Revue Gouvernance
Governance Review

Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis

Stany Nzobonimpa

Volume 19, numéro 2, 2022

Varia

URI : https://id.erudit.org/iderudit/1094078ar
DOI : https://doi.org/10.7202/1094078ar

Aller au sommaire du numéro

Éditeur(s)

Centre d'études en gouvernance de l'Université d'Ottawa

ISSN

1912-0362 (numérique)

Découvrir la revue

Citer cette note

Nzobonimpa, S. (2022). Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis. *Revue Gouvernance / Governance Review*, *19*(2), 99–114. https://doi.org/10.7202/1094078ar

Résumé de l'article

Que ce soit par des organismes privés ou publics, l'adoption des technologies de reconnaissance faciale est sujet de controverses, en particulier en raison du manque de lois spécifiques réglementant leur usage. Malgré les questionnements et débats qu'engendrent l'utilisation de l'intelligence artificielle (IA) et la prise de décision automatique dans les pays comme le Canada et les États-Unis, des services de police, entre autres, reconnaissent avoir eu recours à de telles technologies dans divers contextes. La littérature existante montre que les défis qu'apporte l'adoption des technologies ayant recours aux algorithmes de reconnaissance faciale vont des biais liés, notamment, aux erreurs d'identification et d'appariement aux questions d'éthique et de valeurs, en passant par des enjeux environnementaux. Alors qu'une prolifération de ces systèmes de haute technologie permettant l'identification biométrique automatique est de plus en plus remarquable, les outils juridiques et politiques en la matière tardent à s'adapter à un domaine en constante évolution. Cette note fait un tour d'horizon des politiques, des instruments juridiques et des cadres légaux en place au Canada et aux États-Unis vis-à-vis de l'adoption et de l'utilisation des technologies de reconnaissance faciale. En particulier, nous montrons que bien que cette adoption soit chose courante à travers différentes entités, les contextes politiques et les cadres légaux et réglementaires ne permettent pas de faire face à un système d'identification biométrique par l'IA. Les préoccupations en matière de droits de la personne, de vie privée et d'équité invitent à un examen plus approfondi de l'état des instruments en place.

NOTE DE RECHERCHE

Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis

Par Stany Nzobonimpa[1]

RÉSUMÉ

Que ce soit par des organismes privés ou publics, l'adoption des technologies de reconnaissance faciale est sujet de controverses, en particulier en raison du manque de lois spécifiques réglementant leur usage. Malgré les questionnements et débats qu'engendrent l'utilisation de l'intelligence artificielle (IA) et la prise de décision automatique dans les pays comme le Canada et les États-Unis, des services de police, entre autres, reconnaissent avoir eu recours à de telles technologies dans divers contextes. La littérature existante montre que les défis qu'apporte l'adoption des technologies ayant recours aux algorithmes de reconnaissance faciale vont des biais liés, notamment, aux erreurs d'identification et d'appariement aux questions d'éthique et de valeurs, en passant par des enjeux environnementaux. Alors qu'une prolifération de ces systèmes de haute technologie permettant l'identification biométrique automatique est de plus en plus remarquable, les outils juridiques et politiques en la matière tardent à s'adapter à un domaine en constante évolution. Cette note fait un tour d'horizon des politiques, des instruments juridiques et des cadres légaux en place au Canada et aux États-Unis vis-à-vis de l'adoption et de l'utilisation des technologies de reconnaissance faciale. En particulier, nous montrons que bien que cette adoption soit chose courante à travers différentes entités, les contextes politiques et les cadres légaux et réglementaires ne permettent pas de faire face à un système d'identification biométrique par l'IA. Les préoccupations en matière de droits de la personne, de vie privée et d'équité invitent à un examen plus approfondi de l'état des instruments en place.

Mots-clés : *reconnaissance faciale ; algorithmes ; politiques ; réglementation ; Canada ; États-Unis*

1. Stany Nzobonimpa est doctorant à l'École nationale d'administration publique (ÉNAP-Gatineau) et analyste de politiques au Gouvernement fédéral du Canada. ORCID : 0000-0001-6196-950X

ABSTRACT

Whether they are used by private or public entities, facial recognition technologies are subject to debate and controversy, notably around the lack of specific legislation on their use. Although artificial intelligence (AI) and automated decision-making systems have raised questions and sparked debate in Canada and the U.S., police departments have used such technologies in various contexts. Literature demonstrates the challenges brought by facial recognition algorithms range from biases related to errors of identification and matching to challenges of values and ethics, including environmental issues. Despite an increasing trend in the use of leading-edge automated biometric identification technologies, existing legal and policy instruments have not kept pace with the highly evolving field of high-tech. This note provides an overview of the policies and legal frameworks in Canada and in the U.S. with respect to the acquisition, use and integration of facial recognition technologies. In particular, we show that despite an increasing integration of such technologies across various entities, the policy, legal and regulatory frameworks are yet to be adapted to the new reality of AI biometric identification. Issues related to human rights, privacy and equity call for further examination of the instruments in place.

Keywords : *facial recognition ; algorithms ; policies ; regulation ; Canada ; United States*

Introduction

Les technologies de reconnaissance faciale sont de plus en plus utilisées, dans des domaines variés allant de la vérification de l'identité à la sûreté publique, en passant par des fins purement commerciales. Des services de police, des hôpitaux, des commerces et des sites de réseaux sociaux ont recours à la technologie d'identification de pointe. Des systèmes de vision automatique permettant la vidéosurveillance sont utilisés dans plusieurs applications et dispositifs électroniques et aux fins d'authentification d'utilisateurs.

