OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

CHAIRE DE RECHERCHE I.A. RESPONSABLE À L'ÉCHELLE MONDIALE

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

Sommaire exécutif et recommandations

Rapport préparé par

Céline Castets-Renard
Professeure à la Faculté de droit de l'Université d'Ottawa

Émilie Guiraud et Jacinthe Avril-Gagnon
Auxiliaires de recherche

Septembre 2020

Ce rapport a été préparé dans le cadre des travaux de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) soutenus par les Fonds de recherche du Québec (FRQ). La production de ce rapport est aussi soutenue et financée par la Chaire de recherche de l'Université d'Ottawa sur l'intelligence artificielle responsable à l'échelle mondiale dont est titulaire la professeure Céline Castets-Renard.

Rédigé par :

- Céline Castets-Renard, professeure à la Faculté de droit – section droit civil de l'Université d'Ottawa, titulaire de la Chaire de recherche de l'Université d'Ottawa sur l'intelligence artificielle responsable à l'échelle mondiale et coresponsable de l'axe Relations internationales, action humanitaire et droits humains de l'OBVIA.

Préparé par :

- Céline Castets-Renard, professeure à la Faculté de droit – section droit civil de l'Université d'Ottawa.
- Émilie Guiraud, auxiliaire de recherche à l'OBVIA et étudiante en droit à l'Université Laval.
- Jacinthe Avril-Gagnon, auxiliaire de recherche et étudiante en droit à l'Université d'Ottawa.

Comité aviseur :

- Pierre-Luc Déziel, professeur à la Faculté de droit de l'Université Laval et coresponsable de l'axe Droit, cyberjustice et cybersécurité de l'OBVIA.
- Benoit Dupont, professeur à l'École de criminologie de l'Université de Montréal et directeur scientifique du Réseau intégré sur la cybersécurité (SERENE-RISC)
- Steve Jacob, professeur au Département de science politique de l'Université Laval, titulaire de la chaire de recherche sur l'administration publique à l'ère numérique et coresponsable de la fonction Politiques publiques de l'OBVIA
- Lyse Langlois, professeure au Département des relations industrielles de l'Université Laval, directrice générale de l'OBVIA
- Guillaume Macaux, conseiller scientifique, OBVIA

ISBN: 978-2-9818996-6-8

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2020. Dépôt légal - Bibliothèque et Archives Canada, 2020.

Illustration de couverture d'après une photo de Tom Marvel sous CreativeCommons 2.0

Sommaire du rapport complet

Sommaire exécutif

Objet et objectifs du pré-rapport

Ce document présente les principaux enjeux de l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada, en comparaison avec les autres provinces, l'Europe et les États-Unis. Dans un contexte où il est de plus en plus question de recourir à cette technologie, il convient de mener une réflexion en amont de son déploiement, afin d'éliminer ou minimiser les risques encourus, en particulier pour les droits et libertés individuelles.

Les principaux objectifs du document sont alors :

1. D'éclairer les législateurs sur ce qu'est cette technologie et les risques encourus, en particulier les risques d'atteinte aux droits et libertés individuelles protégés par les Chartes du Canada et du Québec

2. De présenter les solutions déjà mises en œuvre pour envisager celles qui minimisent les risques et l'intrusion de cette technologie sur la vie privée, afin de poser les conditions d'une transparence et meilleure acceptabilité sociale.

Définition

Les dispositifs de reconnaissance faciale font partie des technologies biométriques et permettent d'identifier ou d'authentifier des personnes à partir d'images de visages (photos ou vidéos).

Contexte

L'affaire Clearview AI a révélé que des dispositifs de reconnaissance faciale ont été mis en œuvre aux États-Unis mais aussi au Canada par la Gendarmerie Royale du Canada (GRC) et par certains départements, comme les services de police d'Edmonton, de Calgary, Vancouver, de Toronto et d'Halifax.

La Sûreté Québec souhaite se servir de cette technologie dans le cadre d'enquêtes criminelles pour comparer des images vidéo automatiquement à sa banque comptant des dizaines de milliers de photos signalétiques. Elle a lancé un appel d'offres et un contrat a été signé en juin 2020 avec la société Idemia pour l'acquisition d'une technologie de reconnaissance faciale et d'empreintes digitales, capable de comparer automatiquement des images de suspects à une banque de dizaines de milliers de photos signalétiques.

