La technologie de reconnaissance faciale au Canada : Un bref survol des inconvénients et des avantages potentiels

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

Christelle Tesssono
4 mai 2022

SOMMAIRE

La présent mémoire recommande au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique d'interdire l'utilisation de la technologie de reconnaissance faciale par les organismes d'application de la loi[1]. Les préjudices associés aux erreurs d'identification et le manque de surveillance des organismes d'application de la loi l'emportent sur les avantages potentiels de son utilisation. Toutefois, si le Comité souhaite utiliser cette technologie dans des circonstances particulières, il devrait d'abord élaborer les garanties nécessaires pour protéger la vie privée des Canadiens.

A. INTRODUCTION

J'ai grandi dans Saint-Michel, un bel arrondissement d'immigrants situé dans l'est de Montréal. Enfant, comme tous les autres enfants du quartier, je jouais souvent dans le parc François-Perrault. La piscine, les terrains de tennis et de basketball étaient très populaires pendant les mois d'été. Au fil de la pandémie, le parc est devenu un endroit où je pouvais, en toute sécurité, passer beaucoup de temps à réfléchir pendant mes promenades quotidiennes.

En octobre 2021, le service de police municipal a annoncé l'installation de caméras de surveillance en circuit fermé dans le parc afin de lutter contre la montée de la violence armée dans la ville[2]. Il n'y a pas eu de consultation de la communauté à ce sujet et, comme de nombreux habitants du quartier, j'étais confuse et je me demandais à quoi serviraient les images. Mais plus important encore, je m'inquiétais de son impact sur les utilisateurs fréquents du parc : les immigrants, les personnes de la classe ouvrière, les jeunes racisés et les personnes âgées. Les images de vidéosurveillance recueillies dans des lieux comme le parc François-Perrault sont particulièrement utiles pour l'utilisation de la technologie de reconnaissance faciale.

En juin 2020, 77 experts et groupes de défense de la vie privée, des droits de la personne et des libertés civiles ont demandé au ministre de la Sécurité publique, Bill Blair, d'« interdire la surveillance par reconnaissance faciale par les services fédéraux d'application de la loi et du renseignement [et] d'établir des politiques et des lois claires et transparentes pour réglementer l'utilisation de la reconnaissance faciale au Canada[3] ». Comme l'affirme l'Association canadienne des libertés civiles, l'utilisation par la police de la technologie de reconnaissance faciale « indique une crise plus importante de la responsabilité de la police lors de l'acquisition et de l'utilisation d'outils de surveillance émergents[4] ». Compte tenu du marché croissant des entreprises qui fournissent cette technologie aux forces de l'ordre et de l'absence persistante de dispositions législatives protégeant les Canadiens, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique doit répondre à l'urgence de cette question avant que d'autres préjudices ne soient causés.

---

[1] Christelle est une chercheuse émergente au Center for Information Technology Policy (CITP) de l'Université de Princeton. Elle a été stagiaire parlementaire à la Chambre des communes du Canada dans le cadre du Programme de stage parlementaire, où elle a soutenu le travail législatif des députés de l'opposition et du gouvernement. Les opinions exprimées dans ce mémoire sont les siennes.

[2] Poirier, Y., « Le SPVM installera neuf nouvelles caméras de surveillance », *TVA Nouvelles*, 25 octobre 2021. Consulté le 27 avril 2022, https://www.tvanouvelles.ca/2021/10/25/le-spvm-installera-neuf-nouvelles-cameras-de-surveillance.

[3] *Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies,* 8 juillet 2020, https://ccla.org/wp-content/uploads/2021/07/facial-recognition-letter-08072020.pdf [TRADUCTION].

[4] McPhail, B., *L'ACLC et Privacy International collaborent sur des soumissions concernant les lignes directrices sur la reconnaissance faciale pour les services de police*, ACLC, 17 novembre 2021. Consulté le 27 avril 2022, à l'adresse https://ccla.org/fr/privacy/ccla-and-privacy-international-collaborate-on-submissions-regarding-facial-recognition-guidelines-for-police-agencies/.

Je suis profondément préoccupée par la sécurité de ma communauté et par les répercussions de la technologie de reconnaissance faciale sur les Canadiens. Pour apporter des solutions aux défis que je vois dans ma communauté et dans le pays, je recommande d'interdire l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre. Je commencerai par un aperçu des inconvénients de la technologie de reconnaissance faciale. Ensuite, je donne un aperçu du paysage législatif aux États-Unis pour illustrer la façon dont les différentes juridictions ont traité cette technologie. Enfin, je présente les principaux arguments en faveur d'une interdiction et explique pourquoi ils l'emportent sur les avantages potentiels de l'utilisation de la technologie de reconnaissance faciale.

B. APERÇU TECHNIQUE

Qu'est-ce que la technologie de reconnaissance faciale?

La technologie de reconnaissance faciale fait référence aux outils informatiques utilisés pour identifier, reconnaître et analyser les visages humains dans des images, des vidéos ou en temps réel[5]. Sur le plan technique, elle englobe l'ensemble des systèmes qui intègrent une ou plusieurs images de visages et produisent un résultat comme la similarité de deux visages, le sexe d'un visage ou une correspondance avec un visage dans une base de données.

Quelles sont les utilisations de la reconnaissance faciale?

La technologie de reconnaissance faciale est utilisée à différentes fins. Les utilisations courantes sont la vérification, l'identification et la caractérisation ou la catégorisation.

- *Vérification* : Autrement connu sous le nom de correspondance un à un (1:1), le logiciel confirme si un visage est le même que celui qui est enregistré[6]. Nous sommes confrontés à cette vérification lorsque nous essayons de déverrouiller nos téléphones intelligents ou d'accéder à nos applications de compte bancaire par reconnaissance faciale.

- *Identification* : Ce système est souvent appelé système un à plusieurs (1:n), car il cherche à identifier un individu précis en utilisant une image de celui-ci et en la comparant à celles d'une base de données. Il est couramment utilisé lorsqu'on essaie d'identifier un individu inconnu – par exemple, lorsque la police compare une photo à une base de données constituée de photos de criminels[7].

