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

Étude sur l'utilisation et les impacts de la technologie de reconnaissance faciale

Le 1er juin 2022

Sommaire

Les progrès technologiques et l'accès à de nouveaux ensembles de données personnelles plus vastes ont permis de réduire les coûts et d'accroître l'adoption publique et privée des technologies de reconnaissance faciale (TRF). Nos recherches et le travail d'autres défenseurs des droits de la personne font ressortir des préoccupations en matière de protection de la vie privée et d'éthique soulevées par les TRF qui, si rien n'est fait, violeraient les droits et libertés dont jouissent les Canadiens. Le gouvernement du Canada doit guider le pays dans la détermination des utilisations acceptables, le cas échéant,

— des TRF par les institutions publiques et privées afin d'assurer que les droits fondamentaux des Canadiens sont protégés.

Cette séance d'information résume notre recherche et nos recommandations pour le gouvernement fédéral :

- Nous faisons écho à l'appel des commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux du Canada pour un cadre réglementaire concernant les utilisations, les interdictions, la surveillance, et la protection des renseignements personnels des TRF pour les services de police, mais il faut ajouter qu'un tel cadre est nécessaire pour les secteurs publics fédéral et provinciaux, ainsi que pour l'ensemble du secteur privé[1].
- Des experts nationaux et internationaux ont soulevé d'importantes préoccupations au sujet des effets discriminatoires des TRF sur les femmes, les personnes âgées et les personnes de couleur[2], ainsi que des effets intrusifs et terrifiants des TRF en ce qui concerne les droits à la vie privée, la liberté d'expression, et la liberté de réunion[3].
- Nous recommandons que les lois fédérales sur la protection des renseignements personnels, y compris la *Loi sur la protection des renseignements personnels* et la LPRPDE, soient modifiées de manière à prévoir une protection spéciale pour les renseignements biométriques comme les images faciales.
- En particulier, nous préconisons une limite permanente dans les lois fédérales sur la protection des renseignements personnels en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements biométriques, comme les images faciales, dans le but d'identifier des personnes au moyen de systèmes algorithmiques. À tout le moins, un avis et un consentement ou une permission législative explicite devraient être requis.

- Nous exhortons également le gouvernement à adopter un moratoire temporaire sur l'utilisation des TRF par le secteur public jusqu'à ce que de telles protections juridiques soient en place et jusqu'à ce que d'autres recherches soient menées sur les répercussions disproportionnées des TRF sur les collectivités qui pourraient être les plus touchées par son utilisation, comme les personnes âgées, les enfants, les communautés racialisées, les personnes handicapées et les personnes transgenres et non binaires. Veuillez consulter la section ci-dessous intitulée « **Une solution provisoire : Un moratoire public sur les TRF** pour la recherche qui doit être entreprise.

Types de systèmes de reconnaissance faciale et risques associés aux autres technologies biométriques

Les visages offrent des données corporelles personnelles qui sont uniques à chacun. Les visages peuvent révéler des renseignements intimes comme la santé, le genre perçu, la race ou l'origine ethnique, les états émotionnels et les habitudes d'une personne, comme les habitudes de voyage, les relations et les préférences politiques ou personnelles.

La reconnaissance faciale est le processus d'identification d'un visage à partir d'une image ou d'une vidéo numérique. Les TRF utilisent généralement la reconnaissance de motifs par ordinateur pour trouver des points communs dans les images représentant des visages humains[4]. Les TRF peuvent être déployées en temps réel ou sur des images statiques. Comme il est expliqué ci-dessous, elles peuvent être utilisées pour confirmer l'identité d'une personne connue ou pour identifier une personne inconnue de façon unique. Les TRF peuvent également permettre la catégorisation et le profilage d'une personne au fil du temps en fonction de ses renseignements faciaux.

Les systèmes de reconnaissance faciale se divisent en deux catégories : un pour un et 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. L'utilisation de ces derniers systèmes dans le domaine de l'application de la loi et de la sécurité publique est particulièrement litigieuse en raison de l'ampleur accrue des comparaisons et de l'ambiguïté juridique entourant la construction de bases de données et de listes de surveillance.

