



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

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

1. Sommaire exécutif.....	5
2. Éléments de contexte.....	9
2.1. Multiplication des technologies de reconnaissance faciale	9
2.2. Usage de la reconnaissance faciale au Canada par les forces de police	11
2.3. Projet de reconnaissance faciale de Sûreté Québec	12
2.4. Futures orientations des autorités de protection sur l'utilisation de la reconnaissance faciale	13
3. Définition de la reconnaissance faciale dans l'espace public.....	14
3.1. Éléments de définition	14
3.2. Qualification juridique des données biométriques en renseignements personnels sensibles.....	17
3.3. Exclusions de certaines technologies ou finalités	20
3.4. Détails de la technologie de reconnaissance faciale.....	20
3.5. Reconnaissance faciale et sécurité intérieure	22
3.6. Notion d'espace public.....	23
4. Principaux enjeux sociaux et juridiques de la reconnaissance faciale.....	24
4.1. Avantages de la reconnaissance faciale à des fins de sécurité publique	24
4.2. Questionnements induits par l'usage de la reconnaissance faciale.....	24
4.3. Conditions de capture d'images : le cas de Clearview AI	25
4.4. Principaux risques sociaux et juridiques.....	28
5. Cadre légal de la reconnaissance faciale au Canada et au Québec	36
5.1. Chartes canadiennes et québécoises des droits et libertés et reconnaissance faciale	36
5.2. Loi fédérale applicable à la reconnaissance faciale et la GRC (secteur public).....	36
5.3. Lois du Québec applicables à la reconnaissance faciale et les polices (provinciale et municipales)(secteur public).....	39
5.4. Projet de réforme de la loi du Québec sur la protection des renseignements personnels (projet de loi n° 64).....	46
Conclusion sur la reconnaissance faciale confrontée aux lois fédérales et provinciales : insuffisance du cadre légal.....	54
6. Comparaison avec le cadre légal applicable à la reconnaissance faciale en Europe et aux États-Unis.....	56
6.1. Droit de l'Union européenne concernant l'usage par les forces de police de la reconnaissance faciale	56

6.2. État des lieux de la reconnaissance faciale dans l'espace public en France et au Royaume-Uni.....	64
6.3. Règlementations aux États-Unis propres aux données biométriques et à la reconnaissance faciale	70
Conclusion sur la réglementation en Europe et aux États-Unis	80
7. Recommandations	81
Annexes	83
Lois provinciales applicables aux renseignements personnels du secteur public	83
Tableau synthétique du droit de l'UE et de quelques lois applicables en Europe	91

1. 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 Massachusetts. 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 un équilibre coût-avantage : balance des intérêts libertés /sécurité**
2. **Renforcer les lois sur la protection des renseignements personnels au Québec et Canada**
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**

2. Éléments de contexte

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 et, plus largement aux technologies de maintien de l'ordre comme la police prédictive ou la lecture automatisée des plaques d'immatriculation¹, 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.

La présentation des cadres légaux de ces juridictions permet d'analyser les solutions mises en œuvre qui peuvent être fondées sur des réglementations spécifiques à la biométrie et à la reconnaissance faciale ou simplement sur les réglementations plus générales de protection des renseignements personnels.

Les principaux objectifs du document sont alors :

- 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
- 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.

2.1. Multiplication des technologies de reconnaissance faciale

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). Cette technologie est utilisée dans la vie quotidienne, par exemple pour l'ouverture de sessions personnelles sur les smartphones, l'autorisation d'accès à des sites sensibles ou encore la surveillance des aéroports et l'accès aux territoires².

Comme le souligne le Commissariat à la vie privée du Canada (CPVP) dans un rapport sur la reconnaissance faciale publié en mars 2013, « les images numériques sont désormais

¹ K. Robertson, C. Khoo, and Y. Song, To Surveil and Predict, A Human Rights Analysis of Algorithmic Policing in Canada, The Citizen Lab, Faculty of Law, University of Toronto, International Human Rights Program, Sept. 2020 : <https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada>.