La technologie de reconnaissance faciale est une catégorie d'identification biométrique qui, grâce aux algorithmes (c.-à-d. des équations mathématiques programmées dans un logiciel), permet de cartographier mathématiquement les traits physiques d'un visage d'une personne. Le système fonctionne avec des bases de données dans lesquelles il entrepose les informations sous forme d'empreintes faciales identitaires. Les logiciels de reconnaissance faciale ont recours à des modèles d'apprentissage profond qui, à leur tour, permettent de vérifier l'authenticité d'une image en comparant celle-ci aux données existant soit dans une base de données, soit sur différents sites Internet.

Malgré ses avancées, ce nouvel outil biométrique a également présenté des défis qui lui sont propres. Loin d'être parfaits, les systèmes de reconnaissance faciale font face à des critiques pour les imperfections qu'ils apportent, que ce soit par rapport à la qualité et à l'authenticité des résultats (Grother et al., 2019a, pp. 26-31), aux failles dans les lois de protection de la vie privée (Senior et Pankanti, 2011), aux questions environnementales (Li et al., 2016 ; Le Page, 2018 ; Lu, 2019 ; Strubell, et al., 2019) ou encore aux biais, notamment la discrimination envers certains groupes ethniques (Garvie et al., 2016 ; Raji et Buolamwini, 2019). Ces défis invitent les responsables de politiques publiques à mettre en place des outils et instruments qui assurent la conformité de nouvelles inventions tout en encourageant l'innovation. En particulier, le Canada et les États-Unis commencent à s'intéresser aux défis politiques que peuvent engendrer les technologies de pointe et, bien que les processus en soient encore à leurs débuts, à mettre en place des cadres politiques de réglementation, notamment en ce qui concerne les systèmes d'intelligence artificielle. De plus, certains intervenants du milieu policier, notamment du Québec, s'intéressent de plus en plus aux conséquences de l'usage de ce type de technologie par la police (Nzobonimpa, 2022, pp. 281-291). La présente note de recherche a pour but de recenser les politiques et instruments juridiques, réglementaires et législatifs en lien avec la régulation des technologies de reconnaissance faciale automatique au Canada et aux États-Unis.

1. Recension des écrits

L'utilisation des technologies de reconnaissance faciale est sujet de controverses, en particulier en raison du manque de lois spécifiques réglementant leur usage. L'une de ces controverses auxquelles fait face ce nouveau venu de la haute technologie est la protection des données sur la vie privée. Alors que la plupart des pays ont en place des lois sur la protection des informations sur la vie privée des citoyens, la particularité des systèmes automatisés fait en sorte qu'il est difficile de les classer selon différents domaines légaux. Par exemple, au Royaume-Uni, la loi sur la protection des données (*Data Protection Act*) n'a inclus les images, notamment celles obtenues par caméra de surveillance ou CCTV (système de télévision en circuit fermé), dans son champ d'application qu'en 2000 (Information Commissioner's Office, 2017). D'après Buckley et Hunter (2011), l'application de la technologie de reconnaissance à l'image faciale d'un individu constitue un traitement de données à caractère personnel et, par conséquent, ne peut avoir lieu que s'il existe une justification légale. Le traitement et l'usage des images des personnes ont un impact important sur la vie individuelle, et l'adoption d'une reconnaissance automatique est souvent vue comme intrusive, particulièrement dans le contexte de l'intelligence artificielle, où une image peut être utilisée pour extraire d'autres informations plus sensibles (LaFrance, 2017).

L'utilisation de la reconnaissance faciale par des services de police est grandement remise en question non seulement en raison des failles et des erreurs que ces technologies sont susceptibles de produire, mais également parce que, même lorsqu'elles produisent des résultats plus ou moins fiables, elles engendrent des questionnements liés aux inégalités économiques (Eubanks, 2018), au profilage et à la catégorisation des individus (Brayne, 2020), entre autres. D'après un rapport publié par le National Institute of Standards and Technology (NIST), un institut des normes et de la technologie au sein du département américain du Commerce, la précision de plusieurs systèmes produits aux États-Unis est discutable, ayant affiché des taux d'erreurs très élevés, en particulier lorsqu'utilisés pour identifier des personnes de couleur (Grother et al., 2019b, pp. 46-49). Ses auteurs ont déterminé que les personnes à la peau foncée pouvaient être mal identifiées à des taux allant jusqu'à 100 %. Or, que ce soit aux États-Unis ou au Canada, des services de police reconnaissent avoir eu recours à de telles technologies dans leurs opérations (Martin, 2019 ; Tunney, 2020).

Ces biais par rapport aux taux d'appariement des systèmes de reconnaissance faciale font l'objet de plusieurs débats. Dans son documentaire *Coded Bias*, Kantayya (2020) a montré que les personnes de couleur, et particulièrement les femmes noires, sont les plus à risque d'être mal identifiées, même par les technologies les plus avancées sur le marché. Cela constitue une entrave à leurs libertés individuelles, et cet obstacle renforce des formes de discrimination existantes. Au-delà des erreurs d'identification, lorsque combinée aux autres possibilités qu'offre l'usage des algorithmes, dont l'exploration de données (*data mining*) et la modélisation prédictive, la collecte des données biométriques sur des individus est non seulement nuisible à leur liberté et à leur vie privée, mais elle peut également aggraver les inégalités socio-économiques existantes en « profilant » et en « punissant » les plus démunis (Eubanks, 2018, p. 223). Eubanks (2018) parle de ce phénomène comme d'une automatisation de la pauvreté qui permet de [traduction] « gérer les individus pauvres dans le but d'éviter la responsabilité commune d'éradiquer la pauvreté » (p. 13).