- *Catégorisation ou caractérisation* : Lorsqu'un logiciel est utilisé pour attribuer à un visage des caractéristiques telles que le sexe, la race et les émotions[8]. La technologie de reconnaissance faciale pour la caractérisation fait l'objet d'une étude[9] et d'un marché[10] croissants. Cependant, malgré les affirmations dans la littérature et des produits sur l'exactitude de leurs modèles, ils ont été largement critiqués pour avoir renforcé le

---

[5] Kroll, J. A., *ACM TechBrief: Facial Recognition Technology*, ACM, 2022, https://dl.acm.org/doi/pdf/10.1145/3520137, p. 2.
[6] Crumpler, W., et Lewis, J. A., *How Does Facial Recognition Work?: A Primer*, Center for Strategic and International Studies (CSIS), 2021, http://www.jstor.org/stable/resrep32894, p. 3.
[7] Balasubramaniam, L., Cooper-Simpson, C., Morello, J., et Pietrusiak, P., *Rapport provisoire : Technologie de reconnaissance faciale au Canada*, 2021. Consulté le 24 avril 2022 à l'adresse : https://ccla.org/wp-content/uploads/2021/07/Interim-Report-Compiled-BM.pdf, p. 8.
[8] Crumpler, W. et Lewis, J. A., *How Does Facial Recognition Work?*, 2021, p. 3.
[9] Peterson, J. C., Uddenberg, S., Griffiths, T. L., Todorov, A. et Suchow, J. W., « Deep models of superficial face judgments », *Proceedings of the National Academy of Sciences*, vol. 119, nº 17, 2022, e2115228119, https://doi.org/10.1073/pnas.2115228119.
[10] *Facial personality analytics*. faception. (sans date). Consulté le 27 avril 2022, à l'adresse : https://www.faception.com/.

racisme et le sexisme[11].

Quels sont les principaux problèmes associés à cette technologie?

1. *Inexactitude et discrimination* : Dans le cadre d'une étude menée par le National Institute of Standards and Technology (NIST) des États-Unis, on a testé 189 algorithmes différents sur 18 millions de photos afin d'examiner la précision des modèles. L'étude a révélé une proportion nettement plus élevée de fausses correspondances chez les Asiatiques, les Afro-Américains et les peuples autochtones. En outre, l'étude a révélé que les femmes, les enfants et les personnes âgées étaient également plus susceptibles d'être mal identifiés par les algorithmes[12, 13, 14]. Étant donné que les personnes marginalisées font l'objet d'une surveillance policière excessive, les modèles inexacts les exposent à un risque accru d'identification erronée et peuvent entraîner des préjudices réels[15]. Dans un récit récent de l'échec de cette technologie aux États-Unis, un jeune homme noir a été arrêté à tort et a passé dix jours en détention dans un centre pénitentiaire, puis s'est battu pendant un an pour que les accusations soient abandonnées[16].

2. *Fragilité* : Cette technologie est sujette à des attaques adverses, ce qui signifie que des acteurs peuvent tromper les modèles pour obtenir une mauvaise identification[17]. Par exemple, des chercheurs ont étudié l'impact du port d'accessoires tels qu'une paire de lunettes sur ces modèles[18].

3. *Interprétation* : Les systèmes de reconnaissance faciale développent leurs propres ensembles de modèles et de règles en analysant de grandes collections de données. Il est très difficile pour les chercheurs d'identifier ces règles et la manière dont le modèle prend ses décisions. Par conséquent, lorsqu'une personne est mal identifiée par un modèle, il n'existe aucun moyen clair pour l'ingénieur qui a construit le modèle de comprendre comment cette décision a été prise[19].

4. *Développement de modèles non éthiques* : Les systèmes de reconnaissance faciale sont formés sur de grands ensembles de données comprenant souvent des millions d'images qui n'ont pas été recueillies avec un consentement valable[20]. Par exemple, Clearview AI a admis avoir recueilli des données disponibles sur des sites Web comme Flickr, Google et Facebook. Dans son rapport d'enquête, le Commissariat à la protection de la vie privée du Canada a déclaré que Clearview AI a soutenu que les informations recueillies

---

[11] Stark, L., et Hutson, J., « Physiognomic Artificial Intelligence », *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3927300.

[12] Grother, P., Ngan, M. et Hanaoka, K., *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280), National Institute of Standards and Technology, 2019, https://doi.org/10.6028/NIST.IR.8280.

[13] Cette étude a révélé que les femmes à la peau foncée constituaient le groupe le plus mal classé, avec un taux d'erreur de 34,7 %, par rapport aux hommes à la peau claire qui ont connu un taux d'erreur de 0,8 % : Buolamwini, J., et Gebru, T., « Gender shades: Intersectional accuracy disparities in commercial gender classification », dans *Conference on fairness, accountability and transparency*, 2018, PMLR https://proceedings.mlr.press/v81/buolamwini18a.html.

[14] Melendez, S., « Uber Driver Troubles Raise Concerns About Transgender Face Recognition », *Fast Company*, 2018.

[15] Browne, S., *Dark matters: On the surveillance of blackness*, Presses de l'Université Duke, 2015.

[16] Johnson, K., « How wrongful arrests based on AI derailed 3 men's lives », *Wired*, 7 mars 2022. Consulté le 25 avril 2022, à l'adresse : https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.

[17] Goodfellow, I. J., Shlens, J. et Szegedy, C., *Explaining and Harnessing Adversarial Examples*, 2014, https://doi.org/10.48550/ARXIV.1412.6572.

[18] Sharif, M., Bhagavatula, S., Bauer, L. et Reiter, M. K., « Accessorize to a Crime: Real and Stealthy Attacks on State-of- the-Art Face Recognition », *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, p. 1528-1540, https://doi.org/10.1145/2976749.2978392.

[19] Linardatos, P., Papastefanopoulos, V., et Kotsiantis, S., « Explainable AI: A Review of Machine Learning Interpretability Methods », *Entropy*, vol. 23, nº 1, 2020, p. 18. https://doi.org/10.3390/e23010018.

[20] Balasubramaniam, L., et coll., *Interim Report*, 2021, p. 6.