² Thierry Ménissier, « Les dispositifs de reconnaissance faciale : une réalité socio-technique en développement, un enjeu pour les libertés publiques et privées, un défi pour l'éthique de l'IA », Intervention au séminaire de la chaire « éthique & IA » MIAI Grenoble : « La reconnaissance faciale est-elle une bonne ou une mauvaise chose (éthiquement parlant)? », 4 Décembre 2019.

omniprésentes en raison de la prolifération des caméras de surveillance, des téléphones intelligents équipés d'un appareil photo et des appareils photos numériques de qualité bon marché. Les dispositifs de stockage à prix modique ont donné lieu à la création de vastes bases de données en ligne renfermant des images d'individus identifiés, par exemple les titulaires de permis de conduire ou de passeport, les personnes possédant une carte d'identité d'employé et celles ayant un casier judiciaire. Les individus ont adopté l'affichage et l'étiquetage des photos en ligne sur des plateformes comme Facebook, Instagram, Picasa et Flickr. En outre, la technologie de reconnaissance faciale a fait l'objet de perfectionnements considérables, notamment au chapitre de l'analyse des images et de l'extraction des données »³. Le CPVP a précédemment publié, en février 2011, un document d'orientation sur l'utilisation de la biométrie, comme la reconnaissance faciale, dans les secteurs public et privé. Ce document, intitulé « Des données au bout des doigts – La biométrie et les défis qu'elle pose à la protection de la vie privée »⁴, propose plusieurs principes visant à atténuer les risques d'atteinte à la vie privée, associés aux systèmes biométriques.

La Commission d'accès à l'information du Québec (CAI) a publié en juillet 2020 un guide d'accompagnement pour les organismes publics et les entreprises intitulé : « Biométrie : principes à respecter et obligations légales des organisations »⁵. Elle constate ainsi que la popularité de la biométrie engendre « une certaine banalisation de ses implications en matière de protection des renseignements personnels. Si on la dit sécuritaire, on oublie cependant trop souvent que son utilisation présente des risques pour la vie privée des personnes. Le cadre légal qui s'applique à la biométrie est par ailleurs méconnu ».

Les applications de reconnaissance faciale supposent le recours à des procédés biométriques. Elles varient ainsi selon leurs finalités mais aussi selon les techniques utilisées. Elles peuvent donc avoir des impacts sociaux potentiellement différents et sont susceptibles d'être encadrées par des règles également différentes selon les usages.

³ Commissariat à la protection de la vie privée du Canada, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303.

⁴ Commissariat à la protection de la vie privée du Canada, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », Février 2011 : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102.

⁵ Commission d'accès à l'information, *Biométrie : principes à respecter et obligations légales des organisations*, Guide d'accompagnement, Juillet 2020 : https://www.cai.gouv.qc.ca/documents/CAI_G_biometrie_principes-application.pdf.

2.2. Usage de la reconnaissance faciale au Canada par les forces de police

La technologie de reconnaissance faciale a été conçue à l'origine pour aider les pouvoirs publics à assurer la sécurité et l'application de la loi. En outre, le secteur public exploite aussi la plupart des bases de données renfermant des images d'individus identifiés, par exemple les titulaires d'un permis de conduire ou d'un passeport et les personnes ayant un casier judiciaire.

Tel est le cas au Canada, où des systèmes de reconnaissance faciale sont utilisés pour certains services publics comme la délivrance des permis de conduire⁶, des titres d'identité, tels les passeports électroniques⁷, des titres d'immigration⁸ ou encore dans des outils de sécurité des frontières⁹.

Par ailleurs, l'affaire Clearview AI¹⁰ a révélé que la reconnaissance faciale est aussi mise en œuvre par certains départements de police et la Gendarmerie Royale du Canada (GRC)¹¹. Ailleurs au Canada, les services de police d'Edmonton¹², de Calgary¹³, Vancouver¹⁴, de

⁶38, , Vol. 6, N° 2, vacy Act, Liabilities, es organisations, Guide d'fiquement mais je pourrais les ajouter au besoin. es.ge « Dans de nombreuses provinces canadiennes, notamment en Ontario, en Colombie-Britannique et au Manitoba, les photos figurant sur le permis de conduire sont adaptées à la reconnaissance faciale. Les autorités utilisent cette technologie au cours de la procédure de demande de permis pour détecter l'usurpation d'identité et la fraude, par exemple pour repérer les individus qui demandent des permis sous différents noms » dans Commissariat à la protection de la vie privée du Canada, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303.

⁷ Gouvernement du Canada, « Le passeport électronique », Juillet 2017 : <https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens/centre-aide/passeport-electronique.html>.

⁸ Le programme est administré conjointement par l'Agence des services frontaliers et la Gendarmerie royale du Canada. Citoyenneté et Immigration Canada, « Les faits concernant la biométrie », Juillet 2020 : <https://www.canada.ca/fr/immigration-refugies-citoyennete/campagnes/biometrie/faits.html>.

