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

par la
Coalition pour la surveillance internationale des libertés civiles (CSILC)

à propos de
l'étude par le Comité de
l'utilisation et des impacts de la technologie de reconnaissance faciale

Le 13 avril 2022

À propos de la Coalition pour la surveillance internationale des libertés civiles

La Coalition pour la surveillance internationale des libertés civiles (CSILC) est une coalition nationale d'organisations de la société civile canadienne qui a été créée après l'adoption de la *Loi antiterroriste* de 2001 afin de protéger et de promouvoir les droits de la personne et les libertés civiles dans le contexte de la soi-disant « guerre contre le terrorisme ». La coalition regroupe quelque 45 organisations non gouvernementales, syndicats, associations professionnelles, groupes confessionnels, organisations environnementales et de protection des droits de la personne et des libertés civiles, ainsi que des groupes représentant des communautés immigrantes et réfugiées au Canada.

Nous avons pour mandat de défendre les libertés civiles et les droits de la personne énoncés dans la Charte canadienne des droits et libertés, les lois fédérales et provinciales (comme la Déclaration canadienne des droits, la *Loi canadienne sur les droits de la personne*, les chartes provinciales des droits de la personne et les lois sur la protection de la vie privée) et les instruments internationaux relatifs aux droits de la personne (comme la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques, la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants).

Actifs dans la promotion et la défense des droits au sein de leurs secteurs respectifs de la société canadienne, les membres de la CSILC se sont réunis au sein de cette coalition pour partager leurs préoccupations relativement à la législation antiterroriste nationale et internationale, et d'autres mesures de sécurité nationale, et leur impact sur les libertés civiles, les droits de la personne, la protection des réfugiés, les groupes minoritaires, la dissidence politique, la gouvernance des organismes de bienfaisance, la coopération internationale et l'aide humanitaire.

Depuis sa création, la CSILC a réuni autour d'une table organisations et communautés touchées par l'application, à l'échelle internationale, de nouvelles lois entourant la sécurité nationale (« antiterroristes ») afin de permettre les échanges stratégiques – y compris des échanges internationaux et Nord-Sud.

La diffusion de renseignements relatifs aux droits de la personne dans le contexte de la lutte contre le terrorisme et de l'élargissement de l'appareil de sécurité nationale, qui n'a pas de comptes à rendre, est un élément important du rôle de la CSILC. Ces renseignements sont distribués aux membres de la coalition qui les diffusent à leur tour sur leurs propres réseaux.

Finalement, et conformément à son mandat, la CSILC est intervenue dans des cas particuliers d'allégations de graves violations des libertés civiles et des droits de la personne. La CSILC est également intervenue pour contester les projets de loi, les règlements et les pratiques contraires à la Constitution du Canada et à d'autres lois canadiennes et internationales relatives aux droits de la personne.

A. Positions de la CSILC sur la technologie de reconnaissance faciale (TRF)

Une partie centrale du travail de notre coalition a porté sur le besoin de mécanismes de reddition de comptes et de transparence et de cadres juridiques clairs pour régir les activités de surveillance des agences fédérales de maintien de l'ordre et du renseignement[1]. Les activités de surveillance des forces de l'ordre doivent rigoureusement respecter la Charte canadienne des droits et libertés, notamment en demandant une autorisation judiciaire pour une surveillance qui constituerait autrement une violation de la charte.

Nous avons régulièrement fait part de nos préoccupations relativement à la surveillance qui cible indûment des communautés particulières sous la forme de profilage racial, religieux ou politique, ainsi que la surveillance massive de lieux publics ou d'événements spécifiques. Ces formes de surveillance ne sont jamais justifiées, dans la mesure où elles violent non seulement le droit à la vie privée, mais aussi les droits de réunion, d'association et de circulation, ainsi que les droits à l'égalité. Cela comprend à la fois la surveillance visuelle – c'est-à-dire par caméra – mais aussi la surveillance en ligne des médias sociaux, des communications et des métadonnées associées.