Avantages de la reconnaissance faciale

Les dispositifs de reconnaissance faciale sont de plus en plus utilisés par les forces de police dans l'espace public, à des fins de surveillance et de sécurité publique. Ces outils se veulent efficaces, notamment dans les enquêtes complexes, par exemple lorsqu'un crime violent se produit dans la rue. Cette technologie est utilisée aussi pour détecter d'éventuels criminels et terroristes parmi les spectateurs de grandes manifestations comme dans des stades ou salles de concerts. Ces systèmes ont particulièrement été déployés dans des régions à risque aux États-Unis pour surveiller les activités criminelles. Les systèmes de reconnaissance faciale sont aussi fortement déployés dans les aéroports, notamment les aéroports américains. Ils ont permis de capturer et de stocker les données faciales de plus de la moitié des citoyens des États-Unis. La reconnaissance faciale permet ainsi d'accroître le niveau de sécurité dans la société lorsqu'elle est couplée avec la vidéosurveillance. D'autres avantages sont mis en avant, tel que le gain de temps ou la simplification du travail des forces de police.

Risques sociaux

Pourtant, les risques d'atteintes aux libertés individuelles susceptibles d'être induits par ces dispositifs de reconnaissance faciale utilisés par les services de police dans l'espace public sont considérables, dont notamment la liberté d'aller et venir (art. 6 de la Charte canadienne des droits et libertés), la liberté de réunion et la liberté de manifestation (art. 2 b) et c) de la Charte canadienne des droits et libertés et art. 3 de la Charte québécoise des droits et libertés de la personne) ainsi que le droit à la liberté (art. 7 de la Charte canadienne des droits et libertés et art. 1 de la Charte québécoise des droits et libertés de la personne). Le recours à la reconnaissance faciale peut nuire à la liberté d'expression, d'association et de réunion. Le droit à la vie privée est aussi menacé (art. 8 de la Charte canadienne des droits et libertés, art. 5 de la Charte québécoise des droits et libertés de la personne et art. 3, 35 à 37 du Code civil du Québec). Le risque de surveillance par ces dispositifs est alors d'entraîner une forme d'autocensure de la part des citoyens, notamment concernant leur participation à la vie publique et plus largement l'exercice de leurs libertés fondamentales.

En outre, les risques d'atteinte à la protection des données sont évidents, dès lors que cette technologie repose sur l'utilisation de données personnelles et notamment des données biométriques qui sont des données sensibles faisant l'objet d'une protection spécifique selon plusieurs législations dans le monde.

La technologie de la reconnaissance faciale peut porter atteinte à la dignité des personnes et avoir aussi des répercussions sur le droit à la non-discrimination. Elle peut affecter les droits des groupes spéciaux, tels que les enfants, les personnes âgées et les personnes handicapées. En outre, si la technologie de la reconnaissance faciale se développe, le taux d'erreur reste toutefois élevé, spécialement envers certaines catégories de populations. De

nombreuses études prouvent que la technologie de reconnaissance faciale est plus efficace pour détecter les personnes à la peau claire et les hommes que les personnes à la peau foncée et les femmes. Ce risque porte naturellement atteinte au principe d'égalité et à la non-discrimination, protégé à l'article 15 de la Charte canadienne des droits et libertés et à l'article 10 de la Charte québécoise des droits et libertés de la personne.

Compte tenu de ces risques et dans ce contexte, l'acceptabilité sociale de cette technologie risque d'être faible, sauf à envisager le recours à cette technologie dans un contexte traumatisant comme des attaques terroristes selon les ressorts de la « politique de la terreur ». En juillet 2020, des ONG et associations de protection de la vie privée, des droits humains et libertés civiles ont adressé une lettre ouverte dans un appel au gouvernement fédéral Canadien pour l'adoption d'une interdiction immédiate de l'utilisation de la reconnaissance faciale par les forces de l'ordre fédérales et les agences du renseignement, incluant la GRC. L'appel invite à une consultation publique et à établir des politiques et lois claires et transparentes pour réguler l'usage de la reconnaissance faciale au Canada.

Enfin, un autre risque résulte pour les services de police de recourir à des entreprises privées pour mettre en place un dispositif de reconnaissance faciale. Dès lors que ces acteurs accomplissent une mission de service public, les services de police doivent être vigilants et vérifier leurs bonnes pratiques. En outre, le choix éventuel d'opérateurs privés étrangers fait peser le risque de perte de contrôle de la souveraineté étatique, ce qui est particulièrement préoccupant.

Inadaptation des lois québécoises pour faire face aux risques sociaux

Or, les lois québécoises, spécialement en matière de protection des renseignements personnels, sont insuffisantes. La plupart d'entre elles ont été adoptées depuis plusieurs années et ne tiennent pas compte des évolutions technologiques. 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 standard minimum de protection de la vie privée, de minimisation des risques ou de transparence publique.

Une réforme sur tous ces aspects s'impose. Au Québec, le projet de loi 64 va dans le bon sens mais certains points de vigilance devront être considérés lors des débats parlementaires. En outre, la reconnaissance faciale présente d'autres risques que ceux liés à l'utilisation des renseignements personnels.