⁹ International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto), "Bots at the Gate : A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", 2018, p.58-59 : <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>.

¹⁰ Voir *infra* partie 4 pour le détail de la procédure.

¹¹ Bryan Carney, "Despite Denials, RCMP Used Facial Recognition Program for 18 Years" (10 Mars 2020), The Tyee : <https://thetyee.ca/News/2020/03/10/RCMP-Admits-To-Using-Clearview-AI-Technology>.

¹² Dylan Short, "Controversial Clearview AI facial recognition program used twice by city police: Privacy commissioner investigating" (28 Février 2020), Edmonton Journal : <https://edmontonjournal.com/news/local-news/controversial-clearview-ai-facial-recognition-program-used-twice-by-city-police-review-launched>.

¹³ Alanna Smith, "Two Calgary officers tested Clearview AI facial-recognition software" (29 Février 2020), Calgary Herald : <https://calgaryherald.com/news/local-news/two-calgary-officers-tested-clearview-ai-facial-recognition-software>.

¹⁴ Nick Eagland, Lori Culbert, "Vancouver detective used controversial facial-recognition software once" (05 Mars 2020), Vancouver Sun : <https://vancouversun.com/news/vancouver-police-used-controversial-clearview-facial-recognition-software-a-single-time>.

Toronto¹⁵ et d'Halifax¹⁶ ont confirmé l'utilisation de cette technologie. Enfin, le service de police d'Ottawa (SPO) a affirmé en février 2020 avoir testé un système de reconnaissance faciale sans l'utiliser¹⁷. Un projet pilote de trois mois aurait été mené en mars 2019 avec l'application NeoFace Reveal. Le but était d'étudier l'efficacité des technologies de reconnaissance faciale dans les enquêtes criminelles. Le chef de police adjoint Steve Bell indique ne pas vouloir l'implanter sans consulter la communauté pour assurer le respect de la vie privée et des droits de la personne. Il ajoute que toute nouvelle technologie serait mise à l'essai en laboratoire avant d'être utilisée, afin d'encadrer son utilisation.

Au Québec, peu d'informations ont circulé sur l'utilisation ou non des technologies de reconnaissance faciale par le Service de Police de la Ville de Montréal (SPVM). En juin 2020, le SPVM a confirmé à la Commission de la Sécurité Publique (CSP) de l'Hôtel de Ville ne pas avoir utilisé ce dispositif¹⁸. Le directeur du SPVM, Monsieur Caron, a ajouté que « l'organisation n'exclut toutefois pas, dans des situations particulières et exceptionnelles, de recourir aux services d'une tierce partie possédant ce type de technologie pour faire avancer une enquête d'envergure, en s'assurant toujours de mener ses opérations et ses enquêtes dans le respect de toutes les lois en vigueur »¹⁹. En juillet 2020, des élus municipaux pressent la Ville de Montréal de créer un règlement afin d'encadrer l'utilisation potentielle de la reconnaissance faciale et d'autres technologies de surveillance par son corps de police²⁰. En outre, la Commission de la Sécurité Publique (CSP) a été mandatée pour faire des recommandations à l'automne 2020 sur le recours à la reconnaissance faciale²¹.

2.3. Projet de reconnaissance faciale de Sûreté Québec

La Sûreté du Québec (SQ) souhaite également en faire l'usage et a lancé à ce titre un appel d'offres. En juin 2020, un contrat pour l'acquisition d'une technologie de reconnaissance faciale et d'empreintes digitales, capable de comparer automatiquement des images de

¹⁵ Kayla Goodfield, "Canadian privacy officials will investigate controversial facial recognition tool used by Toronto police" (21 Février 2020), Toronto CTV News : <https://toronto.ctvnews.ca/canadian-privacy-officials-will-investigate-controversial-facial-recognition-tool-used-by-toronto-police-1.4822198>.

¹⁶ Alexander Quon, "Halifax police confirm use of controversial Clearview AI facial recognition technology" (28 Février 2020), Global News : <https://globalnews.ca/news/6607993/halifax-police-confirm-clearview-ai-facial-recognition-technology>.

¹⁷ CBC, « Le SPO a testé un logiciel de reconnaissance faciale, mais affirme ne pas l'utiliser » (15 février 2020), Radio-Canada : <https://ici.radio-canada.ca/nouvelle/1524411/police-ottawa-reconnaissance-faciale-intelligence-artificielle-new-york-times>.