Les TRF font partie d'une vaste gamme de technologies de « reconnaissance » biométrique. Ces systèmes catégorisent les personnes en fonction d'identificateurs biométriques plus traditionnels (« forts »), comme les empreintes digitales et les lectures rétiniennes, d'indicateurs moins uniques (« faibles ») comme la forme du corps ou la voix, et non uniques (« secondaires ») des indicateurs comme le sexe ou l'âge[5]. La réglementation des TRF à elle seule ne suffit pas, car les renseignements sur le visage ne sont qu'un type d'information biométrique. Les renseignements biométriques sont de nature très délicate, étant donné qu'ils révèlent « un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État », ainsi que les acteurs privés, en particulier lorsqu'ils fournissent des services à l'État[6].

Préjudices et obligations : Risques importants des TRF pour identifier de façon unique les individus

L'utilisation des TRF peut entraîner des coûts importants. Les experts ont identifié les préjudices suivants associés à l'utilisation d'un logiciel de reconnaissance faciale[7] :

- Manque d'autonomie humaine à l'égard des décisions;
- Manque de transparence pour des raisons associées à certains résultats;
- Inexactitude (p. ex., faux négatifs);
- Discrimination;
- Risque d'accès et de manipulation non autorisés de données sensibles (y compris les données sur les enfants).

Les TRF peuvent permettre la surveillance, les atteintes à la vie privée, la discrimination et les limites à la liberté d'expression à grande échelle. Des experts ont déterminé que les TRF peuvent êtreutilisées pour l'identification des personnes en temps réel, ce qui entraîne la surveillance de masse de groupes de personnes. Une telle surveillance peut priver les gens de leur droit à la vie privée à une vitesse et à une échelle importantes, y compris la liberté de demeurer anonymes, y compris dans des contextes publics. Les TRF ont été utilisées pour faciliter l'arrestation en temps réel de personnes, ce qui a des effets terrifiants sur la liberté d'expression et de parole des personnes[8]. Une telle utilisation des TRF a des effets particulièrement néfastes sur les communautés revendiquant l'égalité, y compris les femmes, les communautés racialisées, les personnes de la communauté LGBTQ+, et d'autres communautés protégées par la loi sur la discrimination.

Par souci de clarté, nous avons dressé une liste non exhaustive d'exemples concrets pour montrer comment les TRF ont été utilisées avec des effets néfastes sur la vie privée et sur les populations en quête d'égalité :

- Trois personnes ont été arrêtées à tort après des correspondances erronées d'un algorithme de reconnaissance faciale[9].
- Cela a été démontré que les classificateurs de genre vendus dans des ensembles d'API offerts par Microsoft, IBM et Face++ pour les modèles de reconnaissance faciale ont des taux d'erreur allant jusqu'à 34,7 % pour les femmes à la peau foncée[10].
- L'intégration de la biométrie dans les systèmes de prise de décisions a causé un tort disproportionné aux personnes handicapées marginalisées[11].
- On a constaté que l'algorithme de recadrage d'images de Twitter avait un biais racial en favorisant les visages blancs par rapport aux visages noirs[12].
- La technologie de Clearview AI a permis aux organismes d'application de la loi et aux organisations commerciales de comparer des photographies de personnes inconnues à la banque de données de l'entreprise contenant plus de 3 milliards d'images, y compris de Canadiens et d'enfants, à des fins d'enquête, ce qui a créé un risque de préjudice important pour les personnes; la grande majorité d'entre eux n'ont jamais été et ne seront jamais impliqués dans un crime[13].
- Des représentants du gouvernement du Canada ont « discrètement » testé la reconnaissance faciale à l'aéroport international Pearson de Toronto en 2016 afin de détecter les voyageurs utilisant de fausses identités, sans en informer le public et sans consentement[14].
- Facebook a reçu une amende de 650 millions de dollars pour avoir enfreint la *Biometric Information Privacy Act* de l'Illinois. Amazon et Microsoft font actuellement l'objet d'une enquête après avoir été accusés d'avoir utilisé une base de données comprenant des images de Flickr pour améliorer l'exactitude de leur logiciel de reconnaissance faciale sans le consentement des personnes figurant sur les images[15].