> étaient réputées accessibles au public et qu'il n'y avait pas d'attente raisonnable en matière de vie privée pour les personnes qui téléchargeaient leurs photos en ligne. Toutefois, le CPVP a fait remarquer que la LPRPDE, en plus des commissaires provinciaux à la protection de la vie privée de la Colombie-Britannique et de l'Alberta, établissait une distinction entre ce qui est disponible publiquement et accessible publiquement. Par conséquent, les informations provenant de sites Web de réseaux sociaux ne sont pas visées par l'exception relative à l'accès public prévue par la LPRPDE. Ainsi, la collecte à partir de ces plateformes ne peut être autorisée qu'avec le consentement de l'intéressé[21].

C. STRATÉGIES LÉGISLATIVES AUX ÉTATS-UNIS

Au niveau fédéral, les États-Unis ne disposent pas d'une approche législative globale pour réglementer la technologie de reconnaissance faciale. Au lieu de cela, il existe une mosaïque d'ordonnances étatiques et locales[22]. Cette mosaïque peut être divisée en trois stratégies législatives : interdictions et moratoires, utilisations autorisées avec surveillance et utilisations non réglementées.

Moratoires

Les moratoires font référence à l'interdiction temporaire de l'utilisation de cette technologie. Ils sont souvent utilisés pour donner aux décideurs politiques le temps d'élaborer une législation. Aux États-Unis, des moratoires ont été adoptés dans très peu d'États, comme la Californie, la Virginie, le Vermont et New York. Ils ont une portée très limitée, car ils ne se concentrent que sur certaines utilisations de cette technologie, au lieu d'englober toutes les applications potentielles.

Par exemple, l'État de Californie a interdit aux forces de l'ordre [TRADUCTION] « d'installer, d'activer ou d'utiliser la surveillance biométrique avec une caméra d'agent ou les données recueillies par une caméra d'agent » jusqu'en 2023. Le projet de loi souligne comment la technologie de reconnaissance faciale pose « des menaces uniques et importantes aux droits civils et aux libertés civiles des résidents et des visiteurs » et a le potentiel de « diminuer l'efficacité du maintien de l'ordre et la sécurité publique[23] ». Toutefois, le projet de loi n'interdit pas à la police d'utiliser cette technologie sur des séquences provenant d'autres sources auxquelles elle a accès[24]. Alors que le Vermont et la Virginie se concentrent également sur l'application de la loi, leur moratoire s'applique à toutes les utilisations potentielles de la technologie de reconnaissance faciale, n'a pas de date d'expiration fixe et ne sera levé qu'en cas de nouvelle législation sur le sujet[25]. L'État de New York a également interdit l'utilisation de cette technologie dans les écoles primaires et secondaires publiques, privées et à charte, en

---

[21] Commissariat à la protection de la vie privée du Canada, *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*, 2021, p. 15-16, https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/21-50/publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-110-2021-fra.pdf.

[22] Feigelson, J., Gesser, A., Skrzypczyk, J., Gressel, A., et Gutierres, A.S. « Face Forward: Strategies for Complying with Facial Recognition Laws ». *Debevoise & Plimpton,* 19 octobre 2021. https://www.debevoisedatablog.com/2021/10/19/part-1-of-face-forward-strategies-for-complying-with-facial-recognition-laws/.

[23] Assemblée de l'État de Californie, *An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement, no. 1215*, 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215 [TRADUCTION].

[24] Samsel, H., « California becomes third state to ban facial recognition software in police body cameras », *Security Today*, 10 octobre 2019. Consulté le 2 mai 2022, à l'adresse : https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx.

[25] Feigelson, J. et coll., « Face Forward ».

attendant un rapport du commissaire à l'éducation[26].

Interdictions

Des interdictions complètes ont été mises en place par plusieurs autorités municipales aux États-Unis. À l'instar des moratoires, la mise en œuvre de ces interdictions a été motivée par des préoccupations concernant les violations des libertés civiles et les effets négatifs disproportionnés de l'utilisation de cette technologie sur les personnes racisées[27]. À l'heure actuelle, plus de 15 conseils municipaux ont mis en œuvre ces interdictions (par exemple, Oakland, San Francisco, Boston, Portland, Minneapolis)[28]. La portée des interdictions est souvent limitée à l'application de la loi, comme c'est le cas avec les moratoires. Il existe toutefois quelques exceptions notables : l'État du Maryland interdit aux employeurs d'utiliser la technologie de reconnaissance faciale, et la ville de Portland interdit également les entités privées dans ses limites[29].

La mise en œuvre des interdictions et des moratoires aux États-Unis est motivée par des préoccupations relatives à la vie privée et aux libertés civiles. En outre, elles fonctionnent toutes deux de la même manière puisqu'elles interdisent l'utilisation de la technologie de reconnaissance faciale. Elles diffèrent toutefois dans la mesure où l'interdiction devient permanente, tandis que le moratoire donne aux décideurs politiques plus de temps pour élaborer un cadre législatif. En somme, les moratoires reportent l'examen des questions de vie privée et de droits de la personne liées à l'utilisation de cette technologie[30].

Utilisation permise avec surveillance : application de la loi dans le Massachusetts

En juillet 2018 et mars 2019, l'American Civil Liberties Union (ACLU) du Massachusetts a déposé plus de 400 demandes de documents publics afin de mieux comprendre l'utilisation de la technologie de reconnaissance faciale au sein de l'État[31]. En examinant les dossiers communiqués, ils ont découvert que les agences gouvernementales, les écoles, les entreprises privées, les forces de l'ordre des villes et des villages avaient utilisé la technologie de reconnaissance faciale avec peu de surveillance[32]. Cela a incité les législateurs de l'assemblée de l'État à adopter l'*Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth* en décembre 2020.

Cette loi interdit aux forces de l'ordre du Massachusetts « d'acquérir, d'accéder ou

---

[26] *Ibid.*

[27] Guariglia, M., « Victory! Boston bans government use of face surveillance », *Electronic Frontier Foundation*, 26 juin 2020. Consulté le 27 avril 2022, à l'adresse : https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance.

