CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

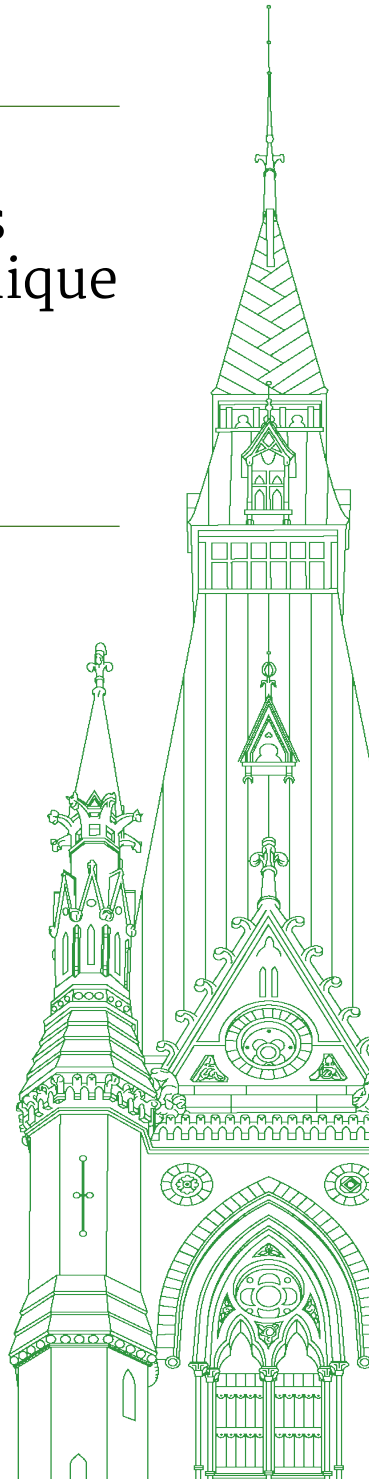
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

**NUMÉRO 015**

Le lundi 4 avril 2022



Président : M. Pat Kelly

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

**Le lundi 4 avril 2022**

● (1100)

[*Traduction*]

**Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)):** La séance est ouverte. Bienvenue à la 15e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

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

La réunion d'aujourd'hui se déroulera en mode hybride, conformément à l'ordre de la Chambre du 25 novembre 2021. Les députés sont présents en personne dans la salle et à distance par Zoom. Conformément à la directive du Bureau de régie interne du 10 mars 2022, toutes les personnes ici présentes doivent porter un masque, sauf lorsqu'elles sont assises à leur place pendant les délibérations.

Aux participants par vidéoconférence, veuillez cliquer sur l'icône du microphone pour activer votre micro. Veuillez le désactiver lorsque vous ne parlez pas.

Aux témoins qui participent pour la première fois, sachez que nous offrons des services d'interprétation. Au bas de votre écran, vous pouvez sélectionner l'option parquet, qui vous permet d'écouter dans les deux langues, ou l'une des options français ou anglais. Ceux qui sont dans la salle peuvent utiliser l'oreillette et sélectionner le canal qu'ils préfèrent.

Je rappelle à tous que les commentaires doivent être adressés à la présidence.

Les députés qui sont dans la salle sont invités à lever la main pour demander la parole. Ceux qui sont sur Zoom sont priés d'utiliser la fonction « lever la main ». La greffière et moi-même ferons de notre mieux pour gérer l'ordre des interventions. Nous vous remercions de votre patience et de votre compréhension.

Je souhaite la bienvenue à tous nos témoins. Nous accueillons ce matin quatre témoins, à savoir le professeur Rob Jenkins, de l'Université de York, M. Sanjay Khanna, conseiller stratégique et expert en prospective, Mme Angelina Wang, chercheuse diplômée en informatique, de l'Université Princeton, et Mme Elizabeth Anne Watkins, attachée de recherche au niveau postdoctoral, de l'Université de Princeton.

Nous allons commencer par M. Jenkins.

Vous avez cinq minutes pour votre exposé préliminaire.

**M. Rob Jenkins (professeur, University of York, à titre personnel):** Bonjour.

Merci, monsieur le président et distingués membres du Comité.

Je m'appelle Rob Jenkins. Je suis professeur de psychologie à l'Université de York, au Royaume-Uni, et je vais aborder la question de la reconnaissance faciale du point de vue des sciences cognitives.

Je vais commencer par vous parler de ce qu'on attend de la reconnaissance faciale et de son exactitude et de la mesure dans laquelle les résultats réels sont à la hauteur de ces attentes.

Nos attentes sont principalement fondées sur notre expérience de la reconnaissance faciale dans la vie de tous les jours, et cette expérience peut être très trompeuse quand il est question de sécurité et de médecine légale.

Les visages que nous voyons la plupart du temps sont des visages familiers, c'est-à-dire les visages de personnes que nous connaissons et que nous voyons souvent, dont nos amis, les membres de notre famille et nos collègues. Les êtres humains savent très bien identifier des visages familiers. Nous les reconnaissons sans effort et avec précision, même dans de mauvaises conditions de visibilité ou sur des images de mauvaise qualité. Le fait que nous sachions reconnaître des visages dans notre vie sociale peut nous inciter à généraliser et à supposer que les êtres humains savent reconnaître des visages en général. Ce n'est pas le cas.

La reconnaissance faciale appliquée, employée, par exemple, dans les dépositions de témoins, la sécurité et la surveillance, et la comparaison de visages à des fins médicolégales, porte presque toujours sur des visages non familiers, c'est-à-dire des visages de personnes que nous ne connaissons pas et que nous n'avons jamais vues auparavant.

Les êtres humains sont étonnamment peu aptes à identifier des visages non familiers. C'est une tâche difficile caractérisée par de nombreuses erreurs, même dans des conditions de visibilité excellentes et sur des images de haute qualité. C'est ce que l'on constate non seulement parmi des personnes ordinaires choisies au hasard, mais aussi parmi des professionnels dûment formés qui ont de nombreuses années d'expérience dans ce genre de rôle, par exemple des douaniers et des policiers.

Il est impératif d'évaluer la technologie de reconnaissance faciale, ou TRF, dans le contexte de la reconnaissance de visages non familiers. Cela s'explique en partie par le fait que l'infrastructure actuelle de reconnaissance faciale repose sur la reconnaissance de visages non familiers par les êtres humains, faisant de la performance humaine un comparatif relatif, et en partie par le fait que, dans la pratique, la TRF est intégrée aux flux de tâches de reconnaissance faciale comprenant des opérateurs humains.

La reconnaissance de visages non familiers par les êtres humains, dont on sait qu'elle est source d'erreurs, demeure une partie intégrante des systèmes de reconnaissance faciale automatisés. Pour vous donner un exemple, dans de nombreuses applications de la TRF au domaine de la sécurité et au domaine médicolégal, une recherche automatisée dans la base de données permet d'obtenir une liste de candidats, mais ce sont des opérateurs humains qui, au final, choisissent les visages de la liste qu'ils vont comparer à la cible recherchée.

Selon le « Surveillance Camera Code of Practice » du Royaume-Uni, l'utilisation de la TRF devrait toujours être accompagnée d'une intervention humaine avant que soient prises des décisions susceptibles de nuire à l'intéressé. Le gouvernement fédéral australien a publiquement adopté un principe semblable de surveillance humaine, estimant que les décisions qui servent à identifier une personne ne devront jamais être prises uniquement par la technologie.

La surveillance humaine fournit des garanties importantes et un mécanisme d'imputabilité, mais elle impose également un seuil maximal à l'exactitude que les systèmes de reconnaissance faciale pourraient atteindre en principe. La technologie de reconnaissance faciale ne donne pas de résultats exacts à 100 %, mais, quand bien même elle le ferait, la surveillance humaine introduit l'erreur humaine dans le système. L'erreur humaine est courante dans ces tâches, mais il y a des façons de l'atténuer. Il faut déployer des mesures délibérées, par un recrutement ciblé ou par une formation fondée sur des données probantes, pour s'assurer que les personnes qui prennent part aux décisions liées à la reconnaissance faciale soient hautement qualifiées.

L'utilisation de la TRF dans les systèmes juridiques devrait être accompagnée d'une divulgation transparente des qualités, des limites et du fonctionnement de cette technologie.

Si la TRF doit être adoptée dans la pratique médicolégale, on aura besoin de nouveaux types de praticiens experts et de chercheurs pour concevoir, évaluer, superviser et expliquer les systèmes qui s'ensuivront. Comme ces systèmes intégreront la prise de décision humaine et un processus décisionnel s'appuyant sur l'intelligence artificielle, on aura besoin de toute une gamme d'expertises.

Merci.

● (1105)

**Le président:** Merci beaucoup, monsieur Jenkins.

Écoutons maintenant M. Khanna.

Vous avez cinq minutes, monsieur.

**M. Sanjay Khanna (conseiller stratégique et expert en prospective, à titre personnel):** Monsieur le président, merci beaucoup de me donner l'occasion de m'adresser à vous et aux membres du Comité. Je vais vous parler de la technologie de reconnaissance faciale du point de vue du sujet, de la société numérique et du gouvernement.

Je suis consultant en prospective stratégique, en planification de scénarios et en changement global, et professeur auxiliaire dans le cadre du programme de maîtrise en politique publique dans la société numérique de l'Université McMaster.

La planification de scénarios est une importante méthode prévisionnelle dans mon travail. Le Canada traverse la période la plus incertaine à laquelle il ait été confronté depuis le début de la période d'après-guerre, et la planification de scénarios peut aider les législateurs à orienter des stratégies et des politiques de résilience. À mon avis, les enjeux suivants sont importants en matière de reconnaissance faciale ou de « TRF ».

Premièrement, les gens sont visés par la TRF sans consentement éclairé ou par des moyens qu'ils ne comprennent pas. Deuxièmement, des sociétés de plus en plus inégalitaires comprennent des populations qui ne sont pas en mesure de défendre leurs intérêts concernant l'utilisation actuelle ou éventuelle de la TRF. Troisièmement, les législateurs seront toujours en retard sur l'actualité s'ils ne prennent pas le temps d'envisager les avenirs plausibles de la société numérique et d'examiner le rôle de nouvelles technologies comme la TRF.

Je vais parler de ces enjeux du point de vue du sujet, de la société et du gouvernement.

Du point de vue du sujet, le visage peut nous ouvrir des portes et nous en fermer. Nous avons des préjugés négatifs et positifs, implicites et explicites, selon toute une gamme de nuances en fonction de la façon dont nos visages sont perçus et d'autres facteurs liés à notre apparence. Cette réalité fondamentale façonne nos vies.

Dans un monde régi par la TRF, que signifierait être reconnu par des systèmes techniques dans lesquels la TRAF est intégrée?

Que se passerait-il si la TRF était combinée à une analyse des sentiments permettant d'identifier rapidement les sentiments à des moments vulnérables où une personne pourrait être influencée ou touchée par une manipulation commerciale, sociale ou politique?

Que se passerait-il si la TRF intégrée aux robots de sécurité permettait d'identifier quelqu'un comme représentant une menace sociale, politique ou de sécurité publique?

Que se passerait-il si la TRF intégrée aux jeux de hasard ou à des services commerciaux permettait de viser quelqu'un comme une occasion d'affaires ou un passif transactionnel?

Les technologies associées à la TRF, comme les mégadonnées, l'apprentissage machine et l'intelligence artificielle, amplifient les risques et les possibilités liés à la TRF et à d'autres technologies biométriques. Certains accueillent favorablement la TRF, mais beaucoup de gens craignent d'être visés et surveillés. Si des droits sont violés, les gens ne sauront peut-être jamais comment ni pourquoi, les entreprises pourront décider de ne pas révéler les réponses, et il pourrait ne pas y avoir de consentement éclairé.

Dans ce cas, les personnes victimes de violation de leurs droits commerciaux, juridiques ou humains n'auraient pas de recours.

Du point de vue social, la société canadienne fait face à des défis sans précédent en matière numérique. Les inégalités sociales et raciales croissantes dans notre pays ont été accentuées par la pandémie. Les Canadiens subissent un stress chronique, et leur santé physique et mentale se détériore. La résilience sociale est compromise par la désinformation. Le Canada affronte des difficultés nouvelles et des menaces à l'ordre d'après-guerre. La crise climatique est un multiplicateur de menaces cooccurrent.

Malgré ces enjeux, les grandes entreprises de technologie profitent des occasions qui se présentent dans un contexte de risque sans précédent, ce qui leur a permis d'accroître leur influence sur le gouvernement et sur notre société numérique. C'est ainsi que quelques entreprises ont acquis un pouvoir considérable grâce à des valorisations de billions de dollars et plus, à une forte influence économique et au verrouillage de l'apprentissage machine et de l'expertise en intelligence artificielle.

Au moment où je vous parle, les grandes entreprises de technologie imaginent les prochaines utilisations de la TRF, notamment dans les entreprises, au gouvernement et dans le secteur industriel. Certaines d'entre elles examinent les menaces et les situations qui justifieraient une utilisation peut-être illégale aujourd'hui, mais susceptible d'être viable dans de nouvelles circonstances, comme un changement de gouvernement, une alerte de sécurité majeure ou des changements dans les lois du travail.

Du point de vue du gouvernement, une société confrontée à des perturbations constantes n'est pas considérée comme une société sûre pour les Canadiens. Les préjudices réels et éventuels pour les personnes et les risques et possibilités pour les entreprises et le gouvernement mettent l'accent sur l'importance d'une gouvernance efficace. À une époque où les risques sont sans précédent, les parlementaires ont la responsabilité de donner un sens à la transformation sociétale et d'envisager les avenirs plausibles de la TRF dans le contexte des systèmes de surveillance sophistiqués utilisés par des villes « intelligentes », de la croissance de la richesse et de l'inégalité des revenus, et des menaces contre les droits des enfants et des groupes marginalisés.

