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

Mémoire présenté par la

Ligue des droits et libertés

Au Commissariat à la protection de la vie privée du Canada
et à la Commission d'accès à l'information

15 octobre 2021

Table des matières

Présentation de la Ligue des droits et libertés

Fondée en 1963, la Ligue des droits et libertés (LDL) est un organisme à but non lucratif, indépendant et non partisan, qui vise à faire connaitre, à défendre et à promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la Charte internationale des droits de l'Homme. La LDL est affiliée à la Fédération internationale pour les droits humains (FIDH).

La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels. Son action a influencé plusieurs politiques publiques et a contribué à la création d'institutions vouées à la défense et à la promotion des droits humains, notamment l'adoption de la *Charte des droits et libertés de la personne* du Québec et la création de la Commission des droits de la personne et des droits de la jeunesse.

Elle interpelle, aux plans local, national et international, les instances gouvernementales pour qu'elles adoptent des lois, mesures et politiques conformes à leurs engagements à l'égard des instruments internationaux de défense des droits humains et pour dénoncer des situations de violation de droits dont elles sont responsables. Elle mène des activités d'information, de formation, de sensibilisation visant à faire connaitre le plus largement possible les enjeux de droits pouvant se rapporter à l'ensemble des aspects de la vie en société. Ces actions visent l'ensemble de la population de même que certains groupes placés, selon différents contextes, en situation de discrimination.

Nous remercions le Commissariat à la protection de la vie privée du Canada (CPVP) et la Commission d'accès à l'information (CAI) du Québec de cette invitation à participer à la consultation sur le *Document d'orientation préliminaire sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*[1]. Nous saluons cette initiative, mais nous regrettons toutefois que l'exercice ne vise pas l'ensemble des organismes gouvernementaux de renseignement et de sécurité chargés de l'application de la loi, tels le Service canadien du renseignement de sécurité et l'Agence des services frontaliers.

[1] CPVP, *Document d'orientation préliminaire sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, 2021. En ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/gd_frt_202106/

1. Principales interrogations soulevées par la reconnaissance faciale

[Question 10] Enjeux à caractère juridique, éthique ou social entourant la RF

La reconnaissance faciale (RF) est l'une des applications de l'intelligence artificielle (IA) les plus menaçantes pour les droits et libertés. Et pourtant, elle s'installe de plus en plus sournoisement dans nos vies, sans réel contrôle légal.

1.1 Menaces à la vie privée et à la démocratie

La Cour suprême du Canada a reconnu que la vie privée s'attache à la personne et non aux lieux ; même dans les lieux publics l'individu conserve une part d'autonomie et un droit à l'anonymat, composantes du droit à la vie privée :

> Le simple fait qu'une personne quitte l'intimité de sa résidence et pénètre dans un lieu public ne signifie pas qu'elle renonce à tous ses droits en matière de vie privée […] il nous faut reconnaitre l'anonymat comme une des conceptions de la vie privée[2].

Ce droit à l'anonymat, prérequis fondamental à l'épanouissement personnel des individus et à l'exercice de leurs droits démocratiques[3], se trouve directement compromis par la RF. Elle rend possible la surveillance de masse des lieux publics et des activités en ligne, ouvrant la porte à une société totalitaire.

1.2 D'autres droits humains en péril

Les **libertés d'expression et de réunion pacifique** s'accommodent mal d'une éventuelle surveillance par l'État et les corps policiers. Ainsi, la Cour suprême soulignait que :

> De nombreuses études empiriques ont confirmé l'« effet paralysant » de la surveillance gouvernementale sur les comportements en ligne. Ces études indiquent que la surveillance électronique par l'État incite les gens à exercer l'autocensure sur leur expression en ligne[4].

Le même « effet paralysant » peut s'étendre au droit de manifester ou de s'assembler. Comme le note le Citizen Lab : « Surveillance tools such as facial recognition technology threaten the anonymity of the crowd that has traditionally protected the identities of protesters[5] ».

