CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

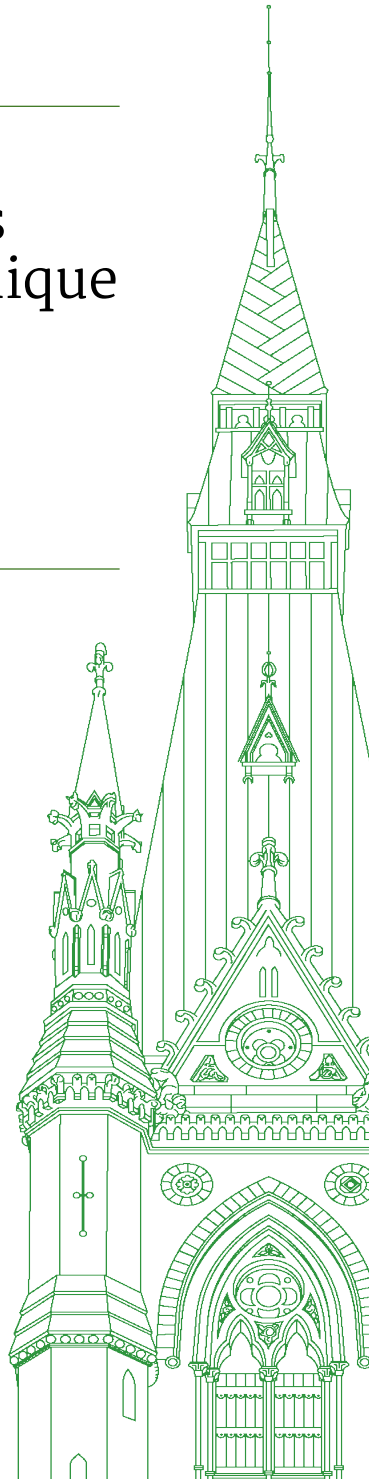
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 025

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 9 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 9 juin 2022

● (1625)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): J'ouvre la séance.

[*Français*]

Je vous souhaite la bienvenue à la 25e 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 répercussions de la technologie de reconnaissance faciale.

[*Traduction*]

J'aimerais souhaiter la bienvenue à nos témoins. Nous accueillons aujourd'hui Nestor Maslej, associé de recherche, Institute for Human-Centred Artificial Intelligence, Stanford University, qui témoignera à titre personnel; et Sharon Polsky, présidente, Conseil du Canada de l'accès et la vie privée.

Monsieur Maslej, vous avez cinq minutes pour faire votre déclaration préliminaire.

M. Nestor Maslej (associé de recherche, Institute for Human-Centered Artificial Intelligence, Stanford University, à titre personnel): Bonjour. J'aimerais commencer par remercier le président et les membres du Comité de m'avoir invité à prendre la parole aujourd'hui.

Je m'appelle Nestor Maslej, et je suis actuellement associé de recherche au Stanford Institute for Human-Centered AI. Je suis également co-auteur et chercheur principal de l'AI Index. Bien que mon témoignage d'aujourd'hui s'appuie sur les données de l'AI Index, je témoigne à titre personnel, et mes opinions ne sont pas représentatives de celles du Stanford Institute for Human-Centered AI.

L'AI Index est un rapport annuel, qui, à l'heure actuelle, en est à sa cinquième édition et qui vise à permettre de suivre, de distiller et de visualiser les principales tendances de l'intelligence artificielle. L'index a pour objet d'être la meilleure et la plus fiable source d'information sur les tendances de l'IA. Il vise à apporter aux décideurs politiques comme vous non seulement une compréhension plus approfondie de l'IA, mais aussi une compréhension fondée sur des données empiriques, ce qui est crucial.

C'est surtout ce dernier objectif qui inspire mon témoignage aujourd'hui. Je suis ici pour répondre à la question suivante: Que nous disent les données au sujet de la technologie de reconnaissance faciale (TRF)? Je répondrai à cette question en abordant deux sous-questions. Je vais d'abord parler de la capacité. À ce jour, que peut accomplit la TRF? Ensuite, j'examinerai son utilisation. Qui utilise la TRF — les acteurs publics et privés —, et comment?

En ce qui concerne la capacité, les performances des algorithmes de reconnaissance faciale ont fait d'énormes progrès au cours des cinq dernières années. L'AI Index a examiné les données provenant des Face Recognition Vendor Tests (FRVT) du National Institute for Standards and Technology (NIST), que le Département du Commerce des États-Unis a fournies et qui mesurent le rendement de la TRF dans le cadre de diverses tâches de sécurité intérieure et d'application de la loi, telles que la reconnaissance faciale appliquée à des images de photojournalisme, l'identification des enfants victimes de la traite, la déduplication des passeports et la vérification croisée des images de visa.

En 2017, certains des algorithmes de reconnaissance faciale les plus performants affichaient des taux d'erreur allant d'environ 20 à 50 % selon certains ensembles de données des FRVT. En 2021, aucun n'a affiché un taux d'erreur supérieur à 3 %, les modèles les plus performants enregistrant un taux d'erreur de 0,1 %, ce qui signifie que ces modèles identifient correctement 999 des 1 000 visages analysés.

L'AI Index montre également que les visages masqués réduisent le rendement de la TRF, mais pas de manière trop significative. Plus précisément, le rendement diminue de 5 à 16 points de pourcentage selon l'algorithme de la TRF et les ensembles de données.

En ce qui a trait à l'utilisation, les TRF sont déployées de plus en plus fréquemment dans des contextes publics et privés. En 2021, 18 des 24 organismes du gouvernement américain ont utilisé ces technologies: 16 départements l'ont fait à des fins d'accès numérique ou de cybersécurité, six, à des fins de création de pistes pour des enquêtes criminelles, et cinq, à des fins de sécurité physique. De plus, 10 départements ont signalé qu'ils espéraient élargir leur utilisation. Ces chiffres sont certes centrés sur les États-Unis, mais ils donnent une idée de l'ampleur de l'utilisation de ces outils par les gouvernements et des objectifs poursuivis.

Depuis 2017, un total de 7,5 milliards de dollars américains a également été investi à l'échelle mondiale afin de financer des entreprises en démarrage spécialisées dans la reconnaissance faciale. Cependant, seulement 1,6 de ces 7,5 millions de dollars ont été consacrés à des entreprises canadiennes de TRF en démarrage. Au cours de la même période, le montant investi dans les TRF a augmenté de 105 %, ce qui semble indiquer que l'intérêt des entreprises pour la TRF augmente aussi. Nos estimations montrent également que la TRF est le 12e secteur le plus financé parmi les 25 secteurs d'intérêt de l'IA.

Enfin, un sondage McKinsey mené auprès des plus grands dirigeants d'entreprises, un sondage que nous avons inclus dans l'AI Index, montre que, dans tous les secteurs étudiés, seulement 11 % des entreprises ont intégré la technologie de reconnaissance faciale dans leurs processus organisationnels standard, la TRF étant devancée par l'automatisation de processus robotisés (26 %) et la compréhension de la parole naturelle (14 %) en tant que technologies les plus intégrées dans les entreprises.

En conclusion, j'ai présenté quelques-unes des principales constatations de l'AI Index en ce qui concerne les capacités et l'utilisation actuelles de la TRF. J'espère que les données que je vous ai communiquées éclaireront efficacement les délibérations du Comité au sujet de la réglementation future des technologies de reconnaissance faciale au Canada. Je me ferai un plaisir de répondre à vos questions concernant les données que j'ai présentées et les conséquences qu'elles peuvent avoir.

Merci.

● (1630)

Le président: Merci.

Nous allons maintenant donner la parole à Mme Polsky pendant cinq minutes.

Mme Sharon Polsky (présidente, Conseil du Canada de l'accès et la vie privée): Merci beaucoup, monsieur le président. Bonjour chers membres du Comité. Je vous remercie de m'avoir invitée à comparaître devant vous aujourd'hui au nom du Conseil du Canada de l'accès et la vie privée.

Les observations que je formulerai aujourd'hui tiendront compte des tables rondes organisées par le conseil et composées de membres des secteurs public et privé, ainsi que de membres des forces de l'ordre, des membres qui s'entendent pour dire que la reconnaissance faciale est l'un des nombreux outils numériques qui présentent un grand potentiel.

