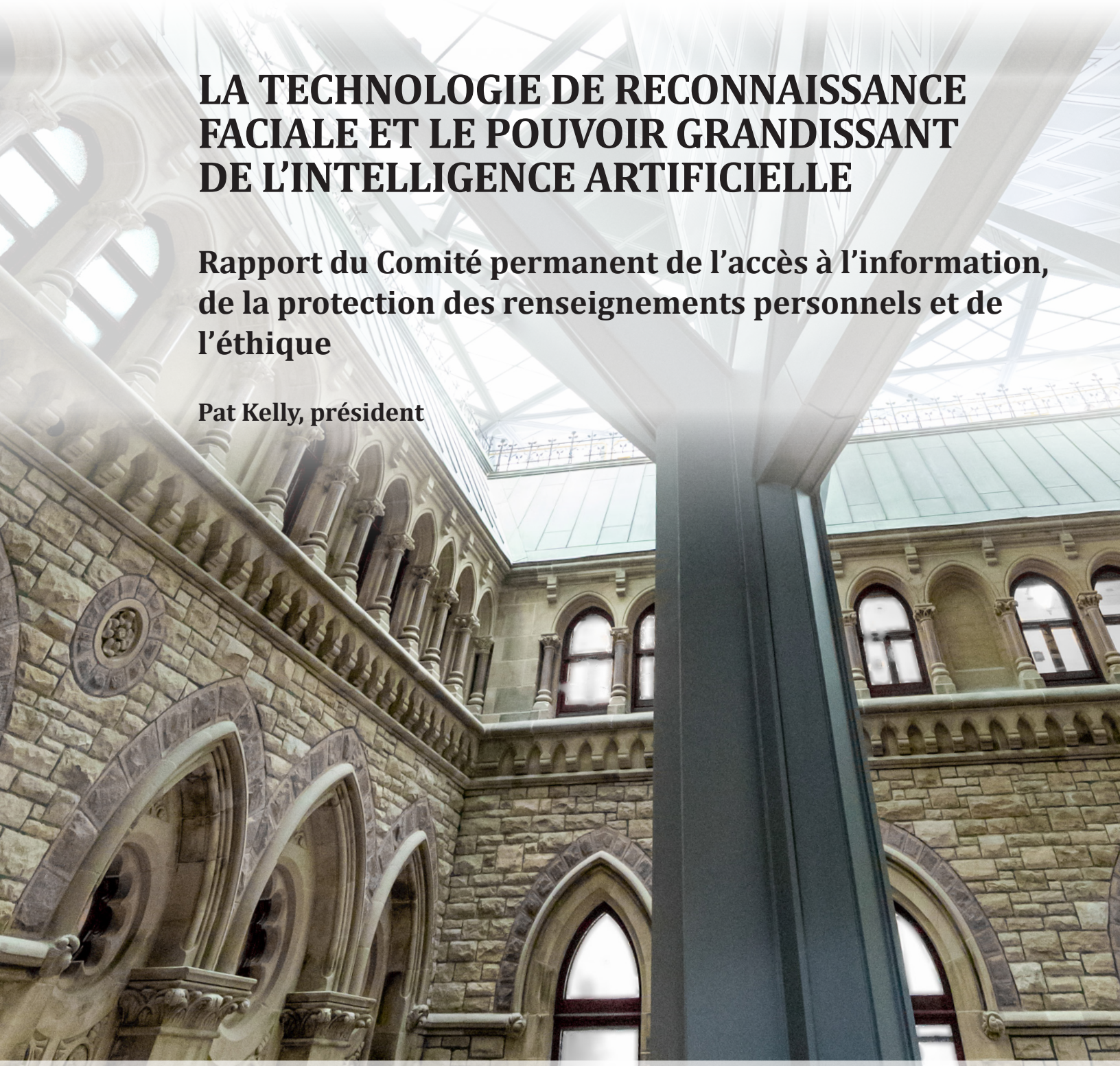
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA



LA TECHNOLOGIE DE RECONNAISSANCE FACIALE ET LE POUVOIR GRANDISSANT DE L'INTELLIGENCE ARTIFICIELLE

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

Pat Kelly, président

OCTOBRE 2022
44e LÉGISLATURE, 1re SESSION

LA TECHNOLOGIE DE RECONNAISSANCE FACIALE ET LE POUVOIR GRANDISSANT DE L'INTELLIGENCE ARTIFICIELLE

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

Le président
Pat Kelly

OCTOBRE 2022

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

Pour guider le lecteur :
Une liste des acronymes utilisés dans ce rapport est disponible à la page ix

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

Pat Kelly

VICE-PRÉSIDENTS

Iqra Khalid

René Villemure

MEMBRES

Parm Bains

James Bezan

L'hon. Greg Fergus

Matthew Green

Lisa Hepfner

Damien C. Kurek

Ya'ara Saks

Ryan Williams

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Richard Bragdon

Iqwinder Gaheer

Jean-Denis Garon

Leah Gazan

Majid Jowhari

Arielle Kayabaga

Jennifer O'Connell

Brad Redekopp

Francesco Sorbara

Joanne Thompson

Anita Vandenbeld

Dominique Vien
Cathay Wagantall

GREFFIÈRE DU COMITÉ

Nancy Vohl

BIBLIOTHÈQUE DU PARLEMENT

Services d'information, d'éducation et de recherche parlementaires

Sabrina Charland, analyste
Alexandra Savoie, analyste

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l’honneur de présenter son

SIXIÈME RAPPORT

Conformément au mandat que lui confère l’article 108(3)h) du Règlement, le Comité a étudié l'utilisation et impacts de la technologie de reconnaissance faciale et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE DES ACRONYMES

ACLC	Association canadienne des libertés civiles
ACLU	American Civil Liberties Union
ASFC	Agence des services frontaliers du Canada
BIPA	*Biometric Information Privacy Act*
CAI	Commission d'accès à l'information du Québec
CIPPIC	Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko
CNCCE	Centre national de coordination contre l'exploitation des enfants
CNMC	Conseil national des musulmans canadiens
CPVP	Commissariat à la protection de la vie privée du Canada
CSILC	Coalition pour la surveillance internationale des libertés civiles
CSPT	Commission des services policiers de Toronto
EIA	Évaluation de l'incidence algorithmique
GRC	Gendarmerie Royale du Canada
IA	Intelligence artificielle
LCCJTI	*Loi concernant le cadre juridique des technologies de l'information*
LPRPDE	*Loi sur la protection des renseignements personnels et documents électroniques*
NIST	National Institute of Standards and Technology
OCDE	Organisation de coopération et développement économique
PNIT	Programme national d'intégration de la technologie de la GRC

RF	Reconnaissance faciale
SPT	Service de Police de Toronto
TRF	Technologie de reconnaissance faciale
SCRS	Service canadien du renseignement de sécurité

SOMMAIRE

La prolifération de l'intelligence artificielle (IA) et l'utilisation croissante de la technologie de reconnaissance faciale (TRF), ainsi que les enquêtes récentes du Commissariat à la protection de la vie privée (CPVP) portant sur la TRF, ont mené le Comité à entreprendre une étude sur la TRF et le pouvoir grandissant de l'IA.

Ce rapport examine les avantages et les risques posés par la TRF et son utilisation dans des contextes spécifiques, comme l'application de la loi. Il explore aussi d'autres questions relatives à la gouvernance de l'IA, comme l'approvisionnement et l'investissement public dans le domaine. Il s'intéresse aussi aux solutions, législatives ou autres, qui permettraient de rassurer les Canadiens et Canadiennes que l'utilisation de la TRF ou d'autres outils d'IA au Canada se fait d'une manière responsable et dans le respect de leurs droits.

En tenant compte des témoignages qu'il a entendus, le Comité formule plusieurs recommandations visant à améliorer le cadre législatif fédéral qui s'applique à la TRF et l'IA, dont imposer un moratoire sur l'utilisation de la TRF au Canada, comme l'a recommandé une majorité des témoins.

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Recommandation 2

Recommandation 3

Recommandation 4

LA TECHNOLOGIE DE RECONNAISSANCE FACIALE ET LE POUVOIR GRANDISSANT DE L'INTELLIGENCE ARTIFICIELLE

INTRODUCTION

Contexte

L'intelligence artificielle (IA) est aujourd'hui omniprésente dans la société. La technologie de reconnaissance faciale (TRF), qui repose sur l'IA, gagne aussi en popularité. Au Canada, la TRF a récemment fait l'objet d'une enquête conjointe du Commissariat à la protection de la vie privée du Canada (CPVP) et de ses homologues provinciaux de l'Alberta, de la Colombie-Britannique et du Québec dans le dossier impliquant Clearview AI.

En février 2021, le CPVP a publié le rapport de son enquête conjointe dans lequel il a conclu que Clearview AI n'avait pas respecté la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en procédant à la collecte massive d'images sans le consentement des individus concernés et à des fins inappropriées[1].

Le CPVP a aussi mené une enquête sur l'utilisation par la Gendarmerie Royale du Canada (GRC) de la technologie de Clearview AI. Dans son rapport spécial au Parlement, publié en juin 2021, le CPVP a conclu que la GRC n'avait pas respecté la *Loi sur la protection des renseignements personnels* en recueillant des renseignements personnels auprès d'un tiers (Clearview AI) qui les a recueillis illégalement[2].

---

1 Commissariat à la protection de la vie privée du Canada (CPVP), *Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta*, 2 février 2021 [*Rapport du CPVP sur Clearview AI*]. Le CPVP a conclu que Clearview AI n'était pas exemptée d'obtenir le consentement en vertu de l'exception de la LPRPDE applicable aux renseignements personnels « accessibles au public », qui se limite à ceux identifiés dans le *Règlement précisant les renseignements auxquels le public a accès*.

2 CPVP, *Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée*, Rapport spécial au Parlement sur l'enquête réalisée par le Commissariat à la protection de la vie privée du Canada sur l'utilisation par la GRC de la technologie de Clearview AI et version préliminaire d'un document d'orientation conjoint à l'intention des services de police qui envisagent d'avoir recours à la technologie de reconnaissance faciale, 10 juin 2021 [*Rapport spécial sur la GRC*]. La GRC a contesté les conclusions du CPVP (voir chapitre 2 du rapport).

C'est dans ce contexte qu'en décembre 2021, le Comité a adopté à l'unanimité une motion visant à entreprendre une étude sur l'utilisation et les impacts de la TRF et le pouvoir grandissant de l'IA.

Le Comité a tenu 9 réunions publiques et entendu 33 témoins. Il a aussi reçu 8 mémoires. Le Comité remercie tous ceux et celles qui ont participé à l'étude.

Organisation du rapport

Le rapport se divise en quatre chapitres. Le chapitre 1 explique ce qu'est la TRF, sa place dans le marché et fait un survol des avantages et des risques qu'elle présente. Le chapitre 2 s'intéresse à certains types d'utilisation spécifiques de la TRF, notamment son utilisation par les services de police. Le chapitre 3 discute de la responsabilisation des acteurs qui utilisent et développent la TRF et l'IA et des enjeux liés à l'approvisionnement et aux investissements publics en matière d'IA. Enfin, le chapitre 4 s'intéresse à la réglementation de la TRF et de l'IA.

CHAPITRE 1 : LA TECHNOLOGIE DE RECONNAISSANCE FACIALE

> **« Comme c'est le cas de toutes les technologies, la reconnaissance faciale peut, si elle est utilisée de manière responsable, offrir d'importants avantages à la société. Cependant, elle peut aussi s'avérer extrêmement envahissante, permettre la surveillance à grande échelle, produire des résultats tendancieux et miner les droits de la personne, y compris le droit de participer librement, sans surveillance, à la vie démocratique. »**
>
> Daniel Therrien,
> commissaire à la protection de la vie privée du Canada,
> qui a comparu devant le Comité le 2 mai 2022.

Définition et fonctionnement de la technologie de reconnaissance faciale

Carole Piovesan, associée directrice chez INQ Law, a expliqué que la TRF utilise des données biométriques faciales extrêmement sensibles pour identifier et vérifier l'identité d'une personne. Brenda McPhail, directrice du Programme de la vie privée, de

technologie et de surveillance de l'Association canadienne des libertés civiles (ACLC), a qualifié la TRF d'empreinte faciale.

La reconnaissance faciale (RF) est un processus d'identification informatique d'un visage à partir d'une image ou d'une vidéo numérique. Elle peut être déployée en temps réel ou sur des images statiques. Elle utilise la reconnaissance de motifs par ordinateur pour trouver des points communs dans les images représentants des visages humains. La TRF peut être utilisée pour confirmer l'identité d'une personne connue ou pour identifier une personne inconnue. Elle peut aussi permettre la catégorisation et le profilage d'une personne au fil du temps en fonction de ses renseignements faciaux[3]. En d'autres termes, la TRF peut être utilisée à des fins d'identification, de vérification, ou de catégorisation ou caractérisation[4].

De façon générale, toutefois, on classe les systèmes de TRF en deux catégories : ceux utilisés pour vérifier l'identité d'une personne (un pour un) et ceux utilisés pour identifier une personne (un pour plusieurs).

> Un système un pour un compare l'image d'un utilisateur à plusieurs images d'une seule personne pour authentifier ou vérifier l'identité connue d'une personne. Un système « un pour plusieurs » compare une image à une base de données de différents visages (comme une liste de surveillance de terroristes ou une base de données de photos signalétiques) afin d'identifier de façon unique une personne au sein d'un groupe de personnes, souvent en direct ou en temps réel[5].

Elizabeth Anne Watkins, attachée de recherche au niveau postdoctoral de la Princeton University, a décrit la vérification faciale ainsi :

> 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

3 Centre for Media, Technology and Democracy et Cybersecure Policy Exchange, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 1 juin 2022, p. 2 [*Mémoire CMTD et CPE*].

4 Christelle Tessono, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 4 mai 2022, pp. 3-4 [*Mémoire Tessono*].

5 Mémoire CMTD et CPE, p. 2.

> 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.

Angelina Wang, chercheuse diplômée en science informatique de la Princeton University, a expliqué que d'un point de vue technique, la TRF est un modèle de technologie entraîné à l'apprentissage automatique. Plutôt que d'appliquer des règles à programmation manuelle le modèle se voit fournir un vaste ensemble de visages annotés à partir desquels il apprend[6]. Ces annotations comprennent entre autres des étiquettes qui indiquent que les images représentent la même personne, ainsi que l'emplacement du visage dans chaque image.

Mme Wang a aussi expliqué que les données qui alimentent les modèles sont généralement recueillies sur des plateformes de production participative, telle Amazon Mechanical Turk, qui selon elle est connue pour faire appel à des groupes de travailleurs homogènes et offrir des conditions de travail désavantageuses, ou simplement d'Internet, dont de sites Web comme Flickr[7]. Ces ensembles de données varient en ordre de grandeur, allant par exemple de 10 000 images jusqu'à plusieurs millions d'images.

La technologie de reconnaissance faciale en 2022

Plusieurs témoins ont confirmé que la TRF prend de plus en plus de place dans le marché et dans la société.

Par exemple, Mme Piovesan a indiqué que l'utilisation de la TRF gagne du terrain dans le secteur public et privé. Elle a mentionné que selon une étude publiée par le Grand Review Research en 2020, le marché mondial de la TRF devrait atteindre 12 milliards de dollars américains en 2028[8]. Selon elle, cette expansion s'explique par des

---

6 Angelina Wang donne l'exemple d'une règle à programmation manuelle qui dit que deux personnes qui ont des yeux de la même couleur ont plus de chance d'être la même personne.

7 Par exemple, Nestor Maslej, associé de recherche au Institute for Human-Centered Artificial Intelligence de la Standford University, a expliqué qu'un système de sélection de CV développé par Amazon par apprentissage automatique s'est révélé discriminatoire, car le système avait été entraîné à partir de données provenant de CV qu'Amazon avait déjà reçus et dont l'écrasante majorité provenait d'hommes. Le système n'a jamais été utilisé pour prendre des décisions d'embauche.

8 Grand View Research, Facial Recognition Market Size, Share & Trends Analysis Report by Technology (2D, 3D, Facial Analytics), by Application (Access Control, Security & Surveillance), by End-use, by Region, and Segment Forecasts, 2021 – 2028 [DISPONIBLE EN ANGLAIS SEULEMENT].

investissements majeurs et des avancées dans l'application de cette technologie à l'échelle planétaire. Elle a ajouté que bien que la TRF est souvent abordée dans le contexte de sécurité et de surveillance, elle est utilisée dans plusieurs secteurs, dont le commerce au détail, le commerce électronique, les télécommunications, les technologies de l'information et les soins de santé. Il s'agit donc d'un débouché économique attrayant pour les concepteurs et les utilisateurs.

Nestor Maslej, associé de recherche du Institute for Human-Centered Artificial Intelligence de la Standford University, a partagé les statistiques suivantes, tirée du 2022 AI Index Report de cet institut[9].

> En 2021, 18 des 24 organismes du gouvernement américain ont utilisé ces technologies: 16 départements l'ont fait à des fins d'accès numérique ou de cybersécurité, six, à des fins de création de pistes pour des enquêtes criminelles, et cinq, à des fins de sécurité physique. De plus, 10 départements ont signalé qu'ils espéraient élargir leur utilisation. Ces chiffres sont certes centrés sur les États-Unis, mais ils donnent une idée de l'ampleur de l'utilisation de ces outils par les gouvernements et des objectifs poursuivis.
>
> Depuis 2017, un total de 7,5 milliards de dollars américains a également été investi à l'échelle mondiale afin de financer des entreprises en démarrage spécialisées dans la reconnaissance faciale. Cependant, seulement 1,6 de ces 7,5 millions de dollars ont été consacrés à des entreprises canadiennes de TRF en démarrage. Au cours de la même période, le montant investi dans les TRF a augmenté de 105 %, ce qui semble indiquer que l'intérêt des entreprises pour la TRF augmente aussi. Nos estimations montrent également que la TRF est le 12e secteur le plus financé parmi les 25 secteurs d'intérêt de l'IA.

Plusieurs autres témoins ont mentionné l'utilisation déjà répandue de la TRF. Par exemple, Mme Watkins a noté que la RF est imposée aux conducteurs d'Uber, aux livreurs d'Amazon et aux fournisseurs de soins à domicile aux fins de vérification électronique de chaque visite. Il s'agit également d'un outil utilisé par de nombreux services de police aux États-Unis, sauf dans les villes qui l'interdisent ou qui ont imposé un moratoire sur l'utilisation de la TRF. Mme Wang a indiqué que la TRF est utilisée par des plateformes d'entrevue comme celle de HireVue. Rob Jenkins, professeur de psychologie à l'Université York au Royaume-Uni, a indiqué que plusieurs pays utilisent aussi la TRF aux contrôles frontaliers et dans d'autres processus, tel le renouvellement de passeport. Les utilisations particulières de la TRF au Canada seront abordées dans le Chapitre 2 du présent rapport.

9 Stanford University, Human-Centered Artificial Intelligence Institute, *Artificial Intelligence Index Report 2022* [DISPONIBLE EN ANGLAIS SEULEMENT]; Voir aussi : Nestor Maslej, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 9 juin 2022.

Diane Poitras, présidente de la Commission d'accès à l'information du Québec (CAI), a expliqué qu'en plus de la vérification d'identité, on utilise parfois le terme RF pour désigner des dérivés de la TRF, qui peuvent être utilisés à des fins commerciales dans les centres d'achat, où l'objectif n'est pas d'identifier l'individu, mais plutôt ses caractéristiques, comme son âge, son sexe, ou le temps qu'il passe à regarder un item[10].

Sanjay Khanna, conseiller stratégique et expert en prospective, a de son côté fait allusion à un avenir où la TRF pourrait être utilisée pour l'analyse de sentiments, par exemple pour des fins de manipulation commerciale, ou intégrée dans des robots de sécurité ou à des jeux de hasard. Toutefois, Mme Wang a indiqué ce qui suit concernant ce type de TRF :

> 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.

Avantages de la technologie de reconnaissance faciale

Plusieurs témoins ont reconnu que certaines utilisations de la TRF pouvaient être bénéfiques pour la société[11]. Par exemple, Mme Piovesan a indiqué que la TRF peut faciliter et accélérer le paiement en toute sécurité à la caisse d'un magasin ou sauver la vie d'un patient. Elle a mentionné l'utilisation de TRF dans le domaine de la santé pour aider à surveiller les patients et s'assurer que leur condition ne change pas. Elle a noté que la TRF peut être utile pour prouver l'identité d'un utilisateur afin d'accéder à des services bancaires ou à son téléphone. La TRF peut aussi être utile pour effectuer une transaction financière.

Françoys Labonté, président-directeur général du Centre de Recherche Informatique de Montréal, a fait remarquer qu'en général « les gens se font une idée favorable de l'utilisation des [TRF] pour des applications ciblées et clairement balisées, lorsqu'il est facile de comprendre à quelles fins les données sont utilisées et de voir les avantages qui en découlent ».

10 ETHI, *Témoignages*, Diane Poitras.

11 ETHI, *Témoignages*, Alex LaPlante; ETHI, *Témoignages*, Carole Piovesan; ETHI, *Témoignages*, Françoys Labonté; ETHI, *Témoignages*, Daniel Therrien; ETHI, *Témoignages*, Sanjay Khanna; ETHI, *Témoignages*, Owen Larter; ETHI, *Témoignages*, Rob Jenkins.

Mme McPhail, a mentionné l'utilisation pratique et répandue de la vérification faciale pour déverrouiller les téléphones, qui moyennant les bonnes protections intégrées, peut comporter relativement peu de risque pour la vie privée.