---

[2] *R c. Spencer,* [2014] 2 R.C.S. 212, par. 44. En ligne : https://canlii.ca/t/g7dzp

[3] *Ibid.*, par. 15 :

> La Cour insiste depuis longtemps sur la nécessité d'adopter, à l'égard de l'art. 8, une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère.

[4] *R. c. Mills*, [2019] 2 RCS 320, par. 99. En ligne : https://canlii.ca/t/hzv2s

[5] Robertson, Khoo et Song, *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*, The Citizen Lab, 2020, p. 100. En ligne : https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada

La RF affecte aussi le **droit à l'égalité**. Des études révèlent nombre d'erreurs dans l'identification de personnes racisées, particulièrement les femmes noires. La RF peut de même stigmatiser certains groupes et communautés en les soumettant à une surveillance disproportionnée sur la base de données historiques biaisées :

> Algorithms trained on dirty data reflect the dynamics that underlie the data's original collection and, thus, perpetuate disadvantage against the affected individuals and groups with protected characteristics[6].

La RF peut aussi permettre le profilage policier en lien avec des caractéristiques ethniques, de genre ou autres.

Le **droit à la liberté** est aussi en cause. De faux « matchs » peuvent entrainer de graves conséquences : interpellation policière abusive, arrestation illégale, détention arbitraire[7], etc.

La RF pourrait aussi accroître le **risque d'erreurs judiciaires** dans les causes où l'identité d'un suspect est mise en doute. Comme le souligne la chercheure Castets-Renard « on peut alors craindre que la technologie souvent vue comme infaillible et crédible auprès des tribunaux conforte les policiers, les témoins et les juges dans leurs certitudes[8] ».

Elle peut aussi compromettre la sécurité physique ou psychologique des personnes par divulgation de leur identité (*doxing*[9]).

1.3 Efficacité non prouvée

Malgré la menace qu'elle représente pour les droits humains, et les coûts importants qu'elle implique[10], peu d'études semblent établir l'efficacité réelle de la RF :

---

[6] *Ibid.*, p. 108.

[7] *Ibid.*, p. 146 :

> Individuals whose images are captured by facial recognition technology may suffer a number of civil liberties violations, including harms associated with being detained or arrested, or invasions of privacy occasioned by other police investigative techniques (e.g., searches of an individual's home, accessing the private contents of a confiscated computer, or strip searches on arrest). Such harms may occur even if the ensuing investigation does not ultimately lead to a criminal charge.

[8] Castets-Renard, *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada. Éléments de comparaison avec les États-Unis et l'Europe*, 2020, p. 32. En ligne : https://www.docdroid.com/YIDTjrr/cadre-juridique-applicable-a-lutilisation-de-la-reconnaissance-faciale-par-les-forces-de-police-dans-lespace-public-au-quebec-et-au-canada-pdf

[9] *Doxing* : Trouver et publier sur Internet des informations privées d'une personne.

[10] Dans le cas de la Sûreté du Québec le contrat intervenu avec la compagnie *Idemia* s'élève à plus de 4,4 millions de dollars. En ligne : https://www.sq.gouv.qc.ca/wp-content/uploads/2021/06/2021-06-08-contrat-societe-idemia.pdf

> L'usage croissant de ces technologies contraste fortement avec le faible nombre d'études empiriques sur leur efficacité et leur efficience dans leur application pratique. La plupart des sources disponibles concernant l'utilisation de la reconnaissance faciale en matière de sécurité se résument aux articles de presse ou à des rapports de travail institutionnels.[11]

Par ailleurs, une autre chercheure indique :