Comme toute technologie, la reconnaissance faciale n'est ni bonne ni mauvaise, mais elle est facile à justifier, surtout lorsqu'elle est étudiée individuellement. La façon dont les gens utilisent la technologie fait toute la différence en ce qui concerne son caractère raisonnable, sa proportionnalité et son incidence sur la vie des gens.

Il y a 34 ans, notre Cour suprême a déclaré que « la notion de vie privée est au coeur de celle de la liberté dans un État moderne », que « la notion de vie privée est essentielle [au bien-être de la personne » et que la vie privée « mériterait une protection constitutionnelle », et j'ose dire qu'elle l'est toujours, sauf qu'aujourd'hui nous luttons pour avoir une quelconque vie privée, chez nous ou ailleurs.

Il est désormais difficile, voire impossible, d'empêcher que nos images faciales soient saisies et analysées et que nos mouvements et nos associations soient calculés et évalués en temps réel. Nous sommes visibles chaque fois que nous sortons dehors, et souvent aussi à l'intérieur, et nos images sont diffusées sur Internet, souvent à notre insu. Nous n'avons pas consenti à ce que ces images soient utilisées, ni à ce que notre démarche, nos frappes ou d'autres données biométriques soient analysées et mises en corrélation avec des bases de données qui contiennent des renseignements sur chacun de nous ayant été amassés.

Nous n'avons pas demandé que des appareils à commande vocale ou les plateformes de messagerie que nos enfants utilisent à l'école ou que nous utilisons au travail analysent nos conversations ou nos émotions, ou que nos téléviseurs nous observent pendant que nous les regardons. Pourtant, c'est désormais chose courante, grâce aux gouvernements et aux entreprises qui ont créé une industrie mondiale de la biométrie non réglementée, dont le chiffre d'affaires devrait atteindre 59 milliards de dollars américains d'ici 2025, tandis que des entreprises technologiques intégrées au secteur public nous incitent à utiliser notre visage pour payer nos courses et obtenir des services publics.

Au cours des 40 années pendant lesquelles les ordinateurs ont fait partie de notre vie quotidienne, aucune sensibilisation aux lois, aux droits ou aux responsabilités concernant la protection de la vie privée ou l'accès à l'information n'a été offerte au Canada. Il n'est donc pas étonnant que les Canadiens croient que les lois elles-mêmes suffisent à protéger la vie privée ou que seulement 14 % d'entre eux considèrent que leur connaissance du droit à la vie privée est « excellente ». Entre-temps, nous avons assisté à la mise en place de technologies automatisées qui portent atteinte à la vie privée et à des investissements de plusieurs millions de dollars dans des technologies de surveillance achetées également par les 86 autres pour cent de la population, des technologies qui visent à créer des collectivités sécuritaires partout au Canada.

Certes, les caméras à reconnaissance faciale installées dans les voitures, les caméras corporelles, les sonnettes et les téléphones cellulaires peuvent aider la police à identifier un suspect ou à élucider un crime, mais même la police admet que les caméras et la reconnaissance faciale ne préviennent pas les crimes et qu'il n'y a guère de corrélation entre le nombre de caméras publiques de télévision en circuit fermé et la criminalité ou la sécurité. Pourtant, leur vente et leur utilisation non réglementées sont une prophétie qui se réalise d'elle-même, car la familiarité engendre le consentement.

Facebook, Cambridge Analytica, Cadillac Fairview et Tim Hortons ne sont que la pointe de l'iceberg. Les entreprises et les gouvernements créent et utilisent des technologies qui violent nos lois sur la protection de la vie privée parce qu'ils le peuvent, parce que le modèle de consentement actuel est une illusion, et parce que Mark Zuckerberg et d'autres savent que le risque de sanction est bien moins important que la récompense liée à la collecte, à la manipulation et à la monétisation des renseignements sur nous.

Nous sommes cependant à un moment où trois changements importants doivent être apportés pour contribuer à protéger nos libertés démocratiques sans entraver l'innovation et pour que les Canadiens puissent retrouver leur confiance dans le gouvernement, la police et le secteur public.

Premièrement, il faut faire de la protection de la vie privée en personne, en ligne et à nos frontières un droit fondamental pour tous les Canadiens.

Deuxièmement, il faut promulguer des lois qui obligent toute personne qui crée, achète ou utilise une technologie à prouver qu'elle a une compréhension claire et correcte de nos lois, nos droits et nos responsabilités en matière de protection de la vie privée.

Troisièmement, de la même manière que les véhicules et les aliments doivent respecter des réglementations gouvernementales strictes avant que leur vente ou leur utilisation soit autorisée au Canada, il faut élaborer des lois qui rendent les créateurs de technologies responsables, en exigeant que leurs technologies fassent l'objet d'un examen indépendant complet visant à évaluer l'intégrité de leurs algorithmes et de leur accès aux renseignements personnels, ainsi que leur impartialité et leur incidence, avant que le produit ou la plateforme puisse être acheté ou utilisé, directement ou indirectement. Il faut aussi s'assurer que les normes sont établies et que les lois sont rédigées sans l'influence ou la contribution directe ou indirecte de l'industrie.

● (1635)

Ce ne sont là que quelques points saillants d'une question très complexe dont je suis impatiente de discuter avec vous.

Le président: Merci.

Cela dit, nous allons passer aux séries de questions.

Pendant les six premières minutes, M. Williams prendra la parole.

M. Ryan Williams (Baie de Quinte, PCC): Je remercie tous nos témoins.

Par votre entremise, monsieur le président, je vais commencer par interroger Mme Polsky.

Je crois que vous avez mentionné la question suivante dans vos recommandations. Avons-nous besoin de campagnes appropriées de sensibilisation sur le consentement numérique et la vie privée à l'ère numérique qui sont conçues à l'intention des Canadiens?

Mme Sharon Polsky: Nous avons besoin d'une sensibilisation qui explique ce qu'est la vie privée. Cela n'existe pas encore. En réalité, c'est la même chose que si je lançais mes clés de voiture à l'enfant d'en face en lui disant « amuse-toi bien, mais sois prudent », sans lui expliquer ce qu'est un panneau d'arrêt ou ce qu'il doit faire quand il en voit un.

Nous avons besoin de concevoir une sensibilisation appropriée, et nous avons besoin que les personnes qui assurent cette sensibilisation soient formées en premier lieu. Voilà ce qui nous manque à l'heure actuelle.

M. Ryan Williams: Nous avons déjà parlé de la lassitude du consentement: les gens ne lisent pas le formulaire de consentement qui fait environ six pages. Les gens le font défiler, et ils font la même chose quand ils téléchargent n'importe quelle application.

Constatez-vous une lassitude du consentement dans votre travail, et que devons-nous faire pour y remédier?

Mme Sharon Polsky: Eh bien, la lassitude du consentement est un terme intéressant. Je pense qu'il s'agit plutôt d'une question de résignation de la part des gens au fait que peu importe ce qu'ils voient ou non dans une soi-disant politique de confidentialité, ce n'est pas pertinent, parce que la formulation qui a été autorisée — et franchement, adoptée avec enthousiasme — par les organismes canadiens, européens et autres de réglementation de la protection des données est si vague qu'elle n'a aucun sens.

Un exemple parfait de cela, c'est le fait qu'habituellement, vous voyez la phrase d'introduction « Nous respectons votre vie privée », puis la phrase « Nous ne recueillons vos renseignements personnels qu'à des fins commerciales », qui sont suivies d'une liste d'autres termes vagues. L'objectif commercial de toute organisation à but lucratif est d'améliorer son bilan et ses bénéfices nets. Tout ce qu'elles peuvent faire pour remplir cette obligation est un objectif commercial légitime, en ce qui les concerne. Cela n'a aucun sens lorsqu'il s'agit de protéger des personnes. Lorsque nous disons oui à l'une de ces politiques de confidentialité, les entreprises ont essentiellement carte blanche pour communiquer nos renseignements à leurs partenaires commerciaux, quels qu'ils soient et où qu'ils soient établis dans le monde. Lorsque ces renseignements sont transférés à l'extérieur du Canada, ces entreprises en font ce qu'elles veulent, aussi longtemps qu'elles le veulent.

● (1640)

M. Ryan Williams: Nous savons que la Loi sur la protection des renseignements personnels est désuète et qu'elle doit être mise à jour, alors comment la mettriez-vous à jour?