[28] Feigelson, J. et coll. Face Forward.

[29] La ville de Portland a prévu trois exceptions à l'interdiction : 1) lorsque cela est nécessaire pour se conformer aux lois locales, étatiques ou fédérales 2) lorsque cela est nécessaire pour vérifier l'identité d'une personne sur les dispositifs de communication personnels ou fournis par l'employeur (par exemple, FaceID d'Apple pour l'iPhone), et enfin 3) sur les plateformes de réseaux sociaux telles qu'Instagram et Snapchat. Ville de Portland, *Prohibit the acquisition and use of Face Recognition Technologies by City bureaus*, n190113, 2020, https://efiles.portlandoregon.gov/Record/13945278.

[30] Owen, T., Ruths, D., Cairns, S., Parker, S., Reboul, C., Rowe, E., et Solomun, S., *Facial Recognition Moratorium Briefing #1: Implications of a Moratorium on the Use of Facial Recognition Technology in Canada*, Centre pour les médias, la technologie et la démocratie de l'Université McGill, 2020. https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1 p. 11.

[31] Peaslee, E., *Massachusetts pioneers rules for police use of Facial Recognition Tech*. NPR, 7 mai 2021. Consulté le 29 avril 2022, à l'adresse : https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech

[32] *The data for Justice Project: ACLU of Massachusetts - facial recognition in Massachusetts*. The Data for Justice Project | ACLU of Massachusetts, 27 février 2021. Consulté le 29 avril 2022 à l'adresse : https://data.aclum.org/public-records/frt-ma/

d'utiliser tout logiciel permettant la reconnaissance faciale, à l'exception du Registry of Motor Vehicles[33] ». Elle exige que les agences obtiennent un mandat de perquisition avant de demander une recherche au Registry of Motor Vehicles (sauf en cas d'urgence, comme un danger immédiat de mort ou de blessure physique grave). En outre, le Registry of Motor Vehicles est tenu de documenter chaque demande des forces de l'ordre et de la rendre publique sur son site Web. Il s'agit d'informations comme le nombre annuel total de perquisitions effectuées par chaque service de police, les perquisitions effectuées avec un mandat et les perquisitions effectuées pour des situations d'urgence sur une base annuelle. Enfin, la loi crée une commission législative chargée d'étudier l'utilisation de la reconnaissance faciale par le ministère des Transports du Massachusetts.

Cette loi est l'une des premières tentatives de l'État et du pays pour réglementer la technologie de reconnaissance faciale. Toutefois, les experts en matière de protection de la vie privée, notamment l'ACLU du Massachusetts, estiment que le projet de loi ne va pas assez loin. La directrice générale de l'organisation, Carol Rose, fait valoir que, si cela [TRADUCTION] « empêche la police d'utiliser ces informations lorsqu'elles ne sont pas pertinentes pour une enquête » – ce qui est important – cela représente une « norme assez faible[34] ».

Juridictions sans législation

Dans les juridictions sans législation, l'utilisation de la technologie de reconnaissance faciale par la police se fait sans aucune surveillance. Les civils peuvent être arrêtés après l'utilisation de cette technologie à leur insu. De fausses arrestations peuvent se produire en raison de l'inexactitude de la reconnaissance faciale, comme ce fut le cas pour Robert Williams, Michael Oliver et Nijeer Parks. Ces trois hommes ont été arrêtés à tort dans des États et des villes qui ne disposent d'aucune protection contre la surveillance par reconnaissance faciale par les forces de l'ordre. Bien que les accusations qui avaient été portées contre eux aient été abandonnées, ces arrestations sont lourdes de conséquences. Nijeer Parks a passé 10 jours en prison, et il a fallu un an pour que les accusations soient abandonnées.
Robert Williams a été arrêté par la police devant sa fille de quatre ans et a été retenu par la police pendant 30 heures. Michael Oliver a perdu son emploi à cause de la fausse arrestation et a passé plus d'un an à reconstruire sa vie[35].

D. RECOMMANDATIONS

1. **Interdire l'utilisation de la technologie de reconnaissance faciale automatisée par les forces de l'ordre.**
2. **Interdire notamment l'utilisation par les forces de l'ordre de séquences en temps réel et enregistrées pour les technologies de reconnaissance faciale automatisée.**
3. **Interdire aux forces de l'ordre de se procurer des technologies de reconnaissance faciale automatisée auprès d'entités tierces.**

---

[33] Association de la police du Massachusetts. (sans date). *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. Association des policiers du Massachusetts, p. 4, https://masspolice.com/wp-content/uploads/2020/07/legislativesummary.pdf [TRADUCTION].

[34] Peaslee, E. *Massachusetts pioneers rules for police use of Facial Recognition Tech* [TRADUCTION].

[35] Johnson, K., « How wrongful arrests based on AI derailed 3 men's lives », *Wired*, 7 mars 2022. Consulté le 25 avril 2022, à l'adresse : https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.

Raisons expliquant l'interdiction de l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre

Les problèmes techniques liés à la reconnaissance faciale ne peuvent être résolus dans un avenir prévisible. Comme je l'ai indiqué dans mon survol technique, les technologies de reconnaissance faciale automatisée ont été testées et se sont révélées inexactes. Les chercheurs continuent d'éprouver des difficultés lorsqu'ils tentent d'interpréter pourquoi et quand les modèles identifient mal les personnes.

En outre, l'imprécision de la technologie exacerbe la discrimination à l'égard des groupes historiquement marginalisés. La recherche a prouvé que cette technologie est discriminatoire envers les femmes, les personnes racisées, les jeunes et les personnes âgées. En raison du profilage racial, ces groupes sont davantage exposés aux préjudices liés à la surveillance.

Enfin, les entreprises qui fournissent des technologies de reconnaissance faciale aux forces de l'ordre sont exposées à des atteintes à la sécurité des données. Les bases de données de reconnaissance faciale contiennent des données très sensibles, et nous n'avons pas encore pris en compte les préjudices causés par les atteintes à ces bases de données. Par exemple, en 2020, les services de police de Toronto ont signalé une atteinte à la sécurité qui a compromis la liste de clients, le nombre de comptes d'utilisateurs et le nombre de recherches qui avaient été effectuées à l'aide de la technologie de reconnaissance faciale[36].

