utilisé. Je pense que les inquiétudes entourant la surveillance des téléphones portables et le traçage des contacts, lorsqu'ils sont effectués sans ces garanties, sont les mêmes pour la reconnaissance faciale.

Encore une fois, nous ne vivons actuellement pas dans une société où l'on s'attend, qu'on soit en public ou non, à ce que tous nos mouvements soient accessibles au gouvernement, aux forces de l'ordre et même à des entreprises privées, potentiellement, qui voudraient essayer de nous vendre des choses ou de nous exploiter d'une manière ou d'une autre. La technologie permet déjà de nous suivre partout où nous allons, toute la journée.

Les préoccupations relatives au suivi de la localisation que ce comité a examinées précédemment s'appliquent également ici.

M. Damien Kurek: Merci.

J'ai une dernière question à poser pendant la dernière minute qu'il me reste.

Nous entendons souvent citer l'exemple de Clearview AI et du fait que cette entreprise n'est plus utilisée au Canada, qu'elle n'a plus de contrat avec les forces de l'ordre. Cependant, il existe assurément toute une série d'autres fournisseurs et d'autres applications qui n'ont peut-être pas un objectif aussi équivoque que Clearview AI.

Pourriez-vous peut-être parler au Comité de votre expérience avec d'autres fournisseurs ou nous donner d'autres exemples que le Comité devrait peut-être connaître?

Il reste environ 30 secondes.

Mme Esha Bhandari: Il y a évidemment d'autres fournisseurs, oui.

L'American Civil Liberties Union a conclu un accord avec Clearview aux États-Unis pour l'empêcher de vendre sa base de données à des entités privées aux États-Unis. Cependant, il s'agit d'une entreprise parmi tant d'autres.

Beaucoup de ces entreprises ne sont pas nécessairement orientées vers les consommateurs. Il ne s'agit pas de grands noms de la technologie que les gens connaissent. Encore une fois, la transparence est la clé. Le public ne connaît peut-être pas ces entreprises autant qu'il connaît les grands médias sociaux, par exemple.

M. Damien Kurek: Merci.

Le président: Nous passerons maintenant à Mme Saks, pour un maximum de six minutes.

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

Je remercie les témoins présents aujourd'hui. Je commencerai par vous, monsieur Israel, si vous le permettez.

En septembre 2020, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko a publié un rapport sur la reconnaissance faciale, dont vous êtes l'auteur. Vous y mettez principalement l'accent sur son utilisation aux frontières.

De façon très concise, étant donné que nous avons peu de temps, quelles sont les principales conclusions de ce rapport? Pouvez-vous nous en donner les trois principales? J'aurai ensuite une question complémentaire.

M. Tamir Israel: Je dirais que les principales conclusions en sont que la reconnaissance faciale est adoptée à la frontière sans égard aux préjudices qu'elle pourrait causer, sans grande surveillance externe et souvent sans égard aux politiques existantes, comme la politique du Conseil du Trésor sur l'intelligence artificielle, qui dicte que l'on est censé solliciter des conseils externes lorsqu'on adopte des technologies aussi intrusives.

Ensuite, une fois adoptées, ces technologies sont souvent très vite utilisées à d'autres fins, qui dépassent le cadre étroit dans lequel elles ont été conçues.

Enfin, ces technologies font souvent le lien entre la présence numérique et la présence physique, d'une manière qui permet l'application de nombreux autres outils d'évaluation automatisés, ce qui est problématique en soi.

Mme Ya'ara Saks: Merci.

Vous avez dit dans votre déclaration préliminaire que l'interaction humaine avec ces plateformes est insuffisante. D'autres témoins nous ont dit que l'interaction humaine est en fait impérative pour pouvoir utiliser cette technologie.

Pourriez-vous nous en parler davantage, s'il vous plaît?

M. Tamir Israel: Je suis d'accord pour dire que cela fait partie intégrante de l'équation, mais il importe de reconnaître aussi que ce n'est pas suffisant.

Je pense que le Comité a également entendu un témoin expliquer comment les humains interagissent avec les images faciales qui leur sont présentées et comment leurs propres préjugés s'insinuent. L'exemple fourni était celui de la parade de photos souvent utilisée par la police, qui reproduit le type d'image que l'on obtient souvent d'un système de reconnaissance faciale, qui donne peut-être les 10 ou 15 meilleures correspondances. Nous savons que dans les enquêtes, cela a causé de nombreux problèmes à la police dans le passé.

C'est la supervision humaine dont on parle. C'est pire quand on utilise un système de reconnaissance faciale, parce que la tendance est de faire confiance aux résultats automatisés du système et de présumer que la correspondance est exacte. On est porté à remettre encore moins l'exactitude en doute que quand on examine une parade de photos générale et qu'on essaie de déterminer qui est la personne. Cela finit par induire des biais cognitifs et autres.

● (1605)

Mme Ya'ara Saks: Je comprends. L'erreur humaine est un facteur dans tout dans la vie.

Cependant, ma prochaine question à ce sujet est la suivante. Si nous mettons en place un garde-fou législatif, pouvons-nous réellement légiférer pour prévenir l'erreur humaine? Nous pouvons légiférer pour régir l'intervention humaine, mais comment légiférer pour prévenir l'erreur humaine? Le train a déjà quitté la gare pour ces technologies, et nous essayons de voir quels seraient les garde-fous possibles. Pouvons-nous véritablement légiférer sur l'erreur humaine?

M. Tamir Israel: Je pense qu'il est important d'inscrire dans la loi qu'un humain doit intervenir dans la prise de décision. Je pense qu'il est également important de reconnaître que cela ne résout pas tous les problèmes. C'est souvent présenté comme la solution, mais il y aura souvent bien des problèmes de partialité, même quand un humain intervient dans l'enquête. Il faut plus que cela.

Nous recommandons toujours l'imposition d'un moratoire, étant donné le grand préjudice que peut causer cette technologie, jusqu'à ce qu'on arrive à établir un cadre réglementaire et technologique plus concret et plus solide.

Mme Ya'ara Saks: Merci beaucoup.

Je m'adresserai maintenant à Mme Bhandari, si vous me le permettez.

J'aimerais aborder un sujet que, malheureusement, nous n'avons pas suffisamment abordé dans cette étude, à savoir les technologies de localisation utilisées dans les lieux commerciaux et de vente au détail. Par exemple, Cadillac Fairview est un grand propriétaire de centres commerciaux ici, au Canada. D'après ce que je comprends, il y a souvent des caméras et d'autres technologies dans ses centres commerciaux.

On parle beaucoup de légiférer la relation entre les entreprises privées et les forces de l'ordre. Je commencerai par vous, madame Bhandari, et je sonderai peut-être aussi M. Israel.