Owen Larter, directeur des Politiques publiques en matière d'intelligence artificielle responsable chez Microsoft, a affirmé que la TRF peut présenter de nombreux avantages. Parmi ceux-ci, il a lui aussi mentionné la vérification de l'identité à l'aide de la RF sur son téléphone ou son portable. Il a soulevé des applications bénéfiques de la TRF en matière d'accessibilité, notant que certaines organisations effectuent des travaux de recherche sur la façon d'utiliser la RF pour aider les personnes aveugles ou malvoyantes à mieux comprendre le monde qui les entoure et à mieux réagir. L'un de ces projets, le projet Tokyo, permet à une personne qui est aveugle équipée d'un casque d'écoute de balayer une pièce et être en mesure d'identifier les personnes qui ont accepté de faire partie de son système de RF, lui permettant ainsi de reconnaître ces personnes et d'entamer une conversation. M. Larter a également mentionné une application qui cherche à aider les personnes atteintes d'Alzheimer ou de maladies similaires à reconnaître leurs amis et proches[12].

M. Khanna a de son côté rapporté que la TRF peut être bénéfique lorsqu'elle est utilisée afin de prévenir les accidents de travail, par exemple pour éviter que des employés s'endorment ou manquent d'attention.

Dubi Kanengisser, conseiller principal en analyse stratégique et politique de la Commission des services policiers de Toronto (CSPT), a expliqué que la RF peut être un outil additionnel utilisé par les forces de l'ordre afin de s'acquitter de leur fonction d'identifier des criminels et des victimes.

Daniel Therrien, l'ancien commissaire à la protection de la vie privée du Canada, a indiqué que la RF peut être utilisée pour des crimes graves, comme les disparitions d'enfants, et pour d'autres objectifs impérieux de l'État, comme dans le contexte des frontières, afin de garantir que les personnes suspectes puissent être identifiées sans entraver le flux des voyageurs vers le pays.

Kristen Thomasen, professeure de droit de la University of British Columbia, a toutefois souligné que la vie privée est un bien social qui profite à tous. Cela inclut les femmes et les enfants qui sont souvent au cœur du fil narratif selon lequel l'une des utilisations bénéfiques de la RF est de protéger les groupes marginalisés ou victimisés dans certains contextes comme la traite de personnes ou l'abus d'enfants. Elle a convenu qu'il faut reconnaître ces utilisations bénéfiques de la TRF, mais en nuançant considérablement ce

12 Microsoft, Project Tokyo [DISPONIBLE EN ANGLAIS SEULEMENT].

fil narratif, car l'érosion de la vie privée en tant que bien social causera aussi un préjudice aux femmes et aux enfants. Selon elle, la TRF renforce et perfectionne la surveillance et plus cette surveillance est perfectionnée, plus de préjudice à la vie privée et d'inégalité il peut y avoir.

Mme Thomasen a donc insisté sur le fait que la TRF n'est pas inévitable et que la mise en évidence de certains cas d'utilisation bénéfique ne devrait pas être suffisante pour limiter la réflexion que l'on porte sur les inconvénients potentiels d'une utilisation plus répandue de cette technologie. Ana Brandusescu, une experte en gouvernance de l'intelligence artificielle, et Mme Poitras ont aussi fait une mise en garde contre la banalisation des risques que la TRF engendre en raison de sa popularité ou du fait qu'elle soit vue comme une commodité.

Préoccupations liées à la technologie de reconnaissance faciale

Erreur d'identification et biais algorithmiques

La plus grande préoccupation liée à l'utilisation de la TRF est le potentiel d'erreur d'identification. Par exemple, Cynthia Khoo, chercheuse universitaire affiliée au Center on Privacy and Technology de l'école Georgetown Law à Washington D.C. et au Citizen Lab de l'Université de Toronto, a indiqué que selon les chercheurs, la TRF peut entraîner cent fois plus d'erreurs d'identification pour les personnes noires et asiatiques. Ce genre d'erreur se produirait aussi plus d'une fois sur trois dans le cas de femmes à la peau plus foncée, alors que pour les hommes blancs, la TRF fonctionne à 99% d'efficacité. Cependant, Mme Wang a noté que bien que les modèles développés en Asie aient également beaucoup de biais, « [i]l s'agit simplement de biais différents de ceux des modèles élaborés par des Canadiens ou des Américains ».

Mme Brandusescu a fourni des statistiques similaires à celles fournis par Mme Khoo :

> La TRF distingue mieux les visages des hommes blancs que les visages noirs, bruns, autochtones et transgenres. Nous le savons grâce aux travaux révolutionnaires d'universitaires comme Joy Buolamwini et Timnit Gebru. Leur étude a révélé que:
>
> [...] les femmes à la peau plus foncée constituent le groupe le plus incorrectement classé (avec des taux d'erreur allant jusqu'à 34,7 %). Le taux d'erreur maximal pour les hommes à la peau claire est de 0,8 %.

Des témoins ont fait référence à une étude menée par le National Institute of Standards and Technology des États-Unis (NIST), qui a démontré que certains algorithmes

performent moins bien pour certains groupes démographiques[13]. Ce rapport conclut entre autres que parmi les algorithmes développés aux États-Unis, les taux de faux positifs sont plus élevés pour les Asiatiques et les Afro-Américains comparativement aux images de personnes de race blanche. Pour les images utilisées par les forces de police locales, le taux de faux positifs les plus élevés concernaient les personnes autochtones. Le rapport a aussi trouvé un plus haut taux de faux positifs chez les femmes que chez les hommes, et des taux plus élevés de faux positifs chez les personnes âgées et les enfants.

Mme Piovesan a aussi soulevé des préoccupations relatives à l'exactitude et l'objectivité des résultats des systèmes, de même que les pratiques de surveillance illégales et arbitraires, et le fait que la technologie est souvent de type boîte noire et qu'elle échappe aux législateurs, de sorte à entraver la liberté et à mettre en danger les valeurs fondamentales qui sont consacrées à la *Charte canadienne des droits et libertés*. Alex LaPlante, directrice principale, Engagement produit et commercial, chez Borealis AI, a fait des commentaires similaires en indiquant :

> [S]i nous ne prenons pas soin d'évaluer correctement l'application, le développement et la gouvernance de l'intelligence artificielle, celle-ci peut avoir des effets négatifs sur les utilisateurs finaux, perpétuer et même amplifier la discrimination et les préjugés envers les communautés racisées et les femmes, et conduire à une utilisation non éthique des données et à des atteintes au droit à la vie privée.

En fait, selon Mme Watkins, les technologies comme l'IA, l'apprentissage automatique et les technologies algorithmiques fondées sur des données recueillies au fils des ans et des décennies reflètent les préjugés humains, comme le racisme et le sexisme institutionnels. Il s'agit de processus « très conservateurs et profondément archaïques, et ils perpétuent les préjugés dont nous, en tant que société, devrions nous débarrasser ».

Cependant, certains témoins ont noté que la TRF a fait beaucoup de progrès. Par exemple, M. Jenkins a noté que des progrès impressionnants ont été réalisés dans les cinq dernières années pour que les systèmes de RF identifient bien les visages. M. Maslej a indiqué ce qui suit :

> En 2017, certains des algorithmes de reconnaissance faciale les plus performants affichaient des taux d'erreur allant d'environ 20 à 50 % selon certains ensembles de données des [Facial Recognition Vendor Test]. En 2021, aucun n'a affiché un taux d'erreur supérieur à 3 %, les modèles les plus performants enregistrant un taux d'erreur

13 ETHI, *Témoignages*, Alex LaPlante; Coalition pour la surveillance internationale des libertés civiles, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 13 avril 2022 [*Mémoire CSILC*], p. 4; National Institute for Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, décembre 2019 [DISPONIBLE EN ANGLAIS SEULEMENT].

> de 0,1 %, ce qui signifie que ces modèles identifient correctement 999 des 1 000 visages analysés.

Malgré cela, quelques témoins ont soulevé le fait que même si la TRF fonctionnait de façon optimale, elle serait tout de même préoccupante[14]. Par exemple, Mme Khoo a indiqué que même si la TRF fonctionnait à la perfection, elle risque d'être utilisée au détriment des groupes sociaux historiquement victimes d'oppression systémique. Mme McPhail a fait des commentaires similaires :

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

Mme Thomasen a de son côté indiqué qu'il faut examiner la surveillance faciale à la lumière de son évolution historique, qui émane des idéologies eugéniques et de suprématie blanche. Elle a aussi mis en garde contre la surveillance faciale à des fins personnelles, qui peut être préjudiciable en ce qui concerne le harcèlement, l'extorsion et d'autres formes de violence facilitée par la technologie.

D'un point de vue technique, Mme Wang a expliqué que puisque les modèles d'apprentissage automatique cherchent à repérer les constantes parmi les données, ils amplifient souvent les biais qui existent dans ces données. Elle a donné l'exemple suivant pour illustrer ce point :

> 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 amplifier[ont] ce taux par rapport au taux de base de la corrélation réelle.

Elle a aussi souligné que même si on réussissait à corriger les problèmes de distorsion des résultats entre les groupes démographiques, deux problèmes persisteraient : la fragilité (moyens connus qui permettent aux utilisateurs malveillants d'altérer les modèles de RF pour les contourner et en fausser les résultats); et les problèmes

14 ETHI, *Témoignages*, Kristen Thomasen; ETHI, *Témoignages*, Tim McSorley; ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Angelina Wang.

d'interprétation des modèles : il est extrêmement difficile de découvrir l'ensemble précis de règles sur lesquelles s'appuie le modèle pour prendre ces décisions[15].

Autres préoccupations

Tim McSorley, le coordinateur national de la Coalition pour la surveillance internationale des libertés civiles (CSILC), a de son côté soulevé trois préoccupations principales à l'égard de la TRF : les algorithmes biaisés et inexacts perpétuent le racisme systémique et le profilage racial; la reconnaissance faciale permet une surveillance de masse sans discernement et sans mandat; et le manque de réglementation, de transparence et de responsabilisation de la part des organismes d'application de la loi et des services de renseignements du Canada[16].

Patricia Kosseim, commissaire à l'information et la protection de la vie privée de l'Ontario, a noté en ce qui concerne l'utilisation de la TRF, la plus grande crainte des commissaires à travers le Canada est la surveillance de masse, qu'elle soit faite par une tierce partie du secteur privé au nom de la police ou par le service de police lui-même. Mme McPhail a noté qu'en plus du droit à l'égalité :

> [L]es outils permettant une identification omniprésente auraient des répercussions négatives sur toute une série de droits protégés par la Charte canadienne des droits et libertés et d'autres lois, notamment la liberté d'association et de réunion, la liberté d'expression, le droit à la protection contre les fouilles, les perquisitions et les saisies abusives par l'État, la présomption d'innocence […] et, enfin, les droits à la liberté et à la sécurité de la personne.

Une autre préoccupation à l'égard de la TRF découle du fait que les gens ne sont pas toujours au courant que leur visage fait partie d'un ensemble de données utilisé par la TRF. Le cas de Clearview AI est un exemple d'une telle situation. Mme Wang a expliqué que « 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 ».

Selon M. Jenkins, lorsqu'une image est intégrée aux algorithmes de la TRF, il devient impossible d'éliminer l'influence de cette image sur l'algorithme. Il a aussi expliqué que l'apparence et le visage sont uniques à chacun et se définissent par le principe de la variabilité intrapersonnelle, c'est-à-dire le fait que notre apparence change constamment. Ce principe est un facteur important dans la reconnaissance faciale

15 ETHI, *Témoignages*, Angelina Wang.

16 Voir aussi : Mémoire CSILC.

puisqu'il implique non seulement le vieillissement naturel du visage, mais également des facteurs tels l'angle, l'éclairage, ou l'expression faciale d'une personne. La variabilité intrapersonnelle cause ainsi plusieurs variations, ce qui pose un obstacle difficile à surmonter lors de l'utilisation de la TRF.

M. Jenkins a aussi noté que la surveillance humaine permet de repérer les erreurs flagrantes. Il a cependant indiqué que la reconnaissance des visages par les humains n'est pas infaillible et peut donc elle aussi introduire des erreurs dans le système[17].

Mme Poitras a de son côté soulevé les risques pour la vie privée que pose la création de banques de données biométriques, notant entre autres le risque qu'elles soient utilisées à des fins autres que celles prévues à l'insu des personnes concernées et sans évaluation adéquate des risques liés à cette nouvelle utilisation. Les failles de sécurité et fuites potentielles de données biométriques ont aussi été soulevées par des témoins[18].

Enfin, pour plusieurs témoins, la nature immuable du visage, qu'on ne peut remplacer comme on le fait avec un mot de passe, rend la TRF d'autant plus envahissante[19].

CHAPITRE 2 : TYPES D'UTILISATION ET RISQUES LIÉS

> **« On ne peut pas demander à un logiciel d'assumer des responsabilités légales et morales que des humains ont par ailleurs abdiqué[e]s à l'égard de la vie et de la liberté de personnes vulnérables. »**
>
> Cynthia Khoo, chercheuse universitaire,
> qui a comparu devant le Comité le 21 mars 2022 à titre personnel.

Au-delà d'observations générales à l'égard de la TRF, certains témoins ont discuté de plusieurs types d'utilisation spécifiques de la TRF.

Offrant une vue d'ensemble des différents types d'application de la TRF, Mme Watkins a noté que l'utilisation de cette technologie par des organisations gouvernementales, tels

17 Voir aussi : Rob Jenkins, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 4 avril 2022.

18 Ligue des droits et libertés, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 15 avril 2022, p. 5 [*Mémoire Ligue des droits et libertés*]; Mémoire Tessono, p. 8.

19 ETHI, *Témoignages*, Angelina Wang; ETHI, *Témoignages*, Daniel Therrien; ETHI, *Témoignages*, Diane Poitras.

les services de police, les autorités frontalières et le gouvernement en général, présente un haut risque. Selon elle, non seulement les machines ne sont pas encore assez fiables, mais elles supposent également que les constructions sociales, comme la race et le sexe, sont lisibles par machine sur le visage d'une personne ce qui, à son avis, « est tout simplement faux ». Elle a rajouté que les technologies d'IA, comme celle de Clearview AI, ne sont pas encore assez précises et ne devraient pas être utilisées dans des scénarios à haut risque, où des vies et des moyens de subsistance sont en jeu.

L'une des scénarios à haut risque dont les témoins ont discuté est l'utilisation de la TRF par les forces policières.

Utilisation de la reconnaissance faciale par les forces policières

Critiques

Selon Mme Khoo, l'un des plus grands problèmes liés à l'utilisation de TRF par les forces policières est le manque de transparence. Le public apprend souvent que la technologie a été utilisée en raison des médias, par des fuites de renseignements et des demandes d'accès à l'information. M. McSorley et Mme McPhail ont eu aussi noté le manque de transparence des forces policières au Canada. Mme McPhail a décrit la situation au Canada comme « une véritable crise de responsabilisation dans l'utilisation de ces technologies par la police ».

M. Jenkins a critiqué l'aspect de la fiabilité de la TRF. Il a comparé différentes méthodes d'identification utilisées par les forces policières, comme les empreintes digitales, à celle de la RF, pour démontrer l'existence de techniques plus fiables, dans certaines circonstances. D'autres méthodes plus traditionnelles ne rencontrent pas le même nombre de problèmes techniques que la TRF comme le changement de l'apparence du visage, l'éclairage, la distance du visage de l'objectif de l'appareil.

Pour M. 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 ». Il a reconnu qu'il faut aussi « éviter l'erreur inverse, à savoir ne pas appréhender quelqu'un qui pourrait représenter un grand danger pour d'autres personnes ».

Mme Khoo, Mme Brandusescu, Mme McPhail et Mme Wang ont chacune mentionné des erreurs d'identification d'hommes noirs aux États-Unis qui ont mené à des arrestations injustifiées. Mme Khoo, a identifié Robert Williams, Nijeer Parks et Michael Olivier comme exemples :

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

Mme McPhail a cependant indiqué ne pas être au courant de cas similaires ou la fausse identification d'un individu aurait mené à des accusations criminelles au Canada. Elle a noté que cela s'explique par le fait que les forces policières au Canada se sont montrées prudentes et modérées dans l'adoption de cette technologie et qu'elles l'ont utilisée de façon relativement limitée.

Mme Khoo a dit que pour les militants de la justice raciale que ses collègues et elles ont rencontrés dans le cadre des recherches qui ont mené au rapport du Citizen Lab, l'utilisation de technologies algorithmiques policières représente de la violence étatique version XXIe siècle : avant, on utilisation des stylos et du papier, alors que maintenant, on utilise des ordinateurs et des algorithmes[20].

Mme Brandusescu a fait remarquer l'existence du racisme systémique dans les services de police du Canada, notant que ce fait a été reconnu par le Comité permanent de la sécurité publique et nationale de la Chambre des communes dans un rapport de 2021[21]. Selon elle, la TRF exacerbe le racisme systémique.

Mme McPhail, de son côté, a indiqué que l'utilisation par la police de la TRF dans des bases de données de photos signalétiques existantes est en soi problématique puisque ces dernières présentent leurs propres problèmes de partialité et de discrimination. La CSILC a fait des commentaires similaires[22].

Sharon Polsky, présidente du Conseil du Canada de l'accès et la vie privée, qui a mené des consultations auprès des forces policières au sujet de l'utilisation de la RF, a souligné qu'à son avis, les agents de police, comme la plupart des habitants du Canada,

---

20 The Citizen Lab, Kate Robertson, Cynthia Khoo, and Yolanda Song, *To Surveil and Predict – A Human Rights Analysis of Algorithmic Policing in Canada*, 1 septembre 2020 [DISPONIBLE EN ANGLAIS SEULEMENT].

21 Comité permanent de la sécurité publique et nationale (SECU), *Racisme systémique au sein des services policiers au Canada*, juin 2021.

22 Mémoire CSILC, p. 5.

ne comprennent pas vraiment ce que la TRF peut faire ni les exigences de conformité à la loi[23].

Risque de surveillance de masse menée par les forces policières

Certains témoins ont soulevé la possibilité que les activités des forces policières mènent à une surveillance de masse[24]. M. McSorley s'est penché sur l'exemple de la GRC :

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

Gordon Sage, directeur général, Services d'enquêtes spécialisées et de nature délicate de la GRC, a expliqué ne pas être d'avis que la simple utilisation de la TRF implique une surveillance de masse, même en ce qui concerne l'utilisation de la technologie de Clearview AI, qui compare les images recherchées dans une base de données de trois milliards d'images du public.

Paul Boudreau, sous-commissaire par intérim des Services de police spécialisés de la GRC, a rapporté que la GRC n'effectue pas de surveillance active, et n'enregistre pas les protestations de masse à l'aide de la TRF. Mustafa Farooq, président-directeur du Conseil national des musulmans canadiens (CNMC), a toutefois indiqué que son organisation reçoit des appels constants de personnes faisant l'objet de surveillance de la part du Service canadien du renseignement de sécurité (SCRS) ou de la GRC lors de rassemblements ou de manifestations. M. Sage, de la GRC, a réfuté cette allégation en assurant au Comité que la GRC n'utilise aucune TRF pour la surveillance de masse. Il a rajouté que la seule TRF utilisée par la GRC était celle de Clearview AI, mais que cette utilisation a cessé en juillet 2020.

M. Therrien a indiqué ne pas avoir de raison de mettre en doute la déclaration de la GRC selon laquelle elle ne fait pas de surveillance de masse ni n'utilise la TRF pour le faire, même si la définition des circonstances dans lesquelles la GRC utilise ce type de technologie lui semblait ambiguë.

---

23 Voir aussi : Conseil du Canada de l'accès et la vie privée, *Utilisation de la reconnaissance faciale par les forces de l'ordre du Canada : Réalités, réserves et recommandations*, 15 octobre 2021. Ce document a été remis au Comité comme document de référence. La version originale en anglais est disponible en ligne.

24 ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Tim McSorley.

Colin Stairs, directeur de l'information du Service de police de Toronto (SPT), a rassuré le Comité que le SPT n'effectue pas de surveillance de masse, qu'il ne prend pas des photos de manifestants de façon méthodique et ne soumet donc aucune photo de ce type à la RF. Il a rajouté que le SPT utilise la TRF comme moyen d'enquête et non comme un moyen de surveillance ou de reconnaissance qui porterait atteinte à la vie privée. Par exemple, il a expliqué au sujet de l'utilisation de la RF par le SPT :

> Notre façon de faire est de prélever des photos des lieux du crime captées par des caméras qui enregistreraient de toute manière la rue, et de comparer ces images fixes à celle des bases de données de photos anthropométriques, ce qui ressemble beaucoup à la déposition d'un témoin oculaire. La différence n'est pas notable.

Dans la même vague d'idée, M. Kanengisser a indiqué que tout ce qui se range dans la catégorie de « surveillance de masse » est une utilisation déraisonnable de la TRF. Par exemple, le suivi d'un grand nombre d'individus sans faire de distinctions serait inacceptable aux yeux de la CSPT – tout comme le serait l'emploi de techniques dont on peut prouver l'inexactitude, les erreurs d'identification et les dommages qu'elles sont susceptibles de créer. Par exemple, l'arrestation liée à une erreur d'identification faite par un logiciel, mais non confirmée par un être humain, est inacceptable.

Les sections suivantes discutent davantage de l'utilisation de la TRF par la GRC et le SPT, dont l'utilisation de la TRF de Clearview AI.