Des questions d'éthique à l'ère de la reconnaissance faciale préoccupent les chercheurs depuis au moins une décennie. D'après un rapport de la Commission de l'éthique en science et en technologie (2020, p. 17), « le recours à la reconnaissance faciale est souvent justifié sur la base des gains d'efficacité ou d'efficience qu'elle permettrait de réaliser ». Cependant, ces gains sont soumis à un examen de valeurs, étant donné les conséquences éthiquement discutables que ces mêmes technologies sont susceptibles d'engendrer. D'ailleurs, dans l'analyse de l'efficacité et de l'efficience, la notion de fiabilité devrait occuper une place importante. Or, comme l'a montré l'étude de Grother et al. (2019b), cette fiabilité n'est pas toujours au rendez-vous lorsqu'on analyse les résultats de plusieurs systèmes de reconnaissance faciale même parmi les

plus avancés de la planète. L'exigence de fiabilité est encore plus importante pour des systèmes opérant grâce à une intelligence artificielle capable d'apprendre et de prendre des décisions qui peuvent avoir un impact important sur la vie de personnes, que ce soit à des fins de justice ou encore de qualification par rapport à un produit bancaire (O'Neil, 2016, p. 142-150).

L'aspect éthique revient également lorsque des chercheurs s'intéressent à l'utilisation de la reconnaissance faciale en milieu public. La combinaison de systèmes de surveillance par vidéo (CCTV) à l'intelligence artificielle suscite des discussions non seulement en raison du manque de fiabilité des résultats, mais également à cause de l'absence de consentement des sujets concernés. Au Canada, en octobre 2020, des rapports médiatiques faisant état de l'existence d'un programme de surveillance par reconnaissance faciale dans des établissements de la compagnie Cadillac Fairview, propriétaire de plusieurs centres commerciaux du pays, ont déclenché des enquêtes par le Commissaire à la protection de la vie privée du Canada et quelques-uns de ses homologues provinciaux (Gilligan, 2020). L'organisme Protégez-Vous, qui offre aux consommateurs du Québec des conseils sur plusieurs milliers de produits, a estimé que «personne n'est à l'abri» de brèches de sécurité après que d'importants établissements financiers canadiens eurent été victimes de vols de données individuelles touchant au moins 6 millions de personnes (Leroux, 2020). Ainsi, la collecte des données biométriques sur des individus sans leur consentement, combinée à de telles fuites des informations personnelles devenues monnaie courante, constitue un véritable problème qui met en jeu non seulement la transparence et le consentement, mais également l'autonomie des personnes, et qui pose une contrainte psychologique à leur liberté (Commission de l'éthique en science et en technologie, 2020, p. 21). De ce fait, certaines valeurs démocratiques sont ainsi confrontées. Parizeau (2010) a montré que le recours à l'identification biométrique peut créer un contexte politique difficile marqué par le «pouvoir de l'État sur l'individu» et susceptible d'introduire «un clivage radical avec l'étranger, l'Autre» (p. 225).

2. La réglementation de la reconnaissance faciale automatique

2.1. Aux États-Unis

Bien que les États-Unis soient parmi les chefs de file mondiaux en matière de production de systèmes d'intelligence artificielle (Statista Research Department, 2022), le pays n'a pas de lois fédérales régissant l'utilisation ou le traitement des données biométriques obtenues par le biais de la technologie de reconnaissance faciale. Or, plusieurs études, rapports et publications médiatiques ont montré que l'utilisation de telles technologies, que ce soit par des agents de la paix, des commerces ou même des institutions judiciaires, est chose courante en Amérique (Buolamwini et Gebru, 2018 ; duPont, 2021 ; Garvie, 2019 ; Grother et al., 2019b). Plus récemment, des mouvements de manifestations dénonçant la brutalité policière, combinés à un intérêt croissant des chercheurs, ont provoqué un débat important par rapport à l'utilisation de la reconnaissance faciale, en particulier par la police. Les services de police de plusieurs États ont été accusés d'utiliser régulièrement la reconnaissance faciale dans le but de trouver des suspects alors même que les résultats semblent discutables. Ainsi, en juin 2020, Robert Julian-Borchak Williams, un homme noir du Michigan, a été identifié par des algorithmes du service de police de Detroit et accusé à tort pour des crimes commis par une autre personne (Hill, 2020).

Il importe de noter que la même technologie est également utilisée dans le but d'aider les services de police à assurer la sécurité dans des lieux publics, comme des écoles, des rues ou d'autres lieux de rassemblement. Néanmoins, malgré les retombées potentiellement positives que les utilisateurs évoquent pour justifier le recours à la technologie de pointe (combattre le crime en identifiant des suspects, localiser des personnes – notamment des enfants – perdues, etc.), la possibilité que l'usage non contrôlé de la reconnaissance faciale soit essentiellement néfaste préoccupe la population américaine. Un sondage du Pew Research Center a révélé qu'une majorité d'Américains ne feraient confiance à l'usage de la reconnaissance faciale par les services de police que dans le cas où cet usage serait fait de façon responsable, ce qui sous-tend une réglementation de telles technologies (Smith, 2019).