Comment pensez-vous que nous devrions légiférer la relation privée ou commerciale lorsque ce genre de technologie est utilisé, dans un monde idéal, s'il y avait un moratoire et que nous avions le temps d'y réfléchir?

Le président: Madame Bhandari, avant de vous laisser répondre à la question de Mme Saks, je vous demanderais de relever un peu la perche de votre microphone. Nous avons eu un peu de mal à bien entendre votre audio.

Allons-y, et je vous arrêterai à nouveau si nous avons besoin d'un autre ajustement.

Mme Esha Bhandari: J'espère que c'est mieux.

Pour répondre à la question sur l'utilisation de ces technologies dans le secteur privé, les préjudices sont réels. Je vais vous en donner quelques exemples.

Dans le Michigan, par exemple, les responsables d'une patinoire utilisaient un outil de reconnaissance faciale pour identifier les clients qui entraient et sortaient. Une jeune fille noire de 14 ans a été expulsée de la patinoire après que le système de reconnaissance faciale l'ait associée à tort à la photo d'une personne soupçonnée d'avoir déjà perturbé les activités de la patinoire.

Nous voyons des entreprises privées utiliser ce type de technologie, dans des salles de concert, des stades ou des installations sportives, pour identifier les personnes figurant sur une liste noire, c'est-à-dire les clients qu'elles ne veulent pas laisser entrer pour une raison quelconque. Encore une fois, le risque d'erreur et d'atteinte à la dignité que cela implique, le déni de service, sont bien réels. Il y a aussi le fait que ces données sont maintenant potentiellement entre les mains de sociétés privées qui peuvent avoir des règles de sécurité très variables.

Il y a par ailleurs des atteintes à la sécurité qui ont été observées, des cas où de grandes bases de données de reconnaissance faciale détenues par des gouvernements ou des entreprises privées ont été révélées au public. Comme les empreintes faciales sont immuables — ce n'est pas comme un numéro de carte de crédit qu'on peut changer —, une fois que les données biométriques d'une personne sont rendues publiques et potentiellement utilisées à des fins d'identification, il y a un risque.

De même, on voit des entreprises, comme Walgreens, aux États-Unis, déployer une technologie de reconnaissance faciale permettant de détecter l'âge et le sexe d'un client pour lui montrer des publicités ou des produits ciblés. Il s'agit d'une autre tactique invasive qui pourrait susciter des inquiétudes quant au fait que les acheteurs et les consommateurs sont orientés vers des remises ou des produits en fonction de stéréotypes de genre, ce qui pourrait aggraver la ségrégation dans la société.

Pire encore, cette technologie est utilisée par des employeurs...

● (1610)

Le président: Je suis désolé de devoir vous interrompre de nouveau, mais nous avons largement dépassé le temps imparti pour ce tour.

Je vais donner la parole à M. Villemure pour six minutes.

[*Français*]

M. René Villemure (Trois-Rivières, BQ): Je vous remercie beaucoup, monsieur le président.

Bonjour, madame Bhandari.

Ce comité a entendu toutes sortes d'histoires d'horreur — et d'erreurs — qui se sont produites. Nous avons entendu parler de préjugés qui étaient principalement dirigés vers des populations racisées, par exemple. Votre association est une association de défense des droits, et elle est donc militante.

Je vais, pour un moment, me faire l'avocat du diable.

Y a-t-il un quelconque avantage à utiliser la reconnaissance faciale?

[*Traduction*]

Mme Esha Bhandari: Merci de votre question.

Je suis d'accord avec ce que M. Israel a dit plus tôt, à savoir que le fardeau devrait incomber aux entités qui cherchent à utiliser la reconnaissance faciale. Je pense que les entreprises privées conviendront certainement qu'il y a un avantage à cela. Elles en tirent de l'argent. La collecte de données, comme nous le savons, est très rentable. Je ne pense toutefois pas qu'il s'agisse d'un avantage que le Comité devrait prendre en considération s'il y a atteinte aux droits.

Pour l'application de la loi et les utilisations gouvernementales, je pense qu'il est vrai que la nouvelle technologie semble toujours résoudre des problèmes de longue date, mais je ne vois rien qui justifie que la reconnaissance faciale et les avantages qu'elle pourrait comporter pour l'application de la loi l'emportent sur le type de transformation qu'elle entraînerait dans la société.

[*Français*]

M. René Villemure: Selon vous, l'atteinte aux droits est tellement importante qu'il ne vaut pas la peine de parler d'avantage, qui est souvent commercial — ce qui, par ailleurs, n'est pas le but de notre étude.

Est-ce bien cela?

[*Traduction*]

Mme Esha Bhandari: Oui.

[*Français*]

M. René Villemure: Vous avez parlé de détecteurs de mouvement un peu plus tôt. Dans le passé, j'ai lu des études à ce sujet, dont certaines étaient un peu frivoles. On parlait de la capacité de reconnaître les préférences sexuelles ou politiques des gens au moyen de la reconnaissance faciale.

Est-ce que tout cela est possible? Ces affirmations sont-elles, au contraire, totalement fantaisistes?

[*Traduction*]

Mme Esha Bhandari: Il y a beaucoup d'entreprises qui se vantent de pouvoir le faire en ce moment. Il n'y a cependant pas de preuves scientifiques pour en attester.

Actuellement, tous les experts disent qu'il n'y a pas de lien fiable entre nos manifestations physiques ou biologiques et ces états ou propensions mentales, mais je pense que la vraie crainte, bien sûr, c'est que la société en vienne à accepter ces liens, qu'on revienne à une époque où l'on pensait que la physionomie ou les caractéristiques physiques révélaient le caractère et que cette nouvelle technologie soit considérée comme apportant une vérité nouvelle et objective.

Je ne suis pas sûre qu'il y ait lieu de craindre que cette technologie révèle vraiment des états mentaux, mais plutôt qu'elle soit commercialisée comme telle.

[*Français*]

M. René Villemure: Je reviens sur votre dernier commentaire.

La population doit-elle s'habituer à la surveillance électronique? N'est-ce pas peine perdue de tenter de légiférer l'utilisation de milliards d'images qui circulent déjà?

[*Traduction*]

Mme Esha Bhandari: Ce n'est absolument pas peine perdue, et le gouvernement a largement le temps d'agir. Il est essentiel de réglementer la circulation de l'information pour mettre un terme à certains préjudices qui s'observent déjà.

Il n'est pas inévitable de continuer d'être inondés d'informations biométriques, de continuer d'être suivis. Ce qui s'est passé s'est passé, bien sûr, mais à partir de maintenant, nous pouvons mettre des garde-fous en place. Nous pouvons nous doter de lois et de règlements robustes. Ce n'est pas parce qu'un secteur n'a pas été réglementé dans le passé qu'il est trop tard pour le réglementer maintenant.