L'élaboration d'une loi et d'une politique efficaces en matière de TRF devra tenir compte des avenirs plausibles.

● (1110)

Je suis conscient du fait que pour vous, législateurs, c'est une tâche difficile, compte tenu des horizons souvent à court terme des élus et des partis. Cependant, une réflexion prospective en complément de l'élaboration d'une loi permettra de tenir compte des conséquences nouvelles et souvent imprévues de technologies aussi puissantes que la TRF, qui est inextricablement liée aux progrès de la vision informatique, aux mégadonnées, à l'interaction entre les ordinateurs et les êtres humains, à l'apprentissage machine, à l'intelligence artificielle et à la robotique.

**Le président:** Monsieur Khanna, je suis désolé. Je vais devoir vous interrompre.

**M. Sanjay Khanna:** Il me reste un paragraphe.

**Le président:** Vous avez légèrement dépassé votre temps de parole. Je vous remercie de votre exposé préliminaire.

Monsieur Fergus.

**L'hon. Greg Fergus (Hull—Aylmer, Lib.):** Pendant que vous parliez, j'ai entendu M. Khanna dire que c'était son dernier paragraphe. Pourrions-nous faire une exception pour l'entendre.

**Le président:** Si vous pouvez le faire en 15 secondes ou moins, c'est d'accord.

**M. Sanjay Khanna:** Un gouvernement qui réagit en temps réel dans ce domaine restera toujours à la traîne. Certaines entreprises technologiques et entreprises en démarrage font le pari que les gouvernements ne rattraperont pas leur retard. Les législateurs devraient prendre des mesures pour corriger cette impression en instaurant des garde-fous à plus long terme pour renforcer la résilience des Canadiens.

**Le président:** Je vous remercie beaucoup.

Je m'excuse auprès des témoins de les interrompre souvent, mais nous sommes en quelque sorte régis par l'horloge.

Veuillez m'en excuser. Je le ferai sans doute encore d'ici la fin de la réunion.

Nous entendrons maintenant Mme Wang.

Vous disposez de cinq minutes pour votre déclaration préliminaire. Allez-y.

**Mme Angelina Wang (chercheuse diplômée en science informatique, Princeton University, à titre personnel):** Bonjour. Je m'appelle Angelina Wang et je suis chercheuse au département d'informatique de l'Université Princeton. Je vous remercie de m'avoir invitée à témoigner aujourd'hui.

Je vais vous donner un aperçu de la technologie de reconnaissance faciale et vous décrire quelques problèmes techniques parmi les plus convaincants justifiant le non-déploiement de cette technologie.

Aujourd'hui, diverses tâches de reconnaissance faciale sont couramment exécutées par un modèle qui a été entraîné à l'apprentissage automatique. Cela veut dire qu'au lieu d'appliquer des règles à programmation manuelle — comme celle qui dit que deux personnes ont plus de chance d'être une même personne si elles ont les yeux de la même couleur —, on fournit au modèle un vaste ensemble de données de visages annotées à partir desquelles on lui demande d'apprendre. Les annotations comprennent notamment des étiquettes qui indiquent que les images représentent la même personne ainsi que l'emplacement du visage dans chaque image. Ces données sont généralement recueillies sur des plateformes de production participative comme Amazon Mechanical Turk, connue pour faire appel à des groupes de travailleurs homogènes et pour offrir des conditions de travail désavantageuses. L'ordre de grandeur de ces ensembles de données est très vaste, variant entre quelque 10 000 images jusqu'à plusieurs millions. La plupart de ces ensembles de données de visages proviennent simplement d'Internet, notamment de sites comme Flickr. Les personnes dont le visage se retrouve dans les ensembles de données ne sont généralement pas au courant que leur image est utilisée à cette fin, et peuvent considérer qu'il s'agit là d'une violation de leur vie privée. Le modèle utilise ces ensembles de données massifs pour apprendre automatiquement comment exécuter des tâches de reconnaissance faciale.

Il convient de souligner qu'on fait beaucoup appel à la pseudoscience pour d'autres tâches de reconnaissance faciale, notamment pour détecter le genre, les émotions et même l'orientation sexuelle et la criminalité. Ce travail a été largement critiqué, à juste titre, parce qu'il s'agit de caractéristiques qui ne sont pas visuellement perceptibles.

Quant aux utilisations de la reconnaissance faciale qui pourraient sembler plus légitimes, il a été largement démontré que ces modèles faisaient une discrimination raciale et sexiste. L'ouvrage le plus notoire à avoir fait la lumière sur ces pratiques est celui de Joy Buolamwini et Timnit Getru intitulé *Gender Shades*. Les autrices ont fait une recherche sur la prédiction du genre à partir du visage, une tâche qui ne devrait normalement pas être exécutée, et ont relevé des lacunes très graves dans ces systèmes. Elles ont démontré que derrière le taux élevé d'exactitude du modèle se cachaient des mesures de rendement très différentes d'un groupe démographique à l'autre. En fait, l'écart le plus important est une marge de 34,4 % entre des femmes à peau foncée et des hommes à peau plus claire. Le rapport démontre que de nombreux modèles de reconnaissance faciale produisaient de moins bons résultats pour les personnes à peau foncée, ce qui explique les nombreuses erreurs d'identification d'hommes noirs aux États-Unis qui ont mené à des arrestations injustifiées.

Il existe des solutions pour corriger ces problèmes de distorsion, par exemple la collecte d'ensembles de données plus diversifiées et plus inclusives et la conduite d'analyses désagrégées pour déterminer les taux d'exactitude entre les divers groupes démographiques, plutôt que le taux d'exactitude de l'ensemble des données. La collecte de ces divers ensembles de données est en soi une forme d'exploitation des groupes marginalisés. La collecte de leurs données biométriques constitue une violation de leur vie privée.

Même s'il est possible, en théorie, d'éliminer ces distorsions au moyen de la technologie actuelle, il existe deux problèmes de taille que la science actuelle ne peut encore résoudre. Ces problèmes sont liés à la fragilité et aux possibilités d'interprétation des modèles. Par fragilité, je veux parler des moyens connus permettant à des utilisateurs malveillants d'altérer les actuels modèles de reconnaissance faciale pour les contourner et en fausser les résultats. Les cyberattaques en sont un exemple. Elles permettent à quelqu'un de manipuler le visage présenté à un modèle pour que celui-ci ne soit plus capable de l'identifier ou pour qu'il le confonde avec celui d'une personne tout à fait différente. Des recherches ont démontré que le simple fait de mettre une paire de lunettes sur un visage pouvait tromper le modèle et l'amener à penser qu'il s'agit d'une personne tout à fait différente.

L'autre problème en est un d'interprétation. Comme je l'ai déjà dit, ces modèles apprennent leurs propres ensembles de caractéristiques et de règles à partir des ensembles de données qui leur sont proposés. Il est extrêmement difficile de découvrir l'ensemble précis de règles sur lesquelles s'appuie le modèle pour prendre ses décisions; l'ingénieur qui a construit le modèle est même souvent incapable de comprendre pourquoi son modèle fait certaines classifications. Cela veut dire que si un modèle de reconnaissance faciale classifie mal une personne, il n'existe pas de moyens efficaces pour contester cette décision et pour savoir sur quoi elle est fondée. Les modèles s'appuient souvent sur ce qu'on appelle des « corrélations fallacieuses », par exemple lorsqu'un modèle utilise une corrélation qui ne correspond à aucune donnée pour faire une classification. À titre d'exemple, les modèles de diagnostics médicaux peuvent faire une classification en s'appuyant sur un artefact d'image produit par un appareil à rayons X, au lieu de s'appuyer sur le contenu précis de l'image. Je crois qu'il est dangereux de déployer des modèles dont nous ne comprenons pas bien le fonctionnement interne dans des contextes aussi délicats que la reconnaissance faciale.

En terminant, je tiens à souligner que les technologies de reconnaissance faciale sont des dispositifs de surveillance qui peuvent être déployés à un coût extrêmement bas et leur prolifération rapide les rend d'autant plus dangereux. Notre visage est un élément central de notre identité et il ne change généralement pas au fil des années. Ce type de surveillance est donc très préoccupant. Je ne vous ai présenté que quelques objections d'ordre technique à l'égard de la technologie de reconnaissance faciale. À l'instar de nombreux autres détracteurs de cette technologie, je crois que les énormes risques qu'elle pose sont de loin supérieurs aux avantages que nous pourrions en tirer.

Je vous remercie.

● (1115)

**Le président:** Je vous remercie.

Madame Watkins, vous avez cinq minutes tout au plus.

**Mme Elizabeth Anne Watkins (attachée de recherche au niveau postdoctoral, Princeton University, à titre personnel):** Je vous remercie de me donner l'occasion de m'exprimer aujourd'hui.

Je m'appelle Elizabeth Anne Watkins et je suis titulaire d'une bourse de recherche postdoctorale au Center for Information Technology. Je fais également partie du groupe d'interaction humain-ordinateur de l'Université Princeton, et je suis affiliée à l'institut de recherche Data & Society de New York.

Je témoigne aujourd'hui à titre personnel pour vous faire part de mes inquiétudes concernant l'utilisation, par le secteur privé, de la technologie de vérification faciale auprès de travailleurs. Ces inquiétudes découlent de la recherche que j'ai effectuée, en tant que spécialiste des sciences sociales, sur les répercussions de l'IA dans des contextes de travail.

Mes observations ont un double objectif: premièrement, je veux sensibiliser le Comité à une technologie de reconnaissance faciale qui a une fonction distincte, la vérification faciale. Deuxièmement, je veux l'inciter à réfléchir au problème que pose l'intégration de ces deux technologies dans des contextes sociotechniques, soit le fait d'appliquer ces outils à des êtres humains et à des situations du monde réel, et à réfléchir aussi aux importantes répercussions de cette intégration sur la vie privée et la sécurité de gens.

Je vais commencer par définir et décrire la vérification faciale. Alors que la reconnaissance faciale est un système 1:n, ce qui veut dire qu'il trouve et identifie des personnes à partir de flux de données provenant de caméras représentant un grand nombre de visages, souvent à l'insu des personnes photographiées, la vérification faciale, bien qu'elle découle de la technologie de reconnaissance faciale, est utilisée de manière différente. Il s'agit d'un système de jumelage 1:1, beaucoup plus intrusif et rapproché, où le visage d'une personne placée directement devant la caméra est apparié à celui qui est déjà intégré à l'appareil ou au compte numérique auquel la personne veut avoir accès. Si le système voit votre visage et détecte une correspondance avec le visage déjà intégré à l'appareil ou au compte, l'accès vous est alors accordé. Si la correspondance ne peut être vérifiée, l'accès ne sera pas déverrouillé. Si vous utilisez le système Face ID ou un iPhone, par exemple, vous savez déjà ce qu'est la vérification faciale.

Je vais maintenant m'attarder au contexte sociotechnique et vous expliquer où cette technologie est intégrée, comment et par qui. Je vais surtout parler du contexte de travail. La vérification faciale est de plus en plus utilisée dans les milieux de travail, en particulier dans celui du travail à la demande et du travail précaire. Dans de nombreux États américains, les livreurs d'Amazon, les chauffeurs d'Uber et les préposés aux soins à domicile sont déjà obligés de se soumettre à la vérification faciale pour prouver leur identité et être autorisés à travailler. Cela veut dire que la personne doit s'assurer que son visage sera visible et correspondra à la photo associée au compte. En général, les travailleurs doivent se prêter à cet exercice non pas une seule fois, mais à répétition.

Le Comité a déjà été informé des distorsions, des échecs et des injustices intrinsèques de la reconnaissance faciale. Je suis ici pour l'exhorter à réfléchir également aux préjudices causés par l'utilisation de la vérification faciale au travail.

Dans le cadre de ma recherche, j'ai recueilli des données auprès de travailleurs qui m'ont décrit un éventail de préjudices. Ils se demandent avec inquiétude combien de temps et où leur photo sera stockée et à qui elle sera communiquée. Dans certains cas, des travailleurs sont forcés de prendre de multiples photos d'eux-mêmes avant que le système trouve la correspondance. Dans d'autres, on leur interdit, par erreur, d'avoir accès à leur compte parce que le système ne trouve pas de correspondance. Ils doivent trouver du temps pour se rendre aux centres de service à la clientèle et attendre des heures ou des jours qu'une vraie personne corrige ces erreurs. Des travailleurs m'ont raconté qu'ils devaient parfois sortir de leur automobile dans des stationnements non éclairés et s'accroupir devant les phares de leur auto pour que le système ait assez de lumière pour les voir. En cas de panne du système de vérification faciale, il incombe alors aux travailleurs de créer et de maintenir les conditions requises pour que le système puisse produire un résultat.

L'utilisation de la reconnaissance faciale par des organismes étatiques comme les services de police fait l'objet d'une surveillance croissante, mais l'utilisation de la vérification faciale par des entreprises privées à l'endroit de leurs travailleurs n'est pas réglementée. J'implore le Comité de réfléchir à ces questions préoccupantes et à des mesures susceptibles de protéger les travailleurs contre tout préjugé, échec et menace à leur sécurité, que ce soit par le biais d'une réglementation de la biométrie, d'une réglementation de l'IA, du droit du travail ou d'une combinaison de ces moyens.

Je suis d'accord avec Cynthia Khoo, que vous avez entendue récemment, pour dire qu'on ne peut pas demander à la technologie de reconnaissance faciale d'assumer les responsabilités légales et morales que les humains sont déjà en train de lui refiler à l'égard de la vie des personnes vulnérables. Un moratoire est la seule réponse réglementaire moralement acceptable.