En ce qui concerne plus particulièrement la technologie de reconnaissance faciale, notre coalition a préconisé l'interdiction de certaines formes de surveillance par reconnaissance faciale, ainsi qu'un moratoire sur d'autres formes d'utilisation de la technologie de reconnaissance faciale, pour tous les organismes fédéraux d'application de la loi et du renseignement, y compris la GRC, l'ASFC et le SCRS.

En juillet 2020, nous avons envoyé une lettre ouverte à cet effet au ministre de la Sécurité publique Bill Blair, cosignée par 30 autres organisations et plus de 40 personnes, toutes actives dans la protection de la vie privée, des droits de la personne et des libertés civiles. Dans ce document, nous avons écrit :

> Dans tout le pays, les forces de l'ordre ont admis avoir caché leur utilisation des outils de reconnaissance faciale, ainsi que l'utilisation de la nouvelle technologie par leurs agents à l'insu de leurs supérieurs ou sans leur approbation. Au palier fédéral, la GRC n'a pas consulté le commissaire à la protection de la vie privée avant de commencer à utiliser la technologie Clearview AI, et une recherche dans les évaluations des facteurs relatifs à la vie privée sur le site Web de la GRC ne révèle aucune mention de la reconnaissance faciale. Ces questions révèlent un

[1] Étant donné que le mandat de notre coalition est de se concentrer sur les activités fédérales, nos commentaires s'adressent principalement à ce niveau de gouvernement. Cependant, nous pensons que nos préoccupations sont également applicables de manière plus large et que les questions relatives à la technologie de reconnaissance faciale doivent être abordées à tous les niveaux de gouvernement.

> manque grave et stupéfiant de reddition de comptes dans l'adoption de cette technologie, ce qui porte atteinte aux droits des personnes au Canada[2].

Bien qu'il y ait eu des développements importants au cours des 20 mois qui ont suivi l'envoi de cette lettre, notamment les rapports du Commissariat à la protection de la vie privée sur Clearview AI et sur l'utilisation de cette la technologie par la GRC, rien n'a changé pour améliorer de manière substantielle la transparence, la reddition de comptes ou le cadre juridique entourant l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre au Canada.

La technologie de reconnaissance faciale continue d'être utilisée par les services de police et du renseignement canadiens à un rythme croissant. Cette technologie s'est avérée être biaisée et inexacte. Elle permet également des violations flagrantes des droits et libertés fondamentaux protégés par le droit canadien et international. Cela inclut la violation des droits de la Charte canadienne protégeant contre les fouilles, perquisitions ou saisies abusives (art. 8), ainsi que la violation du droit de réunion pacifique (alinéa 2(c)), de la liberté d'expression (alinéa 2(d)) et de l'égalité (paragraphe 15(1)). De même, elle enfreint les articles 17 (droit à la vie privée) et 21 (liberté de réunion) du Pacte international relatif aux droits civils et politiques. Les lacunes de la législation canadienne font que cette technologie est adoptée sans véritable imputabilité ni transparence.

Nos préoccupations quant à l'utilisation de la TRF par les forces de l'ordre peuvent être subdivisées en quatre domaines :

1. Les systèmes de reconnaissance faciale sont imprécis et biaisés.

De multiples études indépendantes ont montré que les algorithmes sur lesquels reposent certaines des technologies de reconnaissance faciale les plus utilisées sont biaisés et inexacts. Cela est particulièrement vrai en ce qui concerne les personnes de couleur, qui font déjà l'objet d'une surveillance et d'un profilage accrus de la part des organismes d'application de la loi et du renseignement au Canada.

Par exemple, une étude du National Institute of Standards and Technology a révélé que la technologie de reconnaissance faciale identifiait faussement les visages afro-américains et asiatiques 10 à 100 fois plus que les visages blancs, et que parmi les bases de données utilisées par les forces de l'ordre américaines, les taux d'erreur les plus élevés concernaient l'identification des personnes autochtones[3].