[*Français*]

M. René Villemure: Vous parlez de contenu fourni par l'utilisateur. Ne devrions-nous pas faire de la sensibilisation quant à la vie privée ou aux risques liés à l'utilisation des données?

[*Traduction*]

Mme Esha Bhandari: C'est certainement une partie de l'équation. Mais je tiens aussi à souligner que souvent, des données sont recueillies sur les gens sans leur consentement. Il y a tellement de gens qui utilisent Internet pour faire des achats ou chercher de l'information, qui ne savent pas comment ils sont suivis.

Comme je l'ai mentionné, les empreintes faciales sont souvent saisies sans notre consentement. Personne ne peut vraiment dire « non » si des caméras de surveillance captent des images. Le problème n'est pas que les gens renoncent volontairement à leurs données biométriques. La plupart du temps, les gens ne le savent pas, c'est pourquoi il est essentiel d'exiger d'informer les gens et d'obtenir leur consentement avant de saisir des données biométriques.

[*Français*]

M. René Villemure: Pourriez-vous nous parler brièvement de la poursuite que vous avez intentée contre Clearview AI dans l'État d'Illinois?

● (1615)

[*Traduction*]

Mme Esha Bhandari: Oui. Nous avons intenté une poursuite contre Clearview en vertu d'une loi de l'État de l'Illinois connue sous le nom de BIPA, la Biometric Information Privacy Act, et nous avons obtenu règlement.

Il y a deux dispositions clés dans ce règlement. Clearview ne peut plus fournir à aucune entité privée l'accès à sa base de données contenant des millions et des millions d'empreintes faciales nulle part au pays, jamais. Il s'agit d'une interdiction permanente de vente à des entités privées dans le pays, à quelques exceptions près, et d'une interdiction d'accès aux forces de l'ordre pendant cinq ans dans l'Illinois.

La seule chose qui nous a permis d'intenter ce procès, c'est que l'Illinois dispose de cette loi sur la confidentialité des informations biométriques, fait rare aux États-Unis. Cette loi montre le potentiel de la réglementation. C'est cette loi qui nous a permis de poursuivre Clearview et de parvenir à un accord selon lequel Clearview ne peut plus vendre sa technologie d'empreinte faciale à des entités privées nulle part au pays.

[*Français*]

M. René Villemure: Je vous demanderais de nous faire parvenir de la documentation sur la loi en question ou sur la poursuite que vous avez intentée, si cela est possible. Cela nous serait utile.

[*Traduction*]

Mme Esha Bhandari: Je le ferai avec plaisir.

[*Français*]

M. René Villemure: Pouvez-vous me dire si Clearview AI peut tout de même vendre sa technologie à l'extérieur des États-Unis pour l'instant?

[*Traduction*]

Mme Esha Bhandari: Notre poursuite ne concerne pas ce que l'entreprise peut faire en dehors des États-Unis. C'est exact.

[*Français*]

M. René Villemure: D'accord.

Je vous remercie beaucoup.

[*Traduction*]

Le président: Le prochain intervenant sera M. Green, pour un maximum de six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Je vous remercie.

J'aimerais poursuivre dans la même foulée. Je me souviens qu'au retour d'un vol international, on m'a fait passer par un poste de contrôle de la sécurité intérieure américaine. Je crois que c'était à Pearson. C'était la première fois que je devais me soumettre à un balayage de l'iris. Je me demande si les témoins peuvent nous parler — et peut-être pouvons-nous entendre d'abord Mme Bhandari — de la façon dont Nexus, dans nos aéroports, a... Son travail aux États-Unis a-t-il donné lieu à des enquêtes ou à des recherches sur le service public-privé de collecte de données biométriques de Nexus?

Mme Esha Bhandari: Nous nous préoccupons justement de l'utilisation croissante de la reconnaissance faciale et d'autres technologies biométriques dans les aéroports. Nous ne nous sommes pas penchés sur les activités de Nexus, en particulier, mais le même principe s'applique, par exemple, au système d'entrée global aux États-Unis.

Le problème, bien sûr, c'est que lorsque les gens sont obligés de fournir des empreintes faciales ou de se soumettre à un balayage de l'iris pour accéder à des services essentiels — aller à l'aéroport, traverser la frontière, entrer dans un bâtiment gouvernemental —, cela facilite le travail des sociétés de contrôle comme jamais auparavant. Ce ne sont pas des contextes auxquels les gens peuvent facilement se soustraire, donc la réglementation pourrait prévoir de véritables solutions de rechange en cas de refus. Ainsi, si l'on ne veut pas prouver son identité au moyen d'un balayage de l'iris, on aurait la possibilité de le faire d'une autre manière, avec le passeport, par exemple, ou une carte Nexus.

À l'aéroport ou à la frontière, parce que c'est un environnement tellement coercitif, les gens ne peuvent pas simplement choisir de s'en aller, donc c'est une grande préoccupation.

M. Matthew Green: Allez-y, monsieur Israel.

M. Tamir Israel: C'est exactement comme Mme Bhandari l'a dit. C'est un gros problème, parce que les programmes comme celui de Nexus sont facultatifs, d'une certaine façon, mais la pression exercée pour traverser la frontière, l'utilisation explicite de la frontière comme élément de persuasion pour convaincre les voyageurs de s'inscrire à ces systèmes pose problème.

Le Canada, par exemple, a piloté un programme avec les Pays-Bas, un programme mis au point par le Forum économique mondial. Il s'agit essentiellement d'une identité numérique, enregistrée dans votre téléphone, qui contient l'essentiel des renseignements sur votre passeport et des renseignements du programme de vérification de l'identité sociale. L'idée était de voir si cela pouvait remplacer le passeport, afin de faciliter le passage aux frontières. La reconnaissance faciale était la technologie intégrée à ce système. L'objectif ultime de ce système — c'est très explicite — est de convaincre les voyageurs de s'y inscrire volontairement pour éviter les délais à la frontière, parce qu'il donne accès à un contrôle de sécurité plus rapide. Toutefois, il sera ensuite mis à la disposition des banques, des sociétés de télécommunications et d'autres entités pour des programmes de vérification de l'identité similaires.

M. Matthew Green: Oh là là, monsieur Israel, je pense que vous avez peut-être touché le troisième rail lorsque vous avez parlé du Forum économique mondial, dans ce contexte.