L'approche actuelle du Canada en matière de réglementation des TRF et des systèmes de reconnaissance biométrique est inadéquate

Au Canada, l'absence de cadres de réglementation clairs entourant les TRF mettent en lumière l'insuffisance de l'approche du Canada en ce qui concerne les risques des systèmes algorithmiques pour la vie privée et les droits de la personne, comme les systèmes de reconnaissance biométrique[16]. Les lois sur la protection des renseignements personnels sont l'un des principaux outils de réglementation pour aider à protéger la dignité humaine, l'intégrité personnelle, le contrôle et l'autonomie des Canadiens à l'égard de leurs renseignements personnels et de leur corps[17]. Les obligations du Canada en matière de protection de la vie privée en vertu du droit international et national comprennent le respect des dispositions suivantes[18] :

- L'article 12 de la Déclaration universelle des droits de l'homme et l'article 17 du Pacte international relatif aux droits civils et politiques, qui interdisent l'ingérence arbitraire dans la vie privée des gens;
- L'article 8 de la *Charte canadienne des droits et libertés*, protège les Canadiens contre les perquisitions et saisies abusives.
- La *Loi sur la protection des renseignements personnels*, qui décrit en détail les lois qui protègent la vie privée des personnes en ce qui concerne les renseignements personnels recueillis, utilisés et divulgués par les institutions fédérales;
- La LPRPDE, qui couvre les règlements sur la protection des renseignements personnels qui s'appliquent au secteur privé dans le contexte fédéral et lorsque les lois provinciales ne s'appliquent pas.

Certaines des préoccupations juridiques les plus graves et des recommandations concernant la Loi sur la *protection des renseignements personnels* du Canada en ce qui a trait aux TRF sont décrites dans notre rapport intitulé *Facing the Realities of Facial Recognition Technology* (Faire face aux réalités de la technologie de la reconnaissance faciale). En particulier, la Cour suprême a conclu que la collecte par l'État de renseignements corporels sans le consentement de la personne constitue une violation grave de son corps, menaçant ainsi les valeurs protégées par les articles 7 et 8 de la Charte, comme la dignité, l'intégrité et l'autonomie[19]. Comme il est indiqué à l'article 7, la collecte de renseignements biométriques par les institutions fédérales peut donc constituer une atteinte au droit d'une personne à la vie, à la liberté et à la sécurité de sa personne. Comme il a été souligné précédemment, la collecte de renseignements biométriques peut également constituer une fouille, une perquisition et une saisie abusives par l'État lorsqu'il n'existe aucune limite raisonnable à ces droits prescrits par la loi qui peut être justifiée de façon démontrable dans une société libre et démocratique[20].

Changements juridiques nécessaires au Canada : Commencer par les lois sur la protection des renseignements personnels concernant les systèmes de reconnaissance biométrique, y compris les TRF

Le Canada ne dispose pas de règlements précis sur l'utilisation des technologies de reconnaissance biométrique, comme les TRF, ni de dispositions précises sur la collecte, l'utilisation et la conservation des données au moyen de tels systèmes biométriques. Plus particulièrement, la *Loi sur la protection* des renseignements personnels et la LPRPDE n'incluent pas explicitement les renseignements faciaux et biométriques comme sous-ensembles de renseignements personnels qui méritent une protection spéciale. Compte tenu des risques juridiques et de droits de la personne déjà établis importants associés à la collecte, à l'utilisation et à la divulgation de renseignements biométriques, cette lacune juridique doit être comblée afin

de protéger les droits et libertés de la personne, en particulier le droit à la vie privée, la liberté d'expression et la protection contre la discrimination, entre autres.

Des changements doivent être apportés aux lois fédérales sur la protection des renseignements personnels afin de bien tenir compte des préjudices liés aux systèmes de reconnaissance biométrique. Comme Sonja Solomun et Yuan Stevens l'ont souligné dans leur rapport de février 2021, le gouvernement du Canada peut atténuer les graves risques liés à la protection des renseignements personnels et à la sécurité en mettant en œuvre les recommandations suivantes pour modifier la *Loi sur la protection des renseignements personnels*, avec des leçons qui peuvent être appliquées pour tout changement ou toute refonte apporté à la LPRPDE :

1. **Reconnaître et rendre compte explicitement de l'existence de renseignements personnels relatifs aux caractéristiques physiques ou biologiques d'une personne ou de** renseignements biométriques, y compris les renseignements faciaux.