Mme Sharon Polsky: En ce qui concerne la Loi sur la protection des renseignements personnels, je dirais qu'il est important de cesser d'avoir autant de mesures législatives fragmentées sur la protection des renseignements personnels aux niveaux fédéral, provincial et territorial. Bien qu'elles se ressemblent beaucoup — elles sont semblables dans la plupart des cas —, chacune de ces lois comporte des exemptions différentes, et il est presque impossible pour quiconque de savoir à quelle loi se conformer. Si c'est une loi provinciale, est-elle conforme à ceci... ou si c'est une loi sur la santé, s'applique-t-elle au secteur public? Puis, lorsque l'information franchit les frontières du pays ou de la province, la conformité devient cauchemardesque.

Veuillez adopter un texte législatif global qui s'applique au secteur public, au secteur privé, au secteur sans but lucratif et aux partis politiques.

M. Ryan Williams: Merci.

Presque tous les témoins qui ont comparu devant le Comité — les universités, les avocats et les experts en matière de libertés civiles — ont demandé un moratoire sur l'utilisation des TRF par les services de police.

Je sais que vous avez organisé des tables rondes auxquelles des agents de police ont participé. Quelle était leur opinion sincère au sujet de l'utilisation de la TRF?

Mme Sharon Polsky: La reconnaissance faciale que nous utilisons à l'heure actuelle extrait une série de photos signalétiques de notre base de données, et une personne doit alors regarder la photo du suspect et la comparer aux photos tirées de la base de données. Cela est acceptable. Aucun des agents de police n'a pu se faire à l'idée qu'une technologie de reconnaissance faciale en temps réel est déjà utilisée dans certaines provinces.

Ils ont insisté sur le fait que c'est la technologie qui est utilisée en ce moment. Ils ne pouvaient pas penser à une technologie qui dépasse celle qu'ils utilisent à l'heure actuelle, ou aux conséquences que cette nouvelle technologie, qu'ils n'utilisent pas encore, a pour la vie privée et la sécurité.

M. Ryan Williams: À votre avis, diriez-vous que les simples agents de police comprennent la TRF qu'ils utilisent?

Mme Sharon Polsky: Non. La réponse est tout simplement non, car ils ne sont pas différents de la plupart des habitants du Canada, et j'ose dire d'ailleurs. En l'absence de sensibilisation aux exigences de conformité exactes, à ce que la loi signifie réellement et à ce que la technologie peut réellement faire — et non aux arguments de vente —, ils ne peuvent compter que sur les arguments de vente d'un vendeur, dont l'intérêt est lié à sa commission et aux résultats financiers de l'entreprise. Ils ne s'intéressent pas à notre protection, à notre vie privée ou, franchement, aux problèmes des services de police.

M. Ryan Williams: Les simples agents de police avec lesquels vous avez participé à ces tables rondes seraient-ils favorables à un moratoire sur l'utilisation de la TRF par la police?

Mme Sharon Polsky: Quand ils peuvent parler d'eux-mêmes ou de leur propre vie, oui. J'ai parlé avec de nombreux agents de police employés par différents organismes canadiens, à l'échelle municipale, fédérale ou militaire, et ils disent essentiellement ce qui suit: je ne veux pas qu'on présume que je suis un criminel. Mon identification n'est qu'une question de temps. Je veux pouvoir vaquer à mes occupations de façon anonyme. Ce n'est pas parce que je franchis le seuil de ma porte que je devrais être sous surveillance en tout temps, et que quelqu'un — je ne sais pas qui est cette personne ni où elle se trouve — devrait tenter de savoir qui je suis, qui m'accompagne et quelles sont mes activités.

Mais lorsque les agents sont en uniforme, ils doivent suivre la ligne de parti.

Le président: Je vous remercie.

Nous passons à M. Bains pendant six minutes.

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

Monsieur Maslej, dans le rapport sur l'indice de l'Institute for Human-Centered Artificial Intelligence pour 2022, on parle des mesures de diagnostic pour évaluer l'incidence ou la performance du modèle concernant, par exemple, les sous-groupes de population ou les minorités par rapport à la population totale. Pouvez-vous nous parler des recherches et des investissements qui sont faits pour améliorer les mesures de diagnostic afin que les modèles n'identifient pas de façon erronée les personnes issues de sous-groupes et de minorités?

● (1645)

M. Nestor Maslej: Oui, c'est une excellente question.

L'indice n'examine pas de manière très détaillée l'ampleur des investissements réalisés dans ce domaine pour le moment, mais l'intérêt est croissant. Au sujet des données que j'ai mentionnées concernant le test de la technologie de reconnaissance faciale réalisé par le NSIT, les données que j'ai examinées...

Le président: Monsieur Maslej, je dois vous interrompre. Nous éprouvons des problèmes avec votre audio. Nous avons fait des tests, et je crois savoir que tout allait bien, mais ce n'est pas le cas maintenant. Pouvez-vous vous assurer d'avoir sélectionné le bon casque d'écoute sur l'application Zoom?

M. Nestor Maslej: Je vais essayer encore une fois.

Est-ce mieux maintenant?

Le président: Je vais demander aux interprètes...

Non. Je vais suspendre la séance quelques minutes pour refaire des tests et régler le problème.

● (1645)

_____(Pause)_____

● (1650)

Le président: Je vous remercie.

Monsieur Bains, pouvez-vous répéter brièvement votre question avant de passer à la réponse de M. Maslej?

M. Parm Bains: Oui.

Nous parlions d'améliorer les mesures de diagnostic afin que les modèles n'identifient pas de façon erronée les personnes issues de sous-groupes et de minorités. Je voulais savoir ce que vous en pensiez.

M. Nestor Maslej: Je m'excuse pour ce problème de micro.

L'indice de l'intelligence artificielle ne traite pas directement du montant des investissements qui existent dans ce domaine, mais il signale que cela devient un sujet de préoccupation croissante dans nombre de domaines. Je vais souligner deux points ici.

Le premier est que dans le cas des données que j'ai fournies relativement au FRVT, le Facial Recognition Vendor Test, du NIST, ce test procède à une vérification un à un. Dans un mémoire que j'ai soumis au Comité, la figure 1.1 montre le taux de succès de différents modèles par rapport à différents ensembles de données. Dans cette figure, l'un des éléments qui ressortent clairement est que le modèle le plus performant est celui qui concerne les photos de visa, et c'est celui pour lequel l'identification était correcte 999 fois sur 1 000, alors que le pire modèle est celui qui concerne les données spontanées.

Les données spontanées sont un ensemble de données qui portent sur des personnes dont le visage peut être partiellement masqué par des ombres ou qui ne regardent pas directement l'objectif de l'appareil photo. Dans ce cas, les modèles les plus performants ont identifié correctement 970 visages sur 1 000. C'est encore très élevé, mais il y a une baisse sensible par rapport aux photos de visa.

Je pense que cela laisse entendre que si les entreprises et les agences veulent utiliser ces technologies et les justifier en disant qu'elles ont été testées en laboratoire et qu'elles avaient un taux de précision très élevé en laboratoire, il faut tenter de préciser la différence entre les environnements dans lesquels ces technologies sont testées et les environnements dans lesquels elles sont utilisées. Je pense que le Comité est conscient de cela, mais l'indice laisse entendre qu'il s'agit d'une préoccupation urgente.

J'ajouterai également que nous citons une recherche qui a été publiée il y a quelques années — et dont le Comité a eu vent, je crois —, sous la forme d'un article paru en 2018 et signé par Timnit Gebru et al, intitulé « Gender Shades », dans lequel on examine le fait que les données de référence pour l'analyse faciale sont en grande majorité des personnes à la peau claire, ce qui entraîne un biais par la suite, et que les systèmes algorithmiques existants classent incorrectement en nombre disproportionné les femmes à la peau foncée, qui constitue de ce fait le groupe le plus incorrectement classé.

Nous y faisons allusion, et je pense que le sentiment général dans la communauté des chercheurs est qu'il aurait dû y avoir plus de travaux de réalisés à ce sujet, mais je ne suis pas en mesure de vous dire le montant exact des investissements réalisés dans ce domaine particulier à l'heure actuelle.