S'il y a aux États-Unis un manque de réglementation fédérale sur la technologie de reconnaissance faciale, des projets de loi sont en cours pour assurer un contrôle et prévenir les effets négatifs liés à la technologie de reconnaissance faciale tout en encourageant l'innovation et la concurrence. Depuis 2019, au moins quatre sénateurs

américains ont proposé des projets de loi sur l'usage de cette technologie. En novembre 2019, les sénateurs Christopher Coons (démocrate, Delaware) et Mike Lee (républicain, Utah) ont déposé au Sénat le projet S. 2878, connu comme [traduction] « projet pour limiter l'utilisation de la technologie de reconnaissance faciale par les agences fédérales et à d'autres fins » (Coons et Lee, 2019). Les sénateurs parrains du texte du projet, qui au moment de la rédaction de la présente note se trouve à l'étape de deuxième lecture par le Comité judiciaire, proposent qu'un [traduction] « agent ou un employé d'une agence ne puisse utiliser la technologie de reconnaissance faciale pour effectuer une surveillance continue d'un individu ou d'un groupe d'individus dans un espace public » (Coons et Lee, 2019, p. 2). Le texte prévoit des exceptions, notamment dans le cas où l'utilisation de la technologie de reconnaissance faciale est autorisée par une ordonnance du tribunal (*court order*) et vise à soutenir le travail d'un agent de la paix. Si une cour de justice détermine la nécessité de l'utilisation de telles technologies, la validité de cette autorisation ne peut excéder 30 jours. Une extension à cette période de validité ne dépassant pas trente jours peut être demandée au tribunal. Une autre exigence du projet de loi est que toute utilisation de la technologie de reconnaissance faciale conformément à une ordonnance du tribunal doit être effectuée de manière à minimiser l'acquisition, la conservation et la diffusion d'informations sur les personnes autres que celles pour lesquelles il y avait un motif probable de demander l'ordonnance du tribunal (Coons et Lee, 2019, art. 3). S'il est adopté, ce projet de loi prescrira au directeur du Bureau administratif des tribunaux américains (*Director of the Administrative Office of the United States Courts*) de faire des rapports et de divulguer les données relatives à l'utilisation de la technologie, entre autres le nombre de demandes d'ordonnances de tribunaux, la nature des dispositifs utilisés dans la collecte des données biométriques et le nombre de personnes dont les données sont traitées grâce à la technologie d'intelligence artificielle (Coons et Lee, 2019).

En octobre 2019, le sénateur Cory Booker (démocrate, New Jersey) a déposé le projet de loi S. 2689 pour [traduction] « interdire l'utilisation de la technologie de reconnaissance biométrique et de l'analyse biométrique dans certains logements locatifs financés par le gouvernement fédéral et à d'autres fins » (Booker, 2019). Le projet est actuellement (février 2022) en lecture par le Comité sur les banques, le logement et les affaires urbaines (*Committee on Banking, Housing, and Urban Affairs*). Il prévoit ce qui suit :

> [Traduction]
>
> À compter de la date qui tombe six mois après la date de promulgation de la présente loi, le propriétaire d'un logement locatif bénéficiant de l'aide fédérale ne peut pas utiliser ou autoriser que soient utilisées la technologie de reconnaissance et l'analyse biométrique faciales, la technologie de reconnaissance biométrique et l'analyse

> biométrique physiques ou la technologie de reconnaissance biométrique et l'analyse biométrique à distance dans l'unité d'habitation ou dans tout bâtiment ou terrain contenant l'unité d'habitation. (Booker, 2019, art.2)

Le projet comprend également une exigence au secrétaire au Logement et au Développement urbain (*Secretary of Housing and Urban Development)* de soumettre des rapports au Sénat et à la Chambre des représentants et de rendre publique toute utilisation de la technologie de reconnaissance faciale par des propriétaires d'unités d'habitation ou de logements locatifs bénéficiant d'une aide du gouvernement fédéral. Ces rapports devraient également inclure, entre autres, l'impact que ces technologies ont sur les résidents et les informations démographiques sur les résidents qui ont été assujettis à l'usage de ces technologies (Booker, 2019).

En février 2020, les sénateurs Jeff Merkley (démocrate, Oregon) et Cory Booker (démocrate, New Jersey) ont déposé le projet de loi S. 3284 pour [traduction] « créer un moratoire sur l'utilisation, par le gouvernement, de la technologie de reconnaissance faciale jusqu'à ce qu'une commission recommande les lignes directrices et limites appropriées de l'utilisation de la technologie de reconnaissance faciale » (Merkley et Booker, 2020). Ce projet de loi sur l'usage éthique de la reconnaissance faciale (*Ethical Use of Facial Recognition Act)* part du constat que les technologies de reconnaissance faciale peuvent être inexactes, « en particulier pour les femmes, les jeunes, les Afro-Américains et d'autres groupes ethniques » (art. 2). Dans le but de limiter l'utilisation de la reconnaissance faciale, le projet stipule ce qui suit :