Votre rapport m'intéresse. Vous faites état de données qui laissent entendre que les agences canadiennes de contrôle des frontières ne semblent pas conscientes des préjugés raciaux inhérents à ces systèmes. Le peu d'informations publiques disponibles porte à croire que ces outils ont peut-être été évalués pour leur niveau général d'inexactitude, mais pas du point de vue des biais raciaux. Je vous cite la saga actuelle des listes d'interdiction de vol pour les enfants. Dans ce pays, des enfants sont littéralement ciblés, identifiés et placés sur des listes d'interdiction de vol parce qu'ils pourraient avoir des noms à consonance musulmane. Ils sont pris dans une sorte de cauchemar bureaucratique, très franchement, lorsqu'ils essaient de voyager.

Pouvez-vous nous parler des risques inhérents à ce manque de sensibilisation aux préjugés raciaux, notamment lorsqu'on met en place des garde-fous humains pour aider à compenser certaines de ces incohérences et inexactitudes?

● (1620)

M. Tamir Israel: Il s'agit certainement d'une inquiétude valable et pertinente.

La liste des personnes interdites de vol représente un problème de longue date. On a proposé de créer des listes fondées sur la reconnaissance faciale avec des objectifs comparables. En fait, l'ASFC a dirigé un tel projet pilote pendant un certain temps, mais l'Agence a décidé de ne pas le mettre en œuvre tout de suite, je pense. Mais cela reste un projet pilote que l'Agence a dirigé, et c'est très problématique.

La réponse de l'ASFC est préoccupante. Par exemple, dans le cadre d'un reportage, CBC a tenté d'examiner les préjugés raciaux de l'un de ces systèmes de reconnaissance faciale. Lorsque CBC a demandé une ventilation plus détaillée des taux d'erreurs et des taux de préjugés raciaux… D'abord par l'entremise de demandes d'accès à l'information, il est apparu que l'ASFC ne savait pas, au moment de l'adoption de cette technologie, que ces problèmes étaient réels. Plus tard, l'Agence a répondu que la divulgation de ce type de données sur les erreurs posait des problèmes de sécurité nationale, ce qui n'est tout simplement pas le cas… En effet, dans d'autres pays, ces données sont accessibles au public et la loi exige même que ce soit le cas. Ce n'est donc pas une bonne approche.

Plus récemment, la situation a évolué, c'est-à-dire que l'ASFC a annoncé qu'elle tenterait de mettre en place un centre d'études biométriques au sein de son infrastructure, mais nous n'avons encore rien vu de concret.

M. Matthew Green: Rapidement, avant que le temps qui m'est imparti ne soit écoulé…

Je pense au cauchemar que représente l'aéroport Pearson, à Toronto, avec les attentes de trois à quatre heures pour les voyages intérieurs parce que des voies de sécurité sont fermées. Pensez-vous que ce sont des conditions adéquates pour vérifier l'identité des gens avec des systèmes comme Nexus?

Lorsque je fais la file et que je regarde les lignes pour la classe affaires, les détenteurs de carte Visa ou Nexus, je constate qu'il n'y a personne. Pensez-vous que les incohérences et les inefficacités à nos frontières pourraient entraîner une forte augmentation de la demande pour des choses comme Nexus?

M. Tamir Israel: Je pense que cela met les gens dans une position injuste de devoir choisir cette solution, si c'est le seul moyen de rendre leur expérience un peu moins désagréable à l'aéroport et pendant leur voyage.

Les choses ne font qu'empirer. En effet, partout dans le monde, on propose d'automatiser ce processus de contrôle de l'identité. Les gens devront donc se présenter devant un écran pour subir une analyse de reconnaissance faciale. Une évaluation du profil sera effectuée numériquement, et chaque personne sera automatiquement dirigée vers une ligne à sécurité élevée, intermédiaire ou peu élevée.

Ce sera la même chose, mais à un niveau beaucoup plus élevé. Si vous n'avez pas le bon profil pour interagir avec ce…

M. Matthew Green: Oui, je peux imaginer où cela va nous mener. J'ai été dirigé vers la zone d'évaluation secondaire plus souvent que raisonnable.

Je vous remercie beaucoup, monsieur le président.

Je remercie également les témoins.

Le président: Je vous remercie. Nous avons dépassé le temps imparti, mais c'est correct, car nous avons obtenu de bons renseignements. J'espère que nous tenterons de respecter le temps imparti pendant les autres séries de questions.

Cela dit, la parole est maintenant à M. Bragdon. Bienvenue au Comité. Vous avez la parole. Vous avez cinq minutes.

M. Richard Bragdon (Tobique—Mactaquac, PCC): Je vous remercie, monsieur le président.

J'aimerais saluer les autres membres du Comité qui sont ici aujourd'hui.

Nous abordons un sujet très important. Un grand nombre de Canadiens ont des préoccupations réelles et sincères à cet égard. Pendant que notre monde continue d'évoluer à un rythme effréné et que nous constatons que les préoccupations relatives à la protection de la vie privée ne cessent de s'accroître — tout en tenant compte du besoin d'assurer la sécurité des populations —, je pense que les Canadiens veulent avoir l'assurance que toutes les mesures de protection nécessaires sont mises en place pour protéger leurs droits individuels et leur droit à la vie privée.

Monsieur Israel, j'aimerais vous poser ma première question. Dans votre rapport, vous formulez plusieurs recommandations intéressantes quant à ce que vous souhaiteriez voir dans un cadre législatif relatif à la technologie de reconnaissance faciale — un cadre dont nous ne disposons pas actuellement. Dans votre rapport, vous indiquez que la nécessité d'un soutien législatif concerne les utilisations aux contrôles à la frontière qui s'appuient sur une forme de consentement, comme l'option de donner son consentement ou de le refuser.

Pensez-vous que toute utilisation de la technologie de reconnaissance faciale par les services de contrôle à la frontière devrait offrir l'option de donner son consentement ou de le refuser?

● (1625)

M. Tamir Israel: Oui. Une partie du problème avec cette technologie, c'est que si l'on n'exige pas le consentement explicite, la personne n'est même pas nécessairement consciente qu'elle est soumise à cette technologie. Par exemple, dans le cas des mécanismes de contrôle douanier installés à Pearson, le voyageur ne se rend pas nécessairement compte qu'une analyse de reconnaissance faciale est en cours. En effet, il n'y a pas d'obligation explicite d'obtenir le consentement de la personne. C'est tout aussi problématique. Aux États-Unis, nous avons vu des exemples où il y avait une obligation d'offrir l'option de refuser le consentement, mais ces affiches étaient cachées dans un coin et les gens ne les voyaient pas très bien.

À mon avis, il serait donc utile d'ajouter une option de refus indiquée très clairement, et peut-être même une obligation de demander d'abord le consentement.

M. Richard Bragdon: Pouvez-vous expliquer plus en détail la différence entre une architecture centralisée et décentralisée dans la technologie de reconnaissance faciale? Comment chaque type de système est-il susceptible de subir des atteintes à la vie privée? À quelles atteintes sont-ils susceptibles d'être exposés? Pouvez-vous nous expliquer tout cela?