M. Parm Bains: En novembre 2020, le HAI a publié un rapport intitulé *Evaluating Facial Recognition Technology*. Je pense que vous en avez un peu parlé en ce qui concerne la clarté des images.

L'une des préoccupations soulevées est que les fournisseurs de technologies de reconnaissance faciale peuvent, pour mettre au point leurs appareils, utiliser des images claires et bien éclairées et avoir recours à des professionnels de l'apprentissage automatique pour faire un bon usage du logiciel, mais que lorsque ces appareils sont utilisés par les forces de l'ordre, les images produites proviennent de caméras corporelles et d'autres sources utilisées dans des conditions « sous-optimales ».

S'agit-il d'un problème qui peut être corrigé? En ce qui concerne les caméras corporelles et la technologie utilisée par les forces de l'ordre, comment cela peut-il être amélioré?

M. Nestor Maslej: Les façons d'améliorer ces appareils dépassent sans doute mon domaine d'expertise.

Je peux dire toutefois que dans l'article que vous citez, le problème dont on parle est lié au « transfert de domaine », c'est-à-dire le fait que très souvent les environnements dans lesquels certains de ces algorithmes sont testés sont radicalement différents des environnements dans lesquels ils sont utilisés.

Il faudrait au moins que l'on fasse preuve d'une certaine transparence et honnêteté à l'égard des agences qui utilisent ces outils — qu'il s'agisse d'entreprises ou d'agences — au sujet de la différence entre les conditions de test et les conditions dans lesquelles ces outils sont réellement utilisés. Je pense que la situation devient problématique lorsque ces outils sont testés dans un environnement et sont ensuite utilisés dans des environnements complètement différents. Si on n'a pas une idée précise et une compréhension claire de l'existence de cette différence, alors ces technologies risquent sans doute fortement d'être mal utilisées et de servir à des fins malveillantes.

● (1655)

M. Parm Bains: Cela m'amène à ma prochaine question, qui concerne l'erreur humaine. C'est également une préoccupation avec la technologie de reconnaissance faciale. Le même rapport indique que si Amazon Rekognition recommande un seuil de confiance de 99 % dans la mise en correspondance d'identités lors de son utilisation par les forces de l'ordre, le responsable d'un des bureaux de shérif qui a été interrogé dans le cadre du rapport a déclaré ne pas fixer et ne pas utiliser de seuil de confiance.

Pensez-vous que toute utilisation de cette technologie doit être faite par un professionnel formé qui comprend comment elle est conçue et structurée?

M. Nestor Maslej: Encore une fois, je n'ai pas contribué directement à ce rapport, donc je ne suis pas le mieux placé pour répondre à la question, mais je pense que le problème auquel on fait allusion dans le rapport est sans doute lié au « transfert institutionnel ».

Ces technologies pourraient potentiellement être utilisées par différentes personnes dans différentes conditions. Il est certain qu'être formé pour utiliser ces systèmes peut être important, mais je pense qu'on reconnaît aussi qu'à moins d'avoir une sorte de norme réglementaire établie sur ce qui constitue une référence acceptable ou un cadre acceptable, on pourrait avoir différentes autorités qui utilisent ces technologies de différentes manières. Quant à la question de savoir quelle est cette référence acceptable, encore une fois, cela ne relève pas de mon domaine d'expertise. Je vous laisse le soin, à vous, décideurs, de répondre à cette question.

Je pense que ce que l'on veut dire, c'est que sans seuil, il est beaucoup plus probable que les agences fassent alors ces affirmations. Certaines pourraient, pour diverses raisons, favoriser des seuils plus bas ou plus élevés, et cela peut mener potentiellement à une mauvaise utilisation de certaines de ces technologies.

Le président: Je vous remercie, monsieur Maslej.

[*Français*]

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

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

Je remercie les témoins de leur présence.

Madame Polsky, si on définit la compréhension comme étant la capacité de saisir l'ensemble de ce qui est en jeu, de votre propos, je conclus qu'il y a une grande incompréhension de la part de la population, des gouvernements et des utilisateurs, bref de tout le monde qui est impliqué de près ou de loin dans la reconnaissance faciale.

J'ai trois questions à vous poser, madame Polsky.

En réalité, le consentement que l'on donne en cliquant sur « J'accepte » n'est pas un choix. On n'a pas le choix d'y consentir. Est-ce exact?

[*Traduction*]

Mme Sharon Polsky: C'est, comme je l'ai dit dans ma déclaration, l'illusion du consentement. M. Zuckerberg lui-même a déclaré au Congrès américain que même lui ne lit pas ce qui est écrit. La dernière fois que j'ai compté — oui, j'ai vraiment compté —, la politique de confidentialité de Google avait 38 pages. Personne ne va la lire. En conséquence, ils cliquent sur... quoi? Ils ne le savent pas.

Le problème ici ou le hic est, à tout le moins dans la législation canadienne, qu'une entreprise ou un organisme n'est censé recueillir des informations personnelles qu'après avoir obtenu un consentement éclairé. Lorsque même M. Zuckerberg reconnaît que personne ne lit ce qui est écrit, cela veut dire qu'ils recueillent des renseignements personnels sans consentement éclairé, contrairement aux dispositions de la Loi sur la protection des renseignements personnels et les documents électroniques et, je pense, de toutes les autres lois sur la protection de la vie privée au Canada.

[*Français*]

M. René Villemure: Je crois que ceux qui ont écrit les politiques ne les ont pas lues.

Du côté européen, on a la possibilité de continuer sans cliquer sur le bouton « accepter ». Croyez-vous que cela devrait aussi être implanté au Canada?

[*Traduction*]

Mme Sharon Polsky: Si vous parlez du fait de se débarrasser des consentements relatifs aux fichiers témoins, c'est devenu une farce, tout simplement. On les voit sur tant de sites Web. Sur certains sites, il est possible de modifier les paramètres des fichiers témoins, mais on ne peut pas ensuite aller plus loin. Vous devez accepter tous les paramètres, ce qui est contraire au Règlement général sur la protection des données.

Pour se débarrasser des politiques de consentement, eh bien, il faut qu'au lieu de nous demander, à vous et à moi, de lire ces politiques d'une longueur interminable, rejeter le fardeau sur les épaules des organismes. Il faut les obliger par la loi à cesser de recueillir et diffuser nos informations.

[*Français*]

M. René Villemure: Faites-vous confiance à l'autoréglementation de l'industrie?

[*Traduction*]

Mme Sharon Polsky: Nous avons déjà vu cela se produire aux États-Unis, où les grandes entreprises technologiques ont littéralement rédigé la loi qui est en train d'être adoptée dans plusieurs États. Ils appellent cela une loi sur la vie privée. Ce n'est pas le cas. Elle ne protège pas les personnes. Elle ne leur donne pas un plus grand droit à la protection ou à la vie privée. C'est pourquoi, dans ma déclaration, j'ai dit qu'il fallait élaborer ces lois sans la participation directe ou indirecte de l'industrie.

● (1700)

[*Français*]

M. René Villemure: Présentement, vous ne connaissez personne dans l'industrie ni aucune entreprise qui, dans un effort d'autoréglementation, viendrait étendre les meilleures pratiques, telles que nous le souhaitons ici?

[*Traduction*]

Mme Sharon Polsky: Il y avait beaucoup... Je suis non seulement présidente du Conseil du Canada de l'accès et la vie privée, mais depuis environ 30 ans, je réalise aussi des évaluations des facteurs relatifs à la vie privée et je suis consultante en matière de protection de la vie privée, au privé. Grâce à cela, j'ai été invitée à aller partout: des gouvernements et organismes publics aux sociétés Fortune 100.

Je comprends comment ils fonctionnent, les technologies qu'ils construisent et ce qu'ils déploient. Certains croient sincèrement qu'ils font bien les choses, mais n'oubliez pas que, sans éducation, ils sont mal informés. Ils évaluent peut-être un peu trop favorablement leur propre compréhension de la chose.

On se retrouve dans des situations où une entreprise canadienne stocke l'information au Canada, mais fait appel à des tiers aux États-Unis pour fournir des services essentiels à cette application ou à ce service. Les entreprises ne se rendent pas compte que c'est un problème. Elles n'en informent pas les utilisateurs. Elles ne s'inquiètent pas. Elles ne savent pas et sont totalement inconscientes qu'il y a des répercussions sur la vie privée.