¹⁸ Elsa Iskander, « Reconnaissance faciale: Les élus obtiennent une réponse du SPVM... après six mois » (30 juin 2020), 24h Montréal : <https://www.journaldemontreal.com/2020/06/29/reconnaissance-faciale--les-elus-obtiennent-une-reponse-du-spvm-apres-six-mois>.

¹⁹ Ibid.

²⁰ Zacharie Goudreault, « Montréal pressée d'encadrer les technologies de surveillance policière », (29 juillet 2020), Métro : <https://journalmetro.com/actualites/montreal/2487085/montreal-pressee-dencadrer-les-technologies-de-surveillance-policiere>.

²¹ Sarah Champagne, « Montréal étudiera l'utilisation des technologies de reconnaissance faciale par le SPVM » (20 août 2019), La Presse : <https://www.lapresse.ca/actualites/grand-montreal/2019-08-20/montreal-etudiera-l-utilisation-des-technologies-de-reconnaissance-faciale-par-le-spvm>.

suspects à une banque de dizaines de milliers de photos signalétiques, fait l'objet d'une analyse par le Centre des services partagés. L'acquisition du logiciel est le résultat d'une soumission de deux appels d'offres successifs, au terme desquels la société française Idemia est la seule à avoir soumissionné pour un montant de 4,4 millions²².

La technologie d'Idemia permet d'identifier des plaques d'immatriculation, des silhouettes et « des personnes d'intérêt en temps réel » afin d'améliorer la sécurité dans les endroits publics comme les aéroports et les gares. L'appel d'offres spécifie aussi reconnaître automatiquement les tatouages. La SQ 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. L'objectif est d'obtenir un logiciel pouvant accéder aux photos de criminels condamnés qui figurent dans la « Banque centrale provinciale d'empreintes digitales et de photographies signalétiques » en plus d'autres banques de photos qui seraient constituées²³. Idemia est également le principal fournisseur de permis de conduire aux États-Unis, fabriquant ceux des conducteurs de 42 États.

2.4. Futures orientations des autorités de protection sur l'utilisation de la reconnaissance faciale

Une réglementation inadéquate de la reconnaissance faciale et un manque d'information signifient créent des risques sociaux. Il est ainsi impossible de savoir quelles forces de police et agences de renseignement utilisent l'outil, et à quelles fins. Tel pourrait être par exemple le cas de l'usage de la reconnaissance faciale pendant des manifestations. Des valeurs démocratiques sont alors en jeu. Dans le cadre de l'enquête conjointe visant Clearview AI, les autorités de réglementation de la protection de la vie privée de toutes les provinces et de tous les territoires ont convenu d'élaborer ensemble des orientations à l'intention des organisations – y compris les organismes d'application de la loi – sur l'utilisation de la technologie biométrique, dont la reconnaissance faciale. Ces orientations font actuellement l'objet de mises à jour.

Cette étude a vocation à apporter un éclairage aux autorités fédérales et provinciales compétentes.

²² Tristan Pélouquin, « Reconnaissance faciale : un risque grave de surveillance de masse » (29 juin 2020), La Presse : <https://www.lapresse.ca/actualites/2020-06-29/reconnaissance-faciale-un-risque-grave-de-surveillance-de-masse.php>.

²³ Tristan Pélouquin, « La vie privée menacée: souriez, vous êtes filmés(et reconnus) » (8 février 2020), La Presse : <https://www.lapresse.ca/actualites/2020-02-08/la-vie-privee-menacee-souriez-vous-etes-filmes-et-reconnus>.

3. Définition de la reconnaissance faciale dans l'espace public

Le recours à la reconnaissance faciale dans l'espace public est souvent dénoncé mais il convient de préciser ce qu'il en est. En particulier, il faut préciser les définitions et bien distinguer la biométrie de la reconnaissance faciale. Cette dernière est une technologie qui utilise des images donc des données biométriques. Toutes les données biométriques ne vont toutefois pas présenter les mêmes risques, aussi convient-il d'être rigoureux dans l'identification des données concernées et leur définition, ainsi que le régime juridique applicable.

3.1. Éléments de définition

Définition de la biométrie

La Commission d'accès à l'information du Québec (CAI) identifie trois types de biométrie²⁴. La biométrie morphologique est basée sur l'identification de traits physiques particuliers. Elle regroupe notamment, mais pas exclusivement, la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil. La biométrie comportementale est basée sur l'analyse de certains comportements d'une personne, comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier, etc. La biométrie biologique est basée sur l'analyse des traces biologiques d'une personne, comme l'ADN, le sang, la salive, l'urine, les odeurs, etc.