> [Traduction]
>
> Un représentant du gouvernement ne peut pas installer de caméra qui serait utilisée conjointement avec la technologie de reconnaissance faciale, accéder à des informations obtenues à partir de la technologie de reconnaissance faciale ou utiliser de telles informations, ou importer une technologie de reconnaissance faciale pour identifier une personne aux États-Unis sans mandat jusqu'à la date à laquelle le Congrès adoptera une loi mettant en vigueur les lignes directrices pour l'utilisation de la technologie de reconnaissance faciale établie par la Commission en vertu de l'article 6. (Merkley et Booker, 2020, art. 4)

Le projet de loi S. 3284 prévoit également la création d'une commission œuvrant pour le compte du Congrès américain et dont le but serait de créer des directives sur l'utilisation des technologies de reconnaissance faciale aux États-Unis. La commission devrait également faire état des limites de ces technologies pour informer le Congrès de biais, d'impact racial disproportionné et de violations aux droits à la vie privée, entre autres

(Merkley et Booker, 2020). Au moment de la rédaction de la présente note (février 2022), le projet est à l'étape de lecture par le Comité de la sécurité intérieure et des affaires gouvernementales (*Homeland Security and Governmental Affairs*).

En juin 2021, le projet de loi S. 2052, qui porte sur la reconnaissance faciale et la technologie biométrique (*Facial Recognition and Biometric Technology Moratorium Act*), a été déposé au Sénat américain. Proposé par le sénateur Edward Markey (démocrate, Massachusetts), ce projet prévoit [traduction] « interdire la surveillance biométrique par le gouvernement fédéral sans autorisation légale explicite et refuser certaines subventions fédérales de sécurité publique aux gouvernements des États et aux administrations locales qui exercent une surveillance biométrique » (Markey, 2021).

Parmi les autres projets de loi qui en sont encore à la première étape au sein du Congrès américain, mentionnons le projet H. R. 6609, déposé à la Chambre par le représentant Bill Huizenga (républicain, Michigan), qui veut interdire à l'agence américaine du revenu d'utiliser la technologie de reconnaissance faciale pour des fins d'identification (Huizenga, 2022), ou encore le projet H. R. 2075, déposé à la Chambre par le représentant John Curtis (républicain, Utah), qui cherche à obliger le Département d'État américain à inclure des informations sur l'état de la surveillance et l'utilisation des technologies de pointe dans son rapport sur l'état des droits de la personne à travers le monde (Curtis, 2021).

Il importe de noter que toutes ces tentatives fédérales restent encore à l'étude et qu'au moment de rédiger cette note, aucune n'avait fait preuve d'avancées remarquables.

Malgré ce « retard » en matière de législation de la reconnaissance faciale au niveau du gouvernement fédéral américain, des villes et États ont mis en place des lois pour protéger la population contre l'usage abusif des systèmes de reconnaissance faciale. Par exemple, en Californie et au Massachusetts, plusieurs villes ont interdit l'utilisation de la reconnaissance faciale par le gouvernement. En Oregon, la Ville de Portland a banni tout usage de cette technologie par des utilisateurs des secteurs public et privé. Dans au moins trois États, la reconnaissance faciale par les caméras de corps des agents de la paix est interdite (duPont, 2021). L'État de Washington a voté une loi qui exige qu'il y ait de la transparence lorsque les autorités utilisent la technologie de reconnaissance faciale. Cette loi stipule qu'un examen humain des résultats fournis automatiquement par l'intelligence artificielle est obligatoire dans les cas où l'identification automatisée pourrait avoir des conséquences importantes sur la vie des personnes. L'utilisation de la reconnaissance faciale pour la surveillance en temps réel est interdite sauf en présence d'un mandat ou dans des situations d'urgence.

2.2. Au Canada

Il n'y a pas de lois ni de politiques fédérales canadiennes qui s'occupent spécifiquement de réglementer les technologies de reconnaissance faciale. Cependant, la présence de ces technologies et leur utilisation par différents organismes, en particulier les services de police, ont récemment suscité des débats sur de possibles projets de lois réglementant les systèmes d'intelligence artificielle, et en particulier ceux qui ont recours à l'identification biométrique. Par exemple, la compagnie américaine Clearview AI a été forcée d'abandonner ses contrats au Canada à la suite des enquêtes et rapports médiatiques qui ont révélé que ses systèmes de reconnaissance faciale avaient été utilisés par la police en violation des lois sur la vie privée (Commissariat à la protection de la vie privée du Canada, 2020, 6 juillet).

Dans un rapport sur la reconnaissance faciale automatique au sein des secteurs privé et public, le Commissariat à la protection de la vie privée du Canada (2013) a présenté l'identification biométrique par l'intelligence artificielle comme étant la forme « la plus envahissante des technologies d'identification biométrique populaires modernes » (p. 2). En ce qui relève de politiques internes au gouvernement fédéral canadien, il existe une directive adoptée par le Secrétariat du Conseil du Trésor du Canada en 2019 dans le but de réglementer l'usage de l'intelligence artificielle par des entités administratives, notamment celles qui ont recours aux technologies dans la prestation de services. Cette réglementation, la Directive sur la prise de décisions automatisée, stipule que les systèmes décisionnels automatisés doivent être déployés « d'une manière qui permet de réduire les risques pour les Canadiens et les institutions fédérales » (Secrétariat du Conseil du Trésor du Canada, 2019, art. 4.1). Cependant, ni cette directive ni la politique qui l'accompagne, la Politique sur les services et le numérique, ne font mention de technologies de reconnaissance faciale ni de la manière dont les organismes fédéraux sont censés les utiliser.