[*Français*]

M. René Villemure: À votre connaissance, la GRC fait-elle usage de la reconnaissance faciale? Dans l'affirmative, est-ce qu'elle en comprend bien les contours?

[*Traduction*]

Mme Sharon Polsky: J'ai eu l'occasion de m'entretenir avec quelques membres très haut placés de la GRC, et je pense qu'ils le comprennent bien. Ils sont vraiment préoccupés. Leurs mains, je dirais, sont parfois liées. La technologie est parfois achetée ou mise à l'essai par quelqu'un, et personne d'autre n'est au courant.

Cela se produit également dans les organismes du secteur privé. Au lieu de passer par un processus d'approbation, quelqu'un va acheter quelque chose et le branche. Si vous ne savez pas que c'est là, vous ne pouvez pas le surveiller et vous ne pouvez pas le sanctionner.

Je ne sais pas si la GRC utilise réellement la reconnaissance faciale. Je n'en suis pas certaine, mais je n'en doute pas.

[*Français*]

M. René Villemure: Pouvez-vous nous dire encore quelques mots sur l'éducation nécessaire? De quel genre de contenu a-t-on besoin pour faire de la sensibilisation auprès des gens qui font une telle éducation?

[*Traduction*]

Mme Sharon Polsky: Il y a quelques années, j'ai discuté avec un professeur de l'Université McGill de l'élaboration d'un programme d'éducation destiné aux écoles. Des organismes médiatiques et divers commissaires à la protection de la vie privée dans tout le pays ont élaboré de petits cours, de petits programmes. Ils sont disponibles, mais ils ne sont pas obligatoires.

Je suis consciente que cela pose problème, parce que c'est de compétence fédérale, et que l'éducation est de compétence provinciale. Cependant, pour avoir, tout d'abord...

Le président: Je suis vraiment désolé, mais nous dépassons le temps prévu. L'horaire est très serré aujourd'hui.

Je dois passer à un autre intervenant et donner la parole à M. Green, qui dispose de six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Merci beaucoup, monsieur le président. Mes questions s'adressent à M. Maslej.

La croissance et le développement rapides de la technologie de l'intelligence artificielle s'accompagnent de risques importants. Au chapitre 3 de votre rapport sur l'indice de l'intelligence artificielle, on décrit certains des méfaits de ces technologies, notamment le fait que les systèmes de reconnaissance faciale commerciaux exercent une discrimination fondée sur la race, les systèmes de sélection de curriculum vitae exercent une discrimination fondée sur le sexe, et les outils de santé clinique axés sur l'intelligence artificielle sont biaisés par la race et les facteurs socio-économiques. On a constaté que ces modèles reflètent et amplifient les préjugés sociaux humains, opèrent une discrimination sur la base d'attributs protégés et génèrent de faux renseignements sur le monde.

Pourriez-vous nous en dire plus sur certains de ces méfaits et risques posés par l'utilisation des technologies d'intelligence artificielle, en particulier à un moment où les investissements dans les technologies et leur développement s'accélèrent si rapidement?

M. Nestor Maslej: Certainement. C'est une excellente question. Cela montre que, même si la réglementation des technologies de reconnaissance faciale est certainement importante, il existe également d'autres cas d'utilisation de l'intelligence artificielle qui pourraient mériter l'attention des organismes de réglementation.

L'une des conclusions des données dont nous disposons sur la reconnaissance faciale est qu'elle se situe au milieu du peloton pour ce qui est de l'investissement privé total. On y investit plus que, par exemple, dans les drones ou les technologies juridiques, mais moins que dans le traitement du langage naturel dans le domaine des soins médicaux et de santé, ce qui laisse entendre également qu'il y a d'autres cas d'utilisation de l'intelligence artificielle qui pourraient mériter une plus grande attention.

Comme le suggèrent les données de l'enquête McKinsey, la reconnaissance faciale n'est pas aussi intégrée dans certaines technologies et certains processus commerciaux que d'autres systèmes d'intelligence artificielle. Encore une fois, cela ne signifie pas nécessairement que nous ne devons pas nous préoccuper de la réglementation de la reconnaissance faciale; c'est une question de la plus haute importance. C'est juste que nous devrions également être conscients des autres problèmes que l'intelligence artificielle pourrait poser, surtout à un moment où elle devient de plus en plus omniprésente.

Vous avez fait allusion à quelques-uns des différents exemples que nous avons cités dans le rapport. J'en aborderai quelques-uns.

Nous avons parlé du fait qu'il existe des systèmes de sélection des CV qui se sont révélés discriminatoires en fonction du sexe. Nous citons un article de presse selon lequel, il y a quelques années, Amazon a mis au point un système de sélection des CV par apprentissage automatique qui s'est révélé déclasser systématiquement les candidatures des femmes.

Encore une fois, ce serait idéal pour beaucoup de ces entreprises, surtout les très grandes, si quelqu'un leur donnait 100 CV et qu'elles pouvaient les confier à une machine qui établirait automatiquement quels sont les trois meilleurs candidats pour les embaucher.

La raison pour laquelle Amazon a entraîné un système biaisé est que ce système a été entraîné à partir de données provenant de CV qu'Amazon avait déjà reçus. Dans l'écrasante majorité des cas, les CV soumis à Amazon l'ont été par des hommes. Cela reflète le fait que le secteur de la technologie est principalement dominé par les hommes. Étant donné que les hommes étaient traditionnellement les plus embauchés, le système d'intelligence artificielle a appris à pénaliser le mot « femmes ». Cela signifie que si vous mentionnez dans votre CV que vous avez été, par exemple, capitaine de l'équipe féminine de natation, l'algorithme voit que, historiquement, très peu de femmes ont été embauchées par Amazon, et comme cette personne a « féminine » dans son CV, il faut le déclasser. Amazon a affirmé que cet outil n'avait en fait jamais été utilisé pour prendre des décisions d'embauche, mais il n'en reste pas moins que ce biais demeure.

Nous parlons également du biais dans les modèles linguistiques multimodaux. Nous parlons également du biais dans la segmentation des images médicales. Je pourrais m'étendre longuement sur ce sujet, mais je vais plutôt vous donner l'occasion de poser des questions supplémentaires.

● (1705)

M. Matthew Green: J'ai, en effet, des questions supplémentaires sur les types de cadres réglementaires qui, selon vous, sont nécessaires. La recommandation de notre comité sera très importante.

Docteur, pourriez-vous nous parler des cadres nécessaires pour protéger les Canadiens lorsqu'il s'agit de l'utilisation de ces technologies d'intelligence artificielle, y compris celles que vous venez d'énumérer?

M. Nestor Maslej: Je vais dire deux ou trois choses.

Premièrement, je ne suis pas techniquement docteur encore. J'apprécie beaucoup le titre que vous m'avez donné, mais je m'en voudrais de ne pas corriger cela.

Deuxièmement, cela ne relève sans doute pas de mes compétences de proposer des recommandations au Comité. Je comprends qu'elles sont très précieuses et essentielles, mais je pense que je peux surtout commenter les données et les répercussions...

M. Matthew Green: Nous pouvons accepter cela.

Puisque nous sommes en bons termes, monsieur Maslej, si je peux me permettre, compte tenu de votre expertise dans le domaine — et je dirais, compte tenu de vos titres de compétences, que vous avez cette expertise —, pourriez-vous nous dire pour le compte-rendu si vous appuyez l'idée d'un moratoire sur l'utilisation des technologies de reconnaissance faciale et d'autres formes d'intelligence artificielle par les forces de l'ordre, jusqu'à ce que le gouvernement ait bien compris leurs répercussions?

M. Nestor Maslej: Encore une fois, je pense que répondre à cette question ne relève pas de mon champ de compétences. Je céderais plutôt la parole à l'autre témoin qui, je pense, a un peu plus d'expérience dans ce domaine et peut davantage répondre en connaissance de cause.

M. Matthew Green: Pourriez-vous alors formuler des commentaires sur les pratiques exemplaires en matière d'intelligence artificielle dont le Canada devrait selon vous s'inspirer, en effectuant des comparaisons avec d'autres législations et administrations?

M. Nestor Maslej: Il ne s'agit peut-être pas nécessairement d'une pratique exemplaire, mais plutôt d'une réalité. L'une des conclusions majeures du rapport sur l'indice de l'intelligence artificielle est que l'intelligence artificielle est de plus en plus omniprésente dans nos vies.