---

[2] CSILC, « Lettre au ministre Bill Blair, objet : Interdiction de l'utilisation de la surveillance par reconnaissance faciale par les agences fédérales de maintien de l'ordre et du renseignement », 8 juillet 2020. [en ligne], https://iclmg.ca/wp-content/uploads/2020/07/facial-recognitionletter-08072020.pdf

[3] Singer, N. et C. Metz, « Many Facial-Recognition Systems Are Biased, Says U.S. Study », *The New York Times*, 19 décembre 2019, [en ligne], https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

La ville de Détroit a réglementé l'utilisation de la reconnaissance faciale, mais selon les propres statistiques du service de police de Détroit pour 2020, elle a été utilisée presque exclusivement contre des personnes noires et a mal identifié des personnes dans 96 % des cas[4].

Même si les algorithmes peuvent être améliorés, les types de bases de données utilisées pour comparer et identifier les modèles faciaux suscitent également des inquiétudes. Par exemple, certains services de police utilisent des bases de données de photos d'identité judiciaire comme base de données de comparaison. Cependant, ces bases de données sont imparfaites et il convient de s'interroger sur leur fiabilité ou sur le fait qu'elles ne font qu'accroître la stigmatisation. Par exemple, une base de données de photos d'identité contient des images de personnes qui ont été arrêtées, mais aussi de personnes dont les accusations ont été abandonnées ou qui ont été acquittées. Est-il raisonnable qu'ils continuent, du fait de leur arrestation, à être inclus dans un ensemble de données qui pourrait donner lieu à de faux positifs et avoir des conséquences désastreuses?

La reconnaissance faciale peut également exacerber le profilage racial et le ciblage des communautés racisées déjà observés dans les opérations de surveillance des forces de l'ordre. C'est ce qu'illustre un rapport d'Amnistie internationale daté du 20 février 2002, qui conclut que la technologie de reconnaissance faciale a renforcé la politique raciste d'interpellation et de fouille à New York. Parmi leurs conclusions :

- la vaste opération de surveillance de la police de New York affecte particulièrement les personnes déjà visées par les contrôles et les fouilles dans les cinq arrondissements de la ville de New York.
- Dans le Bronx, Brooklyn et le Queens, la recherche a également montré que plus la proportion de résidents non blancs était élevée, plus la concentration de caméras de vidéosurveillance compatibles avec la reconnaissance faciale était importante[5].

Ce problème peut également être observé dans le domaine de la lutte contre le terrorisme. Il a été révélé que la GRC a fait appel aux services d'un service de reconnaissance faciale connu sous le nom d'IntelCentre. Cette société prétend offrir l'accès à des outils de reconnaissance faciale et à une base de données de plus de 700 000 images de personnes associées au « terrorisme »[6]. Selon l'entreprise, ces images sont acquises à partir de diverses sources en ligne, notamment les réseaux sociaux, en utilisant les mêmes méthodes controversées que les autres entreprises. En outre, il n'est pas clair comment ils déterminent les personnes à inclure dans leur base de données, comment ils vérifient l'exactitude des informations qu'ils fournissent, ou comment ils

---

[4] Koebler, J., « Detroit Police Chief : Facial Recognition Software Misidentifies 96% of the Time », *Vice*, 29 juin 2020, [en ligne], https://www.vice.com/en_us/article/dyzykz/detroit-police-chief-facial-recognition-softwaremisidentifies-96-of-the-time

[5] Amnistie internationale, « Facial recognition technology reinforcing racist stop-and-frisk policing in New York - new research », amnesty.org, 15 février 2022. [en ligne], https://amnesty.ca/news/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/