Malgré le manque de réglementations spécifiques en matière de reconnaissance faciale automatique au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) exige aux organisations du secteur privé ayant recours à la collecte de renseignements sur les individus d'obtenir le consentement de ces derniers avant d'utiliser ou de communiquer leurs renseignements (Ministère de la Justice du Canada, 2019). Ainsi, une organisation ne peut recueillir de renseignements personnels à l'insu de l'intéressé sans son consentement que dans quelques cas spécifiques, entre autres lorsque la collecte est dans l'intérêt de l'individu en question, lorsqu'il s'agit d'un renseignement produit par l'intéressé, notamment dans le cadre de son emploi ou d'une autre activité professionnelle, et lorsque ces renseignements sont

collectés pour des fins journalistiques ou artistiques (Ministère de la Justice du Canada, 2019). La *Loi* interdit également l'utilisation des renseignements personnels que détiennent les entreprises privées à moins que celles-ci n'obtiennent le consentement de la personne concernée. Quelques exceptions portent sur des cas spécifiques, notamment (Ministère de la Justice du Canada, 2019, p. 8-11) :

- lorsque l'organisation privée détermine que l'utilisation des renseignements peut être utile dans une enquête ayant rapport avec des contraventions aux lois fédérales, provinciales ou étrangères ;

- dans une situation d'urgence lorsque la vie, la santé ou la sécurité d'un individu est en jeu ;

- dans une déclaration de témoin qui implique le traitement ou le règlement d'une entente ;

- lorsque l'utilisation est faite pour des fins de recherche (statistiques ou études).

Dans le cas où les renseignements personnels sont recueillis, la LPRPDE accorde aux individus concernés le droit de consulter leurs renseignements et le pouvoir de contester leur exactitude au besoin. Les institutions publiques fédérales sont également tenues de respecter les exigences sur la protection des renseignements privés de la *Loi sur la protection des renseignements personnels* et de la Politique sur la protection de la vie privée (Secrétariat du Conseil du Trésor du Canada, 2020), qui leur exigent de protéger les renseignements privés détenus par le gouvernement fédéral sur les citoyens. Les services frontaliers, les prestations, la police fédérale et les services d'impôt fédéral sont tenus de ne recueillir les renseignements individuels que lorsqu'il existe un lien direct avec leurs différents programmes et activités. De plus, cette seconde loi interdit de passer par les services des tiers dans l'obtention de ces renseignements, sauf lorsqu'il y a autorisation de la personne concernée. Aucune de ces deux lois importantes dans la protection des renseignements individuels ne fait mention de la reconnaissance faciale dans l'obtention des renseignements privés. Ce manque de précision crée une zone grise et laisse ouverte la question de savoir si des renseignements recueillis par l'intelligence artificielle devraient rentrer dans les catégories des renseignements telles que définies dans la loi. Dans un récent rapport, le Commissariat à la protection de la vie privée du Canada a reconnu ce manque de lois sur la protection de renseignements individuels dans un contexte numérique et déploré l'inaptitude des lois en place :

> *Il n'en reste pas moins que notre cadre législatif actuel en matière de protection de la vie privée est dépassé et ne traite pas suffisamment de l'environnement numérique pour garantir une réglementation appropriée des nouvelles technologies. Une reprise fondée sur l'innovation ne sera durable que si l'on protège adéquatement les intérêts et les droits de tous les citoyens. Nos lois peuvent et doivent prendre en compte ces intérêts et ces droits. Nous avons besoin de lois qui permettent aux Canadiens de profiter des avantages de la technologie, dans l'intérêt public, tout en préservant leur droit à la vie privée. Le moment est venu de montrer aux Canadiens qu'ils peuvent avoir les deux à la fois. (Commissariat à la protection de la vie privée du Canada, 2020, 8 octobre)*

Le Commissariat a soumis des recommandations pour la réforme de la *Loi sur la protection des renseignements personnels* dans lesquelles il indique que « les usages de l'IA fondés sur les renseignements personnels peuvent avoir de graves conséquences sur la vie privée » (Commissariat à la protection de la vie privée du Canada, 2020, 12 novembre).

Mais, comme le suggèrent les écrits parcourus à travers la présente note, la protection des renseignements privés n'est qu'une face de la grande forme que peuvent prendre les nombreux défis que pose l'utilisation des systèmes d'intelligence artificielle, notamment ceux utilisant la reconnaissance faciale. Les questions liées aux droits de la personne occupent une place de plus en plus importante dans les débats sur la régulation et le contrôle des technologies de reconnaissance faciale. Néanmoins, à l'instar des lois canadiennes sur la protection de la vie privée, les codes canadiens sur les droits de la personne sont également muets quant aux défis que posent ces systèmes sur les droits et libertés individuels. Une étude publiée par le Programme international sur les droits de la personne de l'Université de Toronto et conduite conjointement par le laboratoire The Citizen Lab et la Munk School of Global Affairs and Public Policy a conclu que l'usage des systèmes d'intelligence artificielle dans le domaine de l'immigration est susceptible de produire de l'injustice, en particulier en défaveur des groupes vulnérables comme les réfugiés (Molnar et Gill, 2018, p. 53). Or, les autrices montrent que le gouvernement canadien a déjà en place un programme expérimental d'intelligence artificielle utilisé par les agents en immigration pour évaluer les demandes d'asile, et que ce programme s'ajoute à un système de reconnaissance faciale déjà en place dans plusieurs aéroports du pays.