> À l'image de la vidéosurveillance, leur utilisation est justifiée par l'existence de risques, quoique leur efficacité ne soit pas prouvée (Castagnino, 2017 ; Gormand, 2017 ; Lemaire, 2019). Par exemple, le renseignement en amont serait plus efficace dans la prévention d'événements tels que des attentats. En outre, jusqu'à présent, les déploiements de reconnaissance faciale à des fins d'identification de personnes recherchées, au Royaume-Uni notamment, témoignent d'une faible effectivité.[12]

1.4 Nécessité non démontrée

Il convient de souligner que même si une mesure ou une technique d'application de la loi s'avère « efficace », elle n'en est pas autant « nécessaire » ou « justifiable ». Tel que le disait la Cour Suprême en 2019 dans l'arrêt *Fleming* :

> […] on ne peut se fonder sur le simple fait qu'une action policière ait été efficace pour justifier qu'elle ait été prise si elle a porté atteinte à la liberté d'un individu. Pour qu'une telle atteinte soit justifiée, la *common law* exige qu'elle soit « raisonnablement nécessaire ». Si les policiers peuvent raisonnablement atteindre le même résultat en prenant une mesure qui porte moins atteinte à la liberté, une mesure plus intrusive ne sera pas raisonnablement nécessaire, quelle que soit son efficacité. Une atteinte à la liberté devrait être une mesure de dernier recours et non la première option choisie par les autorités. Conclure autrement aurait pour effet d'autoriser généralement des actions qui portent considérablement atteinte à la liberté des individus, tant qu'elles sont efficaces. Il s'agirait d'une recette pour un État policier et non pour une société libre et démocratique.[13]

1.5 Failles de sécurité

Vu la spécificité des données biométriques, toute faille de sécurité peut entrainer un préjudice irréparable. Or les fuites de renseignements personnels (RP) sont fréquentes ; elles se sont multipliées au pays ces dernières années. Elles concernaient de réputées institutions financières et gouvernementales dont on a pu mesurer la nonchalance dans la protection de données personnelles, mêmes sensibles[14].

---

[11] Jacquet et Grossrieder, « Enjeux et perspectives de la reconnaissance faciale en sciences criminelles », *Criminologie*, 54 (1), 2021, pp. 135-170. En ligne : https://doi.org/10.7202/1076696ar

[12] Picaud, *La reconnaissance faciale : un marché en construction ?*, Association Futuribles, 2020. En ligne : https://halshs.archives-ouvertes.fr/halshs-02923698/document

[13] *Fleming c. Ontario*, 2019 CSC 45, par. 98. En ligne : https://canlii.ca/t/j2pd3

[14] Notamment au Québec, le ministère de la Famille, la Régie de l'assurance maladie du Québec (RAMQ), le ministère de l'Éducation et le ministère du Revenu. Et au fédéral, l'Agence du revenu du Canada : « […] a suspendu 800 000 comptes d'utilisateurs par précaution après avoir découvert que leurs informations de connexion étaient

Enfin, le possible stockage des données biométriques en dehors des frontières canadienne ou québécoise est susceptible de diluer la protection des RP accordée par les lois applicables au pays[15].

1.6 Partenariat avec le secteur privé

La non-régulation du lucratif marché privé de la RF[16] accentue encore les craintes de dérapages. Les services de police (SP) constituent une cible de choix pour la vente de tels produits :

> On peut ainsi analyser la mise en avant croissante de la reconnaissance faciale à l'aune du juteux marché qu'elle recouvre. Or, dans le cas de la sécurité, ces marchés reposent en grande partie sur des clients publics, en particulier en France : forces de l'ordre, administrations nationales ou locales, etc.[17]

Le manque de contrôle sur les produits vendus et le peu d'expertise des SP engendrent une sujétion dangereuse, comme le souligne la chercheure Castets-Renard :

> Également, un enjeu de dépendance peut également se poser si les forces de police deviennent dépendantes d'une solution privée qu'elles ne maitrisent pas. Il y a là des risques de perte de contrôle technologique et éventuellement de subir des pressions monétaires faisant peser un coût financier élevé pour l'administration[18].