[6] Bryan Carney, « RCMP Secret Facial Recognition Tool Looked for Matches with 700,000 'Terrorists' », *The Tyee*, 28 avril 2021. [en ligne], https://thetyee.ca/News/2021/04/28/RCMP-Secret-Facial-Recognition-Tool-LookedMatches-Terrorists/

définissent un lien avec le « terrorisme ». Une base de données non réglementée de terroristes potentiels soulève d'importantes préoccupations quant à l'exactitude et au profilage racial, sachant ce que nous savons des failles et des préjugés dans l'approche de la police antiterroriste au Canada, aux États-Unis et dans le monde. Il ne fait nul doute que ce type de système aura des effets dévastateurs sur une personne accusée à tort, puisque, contrairement à d'autres services de reconnaissance faciale, ce système s'accompagne du stigmate supplémentaire d'être prétendument lié au terrorisme.

Tous ces éléments peuvent conduire les communautés déjà marginalisées à être encore plus susceptibles d'être confrontées au profilage, au harcèlement et aux violations de leurs droits fondamentaux. Cette situation est particulièrement préoccupante si l'on considère l'utilisation de la technologie dans des situations où les préjugés sont courants, notamment les protestations contre les politiques et les actions du gouvernement, lorsque des personnes voyagent et traversent des frontières, ainsi que dans le cadre d'enquêtes criminelles, d'opérations de sécurité nationale et de la soi-disant « guerre contre le terrorisme ».

2. La reconnaissance faciale permet une surveillance massive, généralisée et sans mandat

Même si la TRF était exacte à 100 %, cela ne pourrait pas justifier son utilisation, car d'autres problèmes importants persisteraient. Les systèmes de surveillance par reconnaissance faciale, tant en temps réel (en direct) qu'après coup, soumettent les membres du public à une surveillance intrusive et généralisée. Cela est vrai, qu'il s'agisse de surveiller les voyageurs dans un aéroport, les personnes qui se promènent sur une place publique, les internautes ou les militants lors d'une manifestation.

La Cour suprême a conclu que les individus conservent un droit à la vie privée même lorsqu'ils se trouvent dans un espace public[7]. Cela devrait sans aucun doute s'appliquer à la collecte, la conservation et l'identification des images faciales des personnes. Toutefois, si les forces de l'ordre doivent obligatoirement demander une autorisation judiciaire pour surveiller des personnes en ligne ou dans des lieux publics, la législation actuelle présente des lacunes quant à savoir si cela s'applique à la surveillance ou à la dépersonnalisation au moyen de la technologie de reconnaissance faciale[8]. En outre, ces lacunes laissent également ouverte la question non seulement du suivi d'un individu particulier, mais aussi de la surveillance de masse dans l'espoir de pouvoir identifier une personne d'intérêt, en temps réel ou après coup, soumettant ainsi tous les passants à une surveillance de masse injustifiée.

3. Absence de réglementation de la technologie et manque de transparence et d'imputabilité de la part des organismes chargés de l'application de la loi et du renseignement

[7] *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212, par. 44.

[8] Kate Robertson, Cynthia Khoo, et Yolanda Song, « To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (septembre 2020), Citizen Lab et International Human Rights Program, Université de Toronto, p. 90.

Comme le démontre le projet de lignes directrices du Commissariat à la protection de la vie privée à l'intention des organismes d'application de la loi sur l'utilisation de la technologie de reconnaissance faciale[9], et comme en témoignent la GRC et d'autres organismes d'application de la loi qui induisent le public en erreur quant à leur utilisation de la technologie de reconnaissance faciale, le cadre juridique actuel régissant cette technologie est totalement inadéquat. Ce mélange de règles de protection de la vie privée aux paliers provincial, territorial et fédéral ne permet pas de garantir que les forces de l'ordre utilisent la technologie de reconnaissance faciale dans le respect des droits fondamentaux.

En outre, le manque de transparence et d'imputabilité signifie que ces technologies sont adoptées sans que le public en soit informé, sans parler de débat public ou de contrôle indépendant[10].