Utilisation par la Gendarmerie Royale du Canada

Selon M. McSorley, la GRC a utilisé différentes formes de RF au cours des 20 dernières années sans en informer le public, sans débat public sur la question et sans informations claires sur la surveillance. M. Boudreau a confirmé que « la GRC emploie la reconnaissance faciale depuis très longtemps » sous différentes formes, mais précisé que les TRF nouvelles « comme Clearview, nous ne les employons pas ». M. Sage a aussi indiqué que la GRC n'utilise pas la TRF à l'heure actuelle. La GRC a clarifié son témoignage relatif à l'utilisation de la TRF dans une lettre au Comité en juillet 2022[25].

25 Gendarmerie Royale du Canada, *Lettre au Comité*, 21 juillet 2022. La lettre clarifie le témoignage de la GRC sur l'utilisation de la technologie de reconnaissance faciale (TRF). Elle indique que la GRC utilise certaines TRF qui n'avaient pas été mises en évidence comme tels auparavant, à savoir Spotlight et Traffic Jam. Ces deux outils utilisent la reconnaissance faciale, et d'autres éléments, pour aider les forces de l'ordre à identifier les victimes d'exploitation sexuelle, de traite des personnes et les personnes disparues qui risquent d'être exploitées, en effectuant des recherches sur des sites Web ouverts. Aucun de ces outils n'a encore été évalué par le Programme national de l'intégration de la technologie (PNIT). La lettre fournit également une liste de l'utilisation de TRF par la GRC, une liste de l'utilisation future probable de nouvelles technologies et décrit le processus d'approbation pour l'achat de licences auprès de Clearview AI.

Cependant, la GRC a admis avoir utilisé la TRF de Clearview AI dans le passé. M. Sage et M. Boudreau ont confirmé que deux licences ont été achetées en octobre 2019 et qu'elles ont été utilisées jusqu'en juillet 2020, lorsque Clearview AI s'est retirée du marché canadien.

M. Sage a indiqué croire que c'est un enquêteur du Centre national de coordination contre l'exploitation des enfants (CNCCE) qui a d'abord obtenu la licence. Il a ajouté que le directeur général de l'époque n'a pas été informé de cet achat lorsqu'il a été effectué. Il a aussi noté que l'employé en question n'a pas fait l'objet d'une enquête. M. Boudreau a aussi confirmé qu'aucun agent de la GRC n'a été réprimandé concernant l'utilisation de la TRF de Clearview AI.

M. Boudreau a expliqué que la GRC est sans cesse à la recherche de technologies nouvelles, qu'il s'agisse de la TRF ou d'autres technologies, c'est pourquoi les différentes divisions étudient et évaluent de nouvelles technologies. Mais il a dit que lorsque la GRC a appris qu'un nombre limité de programme et services de la GRC avait commencé à employer Clearview AI, une enquête interne a été lancée.

M. Sage a précisé que comme il n'y avait pas de politique en vigueur au moment où la licence a été obtenue, « les agents sur le terrain pouvaient obtenir des licences comme bon leur semblait ». M. Sage a rajouté qu'aucune évaluation de conformité de la technologie avec la Charte n'avait eu lieu à ce moment-là. La GRC a aussi confirmé qu'aucune évaluation éthique n'avait été faite avant que la TRF de Clearview AI ne soit utilisée[26]. Roch Séguin, directeur à la sous-direction des Services stratégiques, Opérations techniques, a affirmé que la GRC n'a fait appel au ministère de la Justice concernant l'utilisation des TRF pour ses enquêtes qu'à une reprise, mais à l'interne.

M. Sage a expliqué que la TRF de Clearview AI a été testée par plusieurs membres de la GRC, soit en utilisant leurs propres photos, à partir de profil et de médias sociaux, ou celles de célébrités. Les tests ont démontré que cette technologie n'était pas toujours efficace puisqu'elle comportait certains problèmes d'identification. Elle est donc devenue un outil parmi tant d'autres exigeant une intervention humaine.

M. Sage a précisé que la TRF n'a été utilisée dans le cadre d'enquêtes de la GRC qu'à trois occasions : le CNCCE s'en est servi à deux occasions afin d'identifier certaines victimes de crimes graves et pour mettre en place des mesures permettant d'assurer la protection des victimes se trouvant au Canada. La troisième occasion était pour localiser un fugitif se trouvant à l'étranger en collaboration avec d'autres forces policières. Il a rassuré le Comité que l'utilisation de la TRF par la GRC n'a jamais donné lieu à des

26 Gendarmerie royale du Canada, *Lettre confidentielle au Comité*, 3 juin 2022.

poursuites judiciaires au Canada[27]. M. Boudreau a aussi spécifié qu'une intervention humaine devait toujours été présente dans l'analyse des résultats.

Cependant, le rapport du CPVP quant à l'utilisation de la TRF de Clearview AI a identifié que seulement 6% des recherches effectuées par Clearview AI semblent liées à l'identification de victimes pour le CNCCE, alors que la GRC n'a fourni aucune justification pour environ 85 % des recherches[28]. Selon M. Sage, 6% des recherches ont été réalisées dans les trois dossiers susmentionnés, alors que les 85% restant représentent les essais pour tester la technologie.

M. Therrien a expliqué qu'à la suite de son enquête, le CPVP a conclu que la GRC n'avait pas pris de mesures pour vérifier la légalité de la collecte de renseignements par Clearview AI et qu'elle ne disposait d'aucun système lui permettant de s'assurer que les nouvelles technologies utilisées par l'entreprise soient conformes à la loi. Le CPVP a déterminé que l'usage de la TRF de Clearview AI était illégal puisqu'il reposait sur la collecte et l'utilisation illégale d'images faciales par son partenaire commercial.

Le CPVP a aussi conclu qu'il y avait des « manquements graves et systémiques à l'obligation de se conformer à la Loi avant de recueillir des renseignements personnels de Clearview et, de façon générale, avant toute nouvelle collecte de renseignements personnels »[29]. M. Therrien a indiqué que les mots utilisés dans le rapport renvoient au fait qu'au moment de l'enquête la GRC n'avait pas de mécanismes de vérification et d'approbation en place pour veiller à ce que lorsque de nouvelles technologies sont utilisées par ses agents, elles respectent la loi et le droit à la vie privée.

M. Therrien a expliqué la GRC a contesté les conclusions du CPVP selon lesquelles elle n'a pas respecté l'article 4 de la *Loi sur la protection des renseignements personnels* en utilisant la technologie de Clearview AI. Il a noté que la GRC affirme que cet article n'exige pas explicitement qu'une institution fédérale s'assure de la légalité des pratiques de son partenaire commercial avant que le secteur public n'utilise l'information[30].

---

27 Par exemple, Gordon Sage a indiqué que la TRF a permis d'identifier et de trouver un enfant victime d'exploitation sexuelle alors que les méthodes traditionnelles avaient échoué pendant les 9 à 10 dernières années.

28 *Rapport spécial du CPVP sur la GRC*, para 18.

29 *Ibid*., para 87.

30 Clearview AI a contesté les conclusions du CPVP et les ordonnances rendues par les commissaires provinciaux. Le commissaire fédéral n'a pas le pouvoir de rendre des ordonnances. Voir : ETHI, *Témoignages*, Brenda McPhail; et ETHI, *Témoignages*, Diane Poitras. Au Québec, Clearview AI conteste l'ensemble de la décision de la Commission d'accès à l'information du Québec (CAI) devant les tribunaux, y compris la compétence de la CAI à l'égard d'une société américaine.

M. Therrien a convenu l'exigence susmentionnée n'est pas explicite, mais indiqué que l'article 4 de la *Loi sur la protection des renseignements personnels* le fait implicitement. Autrement, les institutions fédérales pourraient, par l'entremise de contrats avec le secteur privé, s'engager dans des pratiques qu'elles ne peuvent pas adopter directement. Il a recommandé de combler l'ambiguïté dans la *Loi sur la protection des renseignements personnels* en exigeant explicitement que les institutions gouvernementales qui y sont assujetties s'assurent que ce qu'elles achètent est légal lorsqu'elles font appel au secteur privé.

M. Boudreau et M. Sage ont confirmé que la GRC n'est pas d'accord avec toutes les conclusions du rapport du CPVP, mais appuie ses recommandations.

En effet, M. Therrien a souligné que malgré la position de la GRC, elle fournit des efforts continus, en collaboration avec le CPVP, pour adopter un meilleur mécanisme de vérification des outils de technologie, qu'il s'agisse de la RF ou d'autres outils. Lors de sa comparution, il a indiqué que la GRC ne réussirait probablement pas à mettre en œuvre toutes les recommandations du CPVP dans la période de 12 mois recommandée, mais il a dit considérer les efforts de la GRC sincères.

M. Séguin a expliqué que les recommandations du CPVP ont mené à l'aboutissement d'une stratégie nationale d'intégration des technologies en mars 2021 : le Programme national d'intégration de la technologie (PNIT). Depuis, la GRC a fait des progrès considérables quant à la mise en œuvre du PNIT afin de s'assurer que les technologies sont évaluées avant d'être utilisées dans le cadre d'opération et d'enquête. Il a indiqué que le PNIT devait être en place en juin 2022, à l'intérieur des 12 mois recommandés par le CPVP, mais noté que la formation du personnel pourrait ne pas être complétée à ce moment-là[31].

M. Séguin a discuté des principaux piliers du PNIT :

> En ce qui concerne les principaux piliers du [PNIT], ou sensibilisation des intervenants et partenariat, qui comprend la formation, il y a évidemment l'examen des politiques en cours d'élaboration, qui sert à cerner toutes les lacunes des politiques existantes ainsi qu'à modifier et mettre à jour les nouvelles politiques. Il y a une partie d'évaluation technologique, pour laquelle nous avons élaboré un processus d'admission complet qui procède d'une série de questionnaires. De plus, nous mettons en place un inventaire des technologies pour la surveillance de la sensibilisation. La dernière composante sera la sensibilisation du public et la transparence.

31 Gendarmerie Royale du Canada, *Lettre au Comité*, 21 juillet 2022. En date du 21 juillet 2022, dans son état opérationnel préliminaire actuel, le Programme national d'intégration de la technologie (PNIT) a vu 31 nouvelles technologies soumises à l'examen. La lettre offre des détails sur le PNIT.

M. Boudreau a indiqué que le PNIT permet d'examiner toutes les nouvelles technologies du point de vue légal, éthique, et en matière de protection de la vie privée. Il a rajouté que la GRC croit que l'utilisation de RF doit « être ciblée, limitée dans le temps et assujettie à des vérifications effectuées par des experts formés » et qu'elle « ne doit pas servir à confirmer l'identité, mais plutôt être considérée comme un outil d'enquête dont les résultats doivent être confirmés, encore une fois, par une intervention humaine ».

Selon les représentants de la GRC, les partenaires de la GRC devront suivre ses politiques[32]. M. Séguin a également rassuré le Comité que pour ce qui est de « la transparence et de la sensibilisation du public, la divulgation des catégories de technologies que la GRC utilisera dans l'avenir fait partie intégrante de notre stratégie de communication ».

M. Sage a rajouté que la PNIT permet d'évaluer les risques et les enjeux éthiques associés à la technologie visée, en incluant une évaluation des facteurs relatifs à la protection de la vie privée. Il a mentionné dans le cadre des efforts de la GRC pour adopter de nouvelles façons de faire les choses, l'organisation a « dépêché un employé au Commissariat et demandé qu'un membre de leur personnel travaille au sein de nos services dans le but de consolider les liens et la mise en commun des connaissances entre les deux organisations ».

M. Boudreau a rajouté que lorsque la GRC se penche sur les technologies comme la TRF, il faut tenir compte de l'aspect juridique, de la protection de la vie privée, de l'analyse comparative entre les sexes et des biais, en plus d'assurer qu'il y ait une intervention humaine.

Quant à l'usage futur de la TRF par la GRC, M. Sage a dit qu'il était malheureux de ne pas pouvoir utiliser la TRF dans les cas d'exploitation d'enfants, afin d'identifier les victimes. Selon lui, il s'agit d'un dossier urgent. Il a dit attendre une décision des opérations techniques nationales, comme l'exige le processus du PNIT, pour faire une évaluation de l'utilisation de la TRF. Une fois l'évaluation complétée, il espère avoir la permission de se servir de la TRF pour le bien-être des victimes en danger.

Malgré les mesures prises par la GRC, Rizwan Mohammad, agent des services d'assistance judiciaire pour le CNMC, a indiqué que le CNMC est choqué de la désinvolture de la GRC dans sa façon d'aborder la question de l'utilisation de Clearview AI. Il a noté que la GRC a d'abord nié avoir utilisé la TRF de Clearview AI pour ensuite

32 ETHI, *Témoignages*, Gordon Sage; ETHI, *Témoignages,* Rock Séguin.

confirmer avoir utilisé le logiciel, tout en indiquant que l'utilisation de la TRF n'était pas largement connue au sein de la GRC.

L'utilisation par la GRC d'autres technologie liée à la RF a aussi été soulevée par certains témoins. Par exemple, M. McSorley a rapporté que la GRC a passé un contrat avec la compagnie IntelCenter, un système américain privé de « reconnaissance faciale des terroristes » qui offre « un accès à des outils de reconnaissance faciale et à une base de données de plus de 700 000 images de personnes associées au terrorisme ». L'entreprise dit extraire les images du Web, comme Clearview AI. Selon lui, l'utilisation d'IntelCenter par les forces de l'ordre est très préoccupante puisqu'il s'agit d'un programme qui pousse la stigmatisation plus loin que Clearview AI en affirmant savoir que les images appartiennent à des personnes en lien avec le terrorisme sans que l'on puisse vérifier le cheminement menant à cette conclusion. Ces données sont ensuite utilisées par les forces de l'ordre.

Cependant, M. Sage a indiqué que le logiciel d'IntelCenter a été acquis par la GRC uniquement aux fins d'essai à l'interne. Il n'a pas été testé ou utilisé dans le cadre d'enquêtes sur la sécurité nationale ou à d'autres fins opérationnelles. De plus, il a précisé qu'en mars 2018, lorsque la GRC a appris que le logiciel de service d'IntelCenter n'était pas approuvé pour de fins opérationnelles, « la Division E a cessé de l'utiliser ».

Enfin, M. Sage a noté que le projet Arachnid du Centre canadien de protection de l'enfance gère, qui collabore avec le CNCCE, n'utilise pas la TRF. La recherche menée par ce programme se fait par mot-clic (défini comme l'ADN d'une photographie) pour fouiller l'Internet[33].

Utilisation par le Service de Police de Toronto

Colin Stairs a confirmé que le SPT utilise la TRF pour comparer des photos sondes trouvées en enquêtant avec les photos de son Intellibook, soit la base de données des photos d'identité judiciaire du SPT. M. Stairs a rassuré le Comité que les images des caméras corporelles utilisées par le SPT ne sont pas versées dans la base de données des photos signalétiques et a noté qu'il n'y a « aucune connexion et aucun lien automatisé entre les caméras corporelles et le système Intellibook ». Il a affirmé que le SPT mène ses activités en conformité avec la *Loi sur l'identification des criminels* et n'utilise donc que des photos d'identité judiciaire, qui provienne d'arrestations et du traitement de

33 Centre canadien de protection de l'enfance, *Projet Arachnid*; Voir aussi : ETHI, *Assurer la protection de la vie privée et de la réputation sur les plateformes comme PornHub*, juin 2021. Le rapport discute du Projet Arachnid.

dossiers. Clearview était une anomalie à cet égard. Le SPT ne se sert pas d'images faciales d'origine publique dans son programme de reconnaissance faciale.

M. Stairs a reconnu qu'il y a une série de problèmes connus par rapport à l'analyse des visages dans différents ensembles d'apprentissage. Il a expliqué que le SPT a choisi la TRF utilisée en tenant compte de la minimisation de biais racial, tout en reconnaissant que les biais qui font partie intégrante des systèmes photographiques demeurent présents (p. ex., les biais sur les visages plus clairs comparativement aux visages plus foncés). C'est pourquoi le SPT utilise « un seuil inférieur » qui englobe ce que le SPT ne considère pas comme une correspondance. Une correspondance n'est pas une confirmation d'identité : l'identité doit être corroborée en utilisant d'autres méthodes.

M. Stairs a affirmé que les TRF peuvent être utiles lorsque des témoins ou des sujets inconnus sont impliqués dans des crimes violents ou des affaires importantes. Leur utilité est cependant limitée par l'étendue de la base de données de photos signalétiques du SPT et les limites imposées par le *Code criminel* et la *Charte canadienne des droits et libertés*.

M. Stairs a confirmé que l'utilisation de la TRF par le SPT est toujours accompagnée par une analyse humaine effectuée par le service de l'identité judiciaire. Il a précisé : « [U]n technicien saisit l'image dans le système et exécute le programme et regarde le résultat. » Il a dit croire que toute information reliée à l'utilisation de la TRF par le SPT dans le cadre d'une enquête suivant une arrestation est communiquée au tribunal ou au prévenu.

En février 2022, la CSPT a adopté une politique d'utilisation de l'IA (politique sur l'IA)[34]. M. Kanengisser a expliqué qu'en vertu de la politique sur l'IA, le recours à la TRF ou d'autres technologies biométriques est considéré comme étant à « haut risque ». Considérant ce niveau de risque, des examens approfondis doivent être complétés avant l'adoption ou le déploiement de cette technologie[35]. Un suivi de la technologie est aussi assuré pour une durée d'au moins deux ans afin d'examiner ses répercussions, y compris ses conséquences imprévues.

34 Toronto Police Services Board, *Politique d'utilisation de l'intelligence artificielle*, 22 février 2022

35 ETHI, *Témoignages*, Remarques introductives, Dubi Kanengisser. Le Service de police de Toronto (SPT) devra démontrer un besoin réel et un plan d'atténuation des risques de partialité ou de violation de la vie privée ou d'autres droits pour pouvoir adopter un nouvel outil à « haut risque » et mettre en place une structure de gouvernance permettant un audit efficace. La politique met aussi l'accent sur la formation des membres du SPT.

M. Kanengisser a noté que la politique sur l'IA inclut des principes directeurs pour décider si une technologie doit être approuvée ou non, qui incluent des questions d'équité et de fiabilité, en plus du caractère légal de l'utilisation et de l'exigence d'une intervention humaine en tout temps.

M. Stairs a expliqué que le SPT est en train de rédiger la procédure qui mettra en œuvre la politique sur l'IA adoptée par la CSPT, et que des consultations similaires à celles qui ont été menées pour développer la politique, auront lieu avec les parties prenantes. En ce qui concerne les résultats espérés, il a expliqué qu'une partie du problème est lié « à une visibilité insuffisante et à des lacunes dans l'orientation des agents de première ligne quant à la façon de s'y prendre avec les nouvelles technologies ». Le SPT cherche donc à établir une procédure qui lui permettra de faire des choix et d'indiquer à la CSPT et à la population si des outils technologies sont utilisés et pourquoi.

M. Stairs a expliqué qu'en vertu de la politique sur l'IA, les différents niveaux de risque pour l'évaluation des outils technologiques sont les suivants : risque extrême, risque élevé, risques moyens, risques faibles et risques très faibles. Les risques extrêmes sont considérés comme étant interdit. Il a rajouté qu'un niveau de risque élevé ou extrême doit nécessairement impliquer une intervention humaine. Il a indiqué que la politique sur l'IA exige aussi que toute technologie utilisée soit affichée et évaluée selon ce cadre, sauf dans le cas des technologies à risque faible ou très faible. Sinon, le fardeau de transparence deviendrait très difficile à assumer par le SPT.

Mme Kosseim a noté que le Bureau de la commissaire à l'information et la protection de la vie privée de l'Ontario a été consulté au sujet de la politique sur l'IA. Elle a expliqué que même si toutes les recommandations de son bureau n'ont pas été adoptées dans la politique, elles pourront être intégrées dans les procédures visant sa mise en œuvre. Vance Lockton, conseiller principal en technologie et politique du bureau de la commissaire a indiqué, par exemple, qu'une des recommandations de la commissaire serait d'inclure dans les procédures de meilleures définitions des niveaux de risques et de clarifier dans celles-ci comment la surveillance de l'IA utilisée par le SPT sera exercée.

Selon Mme Thomasen, la politique sur l'IA du SPT présente encore des faiblesses. Par exemple, elle traite encore des technologies algorithmiques policières comme si elles étaient inévitables – comme un avantage net dont on peut atténuer les risques. À son avis, ce n'est pas le bon cadre pour aborder ces technologies étant donné les préjudices qu'elles peuvent causer et le contexte social dans lequel elles sont introduites.

Utilisation de la reconnaissance faciale par d'autres organismes fédéraux

En 2020, un groupe de 77 défenseurs de la vie privée, des droits de la personne et des libertés civiles, dont la CSILC, a soumis une lettre au ministre de la Sécurité publique lui demandant d'interdire toute utilisation de la surveillance de reconnaissance faciale par les agences de police et de renseignement fédérales[36]. M. McSorley a indiqué avoir assisté à une séance d'écoute avec le directeur des politiques du cabinet du ministre à la suite à la transmission de cette lettre, lors de laquelle on a indiqué que l'Agence des services frontaliers du Canada (ASFC) n'utilisait pas la RF en temps réel. Selon M. McSorley, aucune information n'a été partagée sur l'utilisation de cette technologie par le SCRS, et il n'y a pas eu d'engagement clair de la part du cabinet du ministre à propos d'autres mesures à venir.

M. McSorley a indiqué, en faisant référence au fait qu'un ensemble disparate de lois s'appliquent à la TRF :

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

M. McSorley a réitéré que le SCRS a refusé de confirmer s'il utilise ou non la TRF dans le cadre de son travail, en déclarant qu'il n'a aucune obligation de le faire.