Le développement incontrôlé de la RF par l'entreprise privée peut aussi entrainer une coopération pernicieuse, les SP récupérant, aux fins de RF, les images et données collectées dans le privé à d'autres fins.

Dans l'état actuel des choses, et pour tous ces motifs, la LDL s'oppose à l'utilisation de la RF par les SP. Nous reviendrons sur cette position à la section 4. Pour le moment, nous discuterons brièvement du premier volet du document d'orientation.

---

accessibles à des "tiers non autorisés". » En ligne : https://www.journaldemontreal.com/2021/03/12/explosion-du-piratage-a-lagence-de-revenu-du-canada-800-000-comptes-ont-ete-compromis

[15] Castets-Renard, précité, p. 35 :

> Par ailleurs, le choix d'opérateurs privés étrangers fait aussi peser le risque de perte de contrôle de la souveraineté étatique, ce qui est particulièrement préoccupant. Les risques d'ingérence et de sécurité des données sont alors élevés, a fortiori si les données sont stockées en dehors du territoire québécois ou canadien.

[16] Marché mondial estimé à 7 milliards de dollars d'ici 2024. Voir Picaud, précité.

[17] *Ibid.*

[18] Castets-Renard, précité, p. 35.

2. Observations sur la version préliminaire du document d'orientation

Le document d'orientation (DO) « vise à clarifier les responsabilités et obligations légales, telles qu'elles existent actuellement, afin de veiller à ce que toute utilisation de la RF par les services de police ne contrevienne pas à la loi, de limiter les risques d'atteinte à la vie privée et de respecter le droit à la vie privée[19] [nous soulignons] ». Pour ce faire, il recommande aux SP de respecter un cadre de protection de la vie privée fondé « sur l'application de principes acceptés mondialement en matière de protection de la vie privée, dont un grand nombre sont repris dans les lois sur la protection des renseignements personnels[20] ».

En résumé, les SP devraient :

- s'assurer qu'il existe une assise légale à l'utilisation de la RF, notamment par un avis juridique ;
- protéger la vie privée dès la conception de systèmes de RF ;
- utiliser des renseignements à jour et exacts ;
- limiter la collecte de RP à ceux nécessaires ;
- protéger les RP ;
- ne pas conserver les RP plus longtemps que nécessaire ;
- mettre en œuvre des mesures de transparence des programmes de RF ;
- mettre en œuvre des mesures de responsabilisation efficaces.

Ce cadre pose plusieurs difficultés, d'abord celle de l'assise légale du recours à la RF. Aucune loi n'autorise spécifiquement l'utilisation de la RF au pays, du moins sans consentement. Et comme le signale le DO, les « tribunaux canadiens n'ont pas eu l'occasion d'établir si l'utilisation de la RF est autorisée par la common law[21] ». Nous voyons mal dans ce cadre en quoi l'obtention d'un simple avis juridique permettrait d'y recourir.

Reste l'obtention d'un mandat en vertu du Code criminel. Mais qui s'assurera que les SP iront bien chercher un tel mandat ? D'ailleurs même l'obtention d'un mandat judiciaire ne nous apparait pas une garantie suffisante dans l'état actuel des choses, vu l'absence de balises légales spécifiques sur l'utilisation de la RF.

Par ailleurs, on peut douter que les SP se plieront rigoureusement, dans le cours de leurs activités habituelles, à la procédure complexe décrite dans le DO. Nous craignons de même que le CPVP et ses homologues provinciaux n'aient ni les moyens ni les pouvoirs de s'assurer du respect de ce cadre par tous les SP du pays.

Enfin, élément plus préoccupant encore, le cadre suggéré soustrait au débat public les questions de **nécessité** et de **proportionnalité** dans l'utilisation de RF. Il renvoie l'évaluation de ces éléments aux SP, aux Commissaires à la vie privée et aux juges. Il s'agit pourtant d'enjeux qui intéressent et concernent l'ensemble de la société.