M. Tamir Israel: Dans un système centralisé, toutes les images sont conservées en un seul endroit. Si je me présentais devant une caméra, ma photo serait prise et comparée à la base de données centralisée qui contient des millions d'images.

Un système décentralisé ressemblerait à ce que nous avons sur nos passeports, où une image numérique est encodée dans le passeport. Lorsque je l'utilise, une photo est prise. L'image numérique sur mon passeport est ensuite comparée à celle qui vient d'être prise. La comparaison se fait de cette manière.

Il y a là encore des risques pour la sécurité, car la sécurité du dispositif radio numérique encodé sur le passeport peut être compromise, mais de cette façon, on ne compromet qu'un seul passeport. Tous les modèles biométriques ne sont donc pas réunis en un seul endroit, ce qui permettrait de s'emparer de l'ensemble de la base de données beaucoup plus facilement.

M. Richard Bragdon: En outre, les images des voyageurs qui sont des enfants ou des personnes âgées sont moins bien identifiées par la technologie de reconnaissance faciale, et c'est la même chose pour les personnes de différentes origines ethniques. Ensemble, toutes ces personnes forment un très grand groupe.

Pour cette raison, tous les voyageurs devraient-ils, une fois de plus, avoir le choix d'accepter ou de refuser de se soumettre aux systèmes de technologie de reconnaissance faciale, afin d'éviter d'être mal identifiés lors de leurs déplacements?

M. Tamir Israel: Dans les aéroports de nombreux pays, la reconnaissance faciale n'est pas utilisée pour les voyageurs âgés de moins de 14 ans et de plus de 79 ans, si je me souviens bien. Encore une fois, cela compromet considérablement les gains d'efficacité que l'on peut tirer de l'adoption de ces systèmes, tout en soumettant tous les autres voyageurs au caractère intrusif de l'obligation de fournir leurs données biométriques. Je pense qu'il faut en tenir compte pour évaluer l'efficacité de ces systèmes.

Il s'agit également d'une mesure de protection qui doit être mise en œuvre et prise en compte, afin que ces systèmes ne soient pas utilisés pour les groupes d'âge pour lesquels on sait que la précision diminue de manière importante. Pour le reste, je pense qu'offrir le choix de donner le consentement peut être une option acceptable, mais je pense qu'un moratoire est toujours une bonne idée, étant donné l'adoption très rapide de cette technologie et des erreurs qu'elle continue de produire.

M. Richard Bragdon: À cet égard, vous recommandez d'appliquer un moratoire jusqu'à ce que nous en sachions plus. Cela semble certainement représenter une approche sage et prudente, car il s'agit en grande partie d'une technologie émergente. Cette technologie arrive à grands pas, et la population canadienne dans son ensemble n'est pas suffisamment sensibilisée aux ramifications de ce type de technologie et aux répercussions qu'elle pourrait avoir sur leur droit à la vie privée, leurs droits individuels, l'endroit où ces renseignements seront entreposés et où ils pourraient être envoyés. D'après ce que nous entendons, je pense que cette technologie soulève beaucoup plus de questions qu'elle n'offre d'avantages.

Je vous remercie.

Le président: Il n'y a pas de quoi. Vous avez utilisé tout votre temps, et même un peu plus. Il n'y a donc pas suffisamment de temps pour entendre la réponse.

La parole est maintenant à M. Bains. Il a cinq minutes.

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

J'aimerais remercier nos témoins d'être ici aujourd'hui. Je vais d'abord poser une question à M. Israel.

Selon l'une des principales conclusions du rapport, la technologie de reconnaissance faciale est mieux acceptée par la société que les autres technologies biométriques. À quelles autres technologies biométriques la technologie de reconnaissance faciale est-elle comparée, et pourquoi la technologie de reconnaissance faciale serait-elle plus acceptable que les autres?

M. Tamir Israel: Je pense que Mme Bhandari a également abordé cette question.

Puisque la reconnaissance faciale fonctionne subrepticement et n'est pas associée à des choses comme les empreintes digitales qui ont traditionnellement été utilisées dans un contexte de justice pénale, elle fait l'objet d'une stigmatisation sociale moindre dans l'esprit des gens, même si ce ne devrait pas être le cas, car elle est de plus en plus utilisée dans le même contexte que les photos anthropométriques, etc.

L'autre aspect concerne ce dont parlait Mme Bhandari plus tôt, c'est-à-dire que puisqu'elle agit à distance et avec moins d'interférence directe avec la personne, les gens ne sont parfois pas conscients du caractère intrusif de la technologie de la reconnaissance faciale comparativement à d'autres technologies biométriques où il faut physiquement saisir les doigts des gens ou leur demander de se pencher pour garantir un bon balayage de l'iris des yeux. Pour ces deux raisons, la reconnaissance faciale a été plus facile à faire adopter.

● (1630)

M. Parm Bains: Voici ma prochaine question. Comment les technologies de reconnaissance faciale devraient-elles être réglementées dans le secteur privé? Cette question s'adresse aussi à M. Israel.

M. Tamir Israel: Je pense que dans certains contextes, le préjudice peut être encore plus grand dans le secteur privé que dans le secteur public. Il y a probablement une plus grande variation.

Comme solution générale à ce problème, nous recommandons de donner au commissaire à la protection de la vie privée le pouvoir de se pencher sur l'adoption de technologies intrusives et d'imposer des conditions, voire des moratoires, sur des technologies précises. Nous recommandons également de coder les renseignements biométriques comme étant de nature délicate et d'exiger le consentement explicite avant de collecter des renseignements biométriques, comme c'est le cas, je crois, dans une loi adoptée par l'Illinois — c'est-à-dire la loi qui a été mentionnée par Mme Bhandari —, ainsi que dans la loi québécoise actuelle.

Je pense que ce sont deux bonnes étapes, et peut-être même un moratoire par la suite. C'est juste un cas d'utilisation élargie.

M. Parm Bains: Je vous remercie.

Madame Bhandari, les autorités policières américaines ont été beaucoup plus disposées à utiliser la technologie de reconnaissance faciale… Je suis désolé, c'est la mauvaise question.

L'État de l'Illinois a adopté une loi — la Biometric Information Privacy Act — qui s'applique précisément à la biométrie et donc à la technologie de reconnaissance faciale. Quels sont les avantages de cette loi?

Mme Esha Bhandari: L'un des principaux avantages, c'est que cette loi nous a permis de tenir une entreprise comme Clearview responsable de la création d'une base de données contenant des centaines de millions d'empreintes faciales de personnes obtenues sans leur consentement et de la vente de cette base de données à des entreprises privées et à des organismes d'application de la loi à toutes sortes de fins.