Les contre-arguments fondés sur les avantages potentiels de la technologie ne sont pas convaincants

Ceux qui s'opposent à l'interdiction soulignent les avantages potentiels liés à l'utilisation de la technologie de reconnaissance faciale. Les services de police affirment être en mesure de résoudre des enquêtes plus rapidement et à moindre coût grâce à cette technologie[37]. Ils soulignent notamment qu'elle a été utilisée avec succès pour retrouver des enfants victimes d'abus et leurs agresseurs[38].

La sécurité des enfants doit être prise au sérieux, et je suis d'accord avec les critiques pour dire qu'il est impératif d'avoir tous les outils à notre disposition. Cependant, je ne pense pas que la technologie de reconnaissance faciale soit l'outil dont nous avons besoin pour résoudre ces enquêtes. Les recherches montrent que la technologie de reconnaissance faciale « n'est pas conçue pour prendre en compte les enfants et peut, en fait, donner de mauvais résultats lorsqu'elle est appliquée aux enfants[39] ». Par conséquent, même dans les cas optimistes, les défis techniques et sociaux associés à l'utilisation de cette technologie sont bien présents et ne peuvent être ignorés[40].

---

[36] Owen, T. et coll. *Facial Recognition Moratorium Briefing #1* p. 8; et Aguilar, B., *Company behind controversial facial recognition software used by Toronto Police Suffers Data Breach,* Toronto, 26 février 2020. Consulté le 26 avril 2022, à l'adresse : https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200.

[37] Hill, K., « What happens when our faces are tracked everywhere we go? », *The New York Times*, 18 mars 2021. Consulté le 28 avril 2022, à l'adresse : https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html.

[38] Hill, K., et Dance, G. J. X., « Clearview's facial recognition app is identifying child victims of abuse », *The New York Times*, 7 février 2020. Consulté le 26 avril 2022, à l'adresse : https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-abus-sexuels-enfants.html.

[39] Berman, G., Carter, K., García-Herranz, M. et Sekara, V., *Digital Contact Tracing and Surveillance during COVID- 19: General and Child-specific Ethical Issues,* 2020, p. 15, https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf, [TRADUCTION].

[40] Stark, L., *Facial Recognition & Canadian Youth* (série d'essais sur les enfants et la technologie), Centre pour les médias, la

À la suite de la tentative d'insurrection dans le Capitole américain le 6 janvier 2021, les forces de l'ordre aux États-Unis se sont efforcées d'identifier les auteurs en utilisant la technologie de reconnaissance faciale[41]. Cela a suscité de nombreux débats, notamment sur la question de savoir si cette technologie devrait être utilisée dans des cas d'urgence nationale comme celui-ci. Si l'on pense à l'occupation du « convoi de la liberté » à Ottawa l'année dernière, la question devrait également être soulevée. Pourrions-nous justifier l'utilisation de cette technologie au Canada pour des cas comme ceux-là? Je soutiens que nous ne devrions pas.

Malgré son utilité potentielle dans des circonstances extrêmes comme celles-ci, l'interdiction de la technologie de reconnaissance faciale reste importante, car en l'absence de surveillance, les forces de l'ordre au Canada ne peuvent être tenues responsables de leurs actions. Nous avons vu comment la présence du racisme systémique dans l'application de la loi met en danger les Canadiens racisés. En outre, la technologie de reconnaissance faciale est utilisée pour opprimer et surveiller les populations dans d'autres pays. En appliquant une interdiction, notre gouvernement a l'occasion de montrer à la communauté internationale comment utiliser la technologie de manière responsable.

Dans son enquête sur Clearview AI, le Commissariat à la protection de la vie privée du Canada a indiqué que la Gendarmerie royale du Canada « nous avait tout d'abord indiqué, à tort, qu'elle n'avait pas recours à la technologie de Clearview AI » et que, lorsqu'elle a ensuite reconnu son utilisation, elle « n'a pas été en mesure de rendre compte de manière satisfaisante de la grande majorité des recherches qu'elle a effectuées[42] ». Le Commissariat à la protection de la vie privée a fait valoir que « les politiques et les systèmes de la GRC présentent des lacunes graves et systémiques au chapitre du suivi, de l'identification, de l'examen et du contrôle des nouvelles collectes de renseignements personnels », ce qui est un élément essentiel pour se conformer à la loi[43]. En l'absence de dispositions protégeant les informations biométriques, les Canadiens sont « plus exposés à la surveillance par les forces de l'ordre ainsi qu'à des violations de nos droits fondamentaux protégés par la Charte des droits et libertés[44] ». Les « faiblesses cumulatives du système juridique canadien peuvent être exploitées par les organismes d'application de la loi et les entreprises technologiques », comme ce fut le cas avec l'utilisation de Clearview AI par la GRC. En l'absence de mécanismes de protection solides, les Canadiens risquent de subir des préjudices plus importants, tant au niveau national qu'international[45].

En juin 2021, le Comité permanent de la sécurité publique et nationale a publié un rapport sur le racisme systémique dans les services policiers au Canada. Le rapport décrit en détail les façons dont le racisme systémique affecte les Canadiens racisés, plus particulièrement les femmes et les filles autochtones, les personnes bispirituelles et les autres membres de la communauté LGBTQ+. L'effet du racisme systémique se traduit notamment par une exposition « disproportionnée [des] femmes et [des] filles autochtones et racialisées à la discrimination

---

technologie et la démocratie de l'Univrsité McGill, 2021, https://www.mediatechdemocracy.com/work/facial-recognition-and-canadian-youth.

[41] Kelley, J., « Face surveillance and the capitol attack », *Electronic Frontier Foundation*, 12 janvier 2021. Consulté le 2 mai 2022, à l'adresse : https://www.eff.org/deeplinks/2021/01/face-surveillance-and-capitol-attack.

[42] Commissaire à la protection de la vie privée du Canada, *Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée,* p. 2-3.