D'ici à ce que cet objectif soit atteint, il y a lieu d'imposer des mesures en matière de responsabilité et de transparence à l'égard non seulement de ces outils, mais également des entreprises qui prétendent vouloir se protéger contre les personnes frauduleuses et malveillantes. Une intervention réglementaire pourrait obliger ces entreprises à produire des données à l'appui de leurs prétentions aux fins d'examen public et les obliger à évaluer l'incidence algorithmique. Il faudrait notamment consulter des travailleurs de groupes marginalisés pour savoir comment ils sont touchés. D'autres mesures pourraient également obliger les entreprises à fournir aux travailleurs l'accès à de multiples formes de vérification d'identité pour faire en sorte que les personnes dont le corps ou l'environnement ne peut être reconnu par les systèmes de vérification faciale puissent quand même avoir accès à leur gagne-pain.

Sincèrement, ces technologies soulèvent de nombreuses questions: qui est protégé, à quoi devrait ressembler la sécurité et à qui incombe la responsabilité d'atteindre cet objectif.

Je vous remercie.

● (1120)

**Le président:** Merci beaucoup pour cet exposé.

Nous allons maintenant passer à la période de questions.

Monsieur Williams, vous allez commencer. Vous avez six minutes.

**M. Ryan Williams (Baie de Quinte, PCC):** Merci beaucoup, monsieur le président, et merci aussi à nos témoins de leur participation aujourd'hui. C'est très intéressant.

Je vais commencer par M. Jenkins.

Dans le cadre de votre examen portant sur l'exactitude de la reconnaissance faciale par des spécialistes comme des agents de passeport, vous avez découvert que l'erreur humaine était très présente. Quel est le pourcentage des erreurs humaines par rapport aux erreurs dues au logiciel d'apprentissage automatique de la technologie de reconnaissance faciale?

**M. Rob Jenkins:** Cela dépend en grande partie de la nature de la tâche. Si on demande à un membre du personnel des passeports qui a reçu une formation et compte de nombreuses années d'expérience de comparer des visages réels à des documents d'identité avec photo semblables à des passeports, on obtient habituellement des taux d'erreur d'environ 10 %. Cela signifie que, sur 10 comparaisons, il y a erreur dans un seul cas. Je parle ici de la correspondance entre la photo et la personne en chair et en os.

Quant aux systèmes informatisés, nous comprenons très peu comment la plupart d'entre eux fonctionnent dans des conditions réalistes. Bon nombre des résultats des tests présentés par les fournisseurs sont obtenus dans des situations idéales où l'image est de qualité suffisante pour être fiable et les conditions dans lesquelles la comparaison se fait sont très bonnes. Dans ces tests, il n'est pas tenu compte du bruit ni de la complexité du monde réel. À mon avis, nous n'en savons tout simplement pas assez à ce sujet.

● (1125)

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

On peut comparer la reconnaissance faciale à d'autres méthodes d'identification, comme les empreintes digitales. Avez-vous des données à ce sujet? Quel serait le taux d'erreur si les empreintes digitales étaient utilisées au lieu de la reconnaissance faciale?

**M. Rob Jenkins:** Je ne peux pas donner de chiffre, mais, pour certaines raisons, le couplage des empreintes digitales peut être plus fiable dans certaines circonstances. L'apparence du visage change beaucoup selon l'éclairage et la distance entre le visage et l'objectif de l'appareil photo. Ces problèmes particuliers ne se posent pas lorsqu'il s'agit des empreintes digitales.

**M. Ryan Williams:** Les erreurs commises par les humains et les ordinateurs sont-elles les mêmes, ou sont-elles complètement différentes? Vous en avez évoqué quelques-unes.

**M. Rob Jenkins:** Il y a des similitudes, mais aussi des divergences frappantes entre les erreurs des ordinateurs et celles des humains. Mme Wang a donné un exemple: le simple fait d'ajouter des lunettes ne gênerait pas la reconnaissance par un humain, mais des changements apparemment superficiels comme celui-là peuvent vraiment faire dérailler les systèmes informatiques, qui donnent des réponses erronées contre toute attente.

**M. Ryan Williams:** Vous avez dit que la TRF devrait toujours s'accompagner d'une intervention humaine. Arrivera-t-on un jour à une exactitude parfaite grâce à la combinaison de la technologie et de l'humain? Comment évolue le degré d'exactitude?

**M. Rob Jenkins:** L'un des avantages de la surveillance humaine comme partie intégrante du système, c'est qu'elle permet de repérer les erreurs flagrantes comme celles dont nous venons de parler et de les signaler avant qu'on agisse en se fondant sur ces erreurs. Pour cette raison, il me semble important qu'un humain vérifie, mais la reconnaissance des visages par les humains n'est pas infaillible non plus et peut donc introduire des erreurs dans le système si on leur laisse la décision finale. C'est là le résultat du biais cognitif que nous avons tous. Je parle d'erreurs commises de bonne foi plutôt que de préjugés ou d'intention malveillante.

**M. Ryan Williams:** Dans l'article « Two Factors in Face Recognition », vous écrivez que l'exactitude de la reconnaissance faciale dépend beaucoup plus de la connaissance qu'on peut avoir du visage de la personne que de la communauté de race. Comment cette tendance se retrouve-t-elle dans les logiciels de reconnaissance faciale fondés sur l'intelligence artificielle?

**M. Rob Jenkins:** Il importe de faire la distinction entre capacité et préjugés. Les deux facteurs existent, mais ils sont indépendants l'un de l'autre.

La capacité variable de reconnaître les visages est influencée par les visages qu'on a l'habitude de croiser, c'est-à-dire par les types de visage qu'on voit couramment autour de soi. C'est important pour au moins deux raisons. Premièrement, il est normal d'avoir des disparités démographiques en reconnaissance faciale, même en l'absence de préjugés. Deuxièmement, ce phénomène a un pendant évident dans la technologie de reconnaissance faciale: la composition des bases de données faciales qui sont utilisées pour former l'algorithme.

La lutte contre les préjugés est clairement importante en soi, mais elle ne peut pas éliminer les disparités démographiques dans l'exactitude de la reconnaissance faciale. C'est un problème distinct.

**M. Ryan Williams:** D'accord.

Merci, monsieur le président. Je renonce à mes 14 secondes.

**Le président:** D'accord. Merci.

Je donne la parole à M. Fergus pour six minutes.

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

Merci à tous les témoins d'être là. Je leur en suis reconnaissant.

Comme j'ai des questions à poser à plusieurs témoins, je les invite à être concis et directs.

Monsieur Jenkins, mon collègue, M. Williams, vous a demandé de comparer les empreintes digitales à la reconnaissance faciale. D'après ce que vous avez dit, vous, Mme Wang et d'autres témoins, ce n'est pas tout à fait la même chose.

Pouvez-vous comparer les deux sous l'angle de l'exactitude? Comment la technologie de reconnaissance faciale est-elle utilisée, par opposition aux empreintes digitales? Je présume qu'il s'agit au fond d'essayer de trouver une correspondance entre deux ensembles de données. Est-ce exact?

● (1130)

**M. Rob Jenkins:** Il y a des similitudes générales.

Dans les deux cas, on prend un échantillon du monde — qu'il s'agisse des empreintes digitales de quelqu'un ou de son image faciale — et on le compare à des représentations stockées où on croit trouver quelque chose qui correspond.

Le problème se pose lorsque la variabilité de l'image captée sur le vif de la personne qu'il s'agit d'identifier... L'image peut varier dans le temps. Il faut toujours tenir compte de cette variabilité lorsqu'on essaie de trouver une correspondance dans les données stockées.

Or...

**L'hon. Greg Fergus:** Autrement dit, la situation change de façon remarquable selon qu'il s'agit du visage ou des empreintes digitales. Ce n'est peut-être pas tout à fait une comparaison entre éléments comparables.

**M. Rob Jenkins:** On peut sans doute le dire. Nous savons avec certitude que des images différentes d'un même visage peuvent être plus variées que des images de visages différents. C'est le nœud du problème.

**L'hon. Greg Fergus:** Merci beaucoup.

Madame Wang, merci beaucoup de votre exposé. Si je peux me permettre, vous n'avez présenté au Comité que quelques-uns des problèmes que vos recherches ont permis de déceler. Y en a-t-il d'autres dont vous voudriez entretenir le Comité? Nous disons souvent entre nous que nous ne pouvons pas faire rapport de ce que nous n'entendons pas ou ne lisons pas. Nous vous saurions gré de bien vouloir nous faire parvenir, si vous en avez le temps, d'autres exemples de ce que vous considérez comme les limites de la reconnaissance faciale.

Je reviens aux deux grands problèmes que vous avez cernés, soit la fragilité et les possibilités d'interprétation.

Pourriez-vous nous en dire un peu plus sur la fragilité du système? Des gens malveillants pourraient le contourner, mais il y a aussi la vulnérabilité des gens qui n'ont pas l'intention de le contourner, mais qui sont quand même victimes de distorsions. Vous avez parlé de l'apprentissage automatique et du fait que cela ne fait qu'atténuer les préjugés qui existeraient dans la société en général.

Ai-je raison?

**Mme Angelina Wang:** Oui.

À propos de la fragilité, étant donné que nous ne savons pas vraiment quel modèle est retenu pour procéder à certaines identifications, nous ne savons pas sur quels schèmes le système s'appuie. Parce qu'ils savent peut-être qu'on peut se maquiller ou porter des lunettes, les humains peuvent gérer ce genre de changements. Si quelqu'un faisait quelque chose d'un peu différent par inadvertance avec son visage et modifiait sa présentation, cela pourrait ne pas être contrôlé, si bien que l'identification serait fautive.

**L'hon. Greg Fergus:** Je m'éloigne de ce que vous avez dit aujourd'hui, mais dans certaines de nos lectures, il est question des limites de la technologie, comme la technologie des appareils photo. Il est clair que la technologie favorise certains types de visage. Elle a été créée de fond en comble et a évolué depuis que nous avons commencé à prendre des photos. Elle privilégie les hommes blancs, en particulier. Pour chaque autre catégorie ou groupe, il y a des niveaux variables d'inexactitude de plus en plus grands.

Pourriez-vous en dire un peu plus à ce sujet? Même si nous tentions de corriger l'apprentissage automatique, nous aurions toujours un problème à cause de la technologie elle-même et des distorsions qu'elle pourrait introduire.

**Mme Angelina Wang:** Depuis que les appareils photo ont été inventés, ils ont toujours beaucoup moins bien fonctionné avec les couleurs de peau plus foncées. Ils ne tiennent pas compte des différences d'éclairage. Ils ont toujours été conçus principalement pour les teints plus clairs. Souvent, dans des conditions d'éclairage différentes, ils ne fonctionnent pas aussi bien pour les gens qui ont des tons de peau différents. Les visages peuvent se fondre davantage dans l'arrière-plan, selon leur apparence.

● (1135)

**L'hon. Greg Fergus:** Par conséquent, cela perpétue cette distorsion qui est déjà intégrée au système.

**Mme Angelina Wang:** Exact. La qualité d'image diffère d'une personne à l'autre.

**L'hon. Greg Fergus:** Monsieur Khanna et madame Watkins, mon temps de parole est presque écoulé, mais je vais voir si je peux poser une très brève question.

Monsieur Khanna, vous avez dit que les hommes et femmes politiques doivent prendre les devants.

Très brièvement, comment s'y prendre pour encadrer correctement la TRF?

**M. Sanjay Khanna:** Oui. Vous devriez utiliser une technique appelée la planification de scénarios. Aux fins pour lesquelles vous utilisez la technologie, l'approche de planification de scénario Oxford, de l'Université Oxford, est très utile, parce qu'elle fait appel à de multiples parties prenantes et...

**Le président:** Il est bien que vous ayez pu donner une réponse claire.

Si vous avez d'autres renseignements à fournir au Comité, je vous invite à les communiquer.

M. Fergus a épuisé son temps de parole avant d'avoir fini de poser sa question.

**L'hon. Greg Fergus:** Je repousse toujours les limites.

**Le président:** Oui. En effet, c'est ce que vous faites.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

**M. René Villemure (Trois-Rivières, BQ):** Je salue tous les témoins et je les remercie de leur disponibilité remarquable.

Au cours de ce premier tour de parole, mes questions s'adresseront à MM. Khanna et Jenkins.

Messieurs Khanna et Jenkins, je vais vous poser une question très générale. Je vous demanderais d'y répondre en quelques secondes et nous creuserons la question par la suite.

Est-ce que la reconnaissance faciale signifie la fin de la liberté individuelle?

Je vous donne la parole, monsieur Khanna.

[*Traduction*]

**M. Sanjay Khanna:** Je vais répondre.

Très brièvement, cela dépend du contexte de la gouvernance des technologies. La nature du gouvernement qui recourt à ces technologies est très importante. La gouvernance législative et d'autres mécanismes de surveillance peuvent changer. Dans certains contextes et types de gouvernement, il se pourrait fort bien que...

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup, monsieur Khanna.

Monsieur Jenkins, je vous demanderais de répondre par oui ou par non.

Est-ce que cela signifie la fin de la liberté individuelle?

[*Traduction*]

**M. Rob Jenkins:** Voulez-vous vraiment que je réponde par oui ou non?

[*Français*]

**M. René Villemure:** Autant que possible.

[*Traduction*]

**M. Rob Jenkins:** La technologie toute seule? Non.

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup.

Monsieur Jenkins, dans votre recherche, vous parlez de la variabilité intrapersonnelle.

Pourriez-vous approfondir cette question?

[*Traduction*]

**M. Rob Jenkins:** Oui. Chacun de nous a un seul visage, qui a sa propre apparence. Cette apparence change souvent, non seulement dans la durée, à mesure que nous grandissons et vieillissons, mais aussi selon l'angle, l'éclairage, l'expression faciale, et par le simple fait que la personne parle.

Il y a énormément de variations, et c'est un problème. Ce qu'on essaie de faire au moyen de la reconnaissance faciale, c'est de savoir quelles personnes on connaît ou ont leur profil dans une certaine base de données. Cette variabilité est un obstacle difficile à surmonter. On ne sait toujours pas si l'image qu'on a devant soi est celle d'une personne qu'on connaît ou celle de quelqu'un de nouveau.