Nous avons plaidé pour que d'autres États adoptent des lois sur la confidentialité des données biométriques et, en particulier, qu'ils y apportent des modifications, car la loi de l'Illinois est maintenant assez ancienne, et nous avons davantage de connaissances sur cette technologie et les risques qu'elle pose.

Parmi les recommandations que nous formulons à l'intention des États qui souhaitent adopter une loi comme la BIPA de l'Illinois, nous recommandons d'exiger clairement que les entreprises obtiennent un avis et un consentement écrit avant de collecter, d'utiliser ou de divulguer des renseignements qui permettent d'identifier une personne, et d'interdire aux entreprises de refuser des services aux personnes qui choisissent de ne pas donner leur consentement, afin d'éviter qu'elles doivent choisir entre accéder à un service ou ne pas y accéder si elles ne sont pas prêtes à fournir leurs renseignements biométriques.

Nous encourageons aussi fortement les législateurs à faire en sorte que toutes ces lois obligent les entreprises à supprimer les identifiants biométriques un an après la dernière interaction de la personne avec l'entreprise. Par exemple, si une personne a donné son consentement à la collecte de ses données biométriques pour accéder à un service, mais qu'elle n'interagit plus avec l'entreprise, cette entreprise ne devrait pas pouvoir conserver et accumuler une base de données constituée de ces données biométriques de nature délicate. Comme l'a mentionné M. Israel, il y a un risque d'atteinte à la vie privée. Nous en avons vu des exemples, et il n'est pas nécessaire que ces entreprises privées conservent ces données. Nous préconisons donc l'adoption d'une loi comme la BIPA de l'Illinois, mais aussi d'une version mise à jour.

M. Parm Bains: D'autres États ont-ils adopté des versions modernisées de cette loi dont le Canada pourrait s'inspirer?

Mme Esha Bhandari: Il faudrait que j'y réfléchisse et que je fasse parvenir une réponse au Comité sur la question de savoir s'il existe une sorte de modèle idéal. Je pense que la loi de l'Illinois est un bon point de départ et je pense qu'il y a eu des projets de loi à cet égard au Maryland et au Maine. Ces lois n'ont pas été promulguées, mais elles existent. Ces modèles existent, et nous encourageons fortement leur adoption. Je me tournerais donc plus précisément vers le Maryland et le Maine pour trouver des modèles de loi.

M. Parm Bains: Je vous remercie.

Combien de temps me reste-t-il, monsieur le président?

Le président: Votre temps est écoulé, car il vous restait environ trois secondes.

La parole est maintenant à M. Villemure. Il a deux minutes et demie.

[*Français*]

M. René Villemure: Je vous remercie, monsieur le président.

Madame Bhandari, ce matin, le gouvernement du Canada a déposé le projet de loi C-27, qui vise notamment à mettre en œuvre la Charte du numérique. La partie 3 du projet de loi est intitulée « Loi sur l'intelligence artificielle et les données ».

Le projet de loi porte donc sur l'intelligence artificielle et la reconnaissance faciale. Il sera renvoyé pour étude en comité afin que nous puissions en discuter et faire des suggestions pour l'améliorer.

D'après ce que vous savez de la Biometric Information Privacy Act, ou BIPA, de quoi devrions-nous nous inspirer dans cette loi pour enrichir notre charte du numérique qui sera éventuellement mise en œuvre?

● (1635)

[*Traduction*]

Mme Esha Bhandari: J'aimerais préciser au Comité que le projet de loi du Maryland est le projet de loi SB 335. C'est une loi sur la confidentialité des renseignements biométriques. Je pense que c'est un modèle dont le Comité pourrait s'inspirer.

[*Français*]

M. René Villemure: Je suis désolé de vous interrompre, mais nous disposons de très peu de temps.

Y a-t-il quelque chose dans la BIPA dont le Canada devrait s'inspirer?

[*Traduction*]

Mme Esha Bhandari: Les dispositions relatives au consentement sont essentielles et il doit s'agir d'un consentement valable. Je pense que M. Israel a parlé des désavantages de l'option de retirer le consentement, et l'une de nos préoccupations principales est que nous interagissons tous avec un si grand nombre d'entreprises, surtout en ligne, que les gens se lassent lorsqu'ils doivent retirer leur consentement chaque fois.

Je pense que le consentement explicite et affirmatif est une option qui devrait inspirer votre comité, ainsi que le consentement valable pour des utilisations particulières.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

Croyez-vous qu'un jour nous pourrons, comme le permet maintenant la législation européenne, invoquer un droit à l'oubli ou un droit de faire retirer nos images des bases de données?

[*Traduction*]

Mme Esha Bhandari: Oui, c'est un élément essentiel de toute réglementation. Il devrait y avoir une période de temporisation, comme je l'ai mentionné. Nous avons suggéré une période d'un an après la dernière interaction avec une entreprise, par défaut, mais il est certain que chaque fois qu'une personne choisit de faire supprimer ses données biométriques d'une base de données, cette option devrait être offerte.

Encore une fois, en reconnaissant que les gens peuvent choisir d'utiliser des données biométriques dans un but très précis, même avec les risques que cela comporte, cela ne donne pas carte blanche à l'entreprise pour les conserver, car il s'agit d'identifiants de nature très délicate qui pourraient mener à un vol d'identité et à toute une série d'autres problèmes.

[*Français*]

M. René Villemure: Il faudra adopter une loi qui donnera clairement la possibilité aux gens de faire retirer facilement leurs images des bases de données.

N'est-ce pas?

[*Traduction*]

Mme Esha Bhandari: Oui, et il devrait également exister une limite clairement établie à toute collecte de données biométriques par le secteur privé. On doit établir une limite claire au partage avec d'autres entités, y compris les forces de l'ordre, sans le consentement de la personne. Nous devrions prendre des règlements qui permettent d'éviter qu'une fois qu'on donne ses données biométriques dans un but précis, ces dernières puissent être diffusées à grande échelle.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Nous allons maintenant entendre M. Green, pour deux minutes et demie.

M. Matthew Green: Merci.

J'aimerais que les invités soient en mesure de résumer dans leurs réflexions finales toute information pour le bien et le bien-être de ce comité afin que nos analystes puissent en tenir compte lors de la rédaction du rapport.

Je vais commencer avec Mme Bhandari.

Voulez-vous prendre une minute et peut-être nous faire part de vos réflexions finales que vous aimeriez que le Comité retienne de ceci?