M. Mohammad a soulevé le fait que divers organismes de sécurité nationale et de maintien de l'ordre ainsi que d'autres organismes gouvernementaux ont dit par le passé que la surveillance qu'ils effectuent se faisait d'une manière conforme à la Constitution et de façon équilibrée, alors que ce n'était pas le cas, comme l'a démontré les cas de Maher Arar, Abdullah Almaki et Mohamedou Ould Slahi[37]. Selon lui :

> Les mêmes organismes qui ont menti à la population canadienne au sujet de la surveillance des communautés musulmanes se présentent maintenant devant vous pour

36 International Civil Liberties Monitoring Group, *Le gouvernement canadien doit interdire l'utilisation de la reconnaissance faciale par les forces policières et les agences de renseignement fédérales* [DISPONIBLE EN ANGLAIS SEULEMENT].

37 Voir : SECU, Étude des constats et recommandations de l'enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (Commission Iacobucci) ainsi que sur le rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (Commission O'Connor), juin 2009.

> affirmer que, même si la surveillance de masse n'aura pas lieu, la TRF peut et doit être utilisée de manière responsable.

M. Farooq a de son côté mentionné une décision de la Cour fédérale qui a récemment reproché au SCRS d'avoir l'habitude de tenter d'induire la Cour en erreur[38]. Il a noté que le gouvernement fait appel de cette décision. Il a affirmé que la question de savoir quelles mesures seront prises pour obliger les organismes de sécurité nationale à rendre des comptes lorsqu'ils induisent les gens en erreur demeure.

Utilisation de la reconnaissance faciale par les autorités frontalières

En septembre 2020, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC) a publié un rapport au sujet de la RF et de son utilisation aux frontières[39]. Tamir Israel, avocat-conseil à l'interne chez la CIPPIC, a résumé les principales conclusions de ce rapport comme suit :

> [L]a reconnaissance faciale est adoptée à la frontière sans égard aux préjudices qu'elle pourrait causer, sans grande surveillance externe et souvent sans égard aux politiques existantes, comme la politique du Conseil du Trésor sur l'intelligence artificielle, qui dicte que l'on est censé solliciter des conseils externes lorsqu'on adopte des technologies aussi intrusives.
>
> Ensuite, une fois adoptées, ces technologies sont souvent très vite utilisées à d'autres fins, qui dépassent le cadre étroit dans lequel elles ont été conçues.
>
> Enfin, ces technologies font souvent le lien entre la présence numérique et la présence physique, d'une manière qui permet l'application de nombreux autres outils d'évaluation automatisés, ce qui est problématique en soi.

M. Israel, a expliqué ce qui suit quant à l'apparition de la TRF aux frontières :

> [P]artout dans le monde, on propose d'automatiser ce processus de contrôle de l'identité. Les gens devront donc se présenter devant un écran pour subir une analyse de reconnaissance faciale. Une évaluation du profil sera effectuée numériquement, et

38 *Loi sur le service canadien du renseignement de sécurité (CA) (Re)*, 2020 CF 616 (CanLII). Le juge a déterminé que le Service canadien du renseignement de sécurité avait manqué à son obligation de franchise. L'obligation de franchise est un concept juridique qui s'applique lors d'une demande de mandats *ex parte* et exige à la partie qui fait la demande de faire preuve d'une bonne foi absolue dans la présentation de ses arguments visant à obtenir un mandat.

39 Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC), *Facial Recognition at a Crossroads: Transformation at our Borders & Beyond*, septembre 2020 [DISPONIBLE EN ANGLAIS SEULEMENT].

chaque personne sera automatiquement dirigée vers une ligne à sécurité élevée, intermédiaire ou peu élevée.

M. Israel a noté qu'il existe différents types de systèmes de RF, mais que c'est un système décentralisé qui décrit le mieux à la technologie utilisé pour la vérification des passeports. Un système centralisé conserve toutes les images dans un seul endroit, alors que dans un système décentralisé il s'agit d'une image numérique encodée, comme une photo de passeport, qui est comparée à la photo prise par l'utilisateur du passeport à l'aéroport. La sécurité du dispositif radio numérique encodé dans un passeport peut être compromise, mais on ne compromet alors qu'un seul passeport.

Plusieurs témoins ont indiqué qu'ils existent des risques élevés à l'égard de l'utilisation de la TRF et d'autres technologies biométriques dans les aéroports et aux frontières[40].

Esha Bhandari, directrice adjointe de l'American Civil Liberties Union (ACLU), s'est dite préoccupée par l'utilisation croissante de la RF et d'autres technologies biométriques dans les aéroports. Elle a expliqué que le problème réside dans l'aspect obligatoire de se soumettre à la TRF ou au balayage d'iris pour accéder à des services essentiels comme aller à l'aéroport ou traverser la frontière, dans des contextes où il est difficile de se soustraire à ces processus en raison de la nature coercitive de l'environnement. Selon elle, la réglementation devrait prévoir de véritables solutions de rechange, pour éviter d'obliger les gens, par exemple à se soumettre à un balayage de l'iris[41].

M. Israel a de son côté soulevé le manque de consentement explicite, indiquant que « la personne n'est même pas nécessairement consciente qu'elle est soumise à cette technologie ». Il a partagé l'exemple du mécanisme de contrôle douanier de l'aéroport Pearson de Toronto où les voyageurs ne savent pas nécessairement qu'une analyse de RF est en cours. Selon lui, « il serait donc utile d'ajouter une option de refus indiquée très clairement, et peut-être même une obligation de demander d'abord le consentement ».

Des préoccupations quant à la discrimination et au profilage racial perpétré aux frontières ont également été soulevées par des témoins[42]. Par exemple, M. Israel a noté que les listes de personnes interdites de vol sont un problème de longue date et qu'un

40 ETHI, *Témoignages*, Tamir Israel; ETHI, *Témoignages*, Esha Bhandari; ETHI, *Témoignages*, Petra Molnar; Refugee Law Lab, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, 25 avril 2022 [*Mémoire du Refugee Lab*].

41 Mémoire du Refugee Lab, p. 11. Le balayage de l'iris est aussi utilisé dans certains camps de réfugiés, par exemple en Jordanie.

42 ETHI, *Témoignages*, Mustafa Farooq; ETHI, *Témoignages*, Tamir Israel.

projet des listes similaires fondées sur la RF avec des objectifs comparables serait problématique.

Mme Molnar a rappelé que la TRF est hautement discriminatoire à l'égard des visages noirs et bruns et que les décisions algorithmiques reposent souvent sur des ensembles de données biaisés. C'est d'ailleurs ce qui inquiète M. Jenkins quant à l'utilisation de la TRF dans les aéroports où même une marge d'erreur de 1% peut s'avérer colossale à grande échelle. Il a illustré cette crainte ainsi :

> Je pense qu'à 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.

De plus, dans le cadre de ses recherches, M. Jenkins a découvert que les autorités frontalières et policières ne sont pas plus aptes à identifier les visages non familiers, malgré leur formation professionnelle et leurs nombreuses années d'expérience. Il a expliqué que le pourcentage d'erreurs humaines fait par des spécialistes, comme des agents de passeport, comparativement aux erreurs de logiciel de TRF peuvent varier dépendamment de la nature de la tâche. Par exemple, un membre du personnel des services de passeport qui est bien formé et possède de nombreuses années d'expérience possède une marge d'erreur se situant à environ 10%. Quant au système informatisé, il est difficile de prévoir une marge d'erreur exacte puisque les résultats présentés par les fournisseurs sont souvent obtenus dans des conditions idéales permettant une analyse fiable pour le marché, où le bruit et la complexité du monde réel ne sont pas pris en compte.

Mme Molnar a aussi partagé ses inquiétudes quant à l'utilisation de la TRF par les autorités frontalières dans le but de mettre en œuvre une surveillance biométrique généralisée pour assurer la gestion des migrations et des frontières. Selon elle, pour bien saisir les répercussions des différentes technologies de gestions des migrations et des frontières (p. ex., des détecteurs de mensonges à l'IA, la surveillance biométrique généralisée et les différents outils de prise de décision automatisée) il faut prendre en compte l'écosystème plus vaste dans lequel ces technologies se développent. Cet écosystème en est un où il y a de plus en plus de criminalisation de la migration, de sentiments anti-migrants et de pratiques frontalières engendrant des milliers de décès, par exemple en Europe, mais aussi aux frontières entre les États-Unis et le Mexique, et entre les États-Unis et le Canada.

Depuis 2018, Mme Molnar a visité des frontières dans le monde entier, dont plus récemment la frontière des É-U et du Mexique et la frontière ukrainienne. Elle a expliqué :

> Les frontières deviennent facilement des terrains d'essai pour les nouvelles technologies, car la migration et l'application des lois à la frontière constituent déjà un espace décisionnel opaque et discrétionnaire, où des décisions qui changent le cours d'une vie sont rendues par des décideurs soumis à peu de surveillance et de responsabilisation dans un système de vastes déséquilibres de pouvoir entre ceux qui sont touchés par la technologie et ceux qui la manient[43].

Dans la détermination de l'asile, en particulier, elle a fait remarquer que si des erreurs sont commises, et qu'une personne est expulsée à tort vers un pays qu'elle fuit, les ramifications peuvent être terribles[44]. De plus, Mme Molnar a noté que l'utilisation de technologies de surveillance et les technologies frontalières intelligentes ne dissuadent pas les gens de tenter des traversées dangereuses, mais fait plutôt en sorte qu'ils modifient leurs itinéraires vers des terrains moins habités, ce qui entraîne des pertes humaines. Elle a donné l'exemple de la famille qui a été retrouvée morte à la frontière entre le Manitoba et les États-Unis.

Ainsi, Mme Molnar est d'avis que remplacer les décideurs humains par des décisions automatisées et une surveillance accrue « ne fait que brouiller le domaine déjà très discrétionnaire du traitement et de la prise de décision en matière d'immigration et de réfugiés ». Elle a rajouté que l'application de la loi aux frontières et la prise de décision en matière d'immigration, les structures fondées sur l'intersection d'un racisme systémique et une discrimination historique à l'endroit des migrants rendent les répercussions de la technologie sur les droits de la personne bien réelles.

Quelques programmes ou projets spécifiques concernant l'utilisation de la TRF aux frontières ont aussi été soulevés par des témoins.

Par exemple, Mme Bhandari a mentionné que ACLU se préoccupe de l'utilisation croissante de la RF dans les aéroports, entre autres dans le contexte du programme Nexus. M. Israel a noté que bien que les programmes de TRF utilisés aux frontières canadiennes, comme Nexus, soient encore facultatifs, la pression exercée pour traverser la frontière est utilisée pour convaincre les voyageurs de s'inscrire à ce type de systèmes.

---

43 Mme Molnar a donné l'exemple de ce qu'elle a vu dans le désert de Sonora à la frontière des É-U et du Mexique ou différentes tours de surveillance automatisée alimentée par l'IA balaie le désert.

44 Mme Molnar a fait référence au rapport suivant : The Citizen Lab, Petra Molnar et Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System*, 26 septembre 2018.

Il a aussi donné l'exemple du projet pilote du programme d'identité numérique du voyageur digne de confiance du Forum économique mondial:

> Le Canada, par exemple, a piloté un programme avec les Pays-Bas, un programme mis au point par le Forum économique mondial. Il s'agit essentiellement d'une identité numérique, enregistrée dans votre téléphone, qui contient l'essentiel des renseignements sur votre passeport et des renseignements du programme de vérification de l'identité sociale. L'idée était de voir si cela pouvait remplacer le passeport, afin de faciliter le passage aux frontières. La reconnaissance faciale était la technologie intégrée à ce système. L'objectif ultime de ce système — c'est très explicite — est de convaincre les voyageurs de s'y inscrire volontairement pour éviter les délais à la frontière, parce qu'il donne accès à un contrôle de sécurité plus rapide. Toutefois, il sera ensuite mis à la disposition des banques, des sociétés de télécommunications et d'autres entités pour des programmes de vérification de l'identité similaires[45].

M. Israel s'est dit préoccupé par la participation du gouvernement du Canada à ce projet pilote, qui a été interrompu par la pandémie. Il a indiqué :

> Je suis très préoccupé par l'idée d'utiliser la localisation de l'expérience de voyage pour encourager les gens à s'inscrire et à créer ce type de profils, sachant que ce sera ensuite utilisé contre eux, non seulement dans le cadre des contrôles aux frontières, où de nombreuses communautés marginalisées sont déjà très désavantagées, mais aussi ici et à l'étranger, dans d'autres pays qui finissent par mettre en œuvre le même système. Ce système est destiné à être mondial. L'idée est également que ces systèmes soient ensuite utilisés par le secteur privé pour détecter les fraudes ou gérer l'identité dans les interactions avec les entreprises privées.

Mme Molnar et M. Farooq ont de leur côté fait mention du projet pilote de l'ASFC dans les aéroports pour mettre à l'essai une technologie appelée AVATAR – une technologie polygraphique qui utilise la TRF et de reconnaissance émotionnelle pour détecter si une personne ment et dont l'utilisation est déjà interdite dans d'autres pays. Alors que Mme Molnar a questionné la capacité d'un tel détecteur de composer avec les différences religieuses ou ethniques, par exemple ceux qui seraient peut-être réticents à établir un contact visuel, ou qui ressentiraient de la simple nervosité ou auraient des traumatismes de mémoire, le CNMC s'est dit préoccupé de la manière dont cette technologie peut être exploitée afin d'établir le profil des gens pour terrorisme potentiel. Mme Molnar a soulevé la question suivante :

45 ETHI, *Témoignages*, Tamir Israel; Gouvernement du Canada, *Le gouvernement du Canada mettra à l'essai des technologies de pointe favorisant la sûreté et la fluidité des déplacements des voyageurs aériens dans le monde entier*, communiqué, 25 janvier 2018.

> Quelles priorités comptent vraiment lorsque nous choisissons de créer des détecteurs de mensonges alimentés par l'intelligence artificielle à la frontière au lieu d'utiliser l'intelligence artificielle pour reconnaître les gardes-frontières racistes?

Enfin, M. Israel a indiqué que récemment « l'ASFC a annoncé qu'elle tenterait de mettre en place un centre d'études biométriques au sein de son infrastructure », mais que rien de concret n'a encore été vu.

Utilisation de la reconnaissance faciale dans les espaces publics

Mme Khoo a indiqué que l'utilisation de la TRF dans les lieux publics brime le droit à la vie privée qui est garanti par l'anonymat dans la vie courante. Elle a rajouté que cette technologie risque d'avoir un effet paralysant sur la liberté d'expression dans le cadre de manifestations publiques contre l'injustice. Elle risque aussi d'exacerber la violence et l'exploitation fondées sur le genre en facilitant le harcèlement de femmes. Des témoins ont aussi rappelé au Comité que la Cour suprême du Canada a déterminé que les citoyens canadiens conservent leur droit à la vie privée, même dans les lieux publics[46].

Mme Watkins a noté que l'utilisation courante de la TRF dans les espaces publics pourrait affecter le droit à la liberté de circulation.

M. McSorley a dit que même en réglant les graves problèmes de partialité et de précision, les systèmes de surveillance par RF risquent de continuer à soumettre les gens à une surveillance intrusive et sans discernement, par exemple dans le cas de piétons sur une place publique ou d'activistes lors d'une manifestation.

M. Farooq a indiqué que son organisation n'a pas reçu de plaintes formelles en matière de droit de la personne en lien avec la technologie d'IA, dont la TRF. Il a cependant noté que le CNMC a parfois vent de préoccupations au sujet de gens qui assistent à des rassemblements pacifiques, par exemple à Vancouver ou Hamilton, où les autorités chargées de l'application de la loi prennent des photos. Il a précisé que le CNMC ne connaît pas toujours l'usage qui est fait de ces données, en grande partie en raison d'un manque de divulgation. En effet, selon lui, l'absence de plaintes est liée au manque de divulgation.

La TRF est aussi utilisée dans des espaces semi-publics, comme des établissements commerciaux. Pour M. Labonté, l'utilisation de la TRF dans les commerces de détails ou centre commercial est comparable au commerce en ligne, où même si les usagers ne se connectent pas au moyen d'un compte d'utilisateur, des témoins de connexion laissent

46 Mémoire CSILC, p. 6; Mémoire Ligue des droits et libertés, p. 2; *R c. Spencer*, 2014 CSC 43.

quand même des traces de ce passage sur le Web. Ces traces sont par la suite utilisées pour pousser de la publicité ciblée en fonction des préférences des usagers.

Mme Bhandari a de son côté donné l'exemple d'entreprises américaines, comme Walgreens, qui utilisent une TRF permettant de détecter l'âge et le sexe d'un client pour lui montrer des publicités ou des produits ciblés. Selon elle, il s'agit d'une tactique invasive qui pourrait susciter des inquiétudes quant au fait que les consommateurs sont orientés vers des produits en fonction de stéréotypes de genre, ce qui pourrait aggraver la ségrégation dans la société.

Mme McPhail a quant à elle mentionné l'enquête menée par le CPVP sur le centre commercial Cadillac Fairview. Elle a rappelé que cette enquête a révélé une utilisation non consensuelle, par le secteur privé, de l'analyse d'images faciales, découverte en raison d'une défaillance de la technologie. À son avis, cet exemple démontre que « les fournisseurs de reconnaissance faciale annoncent qu'ils peuvent aider les organismes du secteur privé à exploiter les données personnelles pour améliorer leur marché, et c'est un problème ».

Dans le cadre de son enquête, le CPVP a conclu que Cadillac Fairview avait recueilli et utilisé des renseignements personnels, dont des renseignements biométriques de nature délicate à l'aide d'analyse vidéo anonyme, sans avoir obtenu un consentement valable des gens qui fréquentaient des centres commerciaux canadiens[47].

Les exemples soulevés par les témoins démontrent comment la surveillance à l'aide de TRF peut se faire dans des espaces publics à l'insu des gens.

Utilisation de la reconnaissance faciale dans le monde du travail

Mme Watkins a fait part de ses inquiétudes au Comité concernant l'utilisation, par le secteur privé, de la vérification faciale auprès des travailleurs. Elle a dit que c'est « la vérification faciale [qui] est de plus en plus utilisée dans les milieux de travail, en particulier dans celui du travail à la demande et du travail précaire ».

Selon Mme Watkins, « ces systèmes ont souvent été mis en place pour protéger la vie privée des travailleurs, prévenir la fraude et assurer la sécurité », mais il doit y avoir des moyens de rechange lorsque les travailleurs ne veulent pas s'y soumettre. Elle a noté qu'il faudrait tenir des consultations avec les travailleurs afin de mieux comprendre à

47 CPVP, *Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique*, 28 octobre 2020.

quel type de technologie ils accepteraient de se conformer et de leur offrir des solutions de rechange leur permettant de se soustraire aux technologies tout en gardant accès à leur moyen de subsistance. Elle a expliqué :

> 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.

Au bout du compte, Mme Watkins a affirmé que l'utilisation de la TRF n'est actuellement pas assez fiable pour être utilisé dans des scénarios à haut risque comme le milieu de travail. Elle a toutefois reconnu que certains travailleurs se disent favorables à la RF pour diverses raisons.

Utilisation de la reconnaissance faciale par les partis politiques

Selon Mme McPhail, l'utilisation de la RF par les partis politiques présente également un risque à la démocratie. Elle a fait mention de l'utilisation récente du Parti libéral du Canada d'« un outil similaire de reconnaissance faciale à correspondance biunivoque dans le cadre de son processus de vote pour l'investiture avant les dernières élections fédérales ». Elle a indiqué qu'« [e]n l'occurrence, il s'agissait d'une utilisation beaucoup plus risquée d'une technologie potentiellement défectueuse et discriminatoire, car c'était dans le contexte d'un processus qui est au cœur de la démocratie populaire ».

Observations et recommandations du Comité

Le Comité est d'avis que les représentants de la GRC ont fait preuve de beaucoup de réticence à fournir des réponses complètes aux questions des membres du Comité. En particulier en ce qui concerne l'utilisation de la technologie Clearview AI, de nombreux membres du Comité ont exprimé leurs préoccupations, pendant le témoignage de la GRC, à l'égard du fait que les témoins faisaient preuve d'évitement dans leurs réponses.

Considérant les propos du commissaire à la protection de la vie privée concernant l'article 4 de la *Loi sur la protection des renseignements personnels* et les nombreuses préoccupations liées à l'utilisation de la TRF dans les divers contextes explorés dans ce chapitre, le Comité recommande :

Recommandation 1

Que le gouvernement du Canada modifie l'article 4 de la *Loi sur la protection des renseignements personnels* de sorte à obliger une institution fédérale à s'assurer de la légalité des pratiques en matière de protection des renseignements personnels de toute tierce partie desquelles elle obtient des renseignements personnels.

Recommandation 2

Que le gouvernement du Canada s'assure que les aéroports et les industries divulguent publiquement l'utilisation de la technologie de reconnaissance faciale, y compris, mais sans s'y limiter, au moyen d'affiches bien en vue dans la zone d'observation et sur le site Web voyage.gc.ca.

Recommandation 3

Que le gouvernement du Canada renvoie l'utilisation de la technologie de reconnaissance faciale dans les opérations militaires ou de renseignement, ou lorsque d'autres utilisations de la technologie de reconnaissance faciale par l'État ont des répercussions sur la sécurité nationale, au Comité des parlementaires sur la sécurité nationale et le renseignement pour étude, examen et recommandation; et que ce Comité fasse rapport de ses conclusions à ce sujet.