[43] *Ibid*, p.3

[44] Stevens, Y., et Brandusescu, A., *Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada*, 2021, p. 13, https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada [TRADUCTION].

[45] Stevens, Y., et Brandusescu, A., *Weak Privacy*, p. 16 [TRADUCTION].

policière, comme le profilage racial et l'usage excessif de la force », mais aussi par « l'inaction des services de police pour protéger ces femmes contre la violence fondée sur le sexe et les homicides[46] ». Le rapport du Comité comprenait une liste de 42 recommandations, qui n'ont pas encore été pleinement mises en œuvre et dont les conséquences n'ont pas encore été examinées. Par conséquent, le déploiement de la technologie de reconnaissance faciale, un outil imprécis et inefficace, présente des risques importants au Canada pour les communautés à la fois visées par des interventions policières excessives et insuffisantes. Les rapports de la police enquêtant sur les activistes et leurs partisans ne sont pas nouveaux; par exemple, la police de Toronto a compilé des rapports de renseignements par courriel sur les activistes du mouvement Black Lives Matters en 2016[47].

Au niveau international, la technologie de reconnaissance faciale est utilisée pour opprimer les communautés marginalisées. Par exemple, les Ouïghours en Chine font l'objet d'un profilage racial par les forces de l'ordre grâce à la technologie de reconnaissance faciale, comme c'est le cas au Brésil pour les Afro-Brésiliens[48, 49]. Au Myanmar, la junte militaire l'utilise pour contrer la dissidence en surveillant les civils[50]. Compte tenu de ces pratiques dommageables, je crois que le gouvernement canadien a ici l'occasion de montrer à la communauté internationale comment protéger efficacement les civils contre la surveillance par les forces de l'ordre.

Comme solution deuxième recours, le Comité pourrait envisager de promulguer un moratoire

Si le Comité décidait d'autoriser l'utilisation de la technologie de reconnaissance faciale dans des circonstances particulières, il devrait mettre en place le cadre législatif nécessaire pour garantir que les Canadiens ne soient pas exposés à des risques d'identification erronée et de surveillance de masse. Dans ce cas, un moratoire donnerait le temps de construire ce cadre législatif. Il pourrait s'agir, entre autres, de veiller à ce que la technologie de reconnaissance faciale ne soit utilisée qu'en cas de mandat délivré par un tribunal dans le cadre d'enquêtes criminelles formelles. En outre, dans ces cas, la technologie de reconnaissance faciale ne devrait être utilisée que sur des séquences enregistrées, et non sur des séquences en temps réel.

En outre, j'invite le Comité à suivre les recommandations de politique générale formulées par le Commissariat à la protection de la vie privée du Canada et les chercheurs d'institutions telles que l'Association canadienne des libertés civiles, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko et Citizen Lab[51, 52]. Le Center on Privacy &

---

[46] Canada, Parlement, Comité permanent de la sécurité publique et nationale, *Racisme systémique au sein des services policiers au Canada*. 43e législature, 2e session, 2021. Extrait du site Web du Parlement du Canada : https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-f.pdf, p. 45.

[47] Davis, S., « Police monitored black lives matter Toronto protesters in 2016, documents show », *CBC News*, 3 mai 2018. Consulté le 2 mai 2022, à l'adresse : https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628.

[48] Ormerod, A. G., « How AI reinforces racism in Brazil », *Rest of World*, 22 avril 2022. Consulté le 26 avril 2022 à l'adresse : https://restofworld.org/2022/how-ai-reinforces-racism-in-brazil/.

[49] Mozur, P., « One month, 500,000 face scans: How China is using A.I. to profile a minority », *The New York Times*, 14 avril 2019. Consulté le 26 avril 2022, à l'adresse : https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[50] Human Rights Watch, « Myanmar: Facial recognition system threatens rights », 12 mars 2021. Consulté le 26 avril 2022, à l'adresse : https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights.

[51] Voir les rapports suivants : Balasubramaniam, L. et coll. (2021). *Interim Report,* Israel, T. (2020). Facial recognition at a crossroads: Transformation at our borders and beyond. *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC). https://cippic.ca/uploads/FR_Transforming_Borders.pdf*, Robertson, K., Khoo, C., et Song, Y. (2020). *To surveil and predict: A human rights analysis of algorithmic policing in Canada.* Citizen Lab et Programme international des droits de la personne, Université de Toronto https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf.

[52] Commissariat à la protection de la vie privée du Canada, « Les autorités de protection de la vie privée réclament un cadre juridique limitant le recours à la technologie de reconnaissance faciale par les services de police », communiqué, 2 mai 2022.

Technology de l'Université de Georgetown, aux États-Unis, propose un modèle législatif et 30 recommandations déterminantes que j'invite les décideurs canadiens à suivre[53]. Et surtout, le Centre pour les médias, la technologie et la démocratie expose des considérations importantes, comme l'élaboration d'un cadre de gouvernance des données et de mécanismes de reddition de comptes[54]. En Europe, la directive sur l'application de la loi est également un modèle de politique à suivre[55].

Mais surtout, j'exhorte les membres du Comité à centrer les voix des victimes de la brutalité policière, qui incluent, sans s'y limiter, les LGBTQ+, les handicapés, les pauvres, les immigrants et les sans-papiers, les Noirs, les Autochtones et les autres personnes racisées. Leurs expériences doivent servir de point de départ pour la réglementation dans le pays, car ils détiennent des connaissances essentielles sur les répercussions de la surveillance policière sur eux et leurs communautés.

E. CONCLUSION

Les quartiers où habitent les gens de la classe ouvrière, les immigrants et les personnes de couleur sont le théâtre de profilage racial depuis des décennies à Montréal[56]. Au nom de la sécurité, les élèves des écoles secondaires de Saint-Michel rencontrent tous les jours des agents de la police municipale qui les attendent devant les locaux de l'école. Apparemment, cette présence policière est censée favoriser les liens entre les jeunes et les agents, afin d'éliminer les conflits. Cependant, cela n'a pour effet que d'accroître le risque de profilage des étudiants. Mais ce qui est encore plus inquiétant, c'est que des plans visant à déployer un programme similaire dans les écoles primaires sont en cours[57]. Les jeunes étant les premières victimes de cette surveillance dans le cadre de contrôles dans la rue et d'un usage excessif de la force, je suis profondément préoccupée par les ramifications potentielles de l'utilisation de la technologie de reconnaissance faciale.