Mme Esha Bhandari: Pour conclure, j'exhorte le Comité à agir rapidement. La technologie évolue chaque année, et dans l'état actuel des choses, c'est un domaine trop peu réglementé qui inflige des dommages chaque jour. Il existe des lois très concrètes et précises qui peuvent être promulguées. Il existe une réglementation qui peut être efficace, peu importe ce qui s'est passé auparavant. J'espère donc que le Comité gardera à l'esprit les recommandations très précises que M. Israel a fournies et d'autres. Il n'est pas trop tard pour agir.

M. Matthew Green: C'est très important.

Monsieur Israel, voulez-vous conclure vos remarques?

M. Tamir Israel: J'appuie ce que Mme Bhandari dit. Il n'est pas trop tard pour agir.

Je voudrais juste ajouter très rapidement que nous avons un énorme problème d'application au Canada. Nous avons évidemment eu des décisions contre Clearview ici aussi. Clearview conteste actuellement les décisions qui ont été rendues contre elle par les commissaires à la protection de la vie privée de la Colombie-Britannique, de l'Alberta et du Québec.

Au niveau fédéral, cependant, elle n'a pas contesté la décision du commissaire à la protection de la vie privée parce que cette décision n'est pas contraignante, alors il s'agit essentiellement de la prendre comme une recommandation et de passer à autre chose. Je pense que les mécanismes d'application qui seront mis en place dans le cadre du droit d'action prévu par le projet de loi C-27 — dont vous serez saisis sous peu, j'imagine — est une chose que vous devriez également examiner de très près lorsque vous réfléchissez à la manière de vous assurer que les lois que vous mettez en place sont respectées par Clearview et toutes les autres sociétés qui suivent son modèle.

M. Matthew Green: Merci beaucoup aux deux témoins. Je suis ravi de mettre fin à mon temps de parole, monsieur le président.

Le président: D'accord. Cela nous donne environ 45 secondes. Merci, monsieur Green.

Les deux dernières séries de questions iront à M. Kurek, puis nous finirons avec M. Fergus.

On vous écoute, monsieur Kurek.

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

Là encore, merci aux témoins.

Madame Bhandari, vous avez mentionné qu'il y a quelques exemptions aux données biométriques de Clearview. Vous en avez fait mention dans l'une de vos réponses précédentes. Pourriez-vous donner plus de détails à ce sujet pour le Comité?

● (1640)

Mme Esha Bhandari: Je suis désolée de ne pas avoir les détails de ces exemptions à vous fournir. Elles sont énoncées dans la loi à des fins très précises. Je peux envoyer des détails à la greffière plus tard sur les particularités de l'accord, qui décrit quelles sont ces exemptions dans la BIPA.

M. Damien Kurek: Je vous en serais reconnaissant.

Monsieur Israel, vous avez fait référence au programme d'identité numérique du voyageur digne de confiance du FEM, le Forum économique mondial. J'ai certainement entendu de nombreux concitoyens qui sont préoccupés par l'idée d'un type très puissant d'identité numérique. Le gouvernement participe à un programme pilote à cet égard. Avez-vous des préoccupations concernant le programme pilote d'identité numérique du voyageur digne de confiance, ou INVDC, dont vous pourriez faire part au Comité, en particulier s'il y a des inquiétudes sur la façon dont un programme comme celui-ci peut nuire de façon disproportionnée à certains éléments de la population, qu'il s'agisse de personnes de couleur, de minorités raciales, de jeunes, de personnes âgées, etc.?

M. Tamir Israel: Oui, tout à fait.

Je suis très préoccupé. Le programme pilote a été un peu interrompu par la pandémie, et je ne sais pas avec quelle vigueur il progresse à l'heure actuelle. Je suis très préoccupé par l'idée d'utiliser la localisation de l'expérience de voyage pour encourager les gens à s'inscrire et à créer ce type de profils, sachant que ce sera ensuite utilisé contre eux, non seulement dans le cadre des contrôles aux frontières, où de nombreuses communautés marginalisées sont déjà très désavantagées, mais aussi ici et à l'étranger, dans d'autres pays qui finissent par mettre en oeuvre le même système. Ce système est destiné à être mondial. L'idée est également que ces systèmes soient ensuite utilisés par le secteur privé pour détecter les fraudes ou gérer l'identité dans les interactions avec les entreprises privées.

La reconnaissance faciale est un élément important. Toutes les erreurs qui sont commises vont, encore une fois, frapper plus lourdement les minorités visibles et les membres des communautés marginalisées. Ensuite, les autres mécanismes d'évaluation et de classement social qui sont inclus dans ce programme de vérification d'identité, qui se trouveront sur votre appareil et seront liés à votre reconnaissance faciale, ont également tendance à peser très lourdement et de manière disproportionnée sur les membres des communautés marginalisées.

En ce qui me concerne, je ne pense pas que c'est la voie à suivre.

M. Damien Kurek: Je comprends ce que vous dites. Si vous voulez bien m'écouter, j'ai certainement entendu des concitoyens qui s'inquiètent de l'inclusion des convictions politiques d'une personne pour déterminer si elle peut ou non voyager, de l'inclusion de facteurs comme la race pour déterminer si une personne peut ou non louer un appartement, ou de toute une série d'hypothèses qui pourraient être incluses dans une base de données nébuleuse qui existe quelque part sur un serveur qui peut ou non faire l'objet d'une surveillance humaine. Je pense certainement que nous devons tous être très prudents à cet égard. En convenez-vous?

M. Tamir Israel: Absolument. Une partie du défi avec ce type de système, c'est que, en s'appuyant sur des outils d'évaluation de l'intelligence artificielle, on est en mesure de faire implicitement ce qu'on ne pourrait pas faire directement. On ne pourrait pas forcément dire, « Je ne vous loue pas un loyer car vous êtes d'origine autochtone », mais on peut adopter un algorithme qui s'appuie sur des données historiques biaisées et qui finit par arriver à cette conclusion sans la transparence qui permettrait à quelqu'un de contester explicitement ce type de décision. C'est un énorme problème à mesure que nous nous dirigeons vers cet ensemble plus vaste de mécanismes d'évaluation. Encore une fois, la reconnaissance faciale est un outil qui permet vraiment la mise en oeuvre de ces types de mécanismes. Le profil de l'INVDC comporte de nombreux éléments de ce type.

M. Damien Kurek: Dans les quelques secondes qui me restent, vous avez fait référence au secteur public et au secteur privé. Je sais qu'Air Canada, KLM et certains aéroports qui sont des entités quasi privées-publiques, selon l'endroit où ils se trouvent dans le monde, font partie des partenaires inclus dans ce programme. Cela vous préoccupe-t-il?

M. Tamir Israel: Absolument. C'est une préoccupation plus générale qui concerne les systèmes de reconnaissance faciale. Il y a beaucoup de va-et-vient dans d'autres instances — et nous pensons que cela finira par arriver ici — où les compagnies aériennes sont encouragées à adopter les systèmes de reconnaissance faciale pour des raisons de contrôle aux frontières. Elles reçoivent même parfois des fonds, qu'elles utilisent ensuite pour leurs propres raisons commerciales.