Il y a dix ans, de nombreux problèmes liés à l'intelligence artificielle étaient très difficiles à résoudre. L'intelligence artificielle n'était donc qu'un sujet de recherche, alors que dix ans plus tard, l'intelligence artificielle fait partie des sujets qui sortent des laboratoires pour entrer dans le monde réel. Beaucoup d'entreprises sont très enthousiastes à l'idée d'utiliser les technologies de l'intelligence artificielle, et elles vont être de plus en plus utilisées. L'investissement dans l'intelligence artificielle explose, tout comme le nombre de brevets dans ce domaine.

Très souvent, je dirais, beaucoup d'entreprises sont très enthousiastes à l'idée d'utiliser l'intelligence artificielle avant de constater les effets négatifs qu'elle peut avoir. En tant qu'organisme de réglementation, il est très souvent utile de se demander quand nous devrions nous en préoccuper. Quand devons-nous mettre en place une réglementation? Je dirais que...

Le président: Je dois vous interrompre. Je suis vraiment désolé, mais nous prenons de plus en plus de retard.

Je vais devoir réduire la durée des tours suivants, et je pense encore que nous pourrions dépasser légèrement 17 h 30 pour avoir quelques minutes de travail en comité supplémentaires.

Nous allons accorder quatre minutes à M. Bezan et à M. Fergus, deux à M. Villemure et à M. Green, puis quatre à M. Kurek et à Mme Hepfner.

Allez-y, monsieur Bezan. Vous avez quatre minutes.

● (1710)

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président, et je tiens à remercier nos témoins de leur présence aujourd'hui.

Monsieur Maslej, vous avez présenté une grande quantité de données et de pourcentages précis après les avoir examinés. Pourtant, dans votre rapport sur l'indice de l'intelligence artificielle de 2021, vous avez déclaré que nous ne disposions pas de suffisamment de données. Avez-vous recueilli suffisamment de données pour nous aider, en tant qu'organisme de réglementation, à élaborer le cadre législatif permettant de contrôler l'intelligence artificielle ou pour fournir un cadre politique adéquat permettant de faire des progrès relativement à des sujets comme la reconnaissance faciale?

M. Nestor Maslej: Je pense que oui.

L'intelligence artificielle est évidemment un sujet en constante évolution. L'année 2022 a été une année extraordinaire pour les progrès de l'intelligence artificielle; il semble que l'on assiste chaque semaine à l'émergence d'un nouveau modèle. Je ne pense pas que nous arriverons un jour à un point où nous aurons les données nécessaires pour obtenir la réponse à toutes les questions, mais nous obtenons de plus en plus de données, et l'absence de données absolues ne signifie pas que nous ne devons pas agir.

Nous savons, par exemple, comme je l'ai dit plus tôt, qu'un grand nombre de ces systèmes de reconnaissance faciale sont beaucoup moins efficaces sur ce genre de photos spontanées, dans lesquelles les personnes ne regardent pas directement l'appareil photo, ou dont l'éclairage n'est pas très bon, et cela pourrait avoir des conséquences importantes sur la manière dont ces technologies sont réglementées.

Nous sommes encore loin du point où nous disposerons de données permettant de répondre à toutes les questions, mais nous obtenons de plus en plus de données, et je pense que celles dont nous disposons actuellement sont suffisantes pour prendre des mesures relativement à certains problèmes.

M. James Bezan: Au sein du Comité, nous avons beaucoup entendu parler des lacunes dans la manière dont les données ont été accumulées et dont la technologie a été adaptée, mais avec des biais et des préjugés. Avons-nous le sentiment d'être dans une situation — dans votre cas, venant de l'Université Stanford — dans laquelle les choses sont plus équilibrées de ce côté-là de l'équation ou...? Je poserai également cette question à Mme Polsky dans les dernières minutes de mon intervention: Dans quelle mesure risque-t-on d'être confronté à des abus, à des faux positifs et, en fin de compte, à des personnes qui veulent absolument utiliser ces technologies pour perpétuer les violations des droits de la personne?

M. Nestor Maslej: Je peux peut-être commencer, puis je cèderai la parole à Mme Polsky.

Je dirais encore une fois que certaines questions restent assurément sans réponse, mais nous disposons d'un grand nombre de données qui indiquent des faits difficilement contestables. Comme je l'ai mentionné, l'article que j'ai cité précédemment montre que les systèmes de reconnaissance faciale peuvent être partiaux, et je pense que c'est un fait généralement bien accepté. Un comité de responsables de la réglementation pourrait agir sur ce point, mais je m'en remets à Mme Polsky, qui pourra fournir une réponse complémentaire.

Mme Sharon Polsky: Merci.

Je ne suis pas universitaire. Je vous laisse le soin de répondre, monsieur, mais je reviens sur les dépêches de la police galloise, dans lesquelles l'officier supérieur a déclaré que la reconnaissance faciale — et je paraphrase — produisait environ 92 % de faux positifs, et il a dit que ce n'était pas grave, car aucune technologie ne pouvait être parfaite. C'était en 2017. En 2020 ou 2021, le chef de la police de Chicago, je crois, a déclaré que la reconnaissance faciale générait environ 95 % d'erreurs.

Les conséquences sur la vie des gens peuvent être profondes, car une fois que vous êtes identifié comme une personne d'intérêt, vous êtes dans le système, et dès qu'un policier s'intéresse à vous, il cherche votre nom et vous êtes déjà là. Il y a déjà une présomption qu'il devrait vous examiner d'un peu plus près, parce que la reconnaissance faciale s'est trompée.

Le président: Merci, madame Polsky.

Sur ce, nous allons donner la parole à M. Fergus pour un maximum de quatre minutes.

L'hon. Greg Fergus (Hull—Aylmer, Lib.): Merci, monsieur le président, et j'aimerais remercier les témoins de leur présence aujourd'hui.

Par votre intermédiaire, monsieur le président, j'aurais posé cette question à nos deux témoins, pour faire suite à ce qu'a dit M. Green, mais étant donné que notre autre témoin n'a pas voulu se prononcer sur cette question, je vais la poser à Mme Polsky.

Madame Polsky, en répondant à une question de mon collègue, vous avez mentionné le problème des faux positifs et le pourcentage extrêmement élevé de faux positifs, qui est de l'ordre de 19 fois sur 20. Compte tenu de ces chiffres et du fait qu'un certain nombre des témoins qui ont comparu devant ce comité ont souligné que nous devrions imposer un moratoire sur l'utilisation de la technologie de reconnaissance faciale par le public et peut-être même par le secteur privé jusqu'à ce qu'un cadre soit mis en place pour cette technologie, pensez-vous qu'il devrait y avoir un moratoire? Êtes-vous d'accord avec ces témoins pour dire qu'il devrait y avoir un moratoire sur l'utilisation de la technologie de reconnaissance faciale dans les espaces publics et privés?

● (1715)

Mme Sharon Polsky: En bref, la réponse est oui, étant donné qu'il y a plusieurs années, lorsque j'ai fait des recherches, Toronto comptait déjà 15 000 caméras de vidéosurveillance en usage public. Ce chiffre ne tient pas compte de celles qui se trouvent dans les magasins, les voitures, les téléphones cellulaires et autres. Calgary a remplacé ses poteaux supports d'appareil d'éclairage par un nouveau type de lampadaire, mais les poteaux eux-mêmes, au nombre de 80 000, peuvent être équipés de microphones et de caméras à haute résolution qui surveillent et écoutent tout et tout le monde.

Trop souvent, les organismes publics ne procèdent pas eux-mêmes à la reconnaissance faciale ou à l'utilisation de ces technologies intégrées d'intelligence artificielle, mais font appel à des organismes du secteur privé pour le faire et contournent l'obligation de rendre des comptes. Je dirais qu'il faut un moratoire sur l'utilisation publique et privée de ces technologies.

L'hon. Greg Fergus: Merci beaucoup, madame Polsky.