La technologie de reconnaissance faciale s'inscrit dans une tendance plus large d'utilisation des algorithmes par les services policiers. À ce titre, les travaux futurs du Comité devraient viser à réglementer les autres types d'outils automatisés utilisés par les services de l'ordre. En outre, bien que la technologie de reconnaissance faciale soit déjà largement utilisée par les forces de l'ordre, elle peut également être utilisée dans le secteur commercial et par d'autres organismes gouvernementaux. Par conséquent, j'exhorte les membres du Comité à prendre également en considération les technologies biométriques, qui comprennent notamment la reconnaissance faciale, dans ces secteurs.

Consulté le 4 mai 2022, à l'adresse : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2022/nr-c_220502/.

[53] Garvie, C., *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law, Center on Privacy & Technology, 2016. https://www.perpetuallineup.org/sites/default/files/2016-12/The Perpetual Line-Up – %20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[54] Owen, T., Ruths, D., Cairns, S., Reboul, C., Rowe, E. et Solomun, S., *Facial Recognition Moratorium Briefing #2: Conditions for Lifting a Moratorium on Public Use of Facial Recognition Technology in Canada*. Centre pour les médias, la technologie et la démocratie de l'Université McGill, 2020, https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1-wfgs7.

[55] Directive (EU) 2016/680 (directive sur l'application de la loi), article 10, https://eur-lex.europa.eu/eli/dir/2016/680/oj.

[56] Livingston, A.-M., Rutland, T., Alix, S., Jean-Claude, R., Abidou, Z. Y., Guillaume, W., Harim, R., Milien, M.-K., et Rémé, L., *Le profilage racial dans les pratiques policières : Points de vue et expériences de jeunes racisés à Montréal*, 2018, https://drive.google.com/file/d/1yCYtzCL-_mTHEZmsVv0hJu4yHL7j3n3Z/view.

[57] Marin, S., « Avant les coups de feu, le filet de prévention du SPVM dans Saint-Michel », *Le Devoir*, 25 avril 2022. Consulté le 29 avril 2022, à l'adresse : https://www.ledevoir.com/societe/703068/montreal-avant-les-coups-de-feu-le-filet-de-prevention-du-spvm-dans-saint-michel.

Liste de références

Aguilar, B. (2020, 26 février). *Company behind controversial facial recognition software used by Toronto Police Suffers Data Breach*. Toronto. Consulté le 26 avril 2022, à l'adresse : https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200

Balasubramaniam, L., Cooper-Simpson, C., Morello, J., et Pietrusiak, P. (2021). *Rapport provisoire : Technologie de reconnaissance faciale au Canada*. Consulté le 24 avril 2022, à l'adresse : https://ccla.org/wp-content/uploads/2021/07/Interim-Report-Compiled-BM.pdf

Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies. (2020, 8 juillet) https://ccla.org/wp-content/uploads/2021/07/facial-recognition- letter-08072020.pdf

Berman, G., Carter, K., García-Herranz, M. et Sekara, V. (2020). *Digital Contact Tracing and Surveillance during COVID-19: General and Child-specific Ethical Issues.* https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Presses de l'Université Duke.

Buolamwini, J., et Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Dans *Conference on fairness, accountability and transparency*. PMLR. https://proceedings.mlr.press/v81/buolamwini18a.html

Assemblée de l'État de Californie. *An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement, no. 1215*, (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

Canada, Parlement. Comité permanent de la sécurité publique et nationale. (2021). *Racisme systémique au sein des services policiers au Canada*. 43e Parl, 2e sess. Extrait du site Web du Parlement du Canada : https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-f.pdf

Ville de Portland. *Prohibit the acquisition and use of Face Recognition Technologies by City bureaus*, n190113 (2020). https://efiles.portlandoregon.gov/Record/13945278

Crumpler, W., et Lewis, J. A. (2021). *How Does Facial Recognition Work?: A Primer*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep32894

Davis, S. (2018, 3 mai). *Police monitored black lives matter Toronto protesters in 2016, documents show | CBC News*. CBCnews. Consulté le 2 mai 2022, à l'adresse : https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628

Facial personality analytics. faception. (sans date). Consulté le 27 avril 2022, à l'adresse : https://www.faception.com/

Feigelson, J., Gesser, A., Skrzypczyk, J., Gressel, A., et S. Gutierres, A.S. « Face Forward: Strategies for Complying with Facial Recognition Laws ». *Debevoise & Plimpton*. 19 octobre 2021.https://www.debevoisedatablog.com/2021/10/19/part-1-of-face-forward-strategies-for-complying-with-facial-recognition-laws/

Garvie, C. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law, Center on Privacy & Technology. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

Goodfellow, I. J., Shlens, J. et Szegedy, C. (2014). *Explaining and Harnessing Adversarial Examples*. https://doi.org/10.48550/ARXIV.1412.6572

Grother, P., Ngan, M. et Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Guariglia, M. (2020, 26 juin). *Victory! Boston bans government use of face surveillance*. Electronic Frontier Foundation. Consulté le 27 avril 2022, à l'adresse : https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance

Hill, K. (2021, 18 mars). *What happens when our faces are tracked everywhere we go?* The New York Times. Consulté le 28 avril 2022, à l'adresse : https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html

Hill, K., et Dance, G. J. X. (2020, 7 février). *Clearview's facial recognition app is identifying child victims of abuse*. The New York Times. Consulté le 26 avril 2022, à l'adresse :

https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html

Israel, T. (2020). Facial recognition at a crossroads: Transformation at our borders and beyond. *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC). https://cippic.ca/uploads/FR_Transforming_Borders.pdf*

Johnson, K. (2022, 7 mars). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Consulté le 25 avril 2022 à l'adresse : https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Johnson, K. (2022, 7 mars). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Consulté le 25 avril 2022 à l'adresse : https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Kelley, J. (2021, 12 janvier). *Face surveillance and the capitol attack*. Electronic Frontier Foundation. Consulté le 2 mai 2022, à l'adresse : https://www.eff.org/deeplinks/2021/01/face- surveillance-and-capitol-attack