La variabilité est une dimension fondamentale du problème dont nous discutons. L'apparence varie d'une personne à l'autre, mais aussi chez une même personne. Il est difficile au plan computationnel de distinguer entre ces deux sources de variabilité pour comprendre ce qu'on regarde.

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup.

Monsieur Khanna, dans des discussions passées, vous avez fait allusion au terrorisme biométrique.

Pourriez-vous nous en dire davantage à ce sujet?

● (1140)

[*Traduction*]

**M. Sanjay Khanna:** J'essaie de me souvenir des discussions auxquelles vous faites allusion, mais il y a certainement des scénarios dans lesquels on réfléchit à des questions comme celle-là. Par exemple, jusqu'à quel point est-il possible de voler l'identité d'une personne pour la faire passer pour un terroriste?

Il y a de nombreux scénarios plausibles. Je ne sais pas exactement comment la technologie de la reconnaissance faciale pourrait jouer un rôle à cet égard, mais c'est là que la planification de scénarios et ce genre de technique peuvent être très utiles pour tenir compte de ce qui vous préoccupe.

[*Français*]

**M. René Villemure:** Pourriez-vous nous en dire un peu plus sur le type d'encadrement gouvernemental auquel nous pourrions réfléchir?

[*Traduction*]

**M. Sanjay Khanna:** Selon moi, l'encadrement ne peut découler que du type d'étude que le Comité effectue déjà. Il y a peut-être des études qui sont menées en parallèle et sur lesquelles vous devez vous appuyer pour examiner ces défis de façon plus globale. Je crois que c'est ce que je demanderais.

La technologie de reconnaissance faciale est intégrée à une foule d'autres technologies. Pour en accélérer le développement, il faut de l'apprentissage automatique, de la vision artificielle et une foule d'autres domaines. Il faut une vue d'ensemble pour que le Parlement puisse élaborer le genre de cadre global qui est nécessaire, à mon avis.

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup, monsieur Khanna.

Monsieur Jenkins, considérant la vitesse à laquelle la technologie évolue, est-il trop tard pour agir?

[*Traduction*]

**M. Rob Jenkins:** Je ne crois pas qu'il soit trop tard pour agir, mais il est important d'agir maintenant. Nous devrions nous baser sur les preuves et sur ce que nous savons, et les utiliser pour essayer d'atteindre nos objectifs.

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup, monsieur Jenkins.

Je vais laisser les 30 secondes qu'il me reste à mes collègues.

[*Traduction*]

**Le président:** D'accord. Merci. C'est apprécié.

La parole est maintenant à M. Green, pour six minutes.

**M. Matthew Green (Hamilton-Centre, NPD):** Monsieur le président, je me ferai un plaisir d'utiliser ces 30 secondes qui m'ont été offertes.

Monsieur le président, je pense que nous pouvons tous nous entendre sur les aspects techniques de ce comité. Je ne suis pas convaincu que nous irons aussi loin que nécessaire pour obtenir le genre de rapport qui est exigé dans le temps qui nous est imparti. Je vais donc poser des questions très concises aux témoins, en commençant par Mme Watkins.

Madame Watkins, en tant qu'experte en la matière, quelles seraient vos principales recommandations législatives? Nous allons rédiger un rapport et nous espérons pouvoir présenter quelques recommandations à la Chambre pour que le gouvernement puisse les étudier.

**Mme Elizabeth Anne Watkins:** Merci beaucoup. J'ai trois principales recommandations.

La première serait de décréter un moratoire. La technologie est trop peu fiable, vu la responsabilité à assumer à l'égard de l'avenir et des moyens de subsistance d'êtres humains.

Mes deux autres recommandations portent sur la responsabilité et la transparence.

Nous devons mieux comprendre comment ces outils sont utilisés, où les données sont stockées, comment les décisions sont prises en fonction de celles-ci, si des humains sont impliqués ou non, et comment ces décisions sont intégrées dans les structures organisationnelles bureaucratiques plus vastes entourant la prise de décisions. Il serait fort utile de disposer de documents qui nous donneraient un aperçu de ces processus, comme les évaluations d'impact algorithmique.

De plus, nous avons besoin de certaines interventions réglementaires pour assurer la reddition de comptes et établir le genre de relations entre le gouvernement, les intervenants privés et l'intérêt public qui permettraient de répondre aux besoins des plus vulnérables.

**M. Matthew Green:** Madame Wang, quelles seraient vos principales recommandations législatives?

**Mme Angelina Wang:** Je ne crois pas avoir quoi que ce soit à ajouter à ce qu'a mentionné Mme Watkins.

**M. Matthew Green:** D'accord.

Monsieur Khanna, que recommandez-vous?

**M. Sanjay Khanna:** Selon moi, il faut renforcer les mesures de protection, particulièrement pour les enfants, les groupes marginalisés et les Premières Nations, pour qui la pandémie de COVID-19 a empiré la situation. Il est important de tenir compte de la trajectoire à suivre pour déterminer quels types de préjudices pourraient vraisemblablement survenir dans les prochaines années, compte tenu des chocs que nous avons déjà subis.

**M. Matthew Green:** Quel genre de mesures de protection recommanderiez-vous? Avez-vous des précisions à ce sujet?

**M. Sanjay Khanna:** Non. Il faudrait que je prenne le temps de réfléchir aux secteurs précis qui pourraient être renforcés, mais il y a certains rapports qui pourraient être très utiles dans ce contexte. Je pense notamment au document de l'UNICEF intitulé *Policy guidance on AI for children*, publié en novembre 2021.

● (1145)

**M. Matthew Green:** Je dirais à tous les témoins que si, plus tard, vous pensez à quelque chose que vous n'avez pas été en mesure d'exprimer lors de notre séance de questions-réponses en rafale, vous devriez envisager de les soumettre à l'examen du comité par écrit. Nous espérons qu'elles seront également incluses dans notre rapport.

Monsieur Jenkins, quelles sont vos principales recommandations législatives?

**M. Rob Jenkins:** Je dirais qu'il faut prêter attention aux opérateurs humains dans la conception et la mise en œuvre de systèmes de reconnaissance faciale, à la transparence et au développement d'une main-d'œuvre spécialisée en reconnaissance faciale.

**M. Matthew Green:** Merci beaucoup.

Madame Watkins, dans un rapport intitulé *Now you see me : Advancing data protection and privacy for Police Use of Facial Recognition in Canada*, j'ai relevé que la députée libérale danoise Karen Melchior avait déclaré, au cours de débats parlementaires, que le profilage prédictif, l'évaluation des risques liés à l'intelligence artificielle et les systèmes automatisés de prise de décisions sont des « armes de destruction mathématiques », car ils sont aussi dangereux pour notre démocratie que les bombes nucléaires le sont pour les créatures vivantes et pour la vie.

Compte tenu de l'utilisation de l'expression « armes de destruction mathématiques », vous avez souligné qu'il y aura une reddition de comptes importante dans le secteur privé. Je remarque qu'un premier syndicat vient d'être créé chez Amazon. J'espère qu'il y aura des discussions à ce sujet.

Quelles mesures de protection devrions-nous imposer au secteur privé pour veiller à ce que ces « armes de destruction mathématiques » ne soient pas utilisées contre la classe ouvrière?

**Mme Elizabeth Anne Watkins:** C'est une excellente question. Le secteur privé est souvent sous-réglementé lorsqu'il s'agit de ce genre de technologies.

La Biometric Information Privacy Act de l'État de l'Illinois est un modèle très intéressant. On a établi que, plutôt que d'avoir un formulaire d'avis et de consentement, où les utilisateurs doivent refuser que leurs renseignements soient utilisés, on doit obtenir le consentement des utilisateurs avant d'utiliser quelque renseignement biométrique que ce soit.

La définition des renseignements biométriques dans le libellé de cette loi est très vague. De mémoire, je dirais qu'elle comprend les empreintes faciales et vocales. Cette loi a été utilisée pour engager des poursuites contre des entreprises privées comme Facebook, par exemple, pour avoir utilisé la reconnaissance faciale dans leurs processus d'identification avec photo.

Il serait donc très avantageux d'examiner ce genre de loi, qui remet le contrôle des renseignements biométriques entre les mains des utilisateurs dès le départ, lorsque viendra le temps de prendre des mesures de protection à l'égard du secteur privé.

**M. Matthew Green:** Je terminerai en disant que dans l'un de vos articles, vous et vos collègues avez écrit ceci: « Malgré de nombreuses promesses selon lesquelles les systèmes algorithmiques peuvent éliminer les vieilles idées préconçues du jugement humain biaisé, il existe désormais de nombreuses preuves que les systèmes algorithmiques exercent leur pouvoir précisément selon ces vecteurs familiers. » Pouvez-vous commenter ce passage?

**Mme Elizabeth Anne Watkins:** Merci.

Bien que l'intelligence artificielle, l'apprentissage automatique et les technologies algorithmiques semblent être très futuristes, très novatrices et tout à fait nouvelles, elles sont fondées sur des données qui ont été recueillies au fil des ans et des décennies, reflétant des choses comme les préjugés, le racisme et le sexisme institutionnels.

Ces données n'ont pas été inventées. Elles proviennent des institutions qui ont exercé une surveillance excessive de certaines collectivités, par exemple. Ce type de processus produit ensuite des ensembles de données qui donnent un certain portrait d'un criminel, alors que nous savons que cela ne reflète pas la réalité. C'est ainsi que les institutions perçoivent les populations.

Ensuite, l'intelligence artificielle et l'apprentissage machine utilisent ces ensembles de données pour apprendre et pour découvrir le monde. Ainsi, plutôt que d'être innovants et futuristes, l'IA, l'apprentissage automatique et les processus algorithmiques sont en fait très conservateurs et profondément archaïques, et ils perpétuent les préjugés dont nous, en tant que société, devrions nous débarrasser et aller de l'avant.

**M. Matthew Green:** Merci beaucoup.

**Le président:** Nous passons maintenant à M. Kurek, pour cinq minutes.

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

Je remercie les témoins de nous faire profiter de leur expertise. Permettez-moi d'abord un bref commentaire. Comme l'ont souligné plusieurs de mes collègues, selon les procédures de ce comité, seules les preuves présentées peuvent se retrouver dans le rapport. Donc, si vous avez d'autres documents, réflexions ou preuves que vous jugez utiles pour le comité, y compris vos recommandations, n'hésitez pas à nous les faire parvenir. Cela devient incroyablement utile lorsque nous préparons nos rapports. Cette offre s'adresse à tout le monde, si vous désirez aller plus loin que vos réponses aux questions que nous vous posons aujourd'hui.

Pour faire suite à une question posée par M. Green, monsieur Khanna, êtes-vous en faveur de l'imposition d'un moratoire sur le TRAF jusqu'à ce qu'il y ait un cadre en place?

● (1150)

**M. Sanjay Khanna:** Personnellement, je serais absolument en faveur.

**M. Damien Kurek:** D'accord, je comprends.

Je vais poser la même question à M. Jenkins.

Seriez-vous en faveur de l'imposition d'un moratoire jusqu'à ce qu'il y ait un cadre en place?

**M. Rob Jenkins:** Je ne suis pas sûr d'avoir une opinion ferme sur le moratoire. Je suis certainement conscient des erreurs qui peuvent survenir lorsque l'on utilise ces systèmes, et j'ai tendance à me concentrer davantage sur ces erreurs que sur les avantages. Ce n'est peut-être pas à moi de parler au nom des Canadiens.

**M. Damien Kurek:** D'accord. Je voulais simplement connaître votre point de vue à ce sujet. Je vous remercie.

Je pense que le Comité, dans le cadre de cette étude et d'autres, a beaucoup entendu parler du concept de consentement. Lorsque vous utilisez la reconnaissance faciale sur un iPhone, un appareil Android ou un ordinateur, vous consentez à ce que votre photo soit utilisée pour ouvrir une session et ainsi de suite. C'est très, très différent de l'utilisation répandue de la recherche d'images sur Internet et la prise de décisions par les forces de l'ordre. C'est une différence importante.

Monsieur Khanna, en 2016, on a rapporté que le gouvernement fédéral avait testé la reconnaissance faciale sur des millions de voyageurs à l'aéroport international Pearson de Toronto. Quelles pourraient être les conséquences négatives pour ces quelques millions de voyageurs qui ont franchi la frontière à l'aérogare 3 de Pearson entre les mois de juillet et décembre 2016, lorsque ce projet pilote était en cours? Pourriez-vous nous décrire certaines de ces préoccupations à l'aide d'un exemple très concret?

**M. Sanjay Khanna:** Je pense que le fait que nous ne soyons pas au courant est une partie du problème. Il n'y a pas eu de transparence au sujet de certaines des répercussions, et s'il y en a eu, ce pourrait ne pas être clair pour ceux qui pourraient avoir subi des préjudices dont ils ne sont pas au courant.

C'est un domaine très délicat et difficile à aborder, ce qui explique en partie pourquoi la transparence est une telle menace pour les gens qui contournent parfois la loi afin de recueillir et de tester ce qui peut se produire grâce à ce genre de surveillance.

Je vais m'arrêter ici avant de spéculer davantage sur cette question.

J'aimerais ajouter très brièvement qu'il y a cette question de... Je pense à une chanson dont le refrain dit « j'ai toujours l'impression que quelqu'un me surveille ». Les Canadiens ne sont plus obligés de se sentir paranoïaques à l'idée qu'ils puissent avoir cette impression.

**M. Damien Kurek:** Bien sûr, je pense que c'est certainement l'un des grands défis.

Je vais m'adresser à M. Jenkins, si vous me le permettez, dans la même veine. Il reste environ 45 secondes, je crois.

Avez-vous des commentaires à faire au sujet des problèmes d'éthique liés à un projet pilote comme celui de l'aéroport international Pearson que j'ai mentionné plus tôt?