Cela a permis à la GRC, par exemple, d'utiliser la technologie de reconnaissance faciale Clearview AI pendant des mois à l'insu du public, puis de mentir à ce sujet avant d'être forcée d'admettre la vérité[11]. De plus, nous savons maintenant que la GRC a utilisé une forme ou une autre de reconnaissance faciale au cours des 20 dernières années, sans aucune reconnaissance publique ou surveillance claire ni débat[12].

Et comme l'a documenté Citizen Lab, il a finalement été révélé qu'au moins sept organismes canadiens chargés de l'application de la loi utilisaient également la technologie Clearview AI, certains ayant initialement nié l'avoir utilisée. Cette situation a été expliquée comme étant attribuable à des agents individuels utilisant la technologie sans autorisation – une excuse totalement inacceptable[13]. Indépendamment de la tentative d'explication, il est évident qu'en l'absence de réglementation et d'une plus grande transparence et imputabilité, il est impossible de savoir si cela s'est réellement produit et si cela ne se reproduira pas avec d'autres systèmes de reconnaissance faciale ou d'autres forces de police.

À la suite d'une enquête, le Commissariat à la protection de la vie privée du Canada a conclu que Clearview AI enfreignait la loi canadienne et que l'utilisation de Clearview AI par la GRC était

---

[9] Commissariat à la protection de la vie privée du Canada, « Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale », gouvernement du Canada, 10 juin 2021. [en ligne], https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et-securite-publique/gd_rf_202205/

[10] Allen, K., W. Gillis et A. Boutilier, « Facial recognition app Clearview AI has been used far more widely in Canada than previously known », *The Toronto Star*, 27 février 2020, [en ligne], https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-morewidely-in-canada-than-previously-known.html

[11] Tunney, C., « RCMP denied using facial recognition technology - then said it had been using it for months », *CBC News*, 4 mars 2020, [en ligne], https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266

[12] Carney, B., « Despite Denials, RCMP Used Facial Recognition Program for 18 Years », *The Tyee*, 10 mars 2020. [en ligne], https://thetyee.ca/News/2020/03/10/RCMP-Admits-To-Using-Clearview-AI-Technology/

[13] Kate Robertson, Cynthia Khoo, et Yolanda Song, « To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (septembre 2020), Citizen Lab et International Human Rights Program, Université de Toronto, [en ligne], https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-ofalgorithmic-policing-in-canada/

illégale[14]. La GRC a cependant rejeté cette conclusion, déclarant qu'elle ne peut être tenue responsable de la légalité des services fournis par des tiers. Cela leur permet essentiellement de continuer à passer des contrats avec d'autres services qui violent la loi canadienne.

Le contrat susmentionné passé par la GRC avec le service de reconnaissance faciale « antiterroriste » IntelCentre a été moins médiatisé, mais il reproduit très fidèlement les problèmes de Clearview AI. Par exemple, selon l'entreprise, elle acquiert les images de sa base de données à partir de diverses sources en ligne, y compris les réseaux sociaux, tout comme Clearview AI. De plus, à l'instar de Clearview AI, on ne sait pas comment ces images sont vérifiées ni quelle est la justification légale de la collecte de ces images. Nous n'avons pas non plus la moindre idée de la manière dont la GRC a utilisé cet outil, et encore moins du fondement juridique sur lequel elle s'appuie pour le faire.

L'enquête de Tyee a également révélé que la GRC a enfreint les règles et a travaillé pour tromper le public. En particulier, la politique de la GRC exige que tout achat de logiciel de plus de 500 $ (et tout autre achat de plus de 10 000 $) soit signalé et approuvé. Cela n'a jamais été fait, bien que le contrat soit d'une valeur de 20 000 $. Les membres de la GRC ont également appliqué différentes étiquettes à l'achat – notamment « logiciel », « base de données » et « services de photographie » – ce qui leur a permis de contourner les règles de surveillance et de divulgation[15].