Kroll, J. A. (2022). *ACM TechBrief: Facial Recognition Technology*. ACM. p.2 https://doi.org/10.1145/352013

Linardatos, P., Papastefanopoulos, V., et Kotsiantis, S. (2020). Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy*, *23*(1), 18. https://doi.org/10.3390/e23010018

Livingston, A.-M., Rutland, T., Alix, S., Jean-Claude, R., Abidou, Z. Y., Guillaume, W., Harim, R., Milien, M.-K., et Rémé, L. (2018). *Le profilage racial dans les pratiques policières : Points de vue et expériences de jeunes racisés à Montréal*. https://drive.google.com/file/d/1yCYtzCL-_mTHEZmsVv0hJu4yHL7j3n3Z/view

Marin, S. (2022, 25 avril). *Avant les coups de feu, le filet de prévention du SPVM dans Saint-Michel*. Le Devoir Consulté le 29 avril 2022, à l'adresse : https://www.ledevoir.com/societe/703068/montreal-avant-les-coups-de-feu-le-filet-de-prevention-du-spvm-dans-saint-michel

Association de la police du Massachusetts. (sans date). *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. Association de la police du Massachusetts https://masspolice.com/wp-content/uploads/2020/07/legislativesummary.pdf

McPhail, B. (2021, 17 novembre). *L'ACLC et Privacy International collaborent sur des soumissions concernant les lignes directrices sur la reconnaissance faciale pour les services de police*. ACLC. Consulté le 27 avril 2022, à l'adresse : https://ccla.org/privacy/ccla-and-privacy-international-collaborate-on-submissions-regarding-facial-recognition-guidelines-for-police-agencies/

Melendez, S. (2018). « Uber Driver Troubles Raise Concerns About Transgender Face Recognition ». *Fast Company*.

Mozur, P. (2019, 14 avril). *One month, 500,000 face scans: How China is using A.I. to profile a minority*. The New York Times. Consulté le 26 avril 2022, à l'adresse : https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Myanmar: Facial recognition system threatens rights. Human Rights Watch. (2021, 12 mars). Consulté le 26 avril 2022, à l'adresse : https://www.hrw.org/news/2021/03/12/myanmar-facial- recognition-system-threatens-rights

Commissariat à la protection de la vie privée du Canada. (2021). *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.* https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/21-50/publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-110-2021-fra.pdf

Commissariat à la protection de la vie privée du Canada. (2022, 2 mai). *Communiqué : Les autorités de protection de la vie privée réclament un cadre juridique limitant le recours à la technologie de reconnaissance faciale par les services de police*. Les autorités de protection de la vie privée réclament un cadre juridique limitant le recours à la technologie de reconnaissance faciale par les services de police – Commissariat à la protection de la vie privée du Canada. Consulté le 4 mai 2022, à l'adresse : https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

Ormerod, A. G. (2022, 22 avril). *How AI reinforces racism in Brazil*. Rest of World. Consulté le 26 avril 2022 à l'adresse : https://restofworld.org/2022/how-ai-reinforces-racism-in-brazil/

Owen, T., Ruths, D., Cairns, S., Parker, S., Reboul, C., Rowe, E. et Solomun, S. (2020). *Facial Recognition Moratorium Briefing #1: Implications of a Moratorium on the Use of Facial Recognition Technology in Canada*. Centre pour les médias, la technologie et la démocratie de l'Université McGill. https://www.mediatechdemocracy.com/work/facial-recognition-moratoire-briefing-1

Owen, T., Ruths, D., Cairns, S., Reboul, C., Rowe, E., et Solomun, S. (2020). *Facial*

Recognition Moratorium Briefing #2: Conditions for Lifting a Moratorium on Public Use of Facial Recognition Technology in Canada. Centre pour les médias, la technologie

et la démocratie de l'Université McGill. https://www.mediatechdemocracy.com/work/facial-recognition-moratoire-briefing-1-wfgs7

Peaslee, E. (2021, 7 mai). *Massachusetts pioneers rules for police use of Facial Recognition Tech*. NPR. Consulté le 29 avril 2022, à l'adresse : https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech

Peterson, J. C., Uddenberg, S., Griffiths, T. L., Todorov, A., et Suchow, J. W. (2022). Deep models of superficial face judgments. *Proceedings of the National Academy of Sciences*, *119*(17), e2115228119. https://doi.org/10.1073/pnas.2115228119

Poirier, Y. (2021, 25 octobre). *Le SPVM installera neuf nouvelles caméras de surveillance*. TVA Nouvelles. Consulté le 27 avril 2022, à l'adresse : https://www.tvanouvelles.ca/2021/10/25/le-spvm-installera-neuf-nouvelles-cameras-de-surveillance

Robertson, K., Khoo, C., et Song, Y. (2020). *To surveil and predict: A human rights analysis of algorithmic policing in Canada.* Citizen Lab et Programme international des droits de la personne, Université de Toronto. https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and- Predict.pdf

Samsel, H. (2019, 10 octobre). *California becomes third state to ban facial recognition software in police body cameras*. Security Today. Consulté le 2 mai 2022, à l'adresse : https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

Sharif, M., Bhagavatula, S., Bauer, L. et Reiter, M. K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stark, L. (2021). *Facial Recognition & Canadian Youth* (série d'essais sur les enfants et la technologie). Centre pour les médias, la technologie et la démocratie de l'Université McGill.https://www.mediatechdemocracy.com/work/facial-recognition-and-canadian-youth

Stark, L., et Hutson, J. (2021). Physiognomic Artificial Intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3927300

Stevens, Y., et Brandusescu, A. (2021). *Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada.https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada*

The data for Justice Project: ACLU of Massachusetts - facial recognition in Massachusetts. The Data for Justice Project | ACLU of Massachusetts. (2021, 27 février). Consulté le 29 avril 2022 à l'adresse : https://data.aclum.org/public-records/frt-ma/