**M. Rob Jenkins:** L'une de mes préoccupations serait la possibilité qu'il y ait une erreur d'identification qui serait alors difficile à détecter ou à corriger. Je pense que l'aéroport d'Heathrow accueille environ 100 000 passagers chaque jour. Donc, dans ce contexte, si nous avions un taux d'exactitude de 99 %, nous parlerions d'environ 100 erreurs d'identification par jour. Nous atteindrions rapidement une somme importante. Cela ne me semble tout simplement pas viable.

**M. Damien Kurek:** Sur ce, je vais utiliser les dernières secondes de mon temps de parole pour vous remercier et vous rappeler mon offre. N'hésitez pas à transmettre de plus amples renseignements au Comité une fois que vous aurez réfléchi davantage à ces questions très importantes.

Merci beaucoup.

**Le président:** Je vous remercie, monsieur Kurek, de votre souci de respecter l'horaire.

Nous passons maintenant à Mme Saks, pour cinq minutes.

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

Je remercie nos témoins de s'être déplacés aujourd'hui.

Je vais commencer en posant une question plutôt ouverte, mais je pense qu'il y a lieu de la poser.

Nous avons beaucoup entendu parler de ce qui ne va pas avec cette technologie et des raisons qui font qu'elle est mauvaise. Mais a-t-elle quelque chose de bon?

Qui veut partir le bal?

**M. Rob Jenkins:** Nous employons l'expression « reconnaissance faciale automatique » de manière englobante, mais cette technologie peut servir dans de nombreuses applications différentes. Quelqu'un a mentionné la commodité qu'elle offre pour déverrouiller son téléphone ou vérifier rapidement son compte bancaire, en l'utilisant en quelque sorte comme un mot de passe. Il me semble qu'une telle utilisation privée est très différente de son utilisation comme moyen de surveillance de lieux publics à l'échelle d'un pays entier.

● (1155)

**Mme Ya'ara Saks:** D'accord.

Dans le même ordre d'idées, Mme Watkins a mentionné les avantages de la vérification individuelle du visage, par opposition à la reconnaissance faciale générale. Il y a donc un certain avantage à utiliser ces technologies. Comme M. Khanna l'a mentionné, en tant que parlementaires, nous devons être conscients du fait que nous prenons du retard. Nous n'arrivons pas à suivre les avancées technologiques. Malgré cela, y a-t-il moyen d'établir des barrières législatives fondamentales à ce stade-ci, qu'elles visent à protéger la vie privée ou à empêcher le moissonnage de plateformes ouvertes, qui constitueraient un filet de sécurité, pour commencer? Nous aurons constamment à nous pencher sur des technologies émergentes et novatrices, mais y a-t-il des principes clés que nous devrions envisager d'introduire dans une loi de protection?

Je me demande si M. Khanna ou Mme Watkins ont des suggestions à faire.

**Le président:** Madame Saks, je vous arrête un instant. Je pense qu'il y a d'autres témoins qui voulaient répondre à votre première question.

**Mme Ya'ara Saks:** Oh. Je m'excuse. Merci.

**Le président:** Comme vous avez adressé, en quelque sorte, votre deuxième question à M. Khanna, je lui laisse la possibilité d'y répondre maintenant. Si Mme Watkins veut répondre à l'une ou l'autre des questions, je l'invite à le faire.

Allez-y, monsieur Khanna.

**M. Sanjay Khanna:** Monsieur le président, je répondrai en disant qu'il pourrait y avoir quelque chose comme — l'expression n'est pas très heureuse — une charte des droits numériques des Canadiens qui leur permettrait d'avoir et d'utiliser une forme portable et sécurisée de données biométriques, qui serait tenue pour sacrosainte.

Je sais que c'est quelque peu ambitieux comme proposition, mais elle m'est venue à l'esprit au cours de cette conversation.

**Mme Ya'ara Saks:** Allez-y, madame Watkins.

**Mme Elizabeth Anne Watkins:** Merci beaucoup d'avoir posé cette question. C'est une question d'une telle importance que je l'ai posée récemment à des collègues. Quand je préconise l'abolition de la vérification faciale, beaucoup me répondent: « Eh bien, qu'est-ce qui se passe après? Par quoi la remplacer? » Cela tient au fait que ces systèmes ont souvent été mis en place pour protéger la vie privée des travailleurs, prévenir la fraude et assurer la sécurité. Les travailleurs ont le droit d'être en sécurité et protégés contre les gens malveillants. Mais il doit y avoir des moyens de rechange, de façon à ce que la reconnaissance et la vérification faciales ne soient pas la seule solution. Il est possible de donner aux travailleurs des options, celle, par exemple, de choisir de ne pas participer à un processus de vérification ou d'y participer avec un mot de passe ou empreintes digitales.

Encore une fois, je pense que les évaluations de l'impact algorithmique seraient un excellent point de départ pour faire la lumière sur certains de ces domaines où nous ne connaissons tout simplement pas les genres d'effets et d'impacts que ces technologies ont sur les collectivités dans différents contextes. Certaines missions de collecte d'information, sous forme d'évaluations d'impact conjointes des secteurs privé et public, serviraient grandement à amorcer l'évaluation de ces effets et impacts.

**Mme Ya'ara Saks:** Merci.

Par votre entremise, monsieur le président, je voudrais poser une autre question ouverte.

On parle beaucoup de moratoire. À mes yeux, la principale question porte sur la façon de le mettre en œuvre. Ce qui me préoccupe le plus, c'est le rapport entre les mesures d'application privées et publiques, le fait qu'il y a des contrats établis avec de tierces parties et qu'il existe actuellement une échappatoire.

Je vous demande, madame Watkins, monsieur Khanna ou monsieur Jenkins, quelles seraient les principales barrières à établir dans un moratoire?

**Mme Elizabeth Anne Watkins:** Ce que je retiens avant tout de toute la discussion autour des interdictions qui fait rage ces dernières années, c'est qu'il s'agit d'un excellent point de départ. Toutefois, ces interdictions ne visent généralement que la façon dont ces technologies sont utilisées par les organismes étatiques, les services de police par exemple. Elles ne restreignent pas la façon dont les outils de surveillance sont utilisés dans les magasins de détail, par exemple, ni la façon dont les données recueillies peuvent être vendues aux forces de l'ordre ou passer par la porte arrière à la faveur, exactement comme vous le dites, d'échanges entre les secteurs public et privé de données recueillies sans le consentement et à l'insu des gens.

Certains règlements, ou certaines barrières déterminant les modalités du transfert de données entre le secteur public et le secteur privé seraient donc une bonne chose.

**Le président:** Merci.

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

● (1200)

[*Français*]

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

Madame Watkins, j'ai écouté l'ensemble de votre témoignage, et je crois que le message qui en ressort pourrait se résumer à ceci: « faites attention ».

Êtes-vous d'accord là-dessus?

[*Traduction*]

**Mme Elizabeth Anne Watkins:** Cela dépend à qui vous adressez cet avertissement. Si « faire attention » signifie, par exemple, qu'il faudrait consulter les travailleurs, les intérêts syndicaux ou les défenseurs des travailleurs pour... Je n'ai pas rencontré tous les travailleurs au Canada et aux États-Unis et je ne peux pas parler en leur nom. Je sais qu'il y a des travailleurs qui se disent favorables à la reconnaissance faciale parce qu'ils veulent que leurs comptes soient protégés, qu'ils veulent assurer leur sécurité et celle de leurs passagers, tous des objectifs valables. Mais je ne sais pas à qui s'adresserait votre avertissement.

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup, madame Watkins.

Monsieur Khanna, parmi les scénarios que vous avez évoqués plus tôt, quel scénario choisiriez-vous pour développer la technologie de reconnaissance faciale telle que vous la connaissez maintenant?

[*Traduction*]

**M. Sanjay Khanna:** Pour faire suite aux observations d'autres témoins, qui ont très bien couvert le sujet à mon avis, nous avons ici trois pays, le Royaume-Uni, les États-Unis et le Canada, où ces technologies ont été utilisées et où beaucoup de leçons ont été tirées, notamment dans le milieu universitaire par des chercheurs indépendants, et cela nous permet d'en apprendre beaucoup sur ce que nous devons protéger; je pense qu'il est d'importance capitale d'en tirer parti. Pour ce qui est des scénarios, encore une fois, il s'agit d'examiner les technologies comme celle de la reconnaissance faciale dans le contexte plus large de l'intelligence artificielle, de l'apprentissage automatique et d'autres technologies qui s'y rattachent, en font partie ou y sont intégrées. Les gouvernements doivent examiner ce contexte général. Nous vivons dans une société numérique où tout progresse à un rythme que nous avons peine à suivre. Quelles mesures de protection sont à prendre pour notre société qui sera aux prises avec des inégalités sociales et économiques plus grandes dans les années à venir, en partie à cause de la COVID et des événements qui l'ont précédée?

Merci.

**Le président:** Merci.

Vous avez deux minutes et demie, monsieur Green.

**M. Matthew Green:** Merci.

Madame Wang, dans vos travaux, vous examinez l'amplification du biais algorithmique dans les systèmes d'apprentissage automatique. Je crains que le Comité, ayant consacré beaucoup de temps à la reconnaissance faciale, n'ait peut-être pas saisi pleinement les impacts de l'intelligence artificielle et de l'apprentissage automatique. Pourriez-vous décrire brièvement le concept d'amplification du biais dans l'apprentissage automatique et peut-être nous dire quelles sont certaines de ses conséquences matérielles et quelles personnes tendent à être davantage touchées?

**Mme Angelina Wang:** L'amplification du biais se rapporte à une notion du biais qui est souvent considérée comme une simple corrélation dans les données. Cette corrélation pourrait être entre un groupe démographique particulier et un concept auquel il est associé de façon stéréotypée. Comme les modèles d'apprentissage automatique cherchent à repérer les constantes parmi les données à apprendre, ils amplifient souvent ces biais et les surestiment chaque fois qu'ils sont présents.

**M. Matthew Green:** Pouvez-vous nous en citer des cas, par exemple, dans le domaine de l'application de la loi? Nous entendons parler d'action policière prédictive, et on nous rappelle le scénario de *Rapport minoritaire*. Pourriez-vous nous parler d'études que vous avez trouvées sur l'utilisation de l'apprentissage automatique par les forces de l'ordre?

**Mme Angelina Wang:** Bien sûr. En ce qui concerne l'action policière prédictive, si des collectivités de couleur et différents quartiers à forte proportion de citoyens noirs ont un taux de criminalité plus élevé, les modèles prédictifs peuvent surestimer à l'avenir leur taux probable de criminalité, même si ce n'est pas le cas, et amplifiera ce taux par rapport au taux de base de la corrélation réelle.

**M. Matthew Green:** Pour résoudre ce problème, vous avez mis au point un outil. Quels sont les principaux avantages de cet outil et qui devrait l'utiliser comme moyen de permettre l'analyse préventive des données?

**Mme Angelina Wang:** Je ne sais pas trop de quel outil vous parlez. Cependant, je pense qu'il faut vérifier ces corrélations et savoir que, même un modèle très précis qui n'amplifie pas lui-même les biais, peut reprendre ceux qui se trouvent dans l'ensemble de données. Même si un modèle n'introduit pas de biais, ceux-ci peuvent être déjà présents dans l'ensemble des données.

**M. Matthew Green:** Merci.

Je voudrais dire, pour le compte rendu, que je croyais avoir vu votre nom associé à l'outil REVISE, mais je me suis peut-être trompé.

**Mme Angelina Wang:** Il s'agit des biais dans les ensembles de données visuelles.

● (1205)

**M. Matthew Green:** D'accord.

Merci beaucoup. Je vous remercie de vos explications.

**Le président:** Merci.

Monsieur Bezan, vous avez cinq minutes.

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

Je tiens à remercier nos témoins de leur temps et de l'expertise qu'ils apportent à cette importante étude que nous entreprenons.

Je voudrais poser aux quatre témoins une question qui fait suite à celle de M. Green.

Si vous prenez l'intelligence artificielle et l'apprentissage automatique, puis les associez à la technologie de la reconnaissance faciale et son éventuelle application dans le système de justice pénale, est-ce que cela ne compromettrait pas sérieusement nos droits constitutionnels, les libertés garanties par la Charte au Canada, pour peu qu'on s'en serve comme outil d'application du Code criminel?

Je vais commencer avec Mme Wang.

**Mme Angelina Wang:** Je suis désolée. Je ne m'y connais pas assez pour répondre.

**M. James Bezan:** En gros, si la technologie de la reconnaissance faciale et l'intelligence artificielle sont utilisées pour établir la preuve dans une poursuite judiciaire, est-ce que cela soulèverait des problèmes aux termes du Code criminel et de la Charte des droits et libertés? La technologie de la reconnaissance faciale est-elle suffisamment fiable pour qu'on l'utilise pour établir la preuve dans notre système de justice pénale et protéger les droits de la personne?

**Mme Angelina Wang:** Je pense que le fait de pouvoir obtenir des images faciales sans aucune forme de consentement, le nombre d'erreurs qui se produisent et notre incapacité à vraiment expliquer pourquoi un modèle aboutit à telle ou telle décision, que tout cela serait contraire aux droits de la personne.

**M. James Bezan:** D'accord.

Madame Watkins, qu'en dites-vous?

**Mme Elizabeth Anne Watkins:** Merci. Pardonnez-moi mon ignorance de la Charte criminelle canadienne.

Aux États-Unis, nous avons le droit de circuler librement. Si la technologie de reconnaissance faciale sert à capter les visages des gens qui se déplacent dans l'espace public, cela signifie que leurs décisions quant aux espaces publics qu'ils utilisent pourraient être contraintes. L'utilisation de la technologie de la reconnaissance faciale dans la surveillance de lieux publics aurait un effet restrictif sur ce droit particulier. Ce n'est qu'un exemple parmi tant d'autres.