Modèles législatifs dans l'Union européenne et les États-Unis

Aucune législation propre à la reconnaissance faciale n'a été adoptée en Europe mais le droit de l'Union européenne, en particulier le règlement général de protection des données (RGPD) et la directive « police-justice » qui encadrent la protection des données personnelles contiennent des dispositions spécifiques à la biométrie applicables à la reconnaissance faciale. Cette législation ne permet toutefois pas de faire face à tous les risques associés à cette technologie. Néanmoins, en Europe, les technologies de surveillance font surtout l'objet d'expérimentations ciblées, spécialement dans les aéroports et gares. En outre, si aucune loi nationale propre à la reconnaissance faciale n'a été prise par les États membres de l'Union européenne, quelques décisions de justice fondées sur la protection des données personnelles et la charte des droits fondamentaux de l'UE commencent à dessiner les contours d'une protection

En comparaison, le déploiement technologique est bien plus important aux États-Unis. Parallèlement, plusieurs lois dédiées à l'usage de technologies de surveillance par les forces de l'ordre dans l'espace public, dont la reconnaissance faciale, ont été adoptées par certaines villes ou certains États, essentiellement en Californie et Massachussetts. Cependant, les dispositions prévoient majoritairement d'encadrer l'usage de cette technologie plutôt que de l'interdire. Les rares lois d'interdiction ont un champ d'application restreint et visent à interdire l'utilisation de la reconnaissance faciale lorsqu'elle est associée à des technologies comme les drones ou les caméras corporelles des policiers.

Recommandations

La tension entre les risques sociaux de l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public et l'inadaptation des lois québécoises et canadiennes conduit à faire trois recommandations :

1. Établir une balance des enjeux de sécurité / libertés pour combiner la protection de la population et le respect des droits humains

L'usage de la reconnaissance faciale dans l'espace public à des fins de police présente des avantages indéniables pour améliorer la sécurité des populations. Mais cette technologie suscite des interrogations et craintes en raison de son potentiel liberticide et d'achèvement de société de surveillance.

Il convient donc de rechercher les points de vigilance pour encadrer légalement et avec pertinence son usage par les forces de police dans l'espace public. Pour ce faire, il faut déterminer les usages appropriés de cette technologie, s'assurer de leur légalité et acceptabilité sociale pour en garantir la légitimité.

La vie privée n'est pas un droit absolu. La législation sur la protection des données au Canada, ainsi que dans d'autres juridictions, établit un équilibre entre le droit à la vie privée des individus et les préoccupations sociétales plus larges. Si une balance des intérêts entre vie privée, liberté, d'une part, et sécurité, d'autre part peut être établie, il faut en préciser les critères et décider collectivement où établir la balance des coûts / avantages.

2. Renforcer les lois sur la protection des renseignements personnels au Québec et Canada

Il faut aussi que les lois sur la protection de la vie privée et des renseignements personnels soient suffisamment fortes en soi pour garantir un minimum de protection. Or, les lois canadiennes et québécoises datent d'il y a 20 ans et sont loin d'être adaptées à la technologie d'aujourd'hui, *a fortiori* s'agissant de technologies intrusives comme la reconnaissance faciale dans l'espace public qui peut conduire à la surveillance généralisée et la perte d'anonymat.

Le projet de loi 64 qui vise à renforcer les législations sur la protection des renseignements personnels au Québec va dans le bon sens mais il faut encore renforcer la protection en cas d'utilisation de données biométriques, ainsi que le contrôle de leur usage par le secteur public. Le risque de glissement de finalité doit aussi être considéré. Également, l'évaluation des facteurs de vie privée (EFVP) devrait s'entendre largement et intégrer aussi l'évaluation des risques pour les autres droits fondamentaux.

3. Adopter une législation spécifique restrictive si on veut autoriser sous conditions la police à recourir à la reconnaissance faciale au Québec et au Canada

Chaque fois qu'il faut trouver un équilibre entre les besoins des individus et ceux de la société, l'élaboration d'une législation est le meilleur moyen d'atteindre cet équilibre, *a fortiori* s'agissant de moyens mis à la disposition des forces de l'ordre et du recours à des technologies particulièrement intrusives pour les droits et libertés.

En conséquence, l'utilisation de la reconnaissance faciale par les forces de police doit être prévue par la loi et encadrée. Son usage doit être rendu public par souci de transparence. Une commission indépendante doit en outre autoriser et contrôler l'usage qui en est fait et le respect du cadre posé. Cette commission doit être dotée de pouvoirs suffisants, notamment des pouvoirs significatifs de sanctions.