Les caractéristiques ou les mesures biométriques issues de ces analyses sont aussi appelées renseignements biométriques. Elles sont généralement regroupées ou enregistrées dans des banques de caractéristiques ou de mesures biométriques, c'est-à-dire des ensembles de renseignements biométriques, au format brut (image ou empreinte) ou codé (code ou gabarit chiffré extrait d'une image ou d'une empreinte).

Sont donc spécifiquement visées les images utilisées dans le cadre de la reconnaissance faciale.

Définition de la reconnaissance faciale

La notion de reconnaissance faciale (RF) n'est pas définie dans les textes ni en droit québécois ni en droit canadien ni dans aucune autre province.

²⁴ Commission d'accès à l'information, « Biométrie » : <https://www.cai.gouv.qc.ca/biometrie>.

La reconnaissance faciale est une technologie combinant les techniques biométriques, l'intelligence artificielle, la cartographie 3D et l'apprentissage automatique (*machine learning*) pour comparer et analyser le visage d'une personne afin de l'identifier.

Le CPVP considère que « la technologie de reconnaissance faciale vise à identifier des individus ou à authentifier leur identité en comparant leur visage avec des visages connus stockés dans une base de données pour trouver une correspondance »²⁵.

En France, la Commission nationale informatique et libertés (CNIL)²⁶ définit la reconnaissance faciale comme une technique informatique et probabiliste qui permet à partir des traits de visage :

- **Soit d'authentifier une personne** : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès)
- **Soit d'identifier une personne** : c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

En pratique, la reconnaissance peut être réalisée à partir d'images fixes (photos) ou animées (enregistrements vidéo) et se déroule en deux phases :

1. À partir de l'image, un modèle ou « gabarit » qui représente, d'un point de vue informatique, les caractéristiques de ce visage est réalisé.
2. La phase de reconnaissance est ensuite réalisée par la comparaison de ces modèles préalablement réalisés avec les modèles calculés en direct sur des visages présents sur l'image candidate.

Dans le cas de l'authentification, le système vérifie si l'identité prétendue est bien la bonne en comparant le modèle du visage présenté au modèle préalablement enregistré correspondant à l'identité prétendue. Dans le cas de l'identification, le système vérifie si le modèle du visage présenté correspond à l'un des modèles contenus dans la base de données. Les résultats de la comparaison correspondent à celui ou ceux présentant le score de similarité le plus élevé parmi ceux dépassant un certain seuil prédéterminé.

Dans son Livre Blanc sur l'intelligence artificielle²⁷, la Commission européenne fait une distinction entre l'identification biométrique à distance et l'authentification biométrique,

²⁵ Commissariat à la protection de la vie privée du Canada, Reconnaissance faciale automatisée dans les secteurs public et privé, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303.

²⁶ Commission Nationale de l'Informatique et des Libertés (CNIL), « Reconnaissance faciale » : <https://www.cnil.fr/fr/definition/reconnaissance-faciale>.

²⁷ Commission européenne, *Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance*, Livre Blanc, COM (2020) 65 final, 19 Février 2020 : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf.

définie comme un processus de sûreté qui s'appuie sur les caractéristiques biologiques uniques d'une personne pour vérifier qu'elle est bien celle qu'elle prétend être. 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. La Commission européenne rejoint les autorités de protection des données qui estiment également que l'authentification est moins intrusive que l'identification.

Comme le remarque le CPVP, « pour que la technologie soit efficace, il faut disposer d'une image numérique de qualité du visage de l'individu en question, d'une base de données d'images numériques d'individus identifiés et d'un logiciel de reconnaissance faciale capable d'établir une correspondance exacte entre l'image d'un individu et une image d'un individu identifié qui est enregistrée dans la base de données »²⁸.

Les algorithmes et les techniques d'apprentissage automatique (notamment le *deep learning*²⁹) réalisent un traitement automatique des images sur un grand volume de données pour mieux détecter les zones de discontinuité comme les yeux ou la bouche et les points d'intérêt comme les narines, les sourcils. En règle générale, les logiciels de reconnaissance faciale actuels analysent environ 80 caractéristiques du visage que l'on appelle aussi points nodaux³⁰. Parmi ces caractéristiques, on compte la distance entre les yeux, la longueur du nez, la forme des joues, la profondeur des orbites, ou encore la largeur de la mâchoire. Ces traits diffèrent sur chaque individu, et c'est pourquoi la reconnaissance faciale permet de reconnaître une personne avec précision. Ces attributs physiques sont ensuite codés sous la forme de « gabarits » (faceprint), c'est-à-dire des représentations mathématiques, permettant de représenter le visage au sein d'une base de données dans laquelle ils sont stockés et éventuellement comparés aux autres gabarits contenus dans une base de données de référence³¹.