[19] CPVP, *Document d'orientation*, précité.

[20] *Ibid.*

[21] *Ibid.*

3. Observations sur le cadre juridique et de politique applicable au recours à la RF par les services de police

[Question 7] Le recours à la RF par les services de police est-il encadré de façon appropriée au Canada par les lois existantes ?

3.1 Un manque patent d'encadrement légal

Le déficit d'encadrement légal de la RF est patent. Le DO le reconnait d'ailleurs :

> L'utilisation de cette technologie est plutôt réglementée par un ensemble disparate de lois et de jurisprudences qui, pour la plupart, ne tiennent pas compte des risques propres à la RF. Cette situation crée une incertitude quant aux utilisations acceptables de la RF et quant aux conditions d'utilisation.

La chercheure Castets-Renard note de son côté :

> L'insuffisance du cadre légal est flagrante aujourd'hui et est d'ailleurs régulièrement dénoncée par les autorités de protection des données personnelles comme le Commissariat à la protection de la vie privée du Canada.
>
> En outre, les lois actuelles ne réglementent pas spécifiquement l'usage de la reconnaissance faciale par les forces de police. Il n'y a ainsi pas de standards minimums de protection de la vie privée, de minimisation des risques ou de transparence publique[22].

Au Québec, malgré quelques dispositions régissant l'usage de données biométriques[23], la situation est tout aussi précaire, comme l'indique la Commission d'accès à l'information :

> L'utilisation de plus en plus répandue de la biométrie soulève des enjeux importants pour la vie privée et la protection des renseignements personnels des individus. La législation actuelle ne permet pas d'encadrer adéquatement certaines utilisations de cette technologie[24].

3.2 Nécessité d'un débat public éclairé et transparent sur l'utilisation de la RF par les SP

Les lois de protection des RP ne sont pas à même de régir convenablement la RF. Une réforme législative s'impose donc afin d'établir un cadre légal spécifique. Cela nécessite la tenue d'un débat public éclairé et transparent.

---

[22] Castets-Renard, précité, p. 7.

[23] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c. C -1.1, art. 44 et 45.

[24] Commission d'accès à l'information, *Mémoire présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques sur le projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 2020, p. 24. En ligne : https://www.cai.gouv.qc.ca/documents/CAI_M_projet_loi_64_modernisation_PRP.pdf

Pour la LDL, il n'appartient ni aux SP, ni aux Commissaires à la vie privée, ni aux juges de poser les jalons d'une utilisation acceptable de la RF.

Une réflexion collective s'impose à cet égard, comme le souligne pertinemment le DO :

> La nature de ces risques nécessite une réflexion collective sur les limites de l'utilisation acceptable de la RF. Ces limites sont définies non seulement par les risques liés à des projets précis de RF, mais aussi par les effets cumulés de tous les projets, mis en place au fil du temps, sur la surveillance générale de l'espace public et privé. Ainsi, les limites de l'utilisation acceptable de la RF dépendent en partie des attentes que nous fixons aujourd'hui pour la protection de la vie privée dans le futur, dans un contexte où les capacités technologiques à transgresser les attentes raisonnables des Canadiens à l'égard de leur vie privée augmentent sans cesse.[25]

Pour mener à bien cette discussion, le secret entourant l'utilisation de la RF par les SP doit être levé et un portrait détaillé et exhaustif de la situation doit être dressé. La population est en droit de connaitre l'usage actuel ou projeté de la RF par les SP.