**M. James Bezan:** D'accord.

Qu'en pensez-vous, monsieur Khanna.

**M. Sanjay Khanna:** Je crois que le critère sera défini peu à peu par les tribunaux. En supposant que les algorithmes de la technologie de la reconnaissance faciale et de l'apprentissage automatique sont utilisés pour identifier les criminels, pas seulement pour suivre leurs activités dans les médias sociaux, comme cela s'est fait à Ottawa, il va falloir que le critère de leur utilisation soit établi en regard de la Charte pour pouvoir, à mon avis, avoir valeur de précédent juridique. Il est certainement plausible qu'il y aura préjudices entretemps.

**M. James Bezan:** D'accord.

Monsieur Jenkins?

**M. Rob Jenkins:** Si la précision de la reconnaissance faciale est faible, cela fait craindre des préoccupations au sujet des erreurs judiciaires. Si elle est faible pour certaines personnes, mais élevée pour d'autres, cela soulève des préoccupations au sujet de l'égalité. Si elle est élevée pour tout le monde, cela soulève des préoccupations au sujet de la protection de la vie privée. Ce sont toutes les options possibles.

**M. James Bezan:** D'accord.

À mesure que nous avançons et que nous entendons clairement les recommandations concernant la reddition de comptes, la transparence, la mise en place d'un moratoire jusqu'à ce que nous ayons une loi en place, comment allons-nous, en tant que parlementaires, mettre de l'avant les mesures de protection appropriées pour s'assurer que la reconnaissance faciale est utilisée correctement, que les préjugés sont éliminés, que la discrimination est éliminée ou, à tout le moins, minimisée, afin que nous puissions inscrire dans le Code criminel, la Loi sur la protection des renseignements personnels, la LPRPDE, les garde-fous nécessaires pour nous assurer de ne pas trop compter sur la technologie de reconnaissance faciale, tout en gardant à l'esprit qu'il y aura toujours des problèmes liés à la sécurité publique et à la sécurité nationale?

Je vais commencer par M. Khanna.

**M. Sanjay Khanna:** Je pense que votre comité parlementaire prend des mesures en ce sens en s'appuyant sur un groupe aussi vaste d'experts interprofessionnels et interdisciplinaires.

Une autre chose importante, c'est qu'il faudrait aussi que les employés des entreprises, qui ont les plus grands ensembles de données, puissent être cités à comparaître au sujet de l'utilisation qu'ils font de ces technologies, afin d'éclairer les approches législatives. Il peut s'agir d'employés de l'entreprise qui dénoncent des actes répréhensibles et qui peuvent ensuite en faire rapport à ces comités d'une façon ou d'une autre.

Il est probablement très important de tirer parti de ce que les gens de l'industrie savent pour égaliser et créer une symétrie appropriée entre ce que vous savez en tant que législateurs et ce que les entreprises savent à l'interne.

● (1210)

**Le président:** Merci.

Nous passons maintenant à Mme Hepfner, pour cinq minutes.

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

Je remercie les témoins de nous consacrer du temps aujourd'hui. Par l'entremise du président, j'aimerais profiter du fait que trois pays différents sont représentés ici.

En commençant par M. Jenkins, vous pourriez peut-être nous dire si le Royaume-Uni envisage des règles ou des garde-fous concernant l'intelligence artificielle. Nous avons parlé de la façon dont les législateurs devraient aborder la question avant qu'il ne soit trop tard. Je me demande ce que font les autres pays.

**M. Rob Jenkins:** Je suis désolé, mais ce n'est probablement pas vraiment mon domaine d'expertise. Je peux parler de la science cognitive de la reconnaissance faciale, mais je ne suis pas un expert du droit ou de la politique.

**Mme Lisa Hepfner:** Vous ne savez donc pas si d'autres pays envisagent de mettre en place des garde-fous, des moratoires ou des mesures législatives concernant l'intelligence artificielle ou la technologie de reconnaissance faciale.

**M. Rob Jenkins:** Je sais qu'ils le font, mais je n'ai pas une connaissance approfondie de ces processus.

**Mme Lisa Hepfner:** Mme Wang ou Mme Watkins pourraient peut-être nous donner leur point de vue. Y a-t-il une loi qui est envisagée du côté américain de la même façon qu'au Canada?

**Mme Angelina Wang:** Je ne suis pas non plus au courant.

**Mme Elizabeth Anne Watkins:** Ce n'est pas mon domaine d'expertise, mais je dirais qu'un domaine de la loi qui a été particulièrement utile pour les travailleurs dans le processus décisionnel automatisé est le RGPD, et son droit fonctionnel à une explication. Bien que le RGPD ne contienne pas les mots « droit à une explication », une bonne partie des garde-fous visant à s'assurer que les entreprises doivent fournir aux travailleurs un aperçu de la façon dont les décisions sont prises à leur sujet par les systèmes automatisés pourrait être un modèle très utile.

**Mme Lisa Hepfner:** À part ce que nous avons entendu, quelqu'un a-t-il d'autres conseils sur la façon dont, en tant que législateurs, nous pouvons contribuer à la mise en œuvre de cette pratique, si elle se concrétise, à part un moratoire? Peut-être plus précisément, quelles mesures de protection pourrions-nous mettre en place pour nous assurer que les risques seront quelque peu atténués?

Personne ne veut s'attaquer à cela.

**M. Sanjay Khanna:** Je vais simplement revenir sur quelque chose que j'ai dit plus tôt au sujet de la nécessité de s'appuyer sur le plus possible de recherches et de connaissances sur les minorités racialisées, les Premières Nations, les enfants ou toute personne qui est plus vulnérable à ce genre d'exploitation, ou pourrait être rendue vulnérable par l'évolution de la situation économique qui préoccupe le gouvernement en place et les députés des divers partis. Il est probablement très important d'examiner la situation de façon prospective pour déterminer comment protéger ces personnes.

**Mme Lisa Hepfner:** Nous avons aussi beaucoup entendu parler aujourd'hui de la façon dont les préjugés de l'intelligence artificielle découlent des préjugés humains que nous avons dans notre société, parce que les machines sont programmées par les humains. Je me demande si c'est universel, parce que j'ai vu brièvement une étude selon laquelle les algorithmes mis au point en Asie n'auraient pas les mêmes problèmes de discrimination que les algorithmes développés en Amérique du Nord.

Madame Wang, vous pourriez peut-être nous en parler. Y a-t-il de meilleures façons de mettre au point cette technologie pour que nous puissions quand même en tirer des avantages tout en atténuant certains des risques de discrimination?

**Mme Angelina Wang:** Merci.

Je pense que chaque modèle est élaboré dans le contexte de l'étude sur laquelle il repose, et les modèles développés en Asie ont donc également beaucoup de biais. Il s'agit simplement de biais différents de ceux des modèles élaborés par des Canadiens ou des Américains.

Par exemple, beaucoup d'outils de reconnaissance d'objets ont démontré qu'ils ne sont pas aussi bons pour reconnaître les mêmes objets — par exemple, le savon — provenant d'un pays différent de celui d'où vient l'ensemble de données.

Il y a des façons de contourner ce problème, mais il faut beaucoup de gens différents qui ont des points de vue différents, parce qu'il n'y a tout simplement pas de point de vue universel. Je pense qu'il n'est jamais possible d'éliminer tous les préjugés dans le modèle, parce que les préjugés sont eux-mêmes très liés à un contexte sociétal particulier.

● (1215)

**Le président:** Merci.

Cela nous amène à la fin du deuxième tour. Nous allons maintenant passer à des tours supplémentaires.

À titre d'information pour les membres du Comité, il semble maintenant peu probable qu'il y ait un vote, alors nous pourrons sans doute terminer cette réunion. Les députés auront amplement l'occasion de poser des questions.

Sur ce, nous passons maintenant à M. Williams.

**M. Ryan Williams:** Merci, monsieur le président.

Je vais enchaîner sur certaines des questions de ma collègue, Mme Hepfner.

Monsieur Jenkins, encore une fois, vous avez écrit au sujet du « other-race effect », qui est une théorie selon laquelle on se souvient mieux des visages de sa propre race que des visages d'autres races. Nous savons que la technologie de reconnaissance faciale est très précise pour les visages blancs, mais que sa précision diminue pour les autres couleurs de peau.

Cela pourrait-il être dû à l'effet de ce biais sur les programmeurs, essentiellement une équipe de programmation majoritairement blanche créant une IA qui reconnaît mieux les visages blancs? Le même biais s'appliquerait-il à une IA de reconnaissance faciale développée par une équipe de programmation majoritairement noire, par exemple? Que révèlent vos recherches et que constatez-vous dans vos études?

**M. Rob Jenkins:** Les préjugés chez les programmeurs pourraient être un facteur, mais je ne pense pas que nous ayons besoin d'invoquer cela pour comprendre les différences démographiques que nous voyons dans les systèmes automatisés de reconnaissance faciale.

Je pense que cela s'explique par la distribution d'images qui servent à former les algorithmes. Si vous alimentez les algorithmes principalement avec, disons, des visages blancs, il sera alors plus facile de reconnaître des visages blancs que des visages d'autres races. Si vous les alimentez principalement avec des visages noirs, il sera plus facile de reconnaître les visages noirs que les visages blancs.

On pourrait peut-être faire une analogie avec la langue. Ce qui se passe dans votre environnement est important lorsque vous êtes un être humain en développement, et c'est également important pendant qu'un système artificiel est programmé.

**M. Ryan Williams:** Madame Wang, nous savons que la technologie de reconnaissance faciale est terriblement inexacte pour ce qui est d'identifier correctement les personnes non blanches. Nous avons entendu parler d'un taux d'erreur allant jusqu'à 34 % pour les femmes à la peau foncée. Ce racisme numérique induit par la technologie de reconnaissance faciale est inacceptable et renforce la raison pour laquelle cette technologie ne devrait pas être utilisée pour l'application de la loi.

Vous avez écrit sur l'atténuation des préjugés dans l'apprentissage automatique. Comment pouvons-nous mettre fin à ce racisme numérique?

**Mme Angelina Wang:** C'est très difficile à imaginer, parce qu'aucune de ces technologies ne sera jamais utilisée en vase clos, et qu'elles sont toujours situées dans un contexte social particulier. Même si vous aviez un système de reconnaissance faciale qui fonctionnerait parfaitement, ou du moins de la même façon pour différentes personnes ayant des tons de peau différents, son utilisation, par exemple, pour la surveillance ou le maintien de l'ordre, n'en serait pas moins très raciste. On ne peut jamais vraiment dissocier la technologie de [*difficultés techniques*]

**M. Ryan Williams:** J'aimerais revenir sur une des questions de ma collègue. Cette technologie peut-elle être utilisée à bon escient?

J'ai lu quelque chose au sujet de l'utilisation de cette technologie pour aider à freiner la traite des personnes, trouver des images à l'aide de l'intelligence artificielle pour identifier, disons, une personne qui avait peut-être 13 ans lorsqu'elle a disparu et qui est maintenant plus âgée. Utilisée à bon escient, cette technologie peut servir pour la traite des personnes ou pour résoudre certains de ces problèmes.

Ma question s'adresse à tous les témoins. Est-il possible que les forces de l'ordre en fasse un usage positif plutôt que négatif? À votre avis, y a-t-il des façons de protéger cela dans le cadre d'une loi?

**M. Rob Jenkins:** Je pense que vous avez décrit la technologie de la reconnaissance faciale comme un outil et, à mon avis, c'est exactement la bonne façon de la décrire. Vous pouvez utiliser un outil pour essayer d'aider d'autres personnes, ou vous pouvez l'utiliser pour essayer de nuire à d'autres personnes, alors nous devons comprendre l'intention des gens ainsi que les capacités de cette technologie.

● (1220)

**M. Ryan Williams:** J'ai la même question pour quiconque peut y répondre en 40 secondes.

**M. Sanjay Khanna:** J'ajouterais que les entreprises de consommation, les marques de consommation et les détaillants examinent de très près la technologie et font progresser leur réflexion sur l'analyse des sentiments et la perception des sentiments des clients dans un environnement de marque ou transactionnel. Certaines personnes pourraient ne pas trouver cela particulièrement menaçant. Elles pourraient y trouver des avantages, mais il faut quand même des garde-fous à cet égard.

Il y aura toujours des arguments économiques pour le trafic, les ventes et différents types de marketing et d'engagement de vente et d'opportunités transactionnelles qui devront probablement être examinés, si ces technologies sont utilisées, du point de vue de la surveillance.

**Le président:** Merci.

C'est maintenant au tour de M. Bains, pour cinq minutes.

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

Merci à tous nos témoins d'avoir pris le temps de venir nous rencontrer aujourd'hui.

Ma question s'adresse à qui voudra y répondre.

D'après les réponses que vous avez données à la question précédente de M. Green, il semble qu'il faille beaucoup de lois avant que la TRF soit largement utilisée.

Mes questions viennent de Richmond, en Colombie-Britannique. On y trouve une forte population d'Asie du Sud et d'Asie. Nous avons appris, d'un autre expert qui s'est joint à nous, que le SPV utilise la TRF sans beaucoup de supervision.

Savez-vous si des organismes d'application de la loi de la Colombie-Britannique utilisent la TRF?

Monsieur Khanna, êtes-vous au courant de cela?

**M. Sanjay Khanna:** Non, je ne sais pas comment le service de police de Vancouver utilise la TRF.

**M. Parm Bains:** D'accord, et je m'en tiendrai à vous, alors.

Dans un document, vous et vos collègues reconnaissez que les systèmes d'apprentissage automatique perpétuent et amplifient certains biais présents dans les données. Par conséquent, vous avez élaboré l'outil révisé pour permettre l'analyse préemptive d'ensembles de données à grande échelle. Comment l'outil révisé atténue-t-il ces biais?