Malgré ces études qui montrent de plus en plus que la prolifération de ce type de programme peut donner lieu à des lacunes en matière de droits de la personne, les principaux cadres légaux canadiens en matière de protection des droits sont encore en

retard quant à la codification de ces nouveaux venus de la légalité. À ce jour, les deux cadres légaux majeurs en matière de droits de la personne au Canada, à savoir la *Charte canadienne des droits et libertés* (qui fait partie de la *Loi constitutionnelle de 1982*) et la *Loi sur l'immigration et la protection des réfugiés*, ainsi que les différentes lois provinciales et territoriales sont encore vus comme inaptes à protéger certains droits des personnes contre l'invasion des hautes technologies, notamment celles de la reconnaissance faciale et de l'intelligence artificielle (Molnar et Gill, 2018, p. 29-35).

Conclusion

La revue des cadres politiques et réglementaires en matière de technologies de reconnaissance faciale a permis quelques observations dans les contextes canadien et américain. D'un côté, le recours à la reconnaissance faciale automatique par des entités tant publiques que privées ne relève plus de la spéculation, mais est bien présent au sein des sociétés modernes. Que ce soit au Canada ou aux États-Unis, on recense de plus en plus la présence des systèmes d'intelligence artificielle et d'apprentissage profond, qui permettent, entre autres, l'utilisation de la technologie d'identification biométrique automatique par des services de police, des centres commerciaux et des agents frontaliers. Ces nouveaux venus du système d'identification apportent bien des défis, notamment ceux liés à la protection de la vie privée, de renseignements personnels et de droits de la personne. De plus en plus d'études ayant démontré que les niveaux de précision et de fiabilité de ces technologies sont plutôt discutables, la confiance des protecteurs de droits, des citoyens et même des décideurs politiques en leur utilité n'est pas chose garantie. Ainsi, l'adoption et l'utilisation des systèmes de reconnaissance faciale se heurtent à des critiques, et plusieurs voix s'élèvent pour réclamer leur contrôle. D'un autre côté, malheureusement, la réglementation peine à s'adapter à un contexte très changeant. Les instruments politiques et cadres réglementaires existants ont du mal à s'élever à la hauteur des défis que pose l'intelligence artificielle, notamment ceux liés à la technologie de reconnaissance faciale automatique.

Bibliographie

Booker, C. A. (2019, 23 octobre). *S.2689 – No Biometric Barriers to Housing Act of 2019*. https://www.congress.gov/bill/116th-congress/senate-bill/2689/text.

Brayne, S. (2020). *Predict and surveil : Data, discretion, and the future of policing*. Oxford University Press.

Buckley, B. et Hunter, M. (2011). Say cheese ! Privacy and facial recognition. *Computer Law & Security Review*, *27*(6), 637-640. https://doi.org/10.1016/j.clsr.2011.09.011.

Buolamwini, J. et Gebru, T. (2018). Gender shades : Intersectional accuracy disparities in commercial gender classification. Proceedings of the 1st Conference on fairness, accountability and transparency. *PMLR*, *81*, 77-91. http://proceedings.mlr.press/v81/buolamwini18a.html.

Commissariat à la protection de la vie privée du Canada. (2013). *Reconnaissance faciale automatisée dans les secteurs public et privé*. https://www.priv.gc.ca/media/1766/fr_201303_f.pdf.

Commissariat à la protection de la vie privée du Canada. (2020, 6 juillet). *Clearview AI cesse d'offrir sa technologie de reconnaissance faciale au Canada*. https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/nr-c_200706/.

Commissariat à la protection de la vie privée du Canada. (2020, 8 octobre). *Rapport annuel au Parlement 2019-2020 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques*. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201920/ar_201920/.

Commissariat à la protection de la vie privée du Canada. (2020, 12 novembre). *Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE*. https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/.

Commission de l'éthique en science et en technologie. (2020). *Les enjeux éthiques soulevés par la reconnaissance faciale* (8e Commission jeunesse). https://www.ethique.gouv.qc.ca/media/2wqngchp/cest-j_2020_reconnaissance_faciale_acc_web.pdf.

Coons, C. A. et Lee, M. (2019, 14 novembre). *S.2878 – Facial Recognition Technology Warrant Act of 2019*. https://www.congress.gov/bill/116th-congress/senate-bill/2878/text.

Curtis, J. R. (2021, 19 mars). *H.R.2075 – Foreign Advanced Technology Surveillance Accountability Act*. https://www.congress.gov/bill/117th-congress/house-bill/2075/text?r=8&s=1.

duPont, S. (2021, 14 avril). *Facial recognition is here but we have no laws*. Nextgov.com. Retrieved July 6, 2022, from https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/.

Eubanks, V. (2018). *Automating inequality : How high-tech tools profile, police, and punish the poor*. St. Martins Press.

Garvie, C., Bedoya, A. M. et Frankle, J. (2016, 18 octobre). *The perpetual line-up : Unregulated police face recognition in America*. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/.

Garvie, C. (2019, 16 mai). *Garbage in, garbage out : Face recognition on flawed data*. Georgetown Law Center on Privacy & Technology. https://www.flawedfacedata.com/.