Recommandation 4

Que le gouvernement, dans la création de son cadre réglementaire sur l'utilisation de la technologie de reconnaissance faciale, établisse des sanctions claires pour les violations commises par la police.

CHAPITRE 3 : RESPONSABILISATION, APPROVISIONNEMENT ET INVESTISSEMENT PUBLICS

> **« Très peu d'argent, de temps et de ressources sont consacrés à la gestion du désordre que ces technologies causent et des dommages qu'elles occasionnent. »**
>
> Ana Brandusescu, experte en gouvernance de l'intelligence artificielle, qui a comparu à titre personnel le 21 mars 2022.

Responsabilisation

Transparence

En ce qui concerne la transparence à l'égard du fonctionnement de la TRF, Mme Wang a indiqué que les modèles entraînés à l'aide d'apprentissage automatique qui permettent aux tâches de RF d'être exécutées sont présentement difficiles à interpréter puisqu'on ne sait pas vraiment sur quelles règles les modèles se basent.

En revanche, rendre le modèle explicable n'est pas nécessairement la solution. Selon Mme Brandusescu, bien que le concept d'IA explicable soit souvent vu comme une solution technique qui devrait être mise en place pour permettre à la TRF d'aller de l'avant, l'explication de l'IA dépend du public qui la reçoit, qui est généralement composé d'informaticiens et non de politiciens. À son avis, il faut tenter de comprendre la boîte noire, mais reconnaître que la disponibilité d'une explication ne signifie pas nécessairement que la technologie doit être utilisée.

Mme Piovesan a aussi soulevé l'importance de s'assurer qu'il y ait une capacité d'expliquer la technologie, c'est-à-dire de comprendre comment les algorithmes fonctionnent, de comprendre les résultats qu'ils fournissent, et d'obtenir une vérification indépendante confirmant que ces résultats sont exacts et fiables. Elle a noté l'importance d'avoir une discussion sérieuse sur l'utilisation des technologies comme la TRF et de leurs incidences avec divers intervenants, avant leur déploiement. Elle a identifié une façon d'atteindre cet objectif : l'adoption et l'application du concept de transparence radicale.

Mme Piovesan a expliqué que la transparence radicale vise l'ensemble du processus de divulgation. Elle invite l'entité qui utilise de la technologie avancée à dire aux gens : qui sont ses fournisseurs; quelles sont les utilisations qu'elle fait de la TRF et pour quelles raisons; et d'où proviennent les données qu'elle utilise. La transparence radicale cherche

aussi à faire participer le public plutôt que de favoriser un contexte secret qui mine la confiance des gens.

M. Jenkins a lui aussi souligné que la transparence est importante puisqu'il faut que les citoyens comprennent comment les technologies sont utilisées, comment elles peuvent être efficaces et comment elles peuvent les affecter. Des audits de l'utilisation de la TRF rendus publics peuvent, par exemple, aider à la transparence. Selon lui, la transparence est aussi un élément important d'un système éthique.

M. McSorley a dit qu'il faut exercer des pressions pour obtenir un plus grand degré de transparence et de responsabilisation de la part du gouvernement. Il a affirmé que les organismes fédéraux doivent souvent procéder à des évaluations des facteurs relatifs à la vie privée avant de mettre en place de nouvelles technologies ou de nouveaux projets ayant une incidence sur la vie privée, mais que ces évaluations ne sont pas effectuées, ou sont tenues secrètes[48]. Par exemple, il a indiqué que l'Office de la surveillance des activités en matière de sécurité nationale a entrepris un examen de l'utilisation de la surveillance biométrique, mais que plusieurs années pourraient s'écouler avant que les résultats de cette étude soient rendus publics[49]. Selon lui, « le manque de transparence et de responsabilisation signifie que cette technologie est adoptée à l'insu du public, en l'absence de débat public ou de surveillance indépendante ».

M. Farooq a fait des commentaires complémentaires. Il a noté qu'il est difficile d'engager un dialogue avec certains organismes publics en l'absence de données fondamentales. Par exemple, en raison du fait que la SCRS refuse de confirmer s'il utilise ou non la TRF, il est difficile de croire à la responsabilisation du SCRS à l'égard de cette technologie.

Mme Khoo a noté que dans le cas des services de police, les politiques qui régissent l'utilisation de la RF « peuvent être des boîtes noires encore plus difficiles à comprendre que les algorithmes ». Selon elle, une telle opacité engendre de graves manquements à l'équité procédurale dans les affaires criminelles. Elle a recommandé d'instaurer des mesures rigoureuses en matière de transparence et de responsabilité.

Mme Brandusescu a de son côté proposé la création d'un registre pour l'IA par le Conseil du Trésor, particulièrement pour l'IA utilisée à des fins d'application de la loi et de

48 La *Directive sur l'évaluation des facteurs relatifs à la vie privée* du gouvernement du Canada est en vigueur depuis 2010. Elle s'applique aux institutions fédérales visées par l'article 3 de la *Loi sur la protection des renseignements personnels*.

49 Office de surveillance des activités en matière de sécurité nationale et de renseignement, *Office de surveillance des activités en matière de sécurité nationale et de renseignement - 2022–2023 - Plan ministériel*. Le plan ministériel indique que l'Office mène un examen continu du recours à la biométrie.

sécurité nationale. Elle a indiqué qu'un tel registre serait utile aux chercheurs, aux universitaires et aux journalistes d'enquête qui informent le public.

De son côté, Mme Watkins a indiqué qu'il vaut mieux comprendre comment les outils technologiques comme la TRF sont utilisés, où les données sont stockées, comment les décisions sont prises en fonction de celles-ci et si des humains sont impliqués ou non. Bref, il faut plus de transparence.

Gouvernance et imputabilité

Mme LaPlante a indiqué que puisque les données biométriques sont sensibles, la sécurité de ces données doit être assurée au moment de leur collecte, de leur utilisation et de leur entreposage. Selon elle, la TRF, comme tout autre système d'IA à haut risque, devrait faire l'objet d'une validation approfondie afin que ses limites soient bien comprises et prises en compte lorsque transposées dans le monde réel. Mme LaPlante dit au sujet de la gouvernance de l'IA:

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

Pour éliminer les préjugés de la technologie, Mme Laplante a recommandé au Comité de s'intéresser au concept d'éthique dès la conception, qui consiste à prendre en compte les considérations éthiques tout au long du cycle de développement, de la collecte initiale des données, à l'élaboration des algorithmes, à la production de la technologie et la surveillance de ces systèmes.

M. Labonté a expliqué que lorsqu'un système est biaisé, cela signifie que les échantillons de données initiaux ne sont pas égaux ou que leur représentativité n'est pas égale. Il a noté qu'il faut encadrer la collecte de données, soulignant que les plus grands joueurs à l'heure actuelle ont des avantages compétitifs grâce à leur accès à d'énormes quantités de données qu'ils ont recueillies afin de procéder à l'entraînement de leurs modèles d'IA.

M. Maslej a affirmé que dans certains cas, plus des données sont fournies à un modèle d'IA, plus il risque de contenir des données biaisées. En d'autres termes, si les données ne sont pas filtrées de manière proactive, il est probable que les modèles d'IA se

comportent de manière problématique. Il a expliqué que le filtrage des données utilisées pour entraîner un modèle d'IA pourrait remédier au problème, mais risquerait d'affecter la capacité du modèle à fonctionner de façon optimale.

Mme Wang a suggéré que pour corriger les problèmes de distorsion entre les résultats de la TRF pour différents groupes démographiques, les fournisseurs devraient adopter certaines mesures dont la collecte d'ensemble de données plus diversifiées et plus inclusives, et la conduite d'analyses désagrégées pour déterminer le taux d'exactitude envers ces différents groupes, plutôt qu'envers l'ensemble des données. Elle a toutefois noté que la collecte de tels ensembles de données peut en soi être une forme d'exploitation des groupes marginalisés et une violation de leur vie privée.

Mme Brandusescu a aussi suggéré de faire de l'imputabilité une priorité. Par exemple, dans le secteur public, elle a noté que la GRC devrait avoir l'obligation de publier un rapport expliquant comment elle utilise la TRF. Une telle pratique pourrait s'appliquer à tous les ministères et organismes fédéraux à l'avenir[50].

Les institutions fédérales doivent déjà se conformer à la Directive sur la prise de décisions automatisées du Conseil du Trésor. La directive fédérale exige, entre autres, la réalisation d'une évaluation de l'incidence algorithmique (EIA) avant la production de tout système de décision automatisé. En fonction du niveau d'impact du système, des mécanismes de responsabilité différents sont requis (p. ex., examen par les pairs ou participation humaine). La directive impose aussi des obligations de transparence et d'assurance qualité, par exemple en rendant l'EIA publique.

Cependant, Mme Brandusescu a indiqué que la directive fédérale doit être améliorée. À son avis, le public devrait disposer des informations relatives à l'usage de technologies comme la TRF et obtenir des mises à jour. Par exemple, elle a suggéré que le Conseil du Trésor publie les récentes interventions du gouvernement en matière d'IA sur sa page Web (p. ex., l'acquisition de nouvelles technologies telles la TRF). Elle aussi recommandé l'imposition d'exigences plus précises à l'égard de la surveillance continue du système

50 Mme Branduscescu a recommandé que le commissaire à la protection de la vie privée exige la production de ce rapport. Le commissaire n'a pas le pouvoir de rendre des ordonnances à l'heure actuelle. Le projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, déposé à la Chambre des communes en juin 2022, si adopté dans sa forme actuelle, donnerait au commissaire le pouvoir d'émettre des ordonnances pour l'application de la loi fédérale sur la protection des renseignements personnels qui s'applique au secteur privé. La *Loi sur la protection des renseignements personnels* s'applique au secteur public, y compris à la GRC.

d'IA après la première EIA, par exemple lorsque l'utilisation ou l'incidence du système change.

Mme Brandusescu a aussi noté que les seuls intervenants non gouvernementaux qui ont participé aux EIA qui ont été publiées par le gouvernement depuis l'entrée en vigueur de la directive fédérale étaient des entreprises[51]. Elle a proposé d'améliorer les EIA en mobilisant la société civile. Selon elle, en ne retenant que des entreprises, on limite la contribution de la population canadienne, des groupes concernés, des organisations de défense des droits numériques et des organismes de la société civile au processus.

Mme Watkins a indiqué qu'il faut établir une responsabilisation, assurer la reddition des comptes et établir le genre de relations entre le gouvernement, les intervenants privés et l'intérêt public qui permettrait de répondre aux besoins des plus vulnérables.

Mme Branduscescu a aussi noté le besoin d'accroître l'expertise interne en matière d'IA pour permettre aux organisations de vraiment comprendre la technologie qu'ils achètent.

Dans la même veine, M. Jenkins a dit 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 ». Il a par contre aussi dit : « [L]a surveillance humaine fournit des garanties importantes et un mécanisme d'imputabilité, mais elle impose également un seuil maximal d'exactitude que les systèmes de reconnaissance faciale pourraient atteindre en principe. » En d'autres termes, dès qu'il y a surveillance humaine, il y a risque d'erreur humaine. Pour atténuer ce risque, il faut s'assurer que les personnes qui prennent part aux décisions liées à la RF soient hautement qualifiées[52].

Approvisionnement et partenariats public-privé

Mme Brandusescu a fait remarquer que l'enjeu lié aux technologies comme la TRF est plus large que la protection des données et de la vie privée; il implique une conversation

51 La Directive sur la prise de décisions automatisées prévoit que selon le niveau d'incidence du système décisionnel automatisé, un examen par les pairs doit être effectué par l'entremise de l'un des groupes ou moyens suivants : experts qualifiés d'une institution gouvernementale fédérale, provinciale, territoriale ou municipale; membres qualifiés d'une faculté d'un établissement postsecondaire; chercheurs qualifiés d'une organisation non gouvernementale pertinente; tiers fournisseurs à forfait avec une spécialisation connexe; publication des spécifications du système décisionnel automatisé dans une revue à comité de lecture; comité consultatif des données spécifié par le Secrétariat du Conseil du Trésor.

52 ETHI, *Témoignages*, Rob Jenkins.

sur la participation du secteur privé à la gouvernance publique. Selon elle, les gens devraient être très inquiets de la mainmise du secteur privé dans l'élaboration de la politique gouvernementale visant à réglementer l'IA et la TRF. Les partenariats public-privé sont un élément clé de l'acquisition, la mise en œuvre, le développement et l'utilisation de ces technologies. Elle a expliqué que dans un rapport récent, son collègue et elle ont affirmé que les contribuables paient essentiellement pour être surveillés, alors que des entreprises comme Clearview AI peuvent tirer profit des processus d'approvisionnement en technologie du secteur public et de l'absence de réglementation[53].

Comme exemple des failles perçues du processus d'approvisionnement, Mme Brandusescu a soulevé le fait que Palantir Technologies inc. se trouve dans la liste de fournisseurs d'IA préqualifiés du gouvernement du Canada, malgré des rapports indiquant que cette entreprise aurait commis certaines violations des droits de la personne, entre autres aux États-Unis (p. ex., arrestations massives et séparation d'enfants de leurs parents dans le contexte d'immigration)[54]. Selon elle, les entreprises liées à des violations des droits de la personne devraient être retirées de la liste du gouvernement.

De plus, Mme Brandusescu a indiqué que l'IA peut parfois échapper aux politiques d'approvisionnement en raison d'essais gratuits de logiciels, comme ça a été le cas pour Clearview AI[55]. Elle a dit que pour améliorer les marchés publics, une politique de divulgation proactive des essais gratuits de logiciels par les autorités chargées de l'application de la loi et de l'ensemble du gouvernement devrait être adoptée. Cette divulgation proactive devrait être accompagnée par la mise sur pied d'un registre des essais gratuits. Ainsi, « la boîte noire deviendrait alors une boîte de verre ».

Mme Molnar a de son côté invité le Comité à se demander pourquoi le secteur privé réussit souvent à déterminer l'objet et l'objectif des innovations du Canada dans le cadre de partenariats public-privé, que les États sont de plus en plus enclins à conclure dans la course mondiale aux armements à l'IA en cours. Elle a rappelé au Comité qu'il faut « accorder une attention particulière aux acteurs de l'écosystème dans lequel ces

53 Centre for Media, Technology and Democracy, Yuan Stevens et Ana Brandusescu, *Weak privacy, weak procurement: The state of facial recognition in Canada*, 6 avril 2021 [DISPONIBLE EN ANGLAIS SEULEMENT].

54 Gouvernement du Canada, Secrétariat du Conseil du Trésor, *Liste des fournisseurs d'intelligence artificielle (IA) intéressés*; Amnesty International, *Failing to do Right : The Urgent Need for Palantir to Respect Human Rights*, 2020 [DISPONIBLE EN ANGLAIS SEULEMENT]; ETHI, *Témoignages*, Ana Branduscescu.

55 *Rapport spécial du CPVP sur la GRC*, para. 1. Le CPVP indique que la GRC a confirmé qu'en 2019 elle a acheté deux licences lui permettant d'utiliser les services de Clearview AI et que certains de ses membres avaient aussi eu recours à la technologie de Clearview AI par l'entremise de comptes d'essais gratuits.

technologies se développent et sont mises en œuvre ». Selon elle : « Rien de tout cela n'est neutre. Tout cela est un exercice politique. »

Mme Khoo et Mme Thomasen ont soulevé l'émergence de partenariats entre Amazon Ring et les services de police aux États-Unis comme exemple d'une infrastructure de surveillance qui peut s'installer à l'aide d'un partenariat public-privé.

M. McSorley a noté qu'en l'absence d'une réglementation appropriée et avec autant d'entreprises qui proposent leur technologie aux organismes d'application de la loi, on peut se demander si ces organismes « utiliseront la technologie la plus précise, ou s'ils utiliseront la plus accessible, celle qui est davantage ciblée et commercialisée pour les organismes d'application de la loi ». Il a lui aussi dit être d'avis que l'absence de réglementation est ce qui a permis à la GRC d'utiliser la TRF de Clearview AI pendant des mois à l'insu du public.

M. Israël et Mme Bhandari n'étaient pas au courant de l'existence d'un registre des entreprises offrant de la TRF, mais ils ont soulevé le fait que certains États américains exigent l'enregistrement des courtiers en données. Selon Mme Bhandari exiger ce genre de transparence des entreprises qui vendent des outils de RF ou d'autres outils algorithmiques pourrait donner lieu à un droit privé d'action ou faire en sorte que les organismes de réglementation sachent qui surveiller.

Mme Thomasen a de son côté suggéré de mettre au point des systèmes internes de RF qui utilisent des données recueillies légalement, avec un consentement éclairé et dans un processus qui garantit la dignité des personnes dont les données sont traitées. Ces systèmes pourraient être conçus et utilisés exclusivement pour des cas d'utilisation très précis, contrairement aux systèmes commerciaux qui ne tiennent pas compte du contexte social particulier dans lequel la TRF est déployée.

Approvisionnement des services policiers

En ce qui concerne l'acquisition de technologie par les services policiers, Mme Khoo a expliqué qu'il faut des garanties juridiques strictes pour éviter qu'ils ne passent par des sociétés privées pour contourner les droits des gens à la liberté et à la protection contre les fouilles et les perquisitions abusives.

Par exemple, les logiciels de compagnies comme Clearview AI, Amazon Rekognition et NEC Corporation sont souvent protégés par les lois sur le secret commercial et achetés dans un contexte de lobbying qui a lieu en arrière-plan. Selon Mme Khoo, de telles pratiques mènent à des partenariats secrets de surveillance public-privé qui peuvent priver des accusés de leur droit à une procédure équitable ou exposer les gens à des

niveaux impénétrables de surveillance de masse. Pour remédier à la situation, elle a suggéré que tout fournisseur privé d'une technologie qui recueille des données personnelles pour le compte d'un service de police devrait être tenu, par contrat ou autrement, de se conformer à des normes en matière de protection et de communication des renseignements personnels.

Mme Khoo a fait trois recommandations précises au sujet du processus d'approvisionnement des autorités chargées de l'application de la loi afin de protéger la vie privée et d'assurer la reddition des comptes:

- L'acquisition d'une TRF ou d'une autre technologie algorithmique policière par les autorités d'application de la loi peut se faire sans collaborer avec un acteur commercial de sorte à ne pas être redevable à des intérêts privés (p. ex., développement d'une TRF à l'interne)[56];

- Si l'approvisionnement doit avoir lieu auprès d'un fournisseur commercial, des conditions d'achats très sévères peuvent être imposées (p. ex., renonciation aux secrets commerciaux aux fins de vérifications indépendantes);

- Le secret entourant les contrats devrait être réduit de sorte que les gens soient informés de leur existence avant qu'ils soient conclus plutôt qu'à la suite de divulgations, de demande d'accès à l'information ou d'enquêtes journalistiques.

Mme Piovesan a dit être d'accord avec les recommandations proposées par Mme Khoo.

Investissements publics

Mme Khoo a fait remarquer les entreprises privées qui recueillent grandes quantités de données afin d'en tirer profit le font souvent grâce à des subventions gouvernementales, obtenues sous le couvert de l'innovation, ou en raison de lobbying. Selon elle, cela fait en sorte que « [c]'est essentiellement le gouvernement et les entreprises privées qui travaillent main dans la main au développement de ce réseau de surveillance ».

Mme Brandusescu a noté qu'une question plus vaste liée au complexe militaro-industriel du Canada et à l'origine des technologies de surveillance comme la TRF se pose. À son

56 Mme Khoo donne l'exemple d'un laboratoire en Saskatchewan (le Saskatchewan Police Predictive Analytics Lab), une collaboration entre le service de police municipal et l'Université de la Saskatchewan, financée par l'État, qui a permis de développer une TRF locale.

avis, le Canada aurait avantage à prendre un pas de recul afin de remettre en question le solutionnisme technologique et d'examiner la raison pour laquelle autant d'argent est investi dans l'innovation technologique, sans accorder de financement aux groupes qui travaillent fort sur des questions sociales afin de comprendre la technologie et de sensibiliser et éduquer les gens à son sujet.

Mme Brandusescu est d'avis que le gouvernement ne devrait pas financer la TRF. Il devrait plutôt financer la société civile, les groupes de défenses des droits numériques et les groupes communautaires qui étudient la TRF et les inviter à participer à la conversation relative à ce que le gouvernement décide de financer. Elle a fait remarquer :

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

Mme Polsky a quant à elle noté un manque de sensibilisation des Canadiens au droit à la vie privée. Elle a soulevé l'idée d'un programme d'éducation destiné aux écoles, reconnaissant toutefois que l'éducation est une compétence provinciale. Elle a aussi noté que certains organismes médiatiques et les commissaires à la protection de la vie privée dans tout le pays ont élaboré certains cours ou programmes, mais que ceux-ci ce ne sont pas obligatoires. Selon elle, il faudrait confier un mandat d'éducation au CPVP et lui fournir le financement requis pour procéder à ces campagnes de sensibilisation[57].

Exemple d'effort de responsabilisation : Microsoft

Microsoft a partagé certaines de ses pratiques internes en matière d'IA et de TRF, s'affichant comme un exemple de fournisseur d'IA responsable dans le secteur privé.

57 Le commissaire à la protection de la vie privée fédéral a déjà un mandat d'éducation en vertu de l'article 24 de la *Loi sur la protection des renseignements personnels et documents électroniques*, en vertu duquel il doit offrir « au grand public des programmes d'information destinés à lui faire mieux comprendre la présente partie et son objet ». Cette obligation demeure présente dans la Loi sur la protection de la vie privée des consommateurs dans le projet de loi C-27. Une telle disposition ne figure pas au texte de la *Loi sur la protection des renseignements personnels*.