> Transparency is an essential component of existing police oversight and accountability mechanisms in Canada, without which lawmakers cannot provide guidance to or appropriately regulate law enforcement authorities. Transparency also enables policymakers and the public to more effectively consider and develop informed law and policy with regard to the range of limitations that are required to safeguard constitutional and human rights and balance the public interests at stake.[26]

4. Usages de la RF à proscrire

[*Question 9] Existe-t-il des situations dans lesquelles les services de police ne devraient jamais être autorisés à recourir à la RF, ou des applications particulières de la RF qui devraient être interdites (c.-à-d. des « zones interdites » telle que le prélèvement systématique des images sur Internet) ?*

Selon nous, trois usages en matière de RF devraient faire l'objet d'une interdiction immédiate par voie législative :

A) la surveillance de masse des lieux et endroits publics ;

B) la surveillance de masse en ligne (plateformes numériques, réseaux sociaux, etc.) ;

C) l'utilisation de banques d'images constituées par des organismes publics ou ministères.

De telles pratiques, dont on peut douter de la légalité, devraient être clairement interdites par la loi.

[25] CPVP, *Document d'orientation*, précité.

[26] Robertson, Khoo et Song, précité, p. 66.

Un moratoire devrait par ailleurs s'appliquer à :

> D) toute autre utilisation de la RF par les SP jusqu'à l'établissement d'un cadre législatif assurant le respect des droits humains.

A. La surveillance de masse des lieux et endroits publics

La Commission européenne utilise l'expression « identification biométrique à distance » pour désigner l'ensemble des données biométriques permettant l'identification d'un individu :

> L'identification biométrique à distance consiste à établir à distance, dans un espace public et de manière continue, l'identité de plusieurs personnes au moyen d'identificateurs biométriques (empreintes digitales, image faciale, iris, réseau veineux, etc.) en les comparant aux données stockées dans une base de données[27].

On parle aussi de *Live Facial Recognition Technology* :

> Faces on video footage are extracted and then compared against the facial images in the reference database to identify whether the person on the video footage is in the database of images[28].

De nombreuses organisations réclament le bannissement d'une telle pratique, notamment : Amnistie internationale[29], European Data Protection Supervisor[30] et la Haute-Commissaire des Nations Unies aux droits de l'homme[31].

Le 6 octobre dernier, le Parlement européen adoptait une résolution visant à interdire la RF à des fins de surveillance de masse dans les lieux publics :

> […] l'interdiction de tout traitement des données biométriques, y compris des images faciales, à des fins répressives conduisant à une surveillance de masse dans les espaces accessibles au public[32].

---

[27] Commission européenne, *Livre blanc. Intelligence artificielle*, 2020, Bruxelles. En ligne : https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

[28] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019. En ligne : https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

[29] Amnistie internationale, *Amnistie internationale et plus de 170 organisations demandent l'interdiction de la surveillance biométrique*, 7 juin 2021. En ligne : https://amnistie.ca/sinformer/2021/amnistie-internationale-et-plus-de-170-organisations-demandent-linterdiction-de-la

[30] European Data Protection Board, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*, 21 juin 2021. En ligne : https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

[31] Haut-Commissariat des Nations Unies aux droits de l'homme, *Les nouvelles technologies doivent favoriser et non entraver le droit de manifester pacifiquement, annonce Michelle Bachelet aux États*, Genève, 25 juin 2020. En ligne : https://www.ohchr.org/fr/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=f

La résolution appelle en outre à interdire les autres formes de reconnaissance biométrique :

> L'interdiction permanente de l'utilisation de l'analyse et/ou de la reconnaissance automatisées, dans les espaces accessibles au public, d'autres caractéristiques humaines telles que la démarche, les empreintes digitales, l'ADN, la voix et d'autres signaux biométriques et comportementaux[33].

La LDL souscrit entièrement à cette demande.

B. La surveillance de masse en ligne (plateformes numériques, réseaux sociaux, etc.)

La même interdiction permanente devrait viser la surveillance en ligne par les SP. Citant en exemple le cas *Clearview*, le Parlement européen « appelle de ses vœux l'interdiction de l'utilisation des bases de données privées de reconnaissance faciale dans le domaine répressif[34] ».