2. **Protéger adéquatement la vie privée et la sécurité des Canadiens en mettant en œuvre des** exigences concernant les renseignements biométriques, comme les images faciales. Ces exigences devraient comprendre :
    a. Limites à la collecte, à l'utilisation et à la communication de ces renseignements biométriques, exigeant à tout le moins un avis et soit un consentement, soit une permission législative explicite;
    b. Les exigences visant à réduire au minimum la collecte de renseignements;
    c. Des mesures de protection plus vastes pour la sécurité des renseignements de nature délicate, une fois recueillies.

3. **En particulier, harmoniser les lois sur la protection des renseignements personnels, comme la *Loi sur la protection des renseignements personnels*, avec les exigences de la Directive sur la prise de décisions automatisée.** Cette harmonisation dicterait des termes plus précis à utiliser par les organismes d'application de la loi, notamment la publication d'avis, les essais de partialité, la formation des employés, les évaluations des risques pour la sécurité et la nécessité pour un être humain de prendre une décision finale dans le cas de décisions à incidence élevée. Ces exigences devraient être élargies afin de prévoir une consultation adéquate et significative avant le déploiement des TRF pour l'identification unique des personnes.

4. **Comme il est indiqué ci-dessous, il importe de mettre en œuvre un moratoire fédéral sur la reconnaissance faciale automatisée et la divulgation de renseignements faciaux, jusqu'à ce que :**
    a. Le cadre décrit dans cette présentation a été élaboré en consultation avec les Canadiens, ainsi qu'avec les institutions gouvernementales et les fonctionnaires des ministères pertinents;
    b. On effectue davantage de recherches sur les répercussions disproportionnées, ou la possibilité d'incidence disproportionnée, sur les membres de certains groupes démographiques, en particulier ce qui concerne les réalités et les populations au Canada.

Une solution provisoire : Un moratoire public sur les TRF

À mesure que le gouvernement fédéral cerne les meilleures solutions juridiques concernant des règlements plus rigoureux en matière de protection des renseignements personnels pour les données biométriques, nous recommandons fortement un moratoire temporaire sur l'utilisation des TRF, à tout le moins par les

institutions fédérales.[21] Les commissaires à la protection de la vie privée du Canada, la Ligue des droits et libertés, la Commission canadienne des droits de la personne et plus de 70 organisations et défenseurs canadiens et internationaux dans les domaines de la protection de la vie privée, des droits de la personne et des libertés civiles ont demandé un tel moratoire sur les services de police et de surveillance[22].

Bien que les organismes d'application de la loi présentent les risques les plus évidents et les abus les plus médiatisés des TRF, d'autres organismes gouvernementaux utilisent actuellement cette technologie ou sont susceptibles de l'adopter. Pour mieux comprendre les risques et protéger les droits des gens, cette interdiction devrait donc s'étendre à l'ensemble du secteur public au niveau fédéral.

Le Centre for Media, Technology and Democracy préconise cette approche depuis août 2020, lorsque nous avons publié deux séances d'information sur la politique à ce sujet. La première séance d'information décrit la raison d'être et les répercussions d'un moratoire sur l'utilisation des TRF par le secteur public canadien. La deuxième séance d'information explore les conditions dans lesquelles un moratoire pourrait être levé.

Une action rapide du gouvernement est nécessaire pour identifier, gérer et atténuer les préjudices possibles qui émanent de ce paysage en évolution rapide[23]. Les moratoires sont devenus l'option stratégique par défaut à l'échelle mondiale pour réglementer l'utilisation des TRF par les organismes gouvernementaux et les forces de police[24]. Un moratoire national n'est pas en soi une solution; elle donne plutôt au gouvernement le temps d'évaluer et de développer les conditions nécessaires que les entreprises de TRF et les acteurs du secteur public devraient respecter. Ces conditions devraient comprendre des cadres juridiques mis à jour pour la protection des renseignements personnels et le traitement automatisé des données, des mesures de responsabilisation pour les institutions qui utilisent les TRF, et des évaluations des incidences sociales, entre autres[25].