M. Larter a expliqué que Microsoft dispose d'un programme général de responsabilisation en matière d'IA qui comprend trois éléments principaux : une équipe de gouvernance de l'IA à l'échelle de l'entreprise qui regroupe de multiples parties prenantes, dont des chercheurs de renommée mondiale; une norme d'IA, qui garantit que toutes les équipes de l'entreprise qui conçoivent ou déploient des systèmes d'IA le font d'une manière conforme aux principes d'IA; et un processus d'examen des utilisations délicates[58].

M. Larter a précisé que l'examen des utilisations délicates est mené si la conception ou le déploiement éventuel d'un système d'IA répond à l'un de trois éléments déclencheurs : le système est utilisé d'une façon qui affecte les perspectives juridiques ou le statut juridique d'une personne; il y a un risque de préjudice psychologique ou physique; il y a un risque d'atteinte aux droits de la personne. Dans un tel cas, l'équipe de gouvernance de Microsoft se réunit et détermine si l'entreprise peut aller de l'avant avec une forme d'IA particulière[59].

En ce qui concerne la TRF, M. Larter a expliqué qu'une note sur la transparence pour l'interface de son programme des applications FACE a été publiée. Cette note explique dans un langage simple comment la TRF fonctionne, quelles en sont les capacités et les limites et quels facteurs influent sur sa performance. Il a précisé qu'au cours du développement de la TRF de Microsoft, l'entreprise a pris grand soin d'avoir un ensemble de données représentatif afin de mettre au point une technologie qui fonctionne adéquatement, y compris envers divers groupes démographiques.

M. Larter a aussi vanté les mérites des tests d'essai considérant l'écart important entre les systèmes de reconnaissance faciale les plus performants et ceux qui performent moins bien. Selon lui, les fournisseurs devraient permettre que leurs systèmes soient testés de manière raisonnable par des tiers indépendants et être tenus de corriger tout écart de performance important[60]. Microsoft se soumet à de tels tests. Il a aussi reconnu que la technologie doit s'accompagner de mesures de cybersécurité robustes.

---

58 *Ibid*. Microsoft, *Putting principles into practice at Microsoft* [DISPONIBLE EN ANGLAIS SEULEMENT.] La norme d'intelligence artificielle de Microsoft consiste en un ensemble d'exigences liées à ses six principes d'intelligence artificielle : équité, fiabilité et sûreté, protection de la vie privée et sécurité, inclusivité, transparence et responsabilité.

59 *Ibid*.

60 ETHI, *Témoignages*, Owen Larter. Selon M. Larter, les organisations qui utilisent la TRF devraient aussi être tenues de procéder à des tests garantissant que le système fonctionne correctement dans l'environnement où il sera utilisé.

Observations et recommandations du Comité

Le Comité est d'avis que le gouvernement devrait faire preuve de plus de transparence à l'égard de son utilisation de la TRF et autres IA, y compris en ce qui concerne son processus d'approvisionnement. Il devrait aussi investir davantage dans l'étude des répercussions de l'IA et la sensibilisation à l'égard du droit à la vie privée.

Par conséquent, il recommande :

Recommandation 5

Que le gouvernement du Canada modifie ses politiques en matière d'approvisionnement afin d'obliger les institutions fédérales qui se procurent de la technologie de reconnaissance faciale ou tout autre outil algorithmique, y compris sous la forme d'essais gratuits, à rendre cette acquisition publique, sous réserves de préoccupations relatives à la sécurité nationale.

Recommandation 6

Que le gouvernement du Canada crée un registre d'IA public dans lequel tous les outils algorithmiques utilisés par des entités opérant au Canada sont répertoriés, sous réserves de préoccupations relatives à la sécurité nationale.

Recommandation 7

Que le gouvernement du Canada améliore la Directive sur la prise de décisions automatisées du Conseil du Trésor afin d'assurer la participation de groupes provenant de la société civile dans les évaluations de l'incidence des algorithmes et d'imposer des exigences plus précises à l'égard de la surveillance continue des systèmes d'intelligence artificielle.

Recommandation 8

Que le gouvernement du Canada augmente ses investissements dans des initiatives visant à étudier les répercussions de l'intelligence artificielle sur divers groupes démographiques, augmenter la littératie numérique et éduquer les Canadiens et Canadiennes à l'égard de leurs droits en matière de protection de la vie privée.

Recommandation 9

Que le gouvernement du Canada assure la divulgation complète et transparente des préjugés raciaux, d'âge ou d'autres préjugés inconscients qui peuvent exister dans la

technologie de reconnaissance faciale utilisée par le gouvernement, dès que de tels préjugés sont découverts dans le cadre de scénarios d'essai ou d'applications réelles de la technologie, sous réserves de préoccupations relatives à la sécurité nationale.

Recommandation 10

Que le gouvernement du Canada établisse des mesures de politique solides dans le secteur public pour l'utilisation de la technologie de reconnaissance faciale qui pourraient inclure un avis public immédiat et préalable et des commentaires du public, une consultation avec les groupes marginalisés et des mécanismes de surveillance indépendants.

CHAPITRE 4 : RÉGLEMENTATION DE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE ET DE L'INTELLIGENCE ARTIFICIELLE

> **« La réglementation de la technologie de reconnaissance faciale doit être façonnée avec un scalpel, pas avec une hache. »**
>
> Carole Piovesan, associée directrice chez INQ law,
> qui a comparu devant le Comité le 21 mars 2022.

Comme Mme Polsky l'a souligné, la Cour suprême du Canada a reconnu il y a longtemps que « la notion de vie privée est essentielle au bien-être de la personne » et que « fondée sur l'autonomie morale et physique de la personne, [elle] est essentielle à son bien-être »[61]. Pourtant, compte tenu de la place qu'occupe déjà l'IA et la TRF dans notre société, le Comité s'est posé la question suivante: est-il trop tard pour agir?

La majorité des témoins était d'accord pour dire qu'il n'est pas trop tard[62]. D'autres ont confirmé que la prolifération de la TRF ne signifie pas la fin de la liberté individuelle[63]. M. Therrien était aussi d'avis qu'il n'est pas trop tard pour intervenir. Il a résumé la situation ainsi:

---

61 *R c. Dyment*, [1988] 2 RCS 417, para. 17 (le Juge LaForest).

62 ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Carole Piovesan; ETHI, *Témoignages*, Rob Jenkins; ETHI, *Témoignages*, Daniel Therrien; ETHI, *Témoignages*, Esha Bhandari; ETHI, *Témoignages*, Tamir Israel.

63 ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Ana Brandusescu; ETHI, *Témoignages*, Sanjay Khanna; ETHI, *Témoignages*, Rob Jenkins.

> Je vous ai entendu demander à certains témoins de ce Comité s'il est trop tard. Il n'est jamais trop tard. D'ailleurs, le fait que certaines pratiques se produisent actuellement ne devrait pas vous empêcher de faire le nécessaire et de réglementer la technologie d'une manière qui respecte les droits des Canadiens.
>
> Nous vivons, pas complètement, mais en partie, dans un monde d'autorégulation qui a engendré certaines pratiques inacceptables. Le fait qu'elles soient routinières ou banales […] ne signifie pas que l'on doive continuer à les autoriser.

Divers moyens pour combler les lacunes du régime législatif actuel ont été proposés par les témoins.

Moratoire, interdiction et autres mesures

Compte tenu des risques liés à la TRF, une majorité d'intervenants a recommandé l'imposition d'un moratoire, particulièrement dans le domaine de l'application de la loi, et ce jusqu'à ce qu'un cadre réglementaire approprié soit en place et que davantage de recherche et de consultations sur l'utilisation de la technologie et ses répercussions soient faites[64].

Par exemple, Mme Khoo a expliqué qu'un moratoire sur le recours à la TRF pour le maintien de l'ordre, une pause nationale, devrait être en place tant que la preuve n'aura pas été faite que la TRF est fiable et que son utilisation est nécessaire et proportionnée compte tenu des objectifs légitimes à atteindre d'une part, et des répercussions profondes que son utilisation peut avoir d'autre part. Elle n'a pas exclu la possibilité de bannir l'utilisation de la TRF dans certaines villes, comme c'est le cas aux États-Unis[65].

Mme Khoo a indiqué qu'un moratoire sur l'utilisation de la TRF pour le maintien de l'ordre donnera le temps de pousser les recherches afin de déterminer si une utilisation est appropriée et les garanties requises, le cas échéant, dont la transparence, des mécanismes de surveillance adéquats, et des exigences de divulgation. Selon elle le

---

64 ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Kristen Thomasen; ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Sanjay Khanna; ETHI, *Témoignages*, Elizabeth Anne Watkins; ETHI, *Témoignages*, Angelina Wang; ETHI, *Témoignages*, Tim McSorley; ETHI, *Témoignages*, Rizwan Mohammad; ETHI, *Témoignages*, Mustafa Farooq; ETHI, *Témoignages*, Sharon Polsky; ETHI, *Témoignages*, Tamir Israel; Mémoire CMTD et CPE; Mémoire CSILC; Mémoire Tessono; Mémoire Ligue des droits et libertés; Commission canadienne des droits de la personne, *Mémoire au Comité ETHI – Étude sur l'utilisation et l'impact de la technologie de reconnaissance faciale*, avril 2022 [*Mémoire CCDP*].

65 ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Esha Bhandari. Selon Mme Bhandari, au moins vingt-trois administrations de villes américaines interdisent le recours à la technologie de reconnaissance faciale par les forces de l'ordre ou le gouvernement. Voir aussi : Mémoire CMTD et CPE, p. 8; Mémoire Tessono, p. 5.

moratoire devrait s'appliquer non seulement à la TRF mais à toutes les technologies algorithmiques policières. Elle a aussi proposé que pendant le moratoire, une enquête soit faite par une commission nationale sur les technologies ou sous la forme d'une enquête judiciaire afin de définir ce qui est approprié et ce qui ne l'est pas à la lumière d'une analyse constitutionnelle et des droits de la personne approfondie[66].

M. McSorley et Mme Thomasen ont de leur côté recommandé que pendant un moratoire, le gouvernement fédéral entreprenne des consultations sur l'utilisation et la réglementation de la TRF, par exemple pour décider quelles utilisations devraient être interdites.

Mme McPhail, de son côté, a noté que l'un des buts du moratoire serait de donner au gouvernement la possibilité de combler la lacune principale du régime de protection des renseignements personnels fédéral : le fait que le commissaire n'a pas de pouvoirs d'exécution. Elle a précisé que l'imposition d'un moratoire aux autorités d'application de la loi est particulièrement importante, car il est question de situations où les conséquences d'une erreur peuvent changer la vie des personnes concernées, mais qu'un moratoire général pourrait aussi être bénéfique étant donné la vente de cette technologie par des fournisseurs du secteur privé au secteur public[67]. Mme Khoo aussi noté qu'un moratoire dans d'autres secteurs pourrait être utile.

Certains témoins étaient contre l'idée d'un moratoire. Par exemple, M. Larter a indiqué que selon Microsoft, plutôt que d'investir du temps et des efforts dans l'imposition d'un moratoire, il faudrait réglementer les utilisations de la TRF faites par les organismes d'application de la loi. Il a indiqué que Microsoft est en faveur d'une réglementation de la TRF qui protège les droits de la personne, interdit la surveillance de masse et qui favorise la transparence et la responsabilisation. À son avis la présence d'un cadre réglementaire permettrait d'engendrer la confiance de la population à l'égard de l'utilisation de la TRF.

M. Larter a toutefois reconnu que Microsoft a imposé un moratoire sur la vente de sa TRF aux forces policières aux États-Unis. Il a confirmé que cette interdiction ne s'applique pas au Canada en raison du fait que contrairement au Canada, les États-Unis

66 ETHI, *Témoignages*, Cynthia Khoo. Le rapport du Citizen Lab co-rédigé par Mme Khoo définit les techniques algorithmiques policières comme toutes les technologies nouvelles qui utilisent des formules de calcul automatisées pour appuyer ou compléter le processus décisionnel de la police.

67 ETHI, *Témoignages*, Brenda McPhail. Mme McPhail a donné l'exemple d'un projet de loi américain visant à imposer un moratoire sur l'utilisation de la technologie de reconnaissance faciale par le gouvernement jusqu'à ce que des règles régissant son utilisation soient en place; Congress.gov., « Text - S.3284 - 116th Congress (2019-2020): Ethical Use of Facial Recognition Act », 12 février 2020. Le projet de loi a été renvoyé à un Comité du Sénat américain, mais il n'a pas progressé depuis.

ne disposent pas d'un régime fédéral en matière de protection des renseignements personnels, c'est-à-dire de lois générales sur la protection de la vie privée[68].

M. Stairs, du SPT, a indiqué qu'il ne croit pas qu'un moratoire sur l'utilisation de la TRF par les forces policières devrait être imposé jusqu'à ce que la technologie soit davantage réglementée. Selon lui, il y a un équilibre entre les avantages qu'offre la TRF sur le plan de la sécurité publique et les problèmes liés aux droits de la personne qu'elle peut présenter. L'important est de savoir quand déployer la technologie. Pour le SPT c'est uniquement dans le cas de crimes graves ou de dossiers importants.

M. Therrien a aussi indiqué ne pas être en faveur d'un moratoire complet. Il a souligné qu'un moratoire ne peut être imposé que par une loi. Le commissaire n'a pas le pouvoir d'imposer un moratoire. La position des commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux est que des lois devraient prescrire quand la RF peut être utilisée à des fins légitimes et utiles et pour le bien de la société (p. ex., enquêtes relatives à des crimes graves ou la recherche d'enfants disparus). Les utilisations permises devraient être définies de manière assez étroite et la loi devrait aussi prescrire les utilisations interdites. Cette interdiction représenterait un moratoire partiel sur l'utilisation de la TRF.

M. Therrien a dit qu'il considère qu'il faut pouvoir utiliser la TRF dans des circonstances impérieuses. Il a noté que si la GRC s'engageait à n'utiliser la TRF qu'en fonction de sa nouvelle politique (utilisation à des fins ciblées, limitée dans le temps, assujettie à des vérifications par des experts formés et comme outil d'enquête et non de vérification d'identité) cela consisterait aussi en une forme de moratoire partiel volontaire jusqu'à ce que la loi soit bonifiée[69].

En ce qui concerne les interdictions, Mme McPhail a indiqué que l'ACLC soutient une interdiction complète de l'utilisation de la TRF à des fins de surveillance de masse[70]. Mme Molnar a mentionné qu'il y a des discussions en cours en Europe sur l'interdiction totale de la surveillance biométrique généralisée, de la TRF à haut risque et des détecteurs de mensonges de type IA dans le domaine des migrations et des frontières. Selon elle, le Canada devrait interdire l'utilisation à haut risque de la TRF à la frontière. M. Farooq a indiqué que l'utilisation de la TRF en temps réel dans les aéroports et les postes frontaliers

68 ETHI, *Témoignages*, Owen Larter, 1550 et 1610.

69 ETHI, *Témoignages*, Daniel Therrien, 1135 et 1210.

70 Voir aussi : Mémoire Ligue des droits et libertés, p. 6. L'organisation estime que trois usages de la technologie de reconnaissance faciale devraient faire l'objet d'une interdiction immédiate par voie législative : la surveillance de masse des lieux et endroits publics ; la surveillance de masse en ligne; et l'utilisation de banques d'images constituées par des organismes publics ou ministères.

devraient être interdite. Mme Bandhari a recommandé d'interdire le recours à la TRF au gouvernement et aux forces de l'ordre. M. Israël a recommandé d'interdire de façon permanente l'utilisation de la reconnaissance biométrique automatisée en direct par la police dans les lieux publics.

Outre un moratoire ou une interdiction, M. Khanna a suggéré l'adoption d'une Charte des droits numériques des Canadiens qui reconnaîtrait le caractère sacro-saint des données personnelles comme les données faciales. Une telle Charte pourrait être en harmonie avec la Charte canadienne des droits et libertés. Selon lui, elle permettrait aux Canadiens d'avoir et d'utiliser une forme portable et sécurisée de données biométriques sachant qu'elles ont un caractère sacro-saint. Il a aussi invité les législateurs à utiliser la planification de scénarios afin de les aider à orienter des stratégies et des politiques de résilience face aux avancées numériques.

Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale

Le 2 mai 2022, le commissaire à la protection de la vie privée fédéral et ses homologues provinciaux et territoriaux ont publié un document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale (document d'orientation)[71].

M. Therrien a expliqué que ce document d'orientation vise à aider les services de police à s'assurer que toute utilisation de la TRF est conforme à la loi, limite les risques d'atteintes à la vie privée et respecte le droit à la vie privée. Il a précisé que le document d'orientation a été rédigé à la suite d'une consultation publique nationale impliquant un large éventail de personnes. Les intervenants étaient d'accord pour dire que dans sa forme actuelle, la loi est insuffisante. Ils ne s'entendaient toutefois pas sur la teneur d'une nouvelle loi ou de nouvelles dispositions législatives[72].

M. Therrien a souligné qu'en attendant la modification des lois, le document d'orientation offre des conseils aux services de police sur la manière d'appliquer les lois

71 CPVP, *Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, mai 2022.

72 Des groupes représentant la société civile, des groupes minoritaires et la police ont participé à la consultation. M. Therrien a entre autres rencontré la Gendarmerie royale du Canada et l'Association canadienne des chefs de police à plusieurs reprises. Ces homologues provinciaux ont rencontré les équivalents provinciaux.

actuelles à la TRF. Il espère que ces conseils atténueront les risques que cette technologie pose.

M. Therrien a aussi reconnu que certains intervenants avaient manifesté le désir que les orientations fournies par les commissaires contiennent des conseils sur des cas d'utilisation précis pendant la consultation. Bien qu'il ait convenu qu'il est nécessaire de fournir des conseils sur des utilisations particulières dans divers contextes, il a indiqué que les commissaires pensent qu'il est important et pertinent de disposer de conseils généraux qui peuvent être complétés à mesure que les cas d'utilisation sont définis.

Mme Kosseim a noté qu'il faudra peut-être plusieurs années avant d'avoir une jurisprudence en vertu de la Charte relative à la TRF. C'est pourquoi les commissaires recommandent l'adoption d'un cadre législatif. Dans l'intervalle, ils ont élaboré les lignes directrices contenues dans le document d'orientation pour atténuer les risques que pose la TRF.

Mme Kosseim a présenté cinq éléments importants du document d'orientation :

> Premièrement, avant de recourir à la reconnaissance faciale à quelque fin que ce soit, les services de police doivent établir que la loi les autorise à le faire. Cela n'est pas acquis et ne peut pas être présumé […]
>
> Deuxièmement, les services de police doivent établir des mesures rigoureuses en matière de responsabilité. Ainsi, ils doivent intégrer des mesures de protection de la vie privée à toutes les étapes d'un projet de reconnaissance faciale et mener une évaluation des facteurs relatifs à la vie privée, ou une EFVP, afin de déterminer les risques et de les atténuer avant la mise en œuvre […]
>
> Troisièmement, les services de police doivent garantir la qualité et l'exactitude des renseignements personnels utilisés par le système de RF, afin de prévenir les faux positifs, de réduire les risques de préjugés et d'éviter de causer des préjudices à des particuliers, des groupes ou des communautés […].
>
> Quatrièmement, les services de police ne devraient pas conserver de renseignements personnels plus longtemps que nécessaire […].
>
> Cinquièmement, les services de police doivent s'occuper des questions de transparence et de communication avec le public. Dans le contexte d'enquêtes policières, il n'est pas toujours possible d'avertir directement le public chaque fois que la reconnaissance faciale est utilisée. Cependant, il est possible pour un service de police de faire preuve de transparence au niveau des programmes […].

Mme Kosseim a aussi précisé que la communication avec le public ne doit pas être à sens unique. Elle a noté que les principaux intervenants et, en particulier, les représentants des groupes faisant l'objet d'une surveillance policière excessive doivent

être consultés au cours de la conception même du programme de RF d'un service de police. Elle a rajouté que compte tenu de l'importance de la réconciliation au Canada, la consultation devrait inclure la participation des communautés et des groupes autochtones.

Mme Kosseim a indiqué que les principes de base mis de l'avant dans le document d'orientation devraient s'appliquer, peu importe le secteur, mais avec les adaptations nécessaires selon le contexte et l'éventail des risques en jeu, puisqu'il a été conçu à la base pour les services policiers.

M. Therrien a fait des commentaires similaires, notant un élément commun qui s'applique de façon horizontale à tous les acteurs qui souhaitent utiliser la TRF, qu'il s'agisse de la police, du gouvernement ou d'entreprises : le principe de nécessité et proportionnalité. Par exemple, dans le cas des services de police, recourir à la TRF peut entraîner des conséquences extrêmement graves, voire une perte de liberté. Ainsi, une interdiction totale pour les services de police d'avoir recours à la TRF dans certaines circonstances ne s'appliquerait pas nécessairement à tous les acteurs. Il a confirmé que les recommandations formulées par les commissaires peuvent également s'appliquer à l'utilisation de la TRF dans les espaces publics.

Législation

En ce qui concerne la réglementation de la TRF et de l'IA, la majorité des témoins se sont entendus pour dire que bien que le cadre législatif actuel offre certaines protections, il est insuffisant.

Par exemple, M. Therrien a dit qu'il existe un ensemble disparate de lois qui régissent la RF : la *Charte canadienne des droits et liberté*, la common law et certaines lois, dont celles sur la protection des renseignements personnels[73]. Le problème, selon lui, est qu'à l'heure actuelle, cet ensemble de lois peut être utilisé de nombreuses façons. Ainsi, il estime que les règles actuelles sont trop vagues pour offrir le niveau de confiance que les citoyens devraient avoir à l'égard de la collecte de renseignements par le secteur public et privé.