**M. Sanjay Khanna:** Je pense qu'il pourrait s'agir d'un autre Sanjay Khanna qui travaille dans le domaine de l'intelligence artificielle et de l'apprentissage machine. Ce n'est pas moi.

**M. Parm Bains:** Oh, d'accord.

**Mme Angelina Wang:** Je pense que c'est pour moi.

L'outil révisé tente surtout de trouver différentes tendances et corrélations présentes dans les ensembles de données qui sont susceptibles de se propager dans les modèles qui sont formés sur les ensembles de données. Il n'est absolument pas garanti qu'il trouvera toutes les corrélations possibles qui pourraient survenir. Il ne fait que présenter les corrélations potentielles aux utilisateurs afin qu'ils soient plus conscients de ces créations de jeux de données lorsqu'ils utilisent un modèle qui a été formé sur un tel ensemble de données.

**M. Parm Bains:** Merci.

J'aimerais partager le reste de mon temps avec mon collègue, M. Fergus.

**L'hon. Greg Fergus:** Merci beaucoup, monsieur Bains. Je vous en suis reconnaissant.

Pour passer à autre chose, madame Wang, vous avez mentionné plus tôt dans votre témoignage, et je veux m'assurer d'avoir bien compris, que même si nous devions résoudre le problème des préjugés et de la discrimination, il y a des préoccupations qui ont été soulevées au sujet de l'utilisation de l'apprentissage automatique pour identifier les gens. Pouvez-vous nous en parler un peu?

**Mme Angelina Wang:** Bien sûr, oui.

Deux des points que j'ai soulevés sont l'interprétabilité et la fragilité. Pour ce qui est de la fragilité, les mauvais acteurs peuvent simplement tromper le modèle de différentes façons. Dans l'étude dont je parle, ils impriment un motif particulier sur une paire de lunettes, et grâce à cela, ils peuvent faire croire au modèle qu'il s'agit d'une personne totalement différente.

L'autre élément est la transparence. À l'heure actuelle, les modèles sont très difficiles à interpréter, parce qu'ils ont été en mesure d'utiliser toutes les règles qu'ils ont identifiées comme pouvant les aider au mieux dans leur tâche. Nous ne savons pas nécessairement sur quelles règles les modèles se basent. Ils pourraient se fier à...

**L'hon. Greg Fergus:** Je suis désolé de vous interrompre. Autrement dit, il semble que les machines ne soient pas en mesure de nous dire ce qu'elles utilisent pour faire ce genre d'évaluation.

**Mme Angelina Wang:** Oui, exactement.

● (1225)

**L'hon. Greg Fergus:** Monsieur Khanna, vous avez évoqué la possibilité d'une charte numérique des droits des Canadiens. C'est une idée très intrigante. Si vous deviez faire preuve d'un peu d'imagination, à quoi vous attendriez-vous dans ce genre de charte?

**M. Sanjay Khanna:** Il y a d'abord le caractère sacro-saint des données personnelles, et il faut donc protéger certaines données, comme les données faciales, qui sont très personnelles pour l'intéressé. Je pense que cela en ferait partie, mais qu'il faudrait aussi assurer l'harmonisation avec la Charte canadienne des droits et libertés et peut-être avoir un dépôt sécurisé de données pouvant être échangées et vérifiées et qui serait beaucoup plus cybersécurisé que ce qui pourrait exister actuellement.

**L'hon. Greg Fergus:** Puis-je vous demander très rapidement, monsieur Khanna, de parler du caractère sacro-saint des données personnelles? Est-ce que cela veut dire que nous avons droit, par exemple, à nos images, que nos images faciales sont à nous? Elles nous appartiennent. Le cheval a-t-il quitté l'écurie? Pouvons-nous le faire revenir?

**M. Sanjay Khanna:** Je pense que le cheval a quitté l'écurie dans une grande mesure, au point où on ne peut pas retirer de Clearview AI ce qui a déjà été pris. Lorsqu'on commence à y réfléchir, surtout à mesure que les enfants grandissent, nous ne sommes pas les seuls à avoir été exposés à la technologie de la reconnaissance faciale. Cela va toucher les générations actuelles et de nombreuses générations futures. Il est extrêmement important de penser à ceux qui n'ont pas encore été exposés, pour qui le cheval n'a pas quitté l'écurie.

**Le président:** Merci. Nous vous avons laissé dépasser un peu le temps qui vous était alloué, mais les témoignages étaient intéressants et importants, et pour une fois, nous avons une petite marge de manoeuvre.

La parole est maintenant à M. Villemure.

Allez-y, s'il vous plaît.

[*Français*]

**M. René Villemure:** Monsieur Jenkins, comment pourrions-nous mettre un peu d'éthique dans toute cette technologie de reconnaissance faciale? Cela pourrait-il passer par la transparence radicale ou encore par le droit à l'oubli?

Je vous laisse nous en parler pendant deux minutes et demie.

[*Traduction*]

**M. Rob Jenkins:** Oui, je crois certainement que la transparence est importante. Nous devrions viser une situation où les citoyens peuvent comprendre comment ces technologies sont utilisées, comment elles pourraient être efficaces, comment elles pourraient les toucher et comment elles l'ont peut-être déjà fait.

Nous savons, d'après les études sur l'utilisation de ces technologies aux États-Unis, par exemple, qu'il y a très peu de traces d'audit, et je pense que l'audit de l'utilisation des technologies de reconnaissance faciale sera un élément important d'une utilisation plus large.

[*Français*]

**M. René Villemure:** Le concept de transparence radicale qui est évoqué habituellement est-il trop applicable, ou, au contraire, ne l'est-il pas suffisamment?

[*Traduction*]

**M. Rob Jenkins:** Je pense que la transparence n'est probablement pas suffisante à elle seule. Je crois que c'est un élément important d'un système éthique.

[*Français*]

**M. René Villemure:** Ma dernière question porte sur la notion de consentement.

Quand nous marchons dans la rue et que notre image est captée, il est à peu près impossible de donner notre consentement.

Cela étant à peu près impossible, à quoi pouvons-nous nous attendre en matière de consentement ou de protection?

[*Traduction*]

**M. Rob Jenkins:** Oui, c'est une question très difficile. Je n'ai pas de réponse claire, mais j'hésite à comparer les technologies de reconnaissance faciale avec un système parfaitement exact et exempt de biais, parce que ce n'est pas une option qui est sur la table.

Nous savons certainement ce que nous obtenons des systèmes de décision qui sont utilisés depuis des décennies. Les systèmes actuels comportent des erreurs et des biais, et nous ne consentons pas, dans mon pays, à être filmés par la télévision en circuit fermé ou par les yeux d'autres personnes. Je pense que c'est une question complexe.

● (1230)

[*Français*]

**M. René Villemure:** Je vous remercie beaucoup.

[*Traduction*]

**Le président:** Merci.

Nous passons maintenant à M. Green.

**M. Matthew Green:** Juste pour clarifier, c'est cinq minutes?

**Le président:** Non. C'est deux et demi, avec un peu de générosité.

**M. Matthew Green:** Bien, voilà. J'apprécie votre générosité.

Je vais passer à M. Khanna.

Monsieur Khanna, j'aimerais approfondir la relation entre l'utilisation de cette technologie par les entreprises et l'État. Si j'ai bien compris, les entreprises et les organisations que vous avez conseillées utilisent la TRF. À quels règlements et mesures ces entreprises doivent-elles se conformer pour protéger les données, la vie privée et les Canadiens à l'heure actuelle?

**M. Sanjay Khanna:** À titre de précision, je n'ai pas conseillé les entreprises sur leur utilisation de la TRF. Si elles l'ont utilisée, ce serait plutôt par accident. Les projets sur lesquels j'ai travaillé ne portaient pas précisément sur la TRF. Un projet auquel j'ai travaillé récemment avec le Congrès mondial sur la justice pour les enfants sur l'avenir de la justice pour les enfants...

**M. Matthew Green:** Si vous me le permettez, en deux minutes et 30 secondes, vous avez parlé de garde-fous. Selon votre expérience, le Canada dispose-t-il d'un cadre approprié pour réglementer l'utilisation de la technologie de reconnaissance faciale par des organismes privés et d'État?

**M. Sanjay Khanna:** Pas encore, et c'est ce que j'espère que vous et d'autres législateurs chercherez à faire.

**M. Matthew Green:** Très bien.

Monsieur Jenkins, à la suite de cette étude, compte tenu des défis que pose la reconnaissance faciale précise, tant par les humains que par l'intelligence artificielle, avez-vous d'autres recommandations pour atténuer les conséquences négatives de l'utilisation de la reconnaissance faciale à des fins de sécurité?

**M. Rob Jenkins:** L'une des principales préoccupations est l'erreur sur la personne et l'idée qu'une personne innocente puisse être appréhendée, accusée et même condamnée pour un crime qu'elle n'a pas commis. C'est clairement une erreur que nous voulons éviter, et nous voulons aussi éviter l'erreur inverse, à savoir ne pas appréhender quelqu'un qui pourrait représenter un grand danger pour d'autres personnes.

Ce n'est pas nouveau. Nous essayons d'atténuer ces problèmes depuis que nous recevons les témoignages de témoins oculaires, mais à l'échelle à laquelle les technologies de reconnaissance faciale sont déployées, cela prend une nouvelle forme. À mon avis, c'est la principale différence.

**M. Matthew Green:** Mme Wang a soulevé la question de l'interprétabilité et l'idée qu'avec les humains, on peut au moins contester une décision. Cependant, dans l'état actuel des choses, il est difficile de contester les décisions qui sont prises.

Avez-vous quelque chose à dire quant aux façons dont nous pouvons atténuer le problème d'interprétabilité et dont nous pouvons contester les décisions?

**M. Rob Jenkins:** Il est possible de demander à un humain comment il en est arrivé à un jugement particulier, mais nous ne savons pas très bien pourquoi nous prenons parfois les décisions que nous prenons. Souvent, nous inventons, après coup, des justifications qui semblent plausibles aux autres, et c'est nouveau pour nous autant que pour eux.

Je ne suis pas certain de pouvoir faire des recommandations qui pourraient être facilement transposées de ce genre de situation aux décisions prises par l'IA.

**M. Matthew Green:** Vous seriez d'accord pour dire que... Merci.

**Le président:** Merci. Je vous ai accordé plus ou moins une minute de plus.

Nous allons maintenant passer à M. Bezan pour cinq minutes ou un partage, si vous voulez bien.

Allez-y.

**M. James Bezan:** Merci, monsieur le président.

J'aimerais adresser mes questions à Mme Watkins.

Vous avez parlé de toute la question de l'imposition d'un moratoire sur l'utilisation de la TRF jusqu'à ce que nous ayons mis en place des garde-fous adéquats au moyen de lois et de règlements. Quand est-il approprié que la TRF soit utilisée en milieu de travail, par des organismes gouvernementaux ou par des particuliers?

**Mme Elizabeth Anne Watkins:** Pour répondre à cette question, il faudrait utiliser des outils législatifs et réglementaires comme évaluation d'impact algorithmique de l'impact, en plus de consulter les groupes marginalisés.

Je ne peux pas parler au nom des travailleurs du genre de technologies de sécurité qu'ils aimeraient voir dans leur milieu de travail. Consultez ces groupes pour leur demander à quel type de technologie ils accepteraient de se conformer. Il faut leur offrir des solutions de rechange, pour qu'ils puissent se soustraire aux technologies auxquelles ils ne veulent pas se conformer, tout en gardant accès à leurs moyens de subsistance. Ce serait de bonnes mesures.

● (1235)

**M. James Bezan:** Croyez-vous que les services de police devraient être autorisés à utiliser la TRF?

**Mme Elizabeth Anne Watkins:** Non.

**M. James Bezan:** Il ne s'agit pas seulement d'un moratoire; vous parlez d'une interdiction complète de l'utilisation de la TRF par les services de police, les services frontaliers et le gouvernement en général.

**Mme Elizabeth Anne Watkins:** Dans les scénarios à haut risque, où des vies et des moyens de subsistance sont en jeu, non seulement ces technologies ne sont pas fiables à l'heure actuelle, mais elles supposent également que les constructions sociales, comme la race et le sexe, sont lisibles par machine sur le visage d'une personne. C'est tout simplement faux.

**M. James Bezan:** Lorsque vous commencez à parler d'entreprises comme Clearview AI, qui ont des antécédents d'identification erronée de personnes et qui ont des préjugés dans leur technologie d'intelligence artificielle avec la TRF, ces entreprises devraient-elles être interdites?

**Mme Elizabeth Anne Watkins:** Je pense que leurs technologies ne devraient pas être utilisées dans des scénarios à haut risque.

**M. James Bezan:** À votre avis, il serait toujours acceptable qu'un employeur les utilise en milieu de travail, même si leurs antécédents indiquent clairement qu'il y a un préjudice.

**Mme Elizabeth Anne Watkins:** Le milieu de travail est un scénario à très haut risque. Ces technologies ne devraient pas être utilisées en milieu de travail. Elles ne devraient pas être utilisées dans un espace public. Elles ne devraient pas être utilisées par la police.

Franchement, je pense qu'il devrait y avoir un moratoire jusqu'à ce que nous en sachions davantage sur les répercussions de ces outils sur les collectivités.

**M. James Bezan:** Madame Wang, voulez-vous intervenir? Vous avez mené une étude approfondie sur la façon dont la TRF et Clearview, en particulier, ont été utilisées contre les personnes marginalisées.

Êtes-vous d'accord avec Mme Watkins?

**Mme Angelina Wang:** Oui. Il y a trop d'inconnues à l'heure actuelle. Ces technologies ne devraient pas être déployées pour le moment, ou même jamais.

**M. James Bezan:** D'accord.

Vous avez examiné la GRC, je crois. L'Agence des services frontaliers du Canada...?