Gilligan, M. (2020, 29 octobre). *Cadillac Fairview covertly collected images of 5M shoppers across Canada : Privacy commissioners*. Global News. https://globalnews.ca/news/7429905/cadillac-fairview-facial-recognition-investgation-findings/.

Grother, P., Ngan, M. et Hanaoka, K. (2019a). *Face recognition vendor test (FRVT). Part 3 : Demographic effects*. National Institute of Standards and Technology, U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Grother, P., Ngan, M. et Hanaoka, K. (2019b). *Face recognition vendor test (FRVT). Part 2 : Identification*. National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8271.

Hill, K. (2020, 24 juin). Wrongfully accused by an algorithm. *The New York Times*. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Huizenga, B. (2022). *H.R.6609 – Facial Authorization Cannot be Enforced Act or the FACE Act*. https://www.congress.gov/bill/117th-congress/house-bill/6609/actions?r=5&s=1.

Information Commissioner's Office. (2017). *In the picture : A data protection code of practice for surveillance cameras and personal information*. https://www.enlutc.co.uk/wp-content/uploads/2019/08/cctv-code-of-practice.pdf.

Kantayya, S. (2020). *Coded bias. An exploration of the fallout of MIT Media Lab researcher Joy Buolamwini's startling discovery of racial bias in facial recognition algorithms*. 7th Empire Media. https://www.grandintheatre.com/shows/coded-bias.

LaFrance, A. (2017, 24 mars). Databases of facial images proliferate. *The Atlantic*. https://www.theatlantic.com/technology/archive/2017/03/who-owns-your-face/520731/.

Le Page, M. (2018, 10 octobre). AI's dirty secret : Energy-guzzling machines may fuel global warming. *New Scientist*. https://www.newscientist.com/article/mg24031992-100-ais-dirty-secret-energy-guzzling-machines-may-fuel-global-warming/.

Leroux, R. (2020, 21 janvier). Vos données personnelles, une cause perdue? *Protégez-vous*. https://www.protegez-vous.ca/technologie/donnees-personnelles#submenu-item-436656.

Li, D., Chen, X., Becchi, M. et Zong, Z. (2016). *Evaluating the energy efficiency of deep convolutional neural networks on CPUs and GPUs*. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/BDCloud-SocialCom-SustainCom.2016.76.

Lu, D. (2019, 6 juin). Creating an AI can be five times worse for the planet than a car. *New Scientist*. https://www.newscientist.com/article/2205779-creating-an-ai-can-be-five-times-worse-for-the-planet-than-a-car/.

Markey, E. J. (2021, 15 juin). *S.2052 – Facial Recognition and Biometric Technology Moratorium Act of 2021*. https://www.newscientist.com/article/2205779-creating-an-ai-can-be-five-times-worse-for-the-planet-than-a-car/.

Martin, N. (2019, 25 septembre). The major concerns around facial recognition technology. *Forbes*. https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/?sh=129082354fe3.

Merkley, J. et Booker, C. A. (2020, 12 février). *S.3284 – Ethical Use of Facial Recognition Act*. https://www.congress.gov/bill/116th-congress/senate-bill/3284/text.

Ministère de la Justice du Canada. (2019, 21 juin). *Loi sur la protection des renseignements personnels et les documents électroniques* (dernière mise à jour). https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.

Molnar, P. et Gill, L. (2018). *Bots at the gate : A human rights analysis of automated decision-making in Canada's immigration and refugees system*. The Citizen Lab, University of Toronto. https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

Nzobonimpa, S. (2022). L'utilisation des technologies d'apprentissage automatique par la police préoccupe-t-elle les intervenants québécois? Analyse d'une récente consultation publique. *Criminologie, 55(1)*, 271–310. https://doi.org/10.7202/1089737ar.

O'Neil, C. (2016). *Weapons of math destruction : How big data increases inequality and threatens democracy*. Broadway Books.

Parizeau, M.-H. (2010). Identité, empreinte génétique et citoyenneté : réflexions philosophiques. *Sociologie et sociétés*, *42*(2), 207-229. https://doi.org/10.7202/045362ar.

Raji, I. et Buolamwini, J. (2019). *Actionable auditing : Investigating the impact of publicly naming biased performance results of commercial AI products*. Conference on Artificial Intelligence, Ethics, and Society. https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf.

Secrétariat du Conseil du Trésor du Canada (2019, 5 février). *Directive sur la prise de décisions automatisée*. Gouvernement du Canada. https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592.

Secrétariat du Conseil du Trésor du Canada (2020, 18 juin). *Politique sur la protection de la vie privée*. Gouvernement du Canada. https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510.

Senior, A. W., & Pankanti, S. (2011). Privacy protection and face recognition. *Handbook of Face Recognition*, 671–691. https://doi.org/10.1007/978-0-85729-932-1_27.

Smith, A. (2019, 5 septembre). *More than half of U.S. adults trust law enforcement to use facial recognition responsibly*. Pew Research Center. https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

Statista Research Department (2022, 17 mars). *Opinions about top countries in race for AI among business leaders in the U.S. 2019*. https://www.statista.com/statistics/1030087/united-states-opinion-leading-countries-in-artificial-intelligence/.

Strubell, E. G., Ganesh, A. et McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*. https://doi.org/10.18653/v1/p19-1355.

Tunney, C. (2020, 5 mars). RCMP denied using facial recognition technology - then said it had been using it for months. *CBC News*. https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266.