Mme Piovesan a fait des commentaires similaires. Elle a expliqué que les lois fédérales en matière de protection des renseignements personnels (la *Loi sur la protection des renseignements personnels* et la LPRPDE), dans leur forme actuelle, prévoient certaines

73 Mémoire CMTD et CPE, p. 4; Mémoire CSILC, p. 4. Ces intervenants mentionnent aussi les obligations du Canada en vertu de l'article 12 de la *Déclaration Universelle des Droits de l'Homme* et des articles 17 et 21 du *Pacte international relatif aux droits civils et politiques*.

garanties qui s'appliquent à l'utilisation de la TRF. Par exemple, elle a noté que la LPRPDE oblige les sociétés à obtenir un consentement pour recueillir les données très sensibles et pour les organismes publics, la loi et la common law encadrent déjà la manière dont certains renseignements peuvent être recueillis, stockés et conservés. Cependant, elle a précisé qu'aucune loi suffisamment exhaustive ou ciblée n'encadre la TRF.

Mme Thomasen a expliqué que les systèmes de surveillance faciale sont des systèmes sociotechniques. On ne peut pas les comprendre en examinant simplement la conception d'un système : « Il faut aussi considérer la manière dont le système interagira avec les utilisateurs, les personnes visées et les milieux sociaux dans lesquels le système est déployé. » Elle a souligné que dans une partie du contexte sociotechnique dans lequel la surveillance faciale est implantée, les lois d'applications générales et leurs théories sous-jacentes ont des lacunes et ne protègent pas adéquatement les gens contre l'utilisation abusive de cet outil.

Le Comité note que le projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, déposé à la Chambre des communes en juin 2022, s'il est adopté dans sa version actuelle, pourrait adresser certaines lacunes du régime législatif actuel en matière de protection des renseignements personnels qui s'applique à la TRF et l'IA[74]. Toutefois puisque le projet de loi n'a pas encore été adopté, le Comité fait ses recommandations en fonction du régime législatif toujours en place.

Cadre législatif pour le secteur public et privé

Pour établir un cadre réglementaire relativement complet de la TRF de sorte à prévenir les menaces que cette technologie représente et à tirer profit des avantages réels qu'elle peut offrir, Mme Piovesan a noté que le Canada devrait considérer quatre principes en matière d'IA qui sont conformes aux Principes sur l'IA de l'Organisation de coopération

74 LegisInfo, Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, 44e Parlement, 1e session (projet de loi C-27). Le projet de loi a été déposé à la Chambre des communes le 16 juin 2022; Sabrina Charland, Alexandra Savoie, Ryan van den Berg, *Résumé législatif du projet de loi C-27 : Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Bibliothèque du Parlement, Publication n° 44-1-C27F, 12 juillet 2022.

et développement économique (OCDE)[75] et aux principales orientations qui guident l'utilisation responsable de l'IA dans le monde. Les Principes sur l'IA de l'OCDE sont : la fiabilité technique, la responsabilité, la légitimé et l'équité.

Par exemple, elle a indiqué qu'en ce qui concerne la fiabilité technique, on peut se demander s'il faut associer des critères techniques précis aux différentes utilisations possibles de la TRF et si des parties tierces indépendantes devraient exercer une surveillance et assurer l'évaluation de la TRF d'un point de vue technique. En matière de responsabilité, on peut se demander, quels seront les mécanismes de contrôle administratifs qui devraient être en place (p. ex., une évaluation sur les incidences), qui les établira, et quelles parties prenantes devront être consultées. En ce qui a trait à la légitimité, on peut se demander quels mécanismes de surveillance sont requis pour assurer une utilisation de la TRF respectueuse des valeurs sociales et du droit. Enfin, en matière d'équité, des questions relatives aux effets préjudiciables de la TRF pour les droits et les libertés et les moyens d'atténuer ces incidences doivent être posées[76].

Le Comité note que les diverses mesures législatives proposées par les témoins pourraient répondre à plusieurs des questions que soulève Mme Piovesan.

En matière d'application de la loi, plusieurs témoins ont recommandé d'octroyer plus de pouvoirs au commissaire à la protection de la vie privée fédéral, dont le pouvoir d'émettre des ordonnances et d'imposer des amendes sévères comme celles que l'on retrouve dans le règlement général sur la protection des données (RGPD) du Parlement européen[77]. M. Therrien a lui-même indiqué que les pouvoirs du commissariat devraient être renforcés pour rendre ses décisions contraignantes[78].

En ce qui concerne le consentement, Mme Piovesan a noté qu'il ne devrait pas être écarté à titre d'exigence pour des données biométriques immuables, même s'il peut varier selon le scénario d'utilisation. Selon elle « [a]voir un avis approprié, et accorder un certain contrôle à la personne sur les décisions relatives au partage des données ou à la façon dont elles sont recueillies est absolument essentiel ». Mme Khoo était aussi d'avis

---

75 Organisation de coopération et développement économique (OECD), *Principes sur l'IA de l'Organisation*.

76 ETHI, *Témoignages*, Carole Piovesan.

77 ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Carole Piovesan; ETHI, *Témoignages*, Tim McSorley; ETHI, *Témoignages*, Brenda McPhail; ETHI, *Témoignages*, Tamir Israel; Mémoire CSILC, pp. 9-12.

78 Le projet de loi C-27, si adopté dans sa version actuelle, donnerait au commissaire à la protection de la vie privée le pouvoir d'émettre des ordonnances contraignantes. Il ne lui donnerait toutefois pas le pouvoir d'imposer des pénalités ou amendes. Ce pouvoir serait réservé au nouveau tribunal que crée le projet de loi. Voir les articles 94-95 de la Loi sur la protection de la vie privée des consommateurs que crée le projet de loi (LPVPC).

que les Canadiens doivent être en mesure de donner leur consentement préalable et éclairé avant la collecte de données les concernant.

Mme LaPlante a indiqué que les règlements doivent fournir aux développeurs, aux personnes chargées de la mise en œuvre et aux utilisateurs de la TRF des exigences et obligations claires à l'égard des utilisations précises de cette technologie, dont « l'obligation d'obtenir un consentement explicite pour la collecte et l'utilisation de données biométriques, ainsi que la limitation de la finalité pour éviter le détournement d'usage ». Elle a toutefois noté que les règlements devraient chercher à adopter une approche équilibrée, qui réduit, dans la mesure du possible, les charges administratives et financières pour les entités publiques et privées.

M. Israel a recommandé de modifier la *Loi sur la protection des renseignements personnels* et la LPRPDE afin que la collecte, l'utilisation et la communication de renseignements biométriques nécessitent un consentement explicite dans tous les contextes. Il a aussi recommandé de définir les renseignements biométriques comme des renseignements sensibles, comme c'est le cas dans la loi québécoise[79]. Mme Bhandari a indiqué qu'il est essentiel d'exiger le consentement des gens lorsque leurs données biométriques sont saisies. M. Labonté a noté que les gens devraient pouvoir comprendre à quelles fins leurs données sont utilisées et donner leur consentement éclairé.

Mme Poitras a toutefois fait remarquer que le consentement des personnes dans le contexte de la RF n'est pas toujours approprié puisqu'il y a une asymétrie de pouvoirs entre le citoyen et l'État ou le citoyen et une grande entreprise comme les géants du Web[80]. Elle a expliqué que la façon de pallier le consentement est de définir, dans la loi, certaines utilisations acceptables et d'interdire les autres, car peu importe qu'il y ait consentement ou autorisation, l'usage n'est pas approprié dans une société démocratique.

M. McSorley a recommandé que les lois sur la protection des renseignements personnels dans le secteur privé soient basées sur les droits de la personne, mais aussi sur la nécessité et la proportionnalité de l'utilisation des renseignements personnels. La réglementation devrait contenir des règles claires sur le consentement et des règles devraient s'appliquer à la surveillance et au développement de l'IA dans le secteur

79 Voir aussi : Mémoire CMTD et CPE, p. 5. Ces intervenants ont aussi recommandé que les lois fédérales sur la protection des renseignements personnels soient modifiées de manière à prévoir une protection spéciale pour les renseignements biométriques, dont un avis et un consentement avant son utilisation ou une permission législative.

80 Voir aussi : ETHI, *Témoignages*, Elizabeth Anne Watkins.

privé[81]. Mme LaPlante a aussi indiqué que les mesures législatives sur la TRF devraient s'appuyer sur les principes de nécessité et de proportionnalité.

En ce qui concerne le secteur public, M. McSorley a recommandé d'établir clairement les utilisations interdites et d'établir des règles claires en ce qui concerne la publication des évaluations des facteurs relatifs à la vie privée. Il a aussi recommandé de prévoir un examen obligatoire des répercussions sur les droits de la personne, de la précision et de la partialité des outils de surveillance algorithmiques ou biométriques utilisés par les forces de l'ordre.

Mme Polsky a affirmé qu'il faut promulguer des lois qui obligent toute personne qui crée, achète ou utilise une technologie à prouver qu'elle a une compréhension claire et correcte des lois canadiennes et des droits en matière de protection de la vie privée. Comme les véhicules et aliments font l'objet de réglementations gouvernementales strictes avant que leur vente ou leur utilisation soit autorisée, les créateurs de technologies devraient être assujettis à des lois qui les obligent à se soumettre à un examen indépendant complet visant à évaluer l'intégrité de leurs algorithmes et de leur accès aux renseignements personnels, de même que l'impartialité et l'incidence de leur technologie[82].

Mme Polsky a proposé que la technologie soit soumise à un banc d'essai neutre dirigé par le commissaire à la protection de la vie privée et impliquant d'autres groupes de la société civile afin qu'elle soit approuvée avant que sa vente ne soit autorisée au Canada. Le Centre for Media Technology and Democracy et le Cybersecure policy exchange ont recommandé l'harmonisation de la *Loi sur la protection des renseignements personnels* et de la LPRPDE avec la *Directive sur la prise de décision automatisée* du gouvernement fédéral[83].

M. Israel a proposé une approche similaire. Selon lui, il incombe au gouvernement de justifier l'utilisation de la TRF. Il a recommandé que la *Loi sur la protection des renseignements personnels* et la LPRPDE soient modifiées afin que les entreprises et les institutions fédérales soient légalement tenues de déposer des évaluations d'incidence

81 *Ibid*.

82 *Ibid*. L'article 15 de la Loi sur l'intelligence artificielle crée par le projet de loi C-27 permettrait au ministre désigné sous la loi d'ordonner, s'il a des motifs raisonnables de croire qu'une personne a contrevenu aux exigences prévues sous la loi, qu'une organisation fasse une vérification de la possible contravention ou retienne les services d'un vérificateur indépendant pour effectuer cette vérification et fournir un rapport au ministre. La vérification ne se ferait pas faite avant la mise en marché d'un produit. Les obligations contenues dans la Loi sur l'intelligence artificielle ne s'appliqueraient pas aux institutions fédérales.

83 Mémoire CMTD et CPE, p. 5.

auprès du commissaire à la protection de la vie privée avant d'adopter des technologies intrusives. Le commissaire devrait alors avoir l'autorité d'examiner ces technologies dans le cadre d'un processus réglementaire public et de mettre en place des restrictions d'utilisation, voire des moratoires, au besoin[84].

M. Israel a aussi indiqué qu'il est important d'inscrire dans la loi qu'un humain doit intervenir dans la prise de décision qui utilise des technologies fondées sur l'IA, même s'il a noté que l'intervention humaine ne résout pas tous les problèmes de partialité. Il a affirmé que quand on utilise un système de reconnaissance faciale, la tendance est de faire confiance aux résultats automatisés et de présumer que la réponse est exacte, ce qui peut finir par induire des biais cognitifs. M. Farooq a aussi convenu que les vérifications humaines sont importantes, mais il a affirmé que dans le contexte d'application de la loi, par exemple, compte tenu du problème de racisme et de préjugés systémiques au sein des services de police, le tribunal est l'endroit indiqué pour assurer l'équilibre des pouvoirs.

Ce faisant, M. Mohammad a recommandé que le gouvernement adopte une loi claire sur la protection de la vie privée qui limite rigoureusement la façon dont la TRF peut être utilisée dans un contexte autre que la consommation. Selon le CNMC, une telle loi devrait imposer une interdiction générale du recours à la TRF par le gouvernement sans autorisation judiciaire, particulièrement pour les organismes de sécurité nationale. Elle devrait aussi contenir des sanctions claires pour les organisations qui violent les règles relatives à la protection de la vie privée. M. Farooq a dit que le processus permettant l'utilisation de la TRF devrait ressembler à celui que la police doit suivre pour obtenir un mandat de perquisition : se présenter devant un juge avec un argumentaire et des documents clairs (éléments de preuve)[85].

En ce qui concerne la LPRPDE, M. Therrien a expliqué qu'une législation fondée sur les principes et neutre sur le plan technologique pour le secteur privé est un bon point de départ. Toutefois, il a dit que la TRF montre les limites des avantages d'une approche basée sur les principes, puisqu'une telle approche laisse beaucoup de latitude, par exemple à la police, pour exercer ces grands principes d'une manière qui convient à ces intérêts. En raison des risques la TRF comporte, il devrait selon M. Therrien y avoir des

84 Le projet de loi C-27 propose de créer une Loi sur l'intelligence artificielle et les données (Loi sur l'IA), qui impose certaines exigences à l'égard de systèmes d'intelligence artificielle à incidence élevée. Le commissaire à la protection de la vie privée n'est pas responsable de l'application de cette loi. La responsabilité revient au ministre de l'Industrie ou au ministre désigné sous la loi. Le ministre peut désigner un cadre supérieur comme commissaire à l'intelligence artificielle et les données. La Loi sur l'IA proposée ne contient pas d'exigence explicite relative à la tenue d'évaluation des facteurs relatifs à la vie privée.

85 ETHI, *Témoignages*, Mustafa Farooq.

dispositions particulières pour interdire l'utilisation de cette technologie, sauf dans certaines catégories de circonstances[86]. Il a expliqué que les commissaires sont d'avis que la législation devrait définir les utilisations « permises » et celles « interdites ».

De son côté, Mme McPhail a dit au Comité qu'il faut accorder une attention particulière non seulement aux protections techniques de la vie privée, mais aussi aux protections contextuelles pertinentes pour l'ensemble des droits mis en cause par cette technologie. Elle a recommandé l'adoption d'une loi intersectionnelle sur la protection des données qui s'appuie sur le cadre des droits de la personne. Elle a noté que des lois ciblées régissant la biométrie ou les technologies algorithmiques pourraient être encore plus adaptées aux besoins. Une mesure législative complète et efficace qui s'applique à la TRF devrait fournir un cadre juridique clair pour l'utilisation de cette technologie; des dispositions rigoureuses en matière de responsabilité et de transparence; une surveillance indépendante et des mesures de coercition efficaces en cas de non-respect.

M. Therrien a aussi fait remarquer que la TRF met en cause plusieurs autres droits que celui de la protection des renseignements personnels, comme le droit à l'égalité et les droits démocratiques. Il a noté qu'il est donc possible qu'un certain nombre d'organismes de réglementation, incluant le CPVP, soient responsables de l'application de la loi en ce qui concerne ce type de technologie. Par exemple, la Commission canadienne des droits de la personne ou les équivalents provinciaux pourraient être responsables dans les cas de discrimination.

M. Khanna a indiqué que la législation applicable à la TRF devrait s'appuyer sur les recherches et connaissances sur les minorités radicalisées, les Premières Nations, les enfants, et toute personne qui est plus vulnérable à ce genre d'exploitation. Par exemple, il a recommandé de consulter les orientations stratégiques de l'UNICEF sur l'IA destinée aux enfants[87]. Il a aussi indiqué qu'il faut tirer parti de l'expérience des gens de l'industrie afin d'égaliser et de créer un système approprié entre les connaissances du législateur et celles des entreprises qui se servent de cette technologie à l'interne.

---

86 Le projet de loi C-27, si adopté dans sa forme actuelle, crée une Loi sur l'intelligence artificielle qui réglemente les échanges et le commerce internationaux et interprovinciaux en matière de systèmes d'intelligence artificielle, en établissant des exigences communes à l'échelle du Canada pour la conception, le développement et l'utilisation de ces systèmes. La loi interdirait aussi certaines conduites relativement aux systèmes d'intelligence artificielle qui peuvent cause un préjudice sérieux aux individus ou un préjudice à leurs intérêts.

87 UNICEF, *Orientations stratégiques sur l'IA destinée aux enfants*. Le rapport souligne l'existence de jouets pour enfants qui interagissent avec eux à l'aide d'intelligence artificielle et des risques qu'ils présentent, entre autres en matière de sécurité et vie privée (p. 24).

Mme Polsky, au contraire, a indiqué que les normes applicables devraient être rédigées sans l'influence ou la contribution directe ou indirecte de l'industrie[88]. Elle a aussi proposé d'adopter un texte législatif global qui s'appliquerait tant au secteur public qu'au secteur privé et aux organismes à but non lucratif et partis politiques et remplacerait les mesures législatives fragmentées qui existent présentement aux niveaux fédéral, provincial et territorial.

Enfin, certains témoins ont suggéré que des modifications pourraient aussi être apportées à des lois autres que celles relatives à la protection des renseignements personnels.

Par exemple, M. Therrien a noté que si dans certaines circonstances on exigeait un mandat délivré par un tribunal pour l'utilisation de la TRF, des modifications devraient peut-être être apportées au Code criminel. M. Israel a recommandé de modifier le Code criminel pour limiter l'utilisation de la TRF par les forces de l'ordre dans le cadre d'enquêtes sur des crimes graves et en l'absence de motifs raisonnables de croire à une infraction. M. Farooq a mentionné la possibilité d'apporter des modifications à la *Loi sur la GRC* ou la *Loi sur le Service canadien du renseignement de la sécurité*, sans toutefois préciser quelles dispositions devraient être modifiées.

Cadre législatif pour les services de police

Mme Kosseim a dit que la principale recommandation des commissaires porte sur l'établissement éventuel d'un cadre législatif complet pour régir l'utilisation de la TRF par les services de police. Il faut établir des balises claires ayant force de loi pour que les services de police puissent faire usage de la TRF dans un cadre transparent et susceptible de mériter la confiance durable du public.

M. Therrien a expliqué que ses collègues et lui sont d'avis que le cadre législatif qui devrait s'appliquer à l'utilisation de la TRF par les services de police devrait être fondé sur quatre éléments :

> Nous recommandons en premier lieu que la loi définisse clairement et de manière explicite les fins pour lesquelles les services de police seraient autorisés à faire usage de la technologie de reconnaissance faciale, en plus d'interdire tout autre usage. Les fins autorisées devraient être impérieuses et proportionnelles aux risques très élevés que présente la technologie.
>
> En deuxième lieu, puisqu'il n'est pas réaliste de penser que la loi puisse prévoir toutes les situations possibles, il importe qu'en plus de prévoir des restrictions concernant les

88 ETHI, *Témoignages*, Sharon Polsky.

> fins autorisées, la loi exige aussi que l'utilisation de la reconnaissance faciale par les services de police soit à la fois nécessaire et proportionnelle pour tout déploiement donné de la technologie.
>
> En troisième lieu, nous recommandons que l'usage de la reconnaissance faciale par les services de police fasse l'objet d'une surveillance indépendante rigoureuse. Cette surveillance devrait inclure des mesures de mobilisation préventive, comme des évaluations des facteurs relatifs à la vie privée, ou EFVP, des autorisations préalables au niveau des programmes, des préavis avant l'utilisation de la technologie ou le pouvoir de réaliser des vérifications et de rendre des ordonnances.
>
> Enfin, nous recommandons que des mesures de protection de la vie privée appropriées soient mises en place afin d'atténuer les risques pour les personnes, y compris des mesures relatives à l'exactitude, à la conservation et à la transparence dans le cadre des projets d'utilisation de la reconnaissance faciale.

M. Therrien a soulevé la possibilité, par exemple, d'imposer l'exigence d'une autorisation d'un commissaire à la protection de la vie privée pour tout programme des forces policières visant l'utilisation de la TRF. Il a suggéré que le cadre de surveillance de la technologie adoptée et utilisée devrait inclure le pouvoir d'enquêter sur les plaintes et de rendre des décisions sur la légalité de l'utilisation de la technologie dans un cas donné.

La Commission canadienne des droits de la personne a indiqué que le cadre juridique relatif à l'utilisation de la TRF par les services de police nécessite une nouvelle approche fondée sur les droits de la personne, qui intègre les mécanismes de protection des droits de la personne concernant les enfants et des jeunes. Une telle approche utilise les droits de la personne internationaux comme fondement[89].

Meilleures pratiques dans d'autres juridictions

Au Québec, comme l'a expliqué Mme Poitras, les banques de données biométriques et le recours à la biométrie à des fins d'identification sont encadrés par la *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI) et par les lois protégeant les renseignements personnels applicables aux organisations publiques et privées[90]. En vertu de la LCCJTI, la création d'une banque de données biométriques doit être

89 Mémoire CCDP, pp. 8-13. Les cinq éléments à la base d'une approche fondée sur les droits de la personne sont : la légalité, la non-discrimination, la participation, l'autonomisation et la reddition de compte.