Il y a souvent des menaces à la sécurité nationale. Il est donc probablement préférable, à votre avis, que nous n'utilisions pas la TRF dans nos organismes d'application de la loi et de contrôle frontalier ici au Canada.

**Mme Angelina Wang:** Oui.

**M. James Bezan:** Voulez-vous prendre la dernière minute?

**M. Damien Kurek:** Merci beaucoup.

Je vais poser la question à tous les témoins et je vais y aller un par un.

Pourriez-vous nous donner le plus rapidement possible des exemples de TRF, publics ou privés, à titre d'information? Ce serait très utile.

Nous allons commencer par Mme Watkins.

**Mme Elizabeth Anne Watkins:** Je suis désolée. Pouvez-vous répéter la question? Vous parlez d'exemples de TRF déjà déployée?

**M. Damien Kurek:** Oui. De mémoire, avez-vous des exemples que le Comité pourrait utiliser comme points de référence de la TRF qui est utilisée?

**Mme Elizabeth Anne Watkins:** À ce que je sache, l'outil de reconnaissance faciale est actuellement imposé aux conducteurs d'Uber, aux livreurs d'Amazon et aux fournisseurs de soins à domicile qui doivent ouvrir une session dans l'ordinateur de leur lieu de travail pour effectuer une vérification électronique de la visite.

Quant à l'outil de vérification faciale, à ma connaissance, de nombreux services de police aux États-Unis l'utilisent, sauf dans les villes qui l'interdisent ou qui ont imposé un moratoire.

**M. Damien Kurek:** Merci.

Madame Wang, vous avez la parole.

**Mme Angelina Wang:** Je pense notamment à HireVue et à certaines autres plateformes d'entrevue.

**M. Damien Kurek:** Merci.

Monsieur Jenkins, vous avez la parole.

**M. Rob Jenkins:** Plusieurs pays l'utilisent aux contrôles frontaliers et dans d'autres processus, comme le renouvellement de passeport, pour vérifier si la personne qui présente la demande est bien celle qu'elle prétend être.

On l'utilise également dans l'examen rétrospectif de foules filmées par des caméras en circuit fermé pour identifier des suspects, par exemple.

● (1240)

**Le président:** M. Kurek a posé une question à laquelle quatre membres ont dû donner de longues réponses. Je vais demander à M. Khanna de répondre très rapidement à votre question, s'il le souhaite. Nous passerons ensuite la parole directement à Mme Khalid.

**M. Sanjay Khanna:** Merci. On entend dire que cette technologie est utilisée dans des jouets d'enfants, dans des logiciels pour enfants et autres, mais ce n'est pas confirmé. Il faudrait vérifier cela, mais je me souviens de l'avoir lu dans un rapport de l'ONU.

Merci.

**Le président:** Merci.

Je crois que Mme Khalid sera notre dernière intervenante. Allez-y.

**Mme Iqra Khalid (Mississauga—Erin Mills, Lib.):** Merci beaucoup, monsieur le président. Par votre entremise, je remercie les témoins pour leurs témoignages très convaincants.

J'aimerais ajouter une chose à la liste que vous avez fournie. En 2018, Taylor Swift a utilisé la technologie de la reconnaissance faciale pour identifier certains de ses harceleurs obsessionnels. C'était une utilisation très fascinante, intéressante et complexe, je crois, de cette technologie.

Nous avons mentionné les moratoires. Je vais commencer par demander à nos témoins ce qu'un moratoire accomplirait dans un environnement où la technologie et l'innovation évoluent si rapidement.

Je pourrais commencer par M. Khanna.

**M. Sanjay Khanna:** Un moratoire, comme vous le savez, c'est une pause. On recueille de l'information et des opinions auprès d'organismes de l'interne et de l'extérieur pour les évaluer, puis pour déterminer le genre de garde-fous à imposer lorsqu'on lèvera le moratoire.

S'il s'agit de « destruction en maths », comme l'a décrit M. Watkins, alors il est logique d'imposer un moratoire pour prendre de bonnes décisions.

**Mme Iqra Khalid:** Combien de temps pensez-vous que cette pause devrait durer? Le fait-on pour trouver une solution parfaite ou pour établir un juste équilibre entre la sécurité publique, la protection de la vie privée et la commodité du grand public?

**M. Sanjay Khanna:** Je m'en remets à mes collègues, qui ont étudié de plus près l'évolution de l'intelligence artificielle et de la technologie de la reconnaissance faciale.

**Mme Iqra Khalid:** Si l'un d'entre vous veut répondre, allez-y.

**M. Rob Jenkins:** Il y a 20 ans, je disais à tout le monde que le problème de ces systèmes de reconnaissance faciale, c'est qu'ils ne fonctionnaient pas. À l'heure actuelle, je passe plus de temps à dire que le problème de ces systèmes de reconnaissance faciale, c'est qu'ils fonctionnent.

Ces cinq dernières années, on a réalisé des progrès impressionnants pour que ces systèmes identifient bien les visages. Il arrive bien sûr qu'ils commettent des erreurs parfois surprenantes et difficiles à prévoir. Toutefois, cette technologie change très rapidement et elle évolue aussi pendant les moratoires.

**Mme Iqra Khalid:** Merci.

Je vais passer à un autre sujet, mais je ne sais pas à qui adresser ma question. Sauriez-vous s'il existe une technologie ou un système qui permette aux Canadiens de retirer leur image de toutes les bases de données sur la reconnaissance faciale et sur l'intelligence artificielle afin de jouir d'un parfait anonymat?

**M. Rob Jenkins:** Je suppose que d'autres témoins en savent plus que moi sur cette technologie, mais si l'on forme des algorithmes à partir d'une multitude d'images et que l'une de ces images, ou plus d'une, est la vôtre, alors c'est cuit. On ne peut plus éliminer l'influence d'une personne sur l'algorithme qui ressort de la base de données.

**Mme Iqra Khalid:** Merci. Essentiellement, dans ce cas-ci, les lois sur la protection des renseignements personnels et de la vie privée sont en jeu, et rien n'est noir ou blanc, on ne peut plus choisir d'en faire partie ou non. Notre image est là, toute cuite, comme vous l'avez dit, monsieur Jenkins.

Dans ce cas, nous voyons que les entreprises de médias sociaux, par exemple, ou d'autres plateformes intègrent ces algorithmes, cette intelligence artificielle, pour faciliter le magasinage. Elles achètent des ensembles de données pour que les entreprises puissent acheter leurs clients, en quelque sorte, afin d'affiner leur publicité. Serait-il possible, selon vous, d'ajouter des règles dans une éventuelle déclaration des droits pour protéger les Canadiens de la vente de leurs données à ces entreprises?

Est-ce que l'un de vous voudrait répondre? Pardonnez-moi, je ne sais pas à qui m'adresser. C'est une question complexe.

● (1245)

**Le président:** Voulez-vous la reformuler très rapidement ou l'adresser à un témoin en particulier?

**Mme Iqra Khalid:** Monsieur Khanna, si vous voulez bien, allez-y.

**M. Sanjay Khanna:** Justement, nous ne savons pas vraiment comment protéger les Canadiens de cette stratégie commerciale. C'est pourquoi il a été question de la transférabilité des données, qui donnerait aux Canadiens l'accès à leurs données et qui leur permettrait de gagner de l'argent s'ils consentent à ce qu'elles soient utilisées commercialement.

Il y a eu beaucoup de résistance à cet égard. En Australie, la société News Corp a enfin été poussée par... ou Google a dû payer la publication de données utilisées en ligne. On pourrait aussi offrir cela aux citoyens, du moins sur le plan conceptuel.

**Le président:** Je remercie beaucoup tous les témoins.

En fait, j'aimerais poser quelques questions dans mon rôle de président.

Tout d'abord, monsieur Khanna, à la toute fin de votre réponse à la question de M. Kurek, vous avez fait référence à un rapport qui mentionnait l'utilisation de la technologie de reconnaissance faciale dans des jouets pour enfants. Je me demande si vous pourriez fournir ce rapport ou ses coordonnées à notre greffière pour que le Comité puisse l'insérer dans son rapport au Parlement.

**M. Sanjay Khanna:** Avec plaisir.

**Le président:** Ce serait très apprécié.

J'ai une question à poser. Dans les exemples présentés aujourd'hui, je suppose que l'utilisation la plus « bénigne », si l'on peut dire, de la technologie de reconnaissance faciale, ou l'une des utilisations les plus bénignes dont on a parlé, est celle que beaucoup d'entre nous connaissent. C'est la reconnaissance faciale utilisée pour déverrouiller un iPhone ou un appareil mobile. La personne consentit à cette utilisation en fournissant une photo d'elle-même à la sécurité biométrique de son téléphone. Personnellement, je trouve qu'une empreinte digitale est beaucoup plus pratique, plus facile à utiliser et plus fiable qu'une photo, si l'appareil le permet.

Si nous avons là une utilisation que ce groupe et les membres du Comité n'hésitent pas à appuyer, voyez-vous des problèmes émerger, même à ce niveau, si le consommateur consent facilement, ou du moins relativement facilement, à ce type d'utilisation?

Je vais demander à chacun de nos témoins de présenter brièvement son opinion à ce sujet. Serait-ce une utilisation acceptable de cette technologie? Inclurait-on cela dans les moratoires que certains demandent?

Je vais demander d'abord à Mme Watkins de répondre brièvement.

**Mme Elizabeth Anne Watkins:** Merci beaucoup. C'est une excellente question.

J'exhorte le Comité à envisager le consentement dans un contexte où il a vraiment lieu. Le consentement est souvent beaucoup plus complexe qu'il n'y paraît de l'extérieur. Ce n'est pas toujours un oui ou un non, ou « non, je ne veux pas faire cela, alors je passe au prochain choix ». Souvent, il n'y a pas d'autre choix. Souvent, les gens subissent des pressions financières qui les obligent à respecter le protocole.

Par exemple, la vérification faciale qui est en place dans de nombreuses entreprises n'offre pas d'autre choix. Les employés qui ne se conforment pas à la vérification faciale sont tout simplement exclus de l'application.

**Le président:** À vous la parole, monsieur Jenkins.

**M. Rob Jenkins:** Je suis d'accord avec tout cela. Le consentement éclairé est très utile, mais il faut l'éclairer.

● (1250)

**Le président:** Allez-y, monsieur Khanna.

**M. Sanjay Khanna:** Je pourrais ajouter un autre cas d'utilisation potentiellement bénigne à ceux de mes estimés témoins. Ils me contrediront peut-être à ce sujet, mais on utilise aussi la reconnaissance faciale pour prévenir les accidents de travail. Elle peut s'avérer utile lorsque les opérateurs sont fatigués ou somnolents, comme les camionneurs voyageant sur de longues distances, les travailleurs des installations nucléaires ou industrielles, les professionnels de la santé, qui risquent de s'endormir ou qui ne se rendent pas compte qu'ils manquent d'attention. Dans ces cas-là, cette technologie s'avérerait bénéfique.

**Le président:** Madame Wang, vous avez le dernier mot.

**Mme Angelina Wang:** Les gens ne savent pas toujours vraiment quel usage on fait de leur image. Je ne sais pas si les téléphones le font à l'heure actuelle, mais ils pourraient recueillir ces données et les utiliser pour concevoir d'autres modèles. Le consentement n'est pas toujours clair, comme le démontrent tous ces cas.

**Le président:** En effet.

Merci à tous.

Monsieur Fergus, vous avez la parole. Vous avez levé la main.

**L'hon. Greg Fergus:** Puis-je poser une question qui complétera la vôtre? Je trouve cette série de questions vraiment intéressante, et je veux...

**Le président:** Oui. Allez-y, monsieur Fergus. Il nous reste quelques minutes.

**L'hon. Greg Fergus:** Pour faire suite à la question de M. Kelly au sujet de l'utilisation individuelle et pour savoir s'il y a ou non... Disons qu'il y a consentement. Lorsque nous utilisons les technologies de reconnaissance faciale pour ouvrir l'accès à nos téléphones, ces images sont-elles transmises au-delà de l'utilisation de ce téléphone et de celle du propriétaire de ce téléphone? Utilise-t-on les empreintes digitales? Cette information est-elle transmise ailleurs?

Je croyais que le consentement sur ces types de téléphones ou d'appareils de sécurité s'effectue entre l'utilisateur final et le téléphone lui-même. Corrigez-moi si je me trompe, car j'aimerais bien le savoir.

**M. Rob Jenkins:** Les entreprises ont des positions différentes à ce sujet. Pour certaines d'entre elles, tout se passe dans l'appareil. Pour les autres, cela ne fait pas partie de l'entente; l'information peut être entreposée dans le nuage et de là, elle peut être transmise ailleurs.

**Le président:** Est-ce que d'autres témoins voudraient intervenir?

Allez-y, madame Watkins.

**Mme Elizabeth Anne Watkins:** Merci.

Je suis d'accord avec M. Jenkins. Cette différence qu'il décrit, le manque de certitude quant à savoir si les données restent dans notre téléphone ou dans les serveurs de l'entreprise ou si, en fait, elles sont utilisées par un fournisseur tiers et stockées dans ses serveurs, montre la nécessité de renforcer la transparence au sujet de l'endroit où ces données sont stockées et de l'usage que l'on en fait.

**Le président:** Oui, madame Wang.

**Mme Angelina Wang:** Il existe un nouveau type de formation appelé « apprentissage fédéré », qui conserve en tout temps votre image sur votre appareil, mais vous consentez quand même à effectuer des mises à jour. Vous indiquez comment vous voulez régler vos paramètres afin de classifier votre image. Dans ce cas, l'image ne vous quitte jamais et elle ne sort pas de votre téléphone, mais le téléphone peut utiliser cette information pour s'améliorer. Il serait cependant assez difficile de déterminer l'application du consentement dans un cas comme celui-ci.

**Le président:** Je comprends.

Merci beaucoup à nos témoins. Cette conversation a été très instructive.

Sur ce, la séance est levée.