Monsieur Maslej, pour en revenir au chapitre 3 de votre rapport... J'ai eu l'occasion de lire votre rapport. J'ai également eu l'occasion de vous en parler avant cette réunion. Pourriez-vous nous dire quelles sont, selon vous ou d'après votre rapport, les mesures que doit prendre la communauté pour éliminer les biais que l'on trouve dans les algorithmes, afin de promouvoir une meilleure équité et la capacité de la technologie de reconnaissance faciale à réduire autant que possible les préjugés contre les femmes ou les personnes de couleur? Quels progrès ont été réalisés dans ce domaine? Qu'avez-vous observé ces deux dernières années?

M. Nestor Maslej: Je dois dire que notre rapport ne fait pas de recommandations concrètes sur les mesures à prendre. Il vise plutôt à faire le point sur le paysage de l'intelligence artificielle. Je vais cependant faire quelques remarques.

Tout d'abord, je pense que le rapport indique clairement que nous devons prendre davantage conscience que les outils d'intelligence artificielle vont devenir de plus en plus omniprésents et qu'un grand nombre de ces outils présentent des défauts. Ils ne sont pas parfaits. Parfois, les gens les utilisent sans être conscients de leurs défauts. Nous devrions peut-être nous demander beaucoup plus tôt quels sont leurs défauts, avant de les utiliser.

En ce qui concerne le deuxième point, je dirais que le chapitre 5 se penche sur la question du législateur...

L'hon. Greg Fergus: Je suis désolé, monsieur Maslej. Permettez-moi de vous interrompre. J'ai très peu de temps...

Le président: Vous n'en avez plus.

L'hon. Greg Fergus: Oh, mince. Eh bien, ça va être très rapide.

Vous avez souligné les arguments qui justifient d'accorder une plus grande attention à l'utilisation de cette technologie, mais cela ne vous amènerait-il pas, vous-même ou dans votre rapport, à conclure qu'il devrait y avoir un moratoire jusqu'à ce que cette technologie bénéficie d'une plus grande certitude ou d'une plus grande précision? Pouvez-vous répondre par oui ou par non?

Le président: Il faudra que ce soit oui ou non. Nous n'avons plus de temps.

M. Nestor Maslej: Encore une fois, je refuserai poliment de répondre à cette question. Je ne pense pas que le rapport...

Le président: D'accord. Merci.

Sur ce, nous allons passer à M. Villemure, pour deux minutes.

[*Français*]

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

Madame Polsky, on nous dit souvent qu'on doit utiliser les données de la reconnaissance faciale pour créer un sentiment de sécurité. Toutefois, il me semble que la surveillance de masse telle que vous la décrivez et telle qu'on la comprend est susceptible de générer un sentiment d'insécurité plutôt que de sécurité. Qu'en pensez-vous?

● (1720)

[*Traduction*]

Mme Sharon Polsky: Je suis d'accord avec vous. N'oubliez pas que les personnes qui nous disent que la demande pour ces nouvelles technologies est forte sont des vendeurs. Ce sont eux qui vont en tirer profit.

C'est aussi simple que cela.

[*Français*]

M. René Villemure: Merci beaucoup.

Monsieur Maslej, à la page 62 du « Articficial Intelligence Index Report 2022 », vous parlez des taux de défaillance des algorithmes. Comment peut-on perfectionner les algorithmes en accumulant une importante quantité de données sans que cela devienne de la surveillance?

[*Traduction*]

M. Nestor Maslej: C'est l'une des difficultés que pose ce type d'entreprise. Je dirais que, de manière générale, nous devons nous demander comment nous allons recueillir ces données. En l'absence d'un cadre réglementaire, il est facile pour différentes entreprises d'opérer dans différents types de capacités. Si les règles sont plus clairement définies et cernées, il est plus facile pour les intervenants d'opérer sur le même terrain.

C'est une difficulté. Les données sont essentielles au fonctionnement de ces systèmes, mais ce n'est pas parce que les données sont essentielles — je le dis à titre personnel et non en tant que représentant de mon organisme — que nous ne devrions pas avoir de réglementation ou...

[*Français*]

M. René Villemure: Je dois vous interrompre, puisqu'il ne me reste que quelques secondes de temps de parole.

Je vous remercie.

Madame Polsky, pourriez-vous nous fournir par écrit des éléments que vous trouvez intéressants dans la loi européenne sur la reconnaissance faciale et la protection des données?

[*Traduction*]

Mme Sharon Polsky: Désolée. J'ai raté le début. Si vous...?

[*Français*]

M. René Villemure: Pourriez-vous nous fournir des écrits sur les politiques intéressantes se trouvant dans le Règlement général sur la protection des données, le RGPD, de l'Union européenne? Ainsi, nous pourrions nous en inspirer.

[*Traduction*]

Mme Sharon Polsky: Avec plaisir.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Allez-y, monsieur Green.

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

À titre d'information, c'est une question que je me pose toujours lorsque nous accueillons des témoins experts.

Monsieur Maslej, pouvez-vous indiquer si l'Université Stanford et son centre d'intelligence artificielle centrée sur les êtres humains sont financés par des entreprises du domaine de l'intelligence artificielle? Avez-vous des conflits potentiels à signaler?

M. Nestor Maslej: Je ne connais pas la situation financière de cet institut, mais je tiens également à préciser que je m'exprime ici à titre personnel et, surtout, pour présenter les données que contient l'indice de la reconnaissance faciale. Mes opinions ne sont pas celles de l'Université Stanford.

M. Matthew Green: D'accord.

Le rapport sur l'indice de la reconnaissance faciale indique que les modèles linguistiques sont aujourd'hui plus efficaces que jamais, mais aussi plus biaisés. Pouvez-vous étoffer cette affirmation?

Pourquoi ces modèles sont-ils de plus en plus biaisés à mesure qu'ils se perfectionnent, et quels sont les risques qui découlent de cette tendance?

M. Nestor Maslej: S'ils sont de plus en plus biaisés, c'est en partie parce que, habituellement, ces modèles sont alimentés par un nombre croissant de données. Pour certains modèles, il est avantageux de disposer d'un grand nombre de données. Plus vous fournissez de données au modèle, plus il risque de recevoir des données qui ne sont pas idéales.

Nous l'avons vu dans le rapport avec le modèle CLIP, qui est un modèle linguistique multimodal. On lui a demandé d'attribuer la probabilité qu'une astronaute américaine, Eileen Collins, soit... On a demandé au modèle: « Que contient cette image? » Le modèle a attribué une probabilité plus élevée que cette photographie représente une femme au foyer souriante dans une combinaison orange avec le drapeau américain qu'une astronaute tenant le drapeau américain.

Il ne s'agit pas de notre conclusion, mais de la conclusion d'un article de Birhane et al., 2021. Elle illustre le fait que, lorsque vous donnez à ces données un grand nombre de modèles, ce qui pourrait être nécessaire pour obtenir des résultats plus précis, ces modèles pourraient capter des données conspiratrices et biaisées. Si nous ne filtrons pas ces données de manière proactive, il est très probable que ces modèles se comportent de manière toxique et problématique.

M. Matthew Green: Ces biais peuvent-elles être atténuées? Si oui, comment?

M. Nestor Maslej: L'une des choses auxquelles je fais allusion — et nous en parlons dans le rapport — est la question du filtrage, qui consiste à demander aux entreprises de filtrer le type de données qu'elles utilisent pour former leurs systèmes. Il a été rapporté dans différents articles qu'il pouvait y avoir une taxe de filtrage. En d'autres termes, si vous filtrez les données avant de les appliquer à un modèle, celui-ci risque de ne pas fonctionner de manière aussi optimale que si vous lui donniez des données non filtrées, car plus un modèle dispose de données, plus il est efficace pour certaines tâches.

Le filtrage peut être un moyen d'y parvenir, mais il peut aussi présenter des inconvénients pour les entreprises.

Le président: Votre temps est écoulé encore une fois. Je suis désolé.

Nous allons finir par dépasser un peu le temps imparti. J'ai promis à nos deux derniers députés quatre minutes chacun, alors je vais tenir ma promesse et donner la parole à M. Kurek pour quatre minutes.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président, et merci à nos témoins pour leur expertise et leur présence ici aujourd'hui.

Madame Polsky, en ce qui concerne la recommandation 19 de votre rapport, si un ressortissant étranger subit les conséquences négatives d'un projet de technologie de reconnaissance faciale au Canada, quelles mesures, correctives ou autres, devraient être prises, selon vous?