Il y a beaucoup d'interactions vraiment problématiques entre la manière dont le secteur privé recueille de plus en plus de données très sensibles aux frontières.

Le président: Merci, monsieur Israel.

Pour les cinq dernières minutes, nous allons entendre M. Fergus.

● (1645)

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

Par votre entremise, j'aimerais vraiment remercier ces deux témoins. Ils ont été remarquables et je leur suis réellement reconnaissant de leurs réflexions.

Pour les deux témoins, si vous ne savez pas comment fonctionnent les comités à la Chambre des communes, nous devons en fait recevoir un témoignage écrit ou verbal pour pouvoir formuler des recommandations. Nous devons entendre des déclarations sur le sujet avant de pouvoir aller de l'avant.

J'aimerais aborder la question sous un angle différent. Je vais poser la question suivante aux deux témoins aujourd'hui.

Monsieur Israel, en réponse à M. Kurek, vous parliez de la transparence — ou plutôt de l'opacité — de ces systèmes de technologie de reconnaissance faciale, ou TRF, et de la façon dont ils prennent subrepticement des photos et identifient les gens. Je suppose que ma question est la suivante: l'un d'entre vous sait-il s'il existe un registre des entreprises qui utilisent la technologie de reconnaissance faciale? Existe-t-il une liste quelque part d'entreprises, de gouvernements ou d'agences gouvernementales qui se livrent à la saisie d'images à des fins de TRF?

M. Tamir Israel: Je ne suis pas au courant s'il existe une liste.

Vous obtenez parfois des listes lorsqu'il y a un processus d'approvisionnement. Souvent, un certain nombre d'entreprises s'inscrivent pour y participer, mais il faut un peu de travail d'enquête de la part des journalistes pour le découvrir, et ce n'est jamais terminé.

Je dirai très brièvement que certains États — et Mme Bhandari peut ou non en savoir plus à ce sujet — exigent en fait que les courtiers en données s'enregistrent. C'est peut-être un élément à prendre en considération en ce qui concerne ces types d'entreprises si nous voulons obtenir plus de transparence sur ce qui se passe exactement sur le terrain.

L'hon. Greg Fergus: Madame Bhandari.

Mme Esha Bhandari: Je ne sais pas non plus s'il existe un registre centralisé.

Je tiens à souligner qu'aux États-Unis, le National Institute of Standards and Technology a réalisé une étude sur les outils de reconnaissance faciale il y a quelques années. C'est une étude largement médiatisée qui a révélé l'inexactitude du préjugé racial. Dans cette étude, je crois qu'on a examiné au moins 99 outils commerciaux de reconnaissance faciale vendus par des entreprises. Cela n'incluait même pas les outils de reconnaissance faciale des grandes entreprises comme Apple, Amazon ou Facebook.

C'est seulement pour vous donner une idée du nombre, mais je ne suis pas au courant s'il existe un registre centralisé.

L'hon. Greg Fergus: La prochaine question s'adresse à vous deux.

Devrait-il y avoir un registre à des fins de transparence?

Madame Bhandari, commençons avec vous.

Mme Esha Bhandari: Je pense certainement que c'est une première étape importante, notamment pour que les autorités chargées de l'application de la loi sachent qui elles réglementent, tout comme dans d'autres secteurs. Si vous réglementez les banques, elles n'exercent généralement pas leurs activités en catimini, si bien que vous ne sauriez pas qu'elles sont assujetties à ces règlements.

Comme M. Israel l'a mentionné, il existe un mouvement en faveur de l'enregistrement des courtiers en données, mais il ne concernerait pas forcément les entreprises qui vendent des outils de reconnaissance faciale ou d'autres outils algorithmiques. Le fait d'exiger ce type de transparence sur un produit que vous vendez permettrait un droit privé d'action ou une application privée des violations des lois ou des règlements, ou ferait en sorte que les organismes de réglementation sachent qui surveiller.

L'hon. Greg Fergus: Monsieur Israel.

M. Tamir Israel: Oui, précisément. Je pense que c'est exact. Je pense que Mme Bandhari a raison de dire que la liste de la base de données ne renfermerait pas ces types d'outils. Elle pourrait être un modèle sur lequel s'appuyer.

Je dirais également que, dans le régime européen, certains types de techniques plus intrusives exigent qu'une évaluation des facteurs relatifs à la vie privée soit déposée auprès de l'organisme de réglementation de la protection des données au début du processus. Quelque chose de ce genre pourrait être utile. Cela ne couvrirait pas nécessairement les petits outils du début ou tous les outils, mais ce pourrait être un autre moyen d'avoir un aperçu de ce qui est conçu au début.

L'hon. Greg Fergus: Je vais voir si je peux poser une dernière question dans la minute qui me reste.

Dans le contexte européen, avec ses protections numériques, ou peut-être dans n'importe quel État ou organisme infranational, savez-vous s'il existe une exigence selon laquelle les entreprises doivent déclarer publiquement qu'elles utilisent cette technologie?

Je ne parle pas seulement des gens qui vendent le service. Je parle des entreprises qui pourraient les utiliser à leurs propres fins.

Mme Esha Bhandari: Certaines lois ont été proposées aux États-Unis pour exiger la divulgation des outils algorithmiques ou de la prise de décisions automatisée, et je pense que la technologie de reconnaissance faciale en ferait partie.

Certaines lois qui ont été adoptées dans des villes ou des États exigent de la transparence pour l'utilisation par le gouvernement. Par exemple, si les forces de l'ordre adoptent une nouvelle technologie telle que la reconnaissance faciale, cette transparence est obligatoire afin qu'il puisse y avoir une surveillance démocratique de la communauté. Dans bien des cas, les conseils municipaux ne savaient pas ce que leurs services de police utilisaient ni de quelle technologie ils disposaient. Ces lois exigeraient que ces renseignements soient rendus publics, et les conseils municipaux et autres institutions démocratiques pourraient alors exercer une surveillance.

Je l'ai vu dans le contexte de l'utilisation gouvernementale.

● (1650)

Le président: Merci beaucoup.

M. Tamir Israel: Je pense que cet ajout serait excellent dans le contexte canadien également. Exiger aussi ce type d'avis serait très...

Le président: Nous avons largement dépassé le temps imparti. Mon microphone n'était pas activé, mais j'étais en train de mettre fin la discussion.

Merci beaucoup à nos deux témoins de leurs déclarations. Nous avons obtenu d'excellents renseignements aujourd'hui. Je vous en remercie infiniment.

Sur ce, la séance est levée.