Entre-temps, nous recommandons que le gouvernement du Canada :

- Créer un groupe d'experts chargé d'étudier l'utilisation actuelle des systèmes de reconnaissance biométrique comme les TRF au Canada, d'examiner les lois sur les données et la protection des renseignements personnels afin de cerner les lacunes et, ultimement, d'élaborer les exigences réglementaires optimales pour lever un moratoire;
- Mener des consultations à grande échelle pour évaluer les points de vue des Canadiens, en particulier ceux des communautés marginalisées, sur les TRF à l'usage du public, en s'appuyant sur les consultations initiales sur l'utilisation des TRF par les services de police;
- Coordonner un effort de recherche national sur l'utilisation des systèmes biométriques comme les TRF dans les secteurs public et privé, avec une série de rapports commandés conjointement par le Commissariat à la protection de la vie privée, les commissaires à la protection de la vie privée des provinces et des territoires et le Conseil national de recherches;
- Évaluations des facteurs relatifs à la vie privée et évaluations des facteurs relatifs à la protection des données de la Commission pour l'utilisation des TRF par chaque institution gouvernementale pertinente[26].

Il s'agissait d'un sujet principal de discussion à la table ronde sur les politiques que nous avons convoquée en novembre 2020 avec le Cybersecure Policy Exchange, de la Toronto Metropolitan University. Une trentaine d'intervenants experts et représentants du gouvernement ont soupesé les pressions en faveur d'une interdiction limitée du secteur public sur les TRF par rapport à d'autres approches pour atténuer les risques liés aux TRF. Leurs prescriptions pour le gouvernement variaient, mais tous les intervenants ont souligné l'importance d'une intervention rapide du gouvernement pour cerner, gérer et atténuer les préjudices possibles qui émanent de ce paysage en évolution rapide[27].

ANNEXE 1 : Organisations et particuliers

À propose du Centre for Media, Technology and Democracy

Le Centre for Media, Technology and Democracy de la Max Bell School of Public Policy de l'Université McGill est un centre de recherche interdisciplinaire voué à la compréhension et à la réponse aux enjeux sociaux, les défis politiques et en matière de politiques posés par l'évolution de notre écosystème de l'information et des technologies numériques. La technologie de reconnaissance faciale est un enjeu crucial pour le Centre depuis son lancement en 2020. Au cours des deux dernières années, le Centre a mené et commandé des recherches, organisé des réunions et présenté plusieurs recommandations stratégiques dans le domaine des TRF au Canada. Pour en savoir plus, consultez le site www.mediatechdemocracy.com/projects/facial-recognition-governance.

À propos du Cybersecure Policy Exchange

Le Cybersecure Policy Exchange (CPX) de la Toronto Metropolitan University (TMU) est une initiative visant à faire progresser des politiques publiques efficaces et novatrices en matière de cybersécurité et de protection des renseignements personnels numériques, parrainée par la Banque Royale du Canada et dirigé par le Rogers Cybersecure Catalyst et le Leadership Lab de TMU. Nous effectuons des recherches et élaborons des politiques sur la gouvernance responsable de la technologie et nous travaillons à élargir et à approfondir les discussions publiques sur ces questions au moyen de discours, de tables rondes et d'ateliers. Nous avons publié un certain nombre de rapports, y compris les résultats d'enquêtes nationales, d'entrevues et de groupes de discussion, et nous avons réuni un vaste réseau de décideurs politiques, d'experts de l'industrie, d'universitaires et de représentants de la société civile sur un certain nombre de questions urgentes liées à la sécurité de l'information et à la démocratie, y compris la réglementation de la technologie de reconnaissance faciale, des plateformes de médias sociaux, des applications de recherche des contacts dans le cadre de la COVID-19, de la technologie de chiffrement et du stockage transfrontalier des données.

Sonja Solomun

Sonja Solomun est directrice de la recherche au Centre for Media, Technology and Democracy de l'École de politique publique Max Bell de l'Université McGill. Elle est attachée de recherche au Data & Society Research Institute, au Center for Information, Technology, and Public Life (CITAP) de l'Université de Caroline du Nord à Chapel Hill, et au Climate Social Science Network à la Brown University's Institute pour l'environnement et la société. Elle est cofondatrice de la Coalition for Critical Technology et membre fondatrice du Platform Governance Research Network.