Dans un autre exemple de faiblesse des règles de transparence, l'ASFC a mené un projet pilote utilisant la surveillance par reconnaissance faciale en temps réel à l'aéroport Pearson de Toronto pendant six mois en 2016, avec peu ou pas d'avertissement public au-delà d'un vague avis publié sur son site Web. Au total, les visages de près de 3 millions de voyageurs ont été numérisés dans une base de données de 5 000 images[16].

Enfin, le SCRS a refusé de confirmer s'il utilise la technologie de reconnaissance faciale dans son travail, affirmant qu'il n'a aucune obligation de le faire. Si les services du renseignement ne sont peut-être pas en mesure d'entrer dans les détails des opérations en cours, rien ne les empêche d'engager un débat public approfondi sur l'utilisation d'une technologie aussi controversée.

4. La technologie de reconnaissance faciale est une pente glissante.

---

[14] 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 », gouvernement du Canada, 10 juin 2021. [en ligne], https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

[15] Bryan Carney, « RCMP Secret Facial Recognition Tool Looked for Matches with 700,000 'Terrorists' », *The Tyee*, 28 avril 2021. [en ligne], https://thetyee.ca/News/2021/04/28/RCMP-Secret-Facial-Recognition-Tool-LookedMatches-Terrorists/

[16] Lauren O'Neill, « Canada under fire for secretly using facial recognition at Toronto's Pearson airport », *BlogTO*, 19 juillet 2021. [en ligne], https://www.blogto.com/tech/2021/07/canada-secretly-using-facial-recognition-torontopearson-airport/

Actuellement, la portée et l'utilisation de la technologie de reconnaissance faciale au Canada par les forces de l'ordre ne sont pas entièrement connues. Même si nous présumons que l'utilisation actuelle de la technologie de reconnaissance faciale par les forces de l'ordre canadiennes est limitée, il faut reconnaître que la nature non réglementée de cette utilisation reste nuisible en soi. Elle présente également une pente glissante, où la technologie gagne du terrain et est acceptée au fil du temps, ce qui permet à son utilisation de se répandre jusqu'à ce qu'on ne puisse plus revenir en arrière.

Nous l'avons constaté dans d'autres juridictions : L'utilisation limitée de la reconnaissance faciale par les forces de l'ordre dans d'autres pays a généralement conduit à un déploiement plus important et beaucoup plus large de cette technologie. Aux États-Unis, par exemple, l'ancien président Donald Trump a publié un décret exigeant l'identification par reconnaissance faciale de tous les voyageurs internationaux dans les 20 principaux aéroports américains d'ici 2021[17].

Au Royaume-Uni, la reconnaissance faciale est déjà utilisée lors de matchs sportifs, de festivals de rue, de manifestations et même dans la rue pour surveiller en permanence les passants[18].

Il est facile d'imaginer qu'en l'absence d'un examen, d'un débat public et d'une réglementation appropriés, le Canada finira par connaître la même chose – si ce n'est pas déjà le cas à notre insu.

B. Recommandations et prochaines étapes

Compte tenu de tout cela, il est manifestement urgent que les parlementaires canadiens agissent pour restreindre et réglementer l'utilisation de la technologie de reconnaissance faciale au Canada.

Notre coalition appelle à trois actions clés :

1. Que le gouvernement fédéral interdise immédiatement l'utilisation de la surveillance par reconnaissance faciale par les forces de l'ordre et les agences du renseignement, et entreprenne des consultations pour la réglementation de la technologie de reconnaissance faciale en général;

---

[17] Alba, D., « The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show », *Buzzfeed*, 11 mars 2019. [en ligne], https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-thegovernments-detailed-plan-for

[18] Smith, A., « Football fans demand end to facial recognition cameras being used at matches », *Metro*, 7 août 2018, [en ligne], https://metro.co.uk/2018/08/07/football-fans-demand-end-to-facial-recognition-cameras-being-used-atmatches-7808677/; Bowcott, Owen. « Police face legal action over use of facial recognition cameras », *The Guardian*, 14 juin 2018. [en ligne], https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-overuse-of-facial-recognition-cameras; BBC Click. « Are you ready for a world of facial recognition? Several UK police forces have been trialling the technology », *Twitter*, 13 mai 2019, [en ligne], https://twitter.com/BBCClick/status/1127961872286789634