90 Québec, Loi concernant le cadre juridique des technologies de l'information, chapitre C-1.1 [LCCJTI]; Québec, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [Loi du Québec dans le secteur public] chapitre A-2.1; Québec, *Loi sur la protection des renseignements personnels dans le secteur privé*, chapitre P-39.1 [Loi du Québec dans le secteur privé].

divulguée à la Commission d'accès à l'information du Québec (CAI). À partir de septembre 2022, la divulgation requise inclura toute utilisation de la biométrique à des fins d'identification. Mme Poitras a noté que la LCCJTI pourrait être améliorée, en élargissant sa portée. La loi impose uniquement des obligations lorsque le recours à la biométrie, dont la TRF, sert à vérifier l'identité. Pourtant, la TRF peut servir à d'autres fins.

Mme Poitras a expliqué que dans sa province :

> [O]n ne peut recourir à la biométrie à des fins d'identification sans le consentement exprès de la personne concernée. Aucune caractéristique biométrique ne peut être saisie à son insu. Seul le minimum de caractéristiques biométriques peut être recueilli et utilisé. Tout autre renseignement qui pourrait être découvert à partir de ces caractéristiques ne peut être ni utilisé ni conservé. Enfin, les renseignements biométriques et toute note les concernant doivent être détruits lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli. La Commission a de larges pouvoirs et peut rendre toute ordonnance concernant de telles banques, incluant les pouvoirs de suspendre ou d'interdire leur mise en service ou d'ordonner leur destruction. En plus de ces dispositions précises, les règles générales relatives à la protection des renseignements personnels s'appliquent. Cela implique, entre autres, que le recours à la reconnaissance faciale soit nécessaire et proportionnel à l'objectif poursuivi.

Mme Poitras a aussi souligné qu'à partir de septembre 2023, une évaluation des facteurs relatifs à la vie privée sera obligatoire au Québec et que les renseignements biométriques sont expressément désignés comme renseignements personnels sensibles[91].

Aux États-Unis, M. Larter a indiqué qu'en 2021, l'État de Washington a adopté une loi, qui comprend d'importantes mesures de transparence et de reddition de comptes à l'égard de l'utilisation de la TRF, dont une obligation de faire des mises à essai et d'assurer une intervention par un humain qui a reçu une formation adéquate[92]. Au Utah, le projet de loi intitulé S.B. 34 Governmental Use of Facial Recognition Technology, adopté en 2021, exige que les organismes gouvernementaux avisent les personnes

91 Assemblée nationale du Québec, Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Adopté en septembre 2021, ce projet de loi modifie la Loi du Québec dans le secteur public et la Loi du Québec dans le secteur privé pour y inclure cette obligation. Sauf exception, les dispositions du projet de loi entrent en vigueur le 22 septembre 2023.

92 Washington State Legislature, SB 6289 – 2019-20, Concerning the use of facial recognition services [DISPONIBLE EN ANGLAIS SEULEMENT]. En vertu de ce projet de loi, les agences locales et de l'État de Washington, y compris les forces de l'ordre, qui utilisent ou prévoient utiliser la technologie de reconnaissance faciale, doivent respecter certaines exigences en matière de rapports et de déploiement.

concernées lorsqu'ils saisissent des images qui pourraient être traitées au moyen de la TRF et un préavis de 30 jours avant l'utilisation proposée[93].

En 2008, l'État de l'Illinois a adopté en 2008 la *Biometric Information Privacy Act* (BIPA). Cette loi interdit aux entreprises de vendre les renseignements biométriques des consommateurs ou d'en profiter de toute manière[94]. Mme Watkins a souligné que la BIPA a permis à d'intenter des poursuites contre Facebook pour avoir utilisé la reconnaissance faciale dans leurs processus d'identification avec photo[95]. Mme Bhandari a expliqué que la loi a aussi permis à l'ACLU d'intenter une poursuite contre Clearview AI, qui s'est soldée par un règlement. En vertu de ce règlement, l'entreprise ne peut plus donner accès à sa base de données contenant des millions d'empreintes faciales à des entités privées partout au pays, à quelques exceptions près, et il lui est interdit de vendre sa technologie aux forces de l'ordre de l'Illinois pour une période de cinq ans[96].

Mme Bhandari a préconisé l'adoption d'une loi comme la BIPA de l'Illinois, mais avec certaines mises à jour. Elle a précisé qu'une loi sur la confidentialité des données biométriques devrait, selon l'ACLU, exiger clairement que les entreprises obtiennent un avis et un consentement écrit avant de faire la collecte, d'utiliser ou de communiquer des renseignements permettant d'identifier une personne. Elle devrait interdire aux entreprises de refuser des services aux personnes qui choisissent de ne pas donner leur consentement. Elle devrait obliger les entreprises à supprimer les identifiants biométriques qu'ils détiennent un an après la dernière interaction de la personne concernée avec l'entreprise[97].

Mme Bhandari a identifié deux autres modèles à suivre. Au Maine, le projet de loi intitulé An Act To Regulate the Use of Biometric Identifiers obligerait entre autres les entités privées à obtenir le consentement exprès des individus pour procéder à la collecte, l'utilisation et la communication d'identifiants biométriques. La loi interdirait aussi la vente de données biométriques et imposerait des limites en matière de

---

93 CPVP, *Lettre au Comité*, 13 mai 2022, p. 3.

94 *Ibid*.

95 Le Comité a invité Facebook à comparaître devant le comité dans le cadre de son étude, mais l'entreprise a refusé l'invitation, en expliquant que Facebook n'utilise plus la technologie de reconnaissance faciale; Meta, *An Update on Our Use of Face Recognition*, 2 novembre 2021 [DISPONIBLE EN ANGLAIS SEULEMENT]. Google a aussi été invité et a refusé l'invitation. Amazon a accepté l'invitation du Comité mais n'a pu comparaître à la suite d'un changement d'horaire. Aucune de ces entreprises n'ont soumis un mémoire au Comité.

96 ACLU, *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law*, 9 mai 2022, communiqué [DISPONIBLE EN ANGLAIS SEULEMENT].

97 Le projet de loi C-27, si adopté dans sa version actuelle, contient un droit au retrait à l'article 55 de la nouvelle LPVPC.

rétention des données. Au Maryland, un projet de loi intitulé The Biometric Data Privacy Act a été déposé. Il vise à créer un régime similaire à celui de l'Illinois[98].

M. Therrien a mentionné certains projets de lois fédéraux aux États-Unis, dont le Fourth Amendment Is Not For Sale Act, qui viserait à empêcher les courtiers de données de vendre des renseignements personnels aux organismes d'application de la loi sans surveillance judiciaire et interdirait l'utilisation de données obtenues illégalement par des organisations publiques[99]. Le Algorithmic Accountability Act, obligerait les organisations du secteur privé à effectuer des évaluations pour déterminer l'existence d'un biais algorithmique et mesurer l'efficacité des systèmes de décisions automatisés[100].

En ce qui concerne l'Europe, plusieurs témoins ont mentionné que le RGPD est un modèle à suivre en matière de protection des données[101]. En vertu du RGPD, les données biométriques, qui incluent les images faciales, sont considérées comme une catégorie spéciale de données qui sont interdites, à moins que le responsable du traitement puisse s'appuyer sur un fondement juridique et un motif de traitement de traitement valable[102].

Mme Piovesan a noté que le RGPD inclut un droit de recours et un droit d'opposition au profilage réalisé uniquement par des moyens automatiques[103]. Elle a aussi fait remarquer qu'en vertu du RGPD, des amendes peuvent être imposées pour l'utilisation de données des résidents de pays européens, même si les activités en question ne sont pas menées en territoires européens. Le RGPD a donc une portée extraterritoriale. Mme Watkins a souligné que le RGPD contient un certain droit à l'explication qui fait en

98 ACLU, *LD 1945 Biometric Identifiers: Fact Sheet*, document soumis au Comité ETHI, 21 juin 2022 (projet de loi du Maine); *ACLU, HB 259 – The Biometric Data Privacy Act: Amendment Recommendations and Fact Sheet* (Maryland), document soumis au Comité ETHI, 21 juin 2022 (projet de loi du Maryland). L'ACLU note que plusieurs amendements apportés au texte original du projet de loi par la Chambre des représentants du Maryland ont affaibli le projet de loi.

99 CPVP, *Lettre au Comité*, 13 mai 2022, p. 3. Un projet de loi identique a été déposé au Sénat : S.1265 - Fourth Amendment Is Not For Sale Act.

100 CPVP, *Lettre au Comité*, 13 mai 2022, p. 3. Un projet de loi identique a été déposé au Sénat : S.3572 - Algorithmic Accountability Act of 2022.

101 ETHI, *Témoignages*, Ana Brandusescu; ETHI, *Témoignages*, Elizabeth Anne Watkins.

102 Union européenne, EUR-Lex, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE); CPVP, *Lettre au Comité*, 13 mai 2022, p. 2.

103 Elle a noté qu'un droit similaire existe sous la loi québécoise également.

sorte, par exemple, qu'une entreprise doit fournir aux travailleurs un aperçu de la façon dont les décisions sont prises à leur égard par les systèmes automatisés[104].

La directive de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, a aussi été soulevée par des témoins[105]. Elle interdit aux forces de l'ordre de traiter des données biométriques dans le but d'identifier une personne de manière unique, sauf si la loi l'autorise, et de prendre des décisions basées uniquement sur le traitement automatisé, y compris le profilage, à moins que la législation européenne ou nationale offre des garanties appropriées pour les droits et libertés individuels[106].

Enfin, certains témoins ont mentionné la proposition de Législation sur l'intelligence artificielle de l'Union européenne (la proposition européenne)[107]. M. Therrien a expliqué ce qui suit à l'égard de cette proposition:

> [S]i elle est adoptée, interdirait aux secteurs public et privé d'utiliser des applications d'intelligence artificielle néfastes qui, entre autres, permettraient de manipuler des personnes ou d'exploiter les vulnérabilités d'individus en raison de certaines caractéristiques personnelles. Les applications non interdites qui présentent un risque élevé (comme celles qui utilisent la biométrie pour l'identification et la catégorisation) sont assujetties à des exigences légales particulières, comme l'adoption de mesures et de systèmes de gestion des risques; l'enregistrement des données; le contrôle humain général; l'utilisation de données exactes et représentatives pour entraîner l'intelligence artificielle; des évaluations *ex ante* de la conformité; et la responsabilité démontrable[108].

104 Le projet de loi C-27, s'il est adopté dans sa version actuelle, contient un droit à l'explication aux articles 63 et 64 de la LPVPC.

105 « Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil », *Journal officiel de l'Union européenne*.

106 Mémoire CMTD et CPE, p. 8.

107 Commission européenne, Proposition de Règlement du Parlement Européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union; ETHI, *Témoignages*, Petra Molnar; ETHI, *Témoignages*, Cynthia Khoo; ETHI, *Témoignages*, Alex LaPlante.

108 CPVP, *Lettre au Comité*, 13 mai 2022, p. 2.

M. Therrien a indiqué que la proposition européenne protège les droits constitutionnels et les droits de la personne. Mme Kosseim et Mme Poitras étaient d'accord avec lui.

Mme Piovesan a souligné qu'aborder la réglementation dans le domaine de l'IA selon une approche axée sur le risque, comme le fait la proposition européenne, est la tendance ailleurs dans le monde. La proposition européenne interdirait aussi l'utilisation de la TRF en temps réel dans les espaces publics pour des fins d'application de la loi[109].

Mme Molnar a indiqué que la proposition européenne reconnaît que les évaluations individuelles des risques aux fins du traitement des demandes d'immigration et d'asile sont à haut risque et interdit une telle évaluation si elle est susceptible d'être utilisée aux fins de profilage et pour renforcer la discrimination systémique.

En ce qui concerne le Royaume-Uni, M. Jenkins a mentionné le Surveillance Camera Code of Practice, qui offre dans ce pays une orientation relative à l'utilisation appropriée, par les autorités locales ou policières, de la surveillance par systèmes de caméras. Le code requiert que l'utilisation de la TRF soit toujours accompagnée d'une intervention humaine avant que soient prises des décisions susceptibles de nuire à la personne concernée[110]. Le Biometrics and Surveillance Camera Commissionner est l'organisme de surveillance indépendant qui assure le respect du code de pratique[111]. L'Écosse a aussi un Biometrics Commissioner depuis 2020, qui a publié une ébauche de code de pratique en avril 2022[112].

Observations et recommandations du Comité

Le Comité est d'avis que les témoins ont bien démontré l'insuffisance du cadre législatif actuel pour encadrer la TRF et l'IA. À la lumière de ce qui précède, le Comité fait les recommandations suivantes :

109 ETHI, *Réponse écrite soumise au Comité par Sharon Polsky*, 17 juin 2022; European Parliamentary Research Service, *STOA study on diverging obligations facing public and private sector applications of artificial intelligence* [DISPONIBLE EN ANGLAIS SEULEMENT].

110 Royaume-Uni, Home Office, *Surveillance Camera Code of Practice, 2021* [DISPONIBLE EN ANGLAIS SEULEMENT].

111 Royaume-Uni, *Biometrics and Surveillance Camera Commissioner* [DISPONIBLE EN ANGLAIS SEULEMENT]; Voir aussi : ETHI, *Réponse écrite soumise au Comité par Sharon Polsky*, 17 juin 2022.

112 Écosse, *Scottish Biometrics Commissioner*; Royaume-Uni, *Scottish Biometrics Commissioner Act 2020*; Voir aussi : ETHI, *Réponse écrite soumise au Comité par Sharon Polsky*, 17 juin 2022. En avril 2022, le commissaire écossais a publié une ébauche d'un code de pratique sur l'acquisition, la conservation, l'utilisation et la destruction des données biométriques à des fins de justice pénale et de la police en Écosse. [DISPONIBLE EN ANGLAIS SEULEMENT].

Recommandation 11

Que le gouvernement définisse dans la ou les lois appropriées les utilisations acceptables de la technologie de reconnaissance faciale ou d'autres technologies algorithmiques et interdise les autres utilisations, dont la surveillance de masse.

Recommandation 12

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'exiger qu'avant l'adoption, la création, et l'utilisation de la technologie de reconnaissance faciale les organismes gouvernementaux demandent l'avis et les recommandations du commissaire à la protection de la vie privée et déposent des évaluations d'incidence auprès de ce dernier.

Recommandation 13

Que le gouvernement mette à jour la *Loi canadienne sur les droits de la personne* afin de s'assurer qu'elle s'applique à la discrimination causée par l'utilisation de la technologie de reconnaissance faciale et d'autres technologies d'intelligence artificielle.

Recommandation 14

Que le gouvernement du Canada mette en œuvre le droit à l'effacement (« droit à l'oubli ») en exigeant des fournisseurs de services, des plateformes de médias sociaux et d'autres entités en ligne qui opèrent au Canada qu'ils suppriment toutes les informations personnelles des utilisateurs après une période déterminée suivant la fin de l'utilisation par les utilisateurs, y compris, mais sans s'y limiter, les photographies téléchargées, les informations de paiement, l'adresse et les coordonnées, les messages et les entrées de sondage.

Recommandation 15

Que le gouvernement du Canada mette en place une exigence de consentement à la collecte d'information biométrique par les entités du secteur privé et interdise à ces entités de subordonner la fourniture de biens ou de services à la communication d'informations biométriques.

Recommandation 16

Que le gouvernement du Canada renforce la capacité du Commissaire à la protection de la vie privée à imposer des pénalités significatives aux institutions fédérales et aux entités privées dont l'utilisation de la technologie de reconnaissance faciale viole la *Loi*

sur la protection des renseignements personnels **ou la** ***Loi sur la protection des renseignements personnels et documents électroniques*****, afin de dissuader toute utilisation abusive de cette technologie.**

Recommandation 17

Que le gouvernement du Canada modifie la ***Loi sur la protection des renseignements personnels*** **et la** ***Loi sur la protection des renseignements personnels et documents électroniques*** **afin d'interdire la pratique de la capture d'images de Canadiens sur Internet ou dans des espaces publics dans le but d'alimenter les bases de données de la technologie de reconnaissance faciale ou les algorithmes d'intelligence artificielle.**

Recommandation 18

Que le gouvernement du Canada impose un moratoire fédéral sur l'utilisation de la technologie de reconnaissance faciale par les services de police (fédéral), et les industries canadiennes à moins qu'elle ne soit mis en œuvre en consultation confirmée avec le Commissariat à la protection de la vie privée ou sur autorisation judiciaire; et que le gouvernement élabore activement un cadre réglementaire concernant les utilisations, les interdictions, la surveillance et la protection de la vie privée à l'égard de la technologie de reconnaissance faciale, et que la surveillance devrait inclure des mesures d'engagement proactives ; une autorisation au niveau du programme ou une notification préalable avant l'utilisation ; et des pouvoirs de vérification et d'ordonnance.

Recommandation 19

Que le gouvernement fédéral veille à ce que des mesures de protection de la vie privée appropriées soient mises en place pour atténuer les risques pour les personnes, y compris des mesures portant sur l'exactitude, la conservation et la transparence des initiatives de reconnaissance faciale, ainsi qu'une stratégie globale portant sur le consentement éclairé des Canadiens à l'utilisation de leurs renseignements personnels.

CONCLUSION

L'étude du Comité a confirmé que le régime législatif actuel au Canada n'est pas suffisant pour bien encadrer la TRF et l'IA. Faute d'encadrement approprié, la TRF et d'autres outils d'IA pourraient causer des dommages irréparables pour certains individus.

Par conséquent, le Comité est d'avis que lorsque la TRF ou d'autres technologies d'IA sont utilisées, elles doivent l'être de façon responsable, dans le respect d'un cadre législatif robuste qui protège le droit des Canadiens et des Canadiennes à la vie privée et

assure le maintien de leurs libertés civiles. Puisque ce cadre législatif n'existe pas à l'heure actuelle, une pause nationale devrait être imposée à l'égard de l'utilisation de la TRF, particulièrement en ce qui concerne les services policiers.

Le Comité encourage fortement le gouvernement du Canada à mettre ses recommandations en œuvre le plus rapidement possible.

ANNEXE A
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
À titre personnel	2022/03/21	11
Ana Brandusescu, experte en gouvernance de l'intelligence artificielle		
Cynthia Khoo, chercheuse universitaire The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto		
Kristen Thomasen, professeure Peter A. Allard School of Law, University of British Columbia		
INQ Law	2022/03/21	11
Carole Piovesan, associée directrice		
Refugee Law Lab	2022/03/21	11
Petra Molnar, avocate York University		
Association canadienne des libertés civiles	2022/03/24	12
Brenda McPhail, directrice Programme de la vie privée, de technologie et de surveillance		
Borealis AI	2022/03/24	12
Alex LaPlante, directrice principale Engagement produit et commercial		
Centre de Recherche Informatique de Montréal	2022/03/24	12
Françoys Labonté, président-directeur général		
Coalition pour la surveillance internationale des libertés civiles	2022/03/24	12
Tim McSorley, coordinateur national		

Organismes et individus	Date	Réunion
À titre personnel	2022/04/04	15
Rob Jenkins, professeur University of York		
Sanjay Khanna, conseiller stratégique et expert en prospective		
Angelina Wang, chercheuse diplômée en science informatique Princeton University		
Elizabeth Anne Watkins, attachée de recherche au niveau postdoctoral Princeton University		
Commission des services policiers de Toronto	2022/04/28	17
Dubi Kanengisser, conseiller principal Analyse stratégique et politique		
Gendarmerie royale du Canada	2022/04/28	17
André Boileau, officier responsable Centre national contre l'exploitation d'enfants		
Paul Boudreau, sous-commissaire par intérim Services de police spécialisés		
Toronto Police Service	2022/04/28	17
Colin Stairs, directeur de l'information		
Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario	2022/05/02	18
Patricia Kosseim, commissaire		
Vance Lockton, conseiller principal en technologie et politique		
Commission d'accès à l'information du Québec	2022/05/02	18
Diane Poitras, présidente		
Commissariat à la protection de la vie privée du Canada	2022/05/02	18
Daniel Therrien, commissaire à la protection de la vie privée du canada		
David Weinkauf, analyste principal de recherche en informatique		

Organismes et individus	Date	Réunion
Conseil national des musulmans canadiens	2022/05/05	19
Mustafa Farooq, président-directeur général		
Rizwan Mohammad, agent des services d'assistance judiciaire		
Microsoft	2022/05/05	19
Owen Larter, directeur Politiques publiques en matière d'Intelligence Artificielle responsable		
Gendarmerie royale du Canada	2022/05/09	20
André Boileau, officier responsable Centre national contre l'exploitation d'enfants		
Gordon Sage, directeur général Services d'enquêtes spécialisées et de nature délicate		
Roch Séguin, directeur Sous-direction des services Stratégiques, Opérations techniques		
Toronto Police Service	2022/05/09	20
Colin Stairs, directeur de l'information		
À titre personnel	2022/06/09	25
Nestor Maslej, associé de recherche Institute for Human-Centered Artificial Intelligence, Stanford University		
Conseil du Canada de l'accès et la vie privée	2022/06/09	25
Sharon Polsky, présidente		
American Civil Liberties Union	2022/06/16	27
Esha Bhandari, directrice adjointe		
Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko	2022/06/16	27
Tamir Israel, avocat-conseil à l'interne		

ANNEXE B
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Commission canadienne des droits de la personne

Centre for Media, Technology and Democracy

Coalition pour la surveillance internationale des libertés civiles

Cybersecure Policy Exchange

Jenkins, Rob

Ligue des droits et libertés

Maslej, Nestor

Refugee Law Lab

Tessono, Christelle

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 11, 12, 15, 17-20, 25, 27, 28, 34 et 35) est déposé.

Respectueusement soumis,

Le président,
Pat Kelly