Yuan Stevens

Yuan (you-anne) Stevens est responsable des politiques sur la technologie, la cybersécurité et la démocratie au Leadership Lab and Cybersecure Policy Exchange de la Toronto Metropolitan University. Elle a obtenu un BCL/JD de la Faculté de droit de l'Université McGill. Auparavant, elle a travaillé au Berkman Klein Center for Internet and Society de l'Université Harvard, où elle est boursière de recherche et candidate à la maîtrise en droit au Centre for Law, Technology and Society de l'Université d'Ottawa.

Julia Bugiel

Julia Bugiel est assistante de recherche au Centre for Media, Technology and Democracy. Elle est étudiante à la maîtrise en communications à l'Université McGill et titulaire d'une bourse d'études supérieures du Canada. Auparavant, elle a travaillé à l'Institut de recherche en politiques publiques.

ANNEXE 2 : Leçons des États-Unis et de l'UE

Compte tenu du risque élevé et de la nature très sensible des TRF pour les groupes en quête d'égalité, il est urgent que le Canada mette en œuvre les leçons communes tirées des cadres de réglementation de l'UE et de plusieurs États des États-Unis[28]. Le gouvernement du Canada pourrait vouloir consulter les précédents internationaux suivants pour en tirer des leçons communes :

- La **loi sur l'intelligence artificielle** de l'UE vise à harmoniser de manière exhaustive le cadre juridique sur l'intelligence artificielle entre les États membres de l'UE en ce qui concerne les échanges, le commerce, la recherche et la protection des droits fondamentaux. L'article 29 impose aux utilisateurs de systèmes d'IA à haut risque (c.-à-d. les systèmes qui posent des risques importants pour la santé et la sécurité ou les droits fondamentaux de la personne) l'obligation d'effectuer une évaluation de l'impact sur la protection des données conformément à l'article 35 du règlement général sur la protection des données (RGPD) de l'UE.
    - 120 organisations de la société civile ont signé une déclaration collective appelant l'UE à adopter une loi sur l'intelligence artificielle centrée sur les droits fondamentaux[29].
- La **directive de l'UE sur le contrôle d'application de la loi** 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, afin de protéger les intérêts vitaux d'une personne, ou lorsque les données sont « manifestement rendues publiques » par une personne. Il interdit également aux forces de l'ordre de prendre des décisions basées uniquement sur le traitement automatisé (y compris le profilage), à moins que la législation européenne ou nationale ne soit promulguée et qu'elle offre des garanties appropriées pour les droits et libertés individuels. De plus, elle interdit le profilage qui entraîne de la discrimination fondée sur des catégories spéciales de données, y compris des renseignements biométriques comme des images faciales[30].
    - **Le Contrôleur européen de la protection des données** a également demandé une interdiction générale de toute utilisation de l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public, tels que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la pression sur des touches et d'autres signaux biométriques ou comportementaux, dans tous les contextes[31].
- Aux **États-Unis**, plusieurs villes (p. ex., San Francisco, CA; Bellingham, WA; Oakland, CA; Somerville, MA) ont interdit l'utilisation de la technologie de reconnaissance faciale par la police. Le Vermont et la Virginie ont interdit cette pratique dans leurs états[32].
- La *Biometric Information Privacy Act* (BIPA) de l'**Illinois** impose des exigences plus strictes aux entreprises qui fournissent des services automatisés de reconnaissance faciale aux organismes d'application de la loi. Elle interdit aux entreprises de recueillir des renseignements biométriques à moins a) d'informer la personne par écrit des données qui sont recueillies et stockées, ainsi que des fins précises et de la durée de la collecte, de l'entreposage ou de l'utilisation, et b) d'obtenir le consentement écrit de la personne.
- Le **Massachusetts** a récemment adopté sa *Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth*, qui exige que les organismes d'application de la loi obtiennent un mandat avant de procéder à une recherche de reconnaissance faciale, sauf en situation d'urgence. Elle interdit également à la police d'acquérir, d'accéder ou d'utiliser elle-même un logiciel de reconnaissance faciale, ainsi que de présenter une demande ou de conclure un contrat à cette fin[33].