2. Que le gouvernement entreprenne des réformes des lois sur la protection de la vie privée dans les secteurs privé et public afin de combler les lacunes dans la réglementation des TRF et d'autres formes de surveillance biométrique;
3. Que le commissaire à la protection de la vie privée se voie accorder des pouvoirs d'exécution accrus, tant en ce qui concerne les infractions aux lois canadiennes sur la protection de la vie privée par le secteur public que par le secteur privé.

Si l'interdiction de l'utilisation de la technologie de reconnaissance faciale à des fins de surveillance par les forces de l'ordre peut sembler controversée, elle est conforme aux positions adoptées dans de nombreuses autres juridictions.

Par exemple, plus d'une douzaine de villes américaines ont interdit l'utilisation de la TRF au niveau municipal, notamment : San Francisco et Oakland, Californie; Boston, Brookline, Cambridge, Northampton, Easthampton et Somerville, Massachusetts; Jackson, Mississippi; King County, Washington; Madison, Wisconsin; Nouvelle-Orléans, Louisiane; Minneapolis, Minnesota; Portland, Maine; et Portland, Oregon.[19]

Plusieurs États américains ont également adopté une réglementation stricte, notamment en interdisant la surveillance par reconnaissance faciale dans les lieux publics, en exigeant l'approbation du législateur avant d'utiliser la technologie de reconnaissance faciale et en limitant strictement les mandats à des cas exceptionnels. Il s'agit notamment du Vermont, du Maine, du Massachusetts, de la Virginie, de l'Oregon, de Washington et de la Californie.[20]

Dans un arrêt historique, la Cour d'appel britannique a jugé que la reconnaissance faciale dans les lieux publics violait les droits de la personne[21].

La Commission australienne des droits de la personne a demandé l'interdiction de l'utilisation de la technologie de reconnaissance faciale [TRADUCTION] « dans le cadre de la prise de décisions ayant un effet juridique, ou un effet significatif similaire, pour les individus, ou lorsqu'il existe un risque élevé pour les droits de la personne, comme dans le cadre du maintien de l'ordre et de l'application de la loi » jusqu'à ce qu'une étude plus approfondie et une réglementation soient mises en place.[22]

---

[19] Kay Lively, T., « Facial Recognition in the United States: Privacy Concerns and Legal Developments », *Security Management Magazine*, 1er décembre 2021, [en ligne], https://www.asisonline.org/security-managementmagazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacyconcerns-and-legal-developments/

[20] *Ibid.*

[21] Fernandez, E., « Facial Recognition Violates Human Rights, Court Rules », *Forbes*, 13 août 2020. [en ligne], https://www.forbes.com/sites/fernandezelizabeth/2020/08/13/facial-recognition-violates-human-rights-courtrules/?sh=5cc7f2b65d44

[22] Hendry, J., « Human Rights Commission calls for temporary ban on 'high-risk' govt facial recognition », *IT News*, 28 mai 2021, [en ligne], https://www.itnews.com.au/news/human-rights-commission-calls-for-temporary-ban-onhigh-risk-govt-facial-recognition-565173

Enfin, le Parlement européen a voté en octobre 2021 pour l'interdiction de l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre dans les espaces publics. Les députés envisagent toujours une législation officielle sur la question[23].

Le Canada serait en bonne compagnie pour aller de l'avant avec des restrictions et des réglementations strictes sur toute utilisation de la technologie de reconnaissance faciale par les forces de l'ordre, y compris une interdiction de son utilisation à des fins de surveillance.