Dans *Clearview*, les commissaires canadiens ont statué qu'une photo postée sur Internet ne constituait pas un renseignement public. Dans le cas du Québec la décision précise :

> […] aucune loi au Québec ne confère un caractère public aux renseignements personnels du seul fait qu'ils sont diffusés sur les réseaux sociaux ou le Web. De plus, la CAI du Québec a déjà statué que même si un renseignement personnel est diffusé sur un site public, cela ne veut pas dire que ce renseignement peut être utilisé à d'autres fins sans le consentement de la personne concernée. La publication d'images sur un site Web ne signifie pas forcément que son auteur consent à ce qu'elles soient utilisées par un tiers[35].

Cela étant, nous estimons que les SP ne peuvent recueillir d'images sur Internet pour les soumettre à la RF. On peut avancer qu'il s'agirait d'une contravention aux lois de protection des RP, voire d'une fouille illégale au sens de la *Charte des droits et libertés de la personne* et de la *Charte canadienne des droits et libertés*[36].

---

[32] Parlement européen, *Résolution sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales*, 2021, par. 31. En ligne : https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_FR.html

[33] *Ibid*., par. 26.

[34] *Ibid*., par. 28.

[35] Enquête conjointe sur *Clearview AI, Inc.* par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta. Conclusions en vertu de la LPRPDE nº 2021-001, février 2021, par. 46. En ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/

[36] Commission des droits de la personne et des droits de la jeunesse, *Mémoire présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques sur le projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 2020, p. 55. En ligne : https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf

C. L'utilisation de banques d'images constituées par des organismes publics ou ministères

Les SP ne devraient pas être autorisés à utiliser les banques d'images constituées par les organismes publics ou ministères dans l'exercice de leurs mandats.

Les RP recueillis par les organismes publics ou ministères doivent l'être à une fin précise. Ils ne peuvent être utilisés ou communiqués qu'à cette fin (ou à une fin compatible). En vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, un organisme peut toutefois transmettre un RP sans le consentement de la personne intéressée « à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec[37] [nous soulignons] ». Une telle disposition ne devrait toutefois pas autoriser les parties de pêches dans les banques gouvernementales.

En 2012, la commissaire à la vie privée de Colombie-Britannique interdisait à *Insurance Corporation of British Columbia* de mettre sa base de photos de conducteurs au service de la police[38]. Comme le résume le CPVP fédéral en 2013 :

> La commissaire à la protection de la vie privée de la Colombie-Britannique a déterminé qu'ICBC peut utiliser la technologie pour détecter et prévenir les cas de fraude liés au permis de conduire, mais qu'elle ne peut se servir de sa base de données pour aider la police à identifier des suspects. Cette décision repose sur le fait qu'il s'agit d'une finalité différente, dont les clients n'ont pas été avisés[39].

Selon la LDL, le détournement de banques gouvernementales à des fins de RF par les SP devrait être strictement prohibé.

D. Moratoire sur toute autre utilisation de la RF par les SP jusqu'à l'établissement d'un cadre législatif assurant le respect des droits humains

Faute de preuve établissant la nécessité de recourir à la RF par les SP, et faute d'un encadrement légal qui assure le respect des droits humains, pose des limites sévères et assure notamment la transparence, la reddition de compte et le contrôle judiciaire de cette technologie, il y a lieu d'imposer un moratoire à son utilisation ; et cela même concernant les banques d'identités judiciaires (*mug-shot*).

> C'est donc dire que lorsque l'État recueille des données produites par l'activité en ligne, et ce, sans mandat de perquisition et sans obtenir l'autorisation des citoyens, il est susceptible de contrevenir à l'article 24.1 de la Charte.

[37] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A-2.1, art. 41.2 (3).