Notes en fin d'ouvrage

1. Déclaration conjointe des commissaires à la protection de la vie privée des gouvernements fédéral, provinciaux et territoriaux, « Cadre juridique recommandé pour le recours à la reconnaissance faciale par les services de police » (2 mai 2022), https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2022/s- d_prov_20220502/.
2. Joy Buolamwini et Timnit Gebru, « Gender Shades : Intersectional Accuracy Disparities in Commercial Gender Classification », *Machine Learning Research*, 81 (2018) : 1-15 (document présenté à la Conférence intitulée Fairness, Accountability and Transparency, New York, 23- 24 février 2018),
3. International Center for Not-for-profit Law, *The Impact of Artificial Intelligence Technologies on the Right to Privacy and Civic Freedoms* (mémoire présenté au Haut-Commissariat aux droits de l'homme, 2021);
4. Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun et Kate Gilbert, *Facial Recognition Moratorium Briefing #1,* Tech Informed Policy Initiative (août 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1.
5. Christiane Wendehorst et Yannic Duller, *Biometric Recognition and Behavioural Detection : Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,* Parlement européen (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_E N.pdf.
6. Voir p. ex., *R . c. Spencer,* 2014 CSC 43 (CanLII), [2014] 2 RCS 212, para 24; *R. c. Tessling*, 2004 CSC 67 (CanLII), [2004] 3 RCS 432, para 25; *R. c. Plant,* 1993 CanLII 70 (CSC), [1993] 3 RCS 281.
7. Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable : Ce que nous avons entendu* (février 2021), https://www.mediatechdemocracy.com/work/facial- recognition-technology-policy-roundtable-what-we-heard.
8. Pete Fussey et Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology,* Human Rights, Big Data and Technology Project, University of Essex (2019), https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.
9. Kashmir Hill, « Wrongfully accused by an algorithm », *The Seattle Times* (24 juin 2020), https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/; Khari Johnson, « How Wrongful Arrests Based on AI Derailed 3 Men's Lives », *WIRED* (7 mai 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
10. Voir Buolamwini et Gebru, « Gender Shades ».
11. Ridhi Shetty et Hannah Quay-de la Vallee, *CDT Comments to OSTP Highlight How Biometrics Impact Disabled People,* Center for Democracy & Technology (2022), https://cdt.org/insights/cdt- comments-to-ostp-highlight-how-biometrics-impact-disabled-people/.
12. Voir Chaim Gartenberg, « Twitter plans to change how image cropping works following concerns over racial bias », *The Verge* (2 octobre 2020), https://www.theverge.com/2020/10/2/21498619/twitter- image-cropping-update-racial-bias-machine-learning.
13. Commissariat à la protection de la vie privée du Canada, « Communiqué : Les pratiques illégales de Clearview AI présentent une surveillance de masse des Canadiens, selon les commissaires » (3 février 2021), https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2021/nr-c_2 10203/.
14. Voir l'article de Tom Cardoso et Colin Freeze, « Ottawa tested facial recognition on millions of travellers at Toronto's Pearson airport in 2016 », *The Globe and Mail* (19 juillet 2021), https://www.theglobeandmail.com/canada/article-ottawa-tested-facial-recognition-on-millions-of- travellers-at-Torontos/.
15. Jennifer Bryant, « Facebook's $650M BIPA settlement 'a make-or-break moment' », *IAPP* (5 mars 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/; Katherine Anne Long, « Amazon and Microsoft team up to defend against facial recognition lawsuits », *The Seattle Times* (15 avril 2021), https://www.seattletimes.com/business/technology/facial-recognition-lawsuits-against-amazon- and-microsoft-can-proceed-judge-rules/.

16. « Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale », Commissariat à la protection de la vie privée du Canada (2 mai 2022), https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et- securite-publique/gd_rf_202205/
17. Giorgio Resta, « Personnalité, Persönlichkeit, Personality », *European Journal of Comparative Law and Governance*, n° 3 (2008) : 215-243, doi : https://doi.org/10.1163/22134514-00103002; Jane Bailey, « Towards an Equality-Enhancing Conception of Privacy », *Dalhousie Law Journal* 31, n° 2 (2008) : p. 267-309
18. Voir Owen et coll., *Facial Recognition Moratorium Briefing #1*.
19. *Loi constitutionnelle de 1982,* Annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11, https://canlii.ca/t/ldsx (la Charte); *R. c. Plant*, 1993 CanLII 70 (CSC), [1993] 3 RCS 281, paragraphe 93, http://canlii.ca/t/1fs0w; *Blencoe c. Colombie-Britannique (Human Rights Commission)*, 2000 CSC 44 (CanLII), [2000] 2 RCS 307, https://canlii.ca/t/525t, paragraphe 50, citant *R. c. Morgentaler*, 1988 CanLII 90 (CSC), p. 166.
20. Yuan Stevens et Sonja Solomun, *Facing the Realities of Facial Recognition Technology : Recommendations for Canada's Privacy Act* (Centre for Media, Technology and Democracy, 17 février 2021), https://www.mediatechdemocracy.com/work/facing-the-realities-of-facial-recognition-technology; *R. c. Oakes*, 1986 CanLII 46 (CSC), [1986] 1 RCS 103, https://canlii.ca/t/1ftv6.
21. Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe, Sonja Solomun et Kate Gilbert, *Facial Recognition Briefing #1*, Tech Informed Policy Initiative (août 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1.
22. Tim McSorley, « Open Letter: Canadian Government Must Ban Use of Facial Recognition Surveillance by Federal Law Enforcement, Intelligence Agencies », *Amnesty International Canada News* (8 juillet 2020), https://www.amnesty.ca/news/open-letter-canadian-government-must-ban-use-of-facial- recognition-surveillance-by-federal-law-enforcement-intelligence-agencies/; D'autres défenseurs canadiens pour l'imposition d'un moratoire quelconque sur les TRF sont Cynthia Khoo, associée au Center on Privacy & Technology de Georgetown Law; Brenda McPhail, directrice de la protection de la vie privée, Programme de technologie et de surveillance à l'Association canadienne des libertés civiles; Ana Brandescu, professeure McConnell de pratique, Centre de recherche interdisciplinaire à Montréal, Université McGill; et Yuan Stevens, responsable des politiques sur la technologie, la cybersécurité et la démocratie, Leadership Lab and Cybersecure Policy Exchange, Toronto Metropolitan University.
23. Voir Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable.*
24. Plusieurs États américains, ainsi que l'UE, ont imposé des interdictions. Voir Owen et coll., *Facial Recognition Moratorium Briefing #1*.
25. Pour plus de détails, voir Taylor Owen, Derek Ruths, Stephanie Cairns, Sara Parker, Charlotte Reboul, Ellen Rowe et Sonja Solomun, *Facial Recognition Moratorium Briefing #2,* Tech Informed Policy Initiative (août 2020), https://www.mediatechdemocracy.com/work/facial-recognition-moratorium- briefing-1-wfgs7.
26. Ibid.
27. Voir Cybersecure Policy Exchange & Tech Informed Policy, *Facial Recognition Technology Policy Roundtable.*
28. Sam Andrey, Sonja Solomun et Yuan Stevens, *Regulating Face Recognition to Address Racial and Discriminatory Logics in Policing | EPIC AI Symposium,* Centre for Media, Technology and Democracy (2021), https://www.mediatechdemocracy.com/work/regulating-face-recognition-to- address-racial-and-discriminatory-logics-in-policing-epic-ai-symposium; Yuan Stevens, N*ow You See Me? Advancing Data Protection and Privacy for Police Use of Facial Recognition in Canada*, Cybersecure Policy Exchange (2021), https://www.cybersecurepolicy.ca/now-you-see-me.
29. European Digital Rights (EDRi), *An EU Artificial Intelligence Act for Fundamental Rights A Civil Society Statement* (2021), https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf; Asha Allen et Ophélie Stockhem, « EU Tech Policy Brief: January 2022 Recap », Center for Democracy & Technology (2 février 2022), https://cdt.org/insights/eu-tech-policy-brief-january-2022-recap/.
30. 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, [2018] JO L/119,https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=celex%3A32016L0680, articles 10 et 11.

31. Le comité européen de la protection des données et le CEPD demandent l'interdiction de l'utilisation de l'IA pour la reconnaissance automatique des caractéristiques humaines dans les espaces accessibles au public, ainsi que d'autres utilisations de l'IA qui peuvent conduire à une discrimination » (21 juin 2021), https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use- ai-automated-recognition-human-features-publicly-accessible_fr.
32. Jake Parker, « Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition », Security Industry Association (9 juillet 2021), https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/.
33. *An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. 2019 MA S2963, https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253.