Au-delà de cette interdiction de la surveillance au moyen de la TRF, nous pensons que d'autres questions doivent être abordées dans une réforme des lois sur la vie privée en général. Il s'agit notamment des lois touchant le secteur privé (par exemple, en ce qui concerne les fournisseurs tiers) et les lois touchant le secteur public (celles qui régissent l'application de la loi, ainsi que l'habilitation des autorités de réglementation de la protection de la vie privée). Plus précisément, il s'agit, entre autres, des suivantes :

- Les lois sur la protection de la vie privée des secteurs privé et public doivent être modifiées afin de reconnaître que la vie privée est un droit fondamental et d'adopter un cadre de protection de la vie privée fondé sur les droits de la personne;
- Les commissaires à la protection de la vie privée doivent se voir accorder des pouvoirs d'application plus importants dans le secteur privé, ainsi que des pouvoirs d'ordonnance plus forts dans le secteur public;
- Les lois sur la protection de la vie privée doivent prévoir des règles de transparence plus strictes dans les secteurs public et privé, ainsi que des règles d'évaluation des incidences sur la vie privée plus strictes pour le secteur public;
- Des changements doivent être apportés en ce qui concerne les réglementations sur l'utilisation de l'IA et de la prise de décision algorithmique dans les secteurs public et privé, afin d'exiger une plus grande transparence, un examen par un tiers indépendant et une surveillance continue (entre autres);
- La législation doit apporter une plus grande clarté et instituer des restrictions plus strictes relativement à la collecte, la conservation et l'utilisation de ce que l'on appelle les « renseignements accessibles au public », tant dans le secteur public que dans le secteur privé, en particulier lorsqu'il s'agit de recueillir des renseignements biométriques, des renseignements dont on peut raisonnablement attendre qu'ils soient protégés par la vie privée, ou des renseignements transmis dans un but précis, mais recueillis et conservés dans un autre;
- La législation future doit supprimer les exceptions pour les organismes chargés de l'application de la loi et de la sécurité nationale lorsqu'il s'agit de divulguer des activités qui ont un impact sur la vie privée et d'autres droits, notamment l'utilisation de la technologie de reconnaissance faciale.

[23] Peets, L. et coll., « European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement », *InsidePrivacy.com*, 12 octobre 2021, [en ligne], https://www.insideprivacy.com/artificialintelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

C. Conclusion

Nous remercions les membres du Comité de s'être penchés sur cette question importante et nous vous demandons instamment de formuler des recommandations solides et précises relativement à l'utilisation de la technologie de reconnaissance faciale par les organismes d'application de la loi et de renseignement au Canada. Nous réitérons les trois principales mesures qui, selon nous, doivent être prises par les parlementaires et le gouvernement sur cette question :

1. Que le gouvernement fédéral interdise immédiatement l'utilisation de la surveillance par reconnaissance faciale par les forces de l'ordre et les agences du renseignement, et entreprenne des consultations pour la réglementation de la technologie de reconnaissance faciale en général;
2. Que le gouvernement entreprenne des réformes des lois sur la protection de la vie privée dans les secteurs privé et public afin de combler les lacunes dans la réglementation des TRF et d'autres formes de surveillance biométrique;
3. Que le commissaire à la protection de la vie privée se voie accorder des pouvoirs d'exécution accrus, tant en ce qui concerne les infractions aux lois canadiennes sur la protection de la vie privée par le secteur public que par le secteur privé.

Bien qu'il s'agisse d'appels au gouvernement pour qu'il agisse, le contexte politique actuel permet également aux parlementaires de présenter des motions pour ces réformes, y compris des changements à la législation pour limiter l'utilisation de la TRF et accorder plus de pouvoirs au Commissariat à la protection de la vie privée, ainsi qu'une motion pour lancer une enquête et une consultation officielles plus larges sur l'utilisation, l'impact et les réformes nécessaires en ce qui concerne le TRF et les lois canadiennes sur la protection de la vie privée en général.

Nous serions heureux de discuter davantage de ces enjeux avec les membres du Comité ou d'autres parlementaires.