● (1725)

Mme Sharon Polsky: Pardonnez-moi, car je n'ai pas le rapport à l'écran, mais si une telle situation touche un ressortissant étranger, je dirais qu'on devrait peut-être leur accorder, tout comme aux immigrants au Canada qui ne sont pas encore des immigrants reçus ou des citoyens, des droits constitutionnels et une protection en vertu de la Charte. C'est une question qui doit être étudiée plus en profondeur, c'est certain.

M. Damien Kurek: Je vous remercie.

J'aimerais parler de la deuxième recommandation. Je signale, pour la gouverne des témoins, que les recommandations sont très utiles parce qu'elles aident certainement les comités à structurer leurs rapports.

En ce qui concerne la deuxième recommandation, lorsqu'il s'agit d'une vaste base de données à l'échelle de la société, comment une telle base de données pourrait-elle causer du tort et éventuellement entraîner des abus à l'égard des personnes dont les renseignements y figurent? À l'inverse, dans le cas des gens qui ne sont pas inclus dans cette base de données, quel tort pourraient-ils subir eux aussi?

Mme Sharon Polsky: Voici un exemple simple de ce qui se passe au Canada, en l'absence d'une réglementation, une fois de plus... Nous avons fait une enquête auprès des régies du logement partout au pays. Si vous voulez louer un appartement ou une maison, il y a une application. Vous ne pouvez pas remplir un formulaire de demande sur papier. Vous devez utiliser cette application. Cela crée aussi, si vous voulez, une liste noire de locataires, parce que les propriétaires peuvent mettre n'importe quel renseignement ou commentaire, comme « Elle a eu deux jours de retard sur son loyer » ou « Elle a un enfant qui est trop bruyant ». Ils peuvent mettre ce qu'ils veulent, et d'autres propriétaires éventuels peuvent voir le tout et décider de ne rien louer à cette personne.

Que se passe-t-il pour la personne qui veut louer une maison et qui ne sait pas que ce commentaire existe? Elle n'a aucun recours. Finira-t-elle par devenir sans-abri? C'est ce qui se passe apparemment aux États-Unis, et certains de ces sites exigent également que les candidats soumettent leurs données biométriques faciales et autres, y compris des renseignements très personnels qui ne pourraient pas être demandés ailleurs. Cette situation est lourde de conséquences.

M. Damien Kurek: C'est intéressant, parce que je regardais récemment une émission de télévision, et il y était question d'une des études de cas ayant de graves conséquences possibles.

J'aimerais laisser de côté l'exemple de la location, si vous le permettez. Il y a eu une collecte de données à l'aéroport international Pearson de Toronto, où nous avons tous été d'innombrables fois, j'en suis sûr. Cette base de données comprend, j'imagine bien, une quantité incroyable de données sur les Canadiens, les personnes qui visitent notre pays et tout le reste. Je suis curieux de savoir si vous avez d'autres réflexions, recommandations ou préoccupations à faire valoir, et comment une organisation comme un aéroport, ou une autre entité, en collaboration avec les forces de l'ordre...

Le président: Votre temps est écoulé. Il ne nous reste pas de temps pour une réponse. J'accorderai peut-être cinq secondes à Mme Polsky, si elle veut répondre très brièvement à cette longue question.

Mme Sharon Polsky: Que ce soit l'entente Par-delà la frontière, l'initiative Au-delà du prédédouanement, la Loi sur les douanes ou toute mesure législative ayant une incidence dans ce domaine, nous devons examiner les divers éléments non pas isolément, mais comme un tout pour l'ensemble du système.

Le président: Je vous remercie.

Les quatre dernières minutes reviennent à Mme Hepfner.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci, monsieur le président, et merci aux témoins d'être des nôtres aujourd'hui.

Monsieur Maslej, vous en avez parlé dans votre déclaration, mais j'ai trouvé très intéressant d'apprendre que, dans la recherche du rapport de 2022 sur l'indice de l'intelligence artificielle, la technologie de reconnaissance faciale en 2017 avait un taux d'erreur de 50 % et qu'en 2021, aucune des plateformes n'affichait un taux d'erreur supérieur à 3 %.

Pouvez-vous nous en dire plus à ce sujet? Pourquoi avons-nous assisté à une telle avancée technologique? Comment cela s'est-il produit? Quelles en sont les ramifications et les conséquences pour l'avenir?

● (1730)

M. Nestor Maslej: Oui, c'est une excellente question.

Je dirais que la raison pour laquelle nous assistons à une telle avancée technologique, c'est que les systèmes d'intelligence artificielle s'améliorent dans tous les domaines. Il y a eu beaucoup de progrès dans l'architecture qui alimente ces systèmes. Ceux-ci sont désormais dotés d'un matériel de meilleure qualité, ce qui signifie qu'ils peuvent fonctionner à des vitesses beaucoup plus élevées. De nombreuses raisons scientifiques et commerciales expliquent pourquoi ces systèmes fonctionnent mieux.

Pour ce qui est des conséquences, là encore, tout cela laisse présager que l'intelligence artificielle fera partie de nos vies, que nous le voulions ou non. Comme je vous l'ai dit aujourd'hui, les systèmes d'intelligence artificielle peuvent exécuter une panoplie de tâches, mais ils peuvent aussi faire beaucoup de choses imprévues ou indésirables. Au lieu d'accueillir ces systèmes à bras ouverts dans nos vies, il est important que nous nous demandions quels en seraient les effets au bout du compte.

Encore une fois, si nous vivons dans un monde où, par exemple, les technologies de reconnaissance faciale obtiennent maintenant des taux de réussite incroyablement élevés, il sera peut-être beaucoup plus facile pour les entreprises d'en justifier l'utilisation, mais je le répète, cela ne signifie pas nécessairement que nous ne devrions pas jeter un regard critique sur la façon dont ces systèmes devraient probablement être réglementés ou gérés par les responsables gouvernementaux.

Mme Lisa Hepfner: Merci beaucoup. C'est une réponse très utile.

Madame Polsky, nous nous sommes déjà parlé, et vous en avez touché quelques mots aujourd'hui, mais vous avez très bien expliqué le manque de sensibilisation à la technologie de reconnaissance faciale. Je me demande ce que vous proposez à cet égard. Comment pouvons-nous améliorer cet aspect? Que devons-nous faire précisément en matière de sensibilisation?

Mme Sharon Polsky: À mon avis, il sera important de confier ce mandat au commissaire à la protection de la vie privée — et cela vaut également pour les provinces ayant des lois essentiellement similaires. Toute législation devrait exiger, premièrement, que les commissariats à la protection de la vie privée soient entièrement financés et qu'ils consacrent un fonds distinct, également entièrement financé, aux campagnes de sensibilisation. Ils n'ont pas tous un tel mandat. Ils font un peu de travail de sensibilisation, mais il doit y avoir un programme beaucoup plus officiel, car c'est qui permettra aux gens d'être plus au courant des lois et plus conscients de leurs droits et responsabilités.

On peut intégrer cela dans la technologie. Ainsi, une fois que la technologie est prête, on pourrait la soumettre à un banc d'essai neutre dirigé par le commissaire à la protection de la vie privée. Par conséquent, les commissaires et les groupes de la société civile auraient l'occasion d'examiner la technologie. Ce serait aussi une belle occasion pour les entreprises, car leur produit serait évalué dans un cadre neutre et digne de confiance, sans que cela porte atteinte à leur droit d'auteur ou à leur propriété intellectuelle. De cette façon, la technologie serait mise à l'essai et approuvée avant d'être autorisée à la vente au Canada.

De plus, il faut financer les efforts de sensibilisation par l'entremise du commissariat à la protection de la vie privée et, je le répète, sans l'influence de l'industrie.

Mme Lisa Hepfner: Merci beaucoup.

Il ne me reste que quelques secondes, alors je voudrais simplement vous remercier tous d'avoir pris le temps de témoigner devant nous aujourd'hui. C'était très utile et très intéressant.

Le président: Merci.

Sur ce, je tiens à remercier nos témoins, mais je dois maintenant leur demander de se déconnecter le plus rapidement possible. Nous allons mettre fin à cette séance et commencer une réunion à huis clos sur Zoom, qui devrait durer, espérons-le, quelques minutes seulement, pour nous occuper des travaux du Comité.

Sur ce, la séance est suspendue pour se poursuivre à huis clos sur Zoom.

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