[38] Office of The Information & Privacy Commissioner for British Columbia, *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia*, Investigation Report F12-01, 16 février 2012. En ligne : https://www.oipc.bc.ca/investigation-reports/1245

[39] CPVP, *Reconnaissance faciale automatisée dans les secteurs public et privé*, 2013, p. 5. En ligne : https://www.priv.gc.ca/media/1766/fr_201303_f.pdf

Les banques de mug-shots ne sont pas anodines. Elles incluent les photos de personnes acquittées ou qui ont simplement fait l'objet d'enquête. En outre, il n'y a apparemment pas destruction automatique des photos une fois le dossier fermé[40].

Un autre élément est à considérer : les biais discriminatoires de telles banques. Dans la mesure où les populations autochtones, racisées et marginalisées sont surreprésentées dans le système judiciaire et carcéral, elles risquent aussi d'être l'objet d'une surveillance par RF disproportionnée.

La demande de la LDL rejoint celle du Parlement européen, qui dans sa résolution du 6 octobre 2021 :

> […] demande toutefois un moratoire sur le déploiement des systèmes de reconnaissance faciale à des fins répressives destinés à l'identification, à moins qu'ils ne soient utilisés qu'aux fins de l'identification des victimes de la criminalité, jusqu'à ce que les normes techniques puissent être considérées comme pleinement respectueuses des droits fondamentaux, que les résultats obtenus ne soient ni biaisés, ni discriminatoires, que le cadre juridique offre des garanties strictes contre les utilisations abusives ainsi qu'un contrôle et une surveillance démocratique rigoureux, et que la nécessité et la proportionnalité du déploiement de ces technologies soient prouvées de manière empirique ; relève que lorsque les critères susmentionnés ne sont pas remplis, les systèmes ne devraient pas être utilisés ou déployés[41] [nous soulignons].

[40] Robertson, Khoo et Song, précité, p. 91 :

> Multiple law enforcement agencies in Canada report using (or are planning to use) facial recognition technology against their mug-shot databases. However, mug-shot databases can contain photos of individuals who have never been charged with a criminal offence, who have had their charges withdrawn, or who have been found innocent of allegations. Individuals have a constitutionally protected right to privacy in relation to their fingerprints and mug-shot images. In particular, the unauthorized retention of images is unconstitutional. In practice, however, each police service has its own internal policies with respect to the destruction of biometric data, and those policies typically entail a discretionary, request-based, or even fee-based process [nous soulignons].

[41] Résolution du Parlement européen sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales, précité, par. 27.

Conclusion

L'intelligence artificielle est en pleine expansion. Elle est capable du meilleur… comme du pire. Les récentes révélations de Frances Haugen[42] sur les algorithmes de Facebook prouvent l'urgence de lois drastiques pour maitriser ces technologies et les entreprises qui en font commerce. La démission des États n'est plus acceptable.

La décision sur *Clearview* marque un tournant. Elle a mis à jour les pratiques illégales de nombreux corps policiers dans l'emploi de la RF ; le tout en partenariat avec le secteur privé. Les commissaires en ont tiré une proposition de directive dans l'utilisation de la RF, fondée sur les lois de protection des renseignements personnels. Bien que nous saluions cette initiative des commissaires, ce guide de bonnes pratiques apparait nettement insuffisant pour règlementer une technologie aussi complexe que redoutable.

Pour la LDL, **trois usages de la RF devraient faire l'objet d'une interdiction immédiate par voie législative** :

1. La surveillance de masse des lieux et endroits publics ;
2. La surveillance de masse en ligne (plateformes numériques, réseaux sociaux, etc.) ;
3. L'utilisation de banques d'images constituées par des organismes publics ou ministères.

De plus, pour la LDL, **un moratoire sur toute autre utilisation de la RF par les SP s'impose** jusqu'à l'adoption d'une législation à la mesure des enjeux, fondée sur un débat public informé et transparent.

[42] Agence France-Presse, « Frances Haugen accable Facebook et pousse le Congrès à agir », *Radio-Canada*, 5 octobre 2021. En ligne : https://ici.radio-canada.ca/nouvelle/1829407/facebook-congres-americain-questions-lanceuse-alerte