Définition des forces de police

Dans ce rapport, la police sera entendue au sens strict et ne seront pas considérés les corps spécifiques comme la police militaire et la police des frontières. Seront aussi exclues en tant

²⁸ Commissariat à la protection de la vie privée du Canada, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303.

²⁹ Yann Lecun, « L'apprentissage profond, une révolution en intelligence artificielle », La lettre du Collège de France, n°41, 2015-2016 : <http://journals.openedition.org/lettre-cdf/3227> ; <https://doi.org/10.4000/lettre-cdf.3227>.

³⁰ Bastien L., « Reconnaissance faciale : qu'est-ce que c'est et quels sont les dangers ? » (23 octobre 2019), Le Big Data : <https://www.lebigdata.fr/reconnaissance-faciale-tout-savoir>.

³¹ Claude Castelluccia, Daniel Le Métayer, *Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode*, Rapport de recherche, Inria Grenoble Rhône-Alpes, 2019, p.6, (hal-02373093) ; Jean-Gabriel Ganascia, « Usages et mésusages de la reconnaissance faciale » (27 avril 2016), The Conversation : <https://theconversation.com/usages-et-mesusages-de-la-reconnaissance-faciale-58445>.

que telles les compagnies privées de gardiennage, parfois sollicitées pour assurer la sécurité et l'accès à des grands événements par exemple.

3.2. Qualification juridique des données biométriques en renseignements personnels sensibles

Qualification de renseignements personnels

Les données extraites pour constituer le gabarit de la reconnaissance faciale sont des données biométriques qualifiables de renseignements personnels. *Un renseignement personnel* est tout renseignement concernant un individu identifiable (personal information).

Le CPVP relève ainsi que « les systèmes biométriques enregistrent des renseignements personnels sur des personnes identifiables. Cela signifie que leur utilisation par le gouvernement fédéral est assujettie à la *Loi sur la protection des renseignements personnels*. Les données biométriques peuvent aussi être réunies, utilisées ou communiquées par des organisations du secteur privé, qui peuvent être assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) »³².

La CAI³³ indique que « les renseignements biométriques sont des renseignements personnels, c'est-à-dire des informations qui concernent un individu et permettent de l'identifier » au sens de l'article 54 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de l'article 2 de la loi sur la protection des renseignements personnels dans le secteur privé. Ils sont uniques, distinctifs et persistent dans le temps.

Tel est notamment le cas des images, qu'elles soient statiques ou dynamiques.

La qualification de « renseignements personnels » s'applique aussi à « tout code (aussi appelé gabarit ou modèle), numérique ou autre, qui est dérivé de ces images à l'aide d'un algorithme. En effet, dans la mesure où ce code, qui constitue une caractéristique ou une mesure biométrique, est conservée pour la reconnaissance ultérieure d'une personne, il permet de l'identifier, puisqu'il est distinctif par nature ».

³² CPVP, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », Février 2011 : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/reenseignements-sur-la-sante-reenseignements-genetiques-et-autres-reenseignements-sur-le-corps/gd_bio_201102.

³³ Commission d'accès à l'information (CAI), « La biométrie au Québec », Fiche info, Janvier 2016, p.6 : https://www.cai.gouv.qc.ca/documents/CAI_FI_biometrie.pdf.

En droit de l'Union européenne, l'article 4-14 du règlement 2016/679/UE soit le règlement général de protection des données personnelles adopté le 27 avril 2016 dit RGPD³⁴ définit les données biométriques comme étant :

« les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopique ».

Les données biométriques sont particulièrement sensibles pour trois raisons principales : elles sont intimement liées par nature à la personne et sont en cela davantage rattachées à la personne qu'une adresse postale ou un mot de passe ; elles ne sont pas choisies par les personnes et ne peuvent être modifiées ou remplacées, ce qui pose de graves problèmes en cas de vols des données ; elles créent de lourdes difficultés pour les individus en cas d'erreurs d'identification provenant de systèmes biométriques « intelligents » qu'il sera quasiment impossible de remettre en cause, alors que les taux d'erreurs sont encore très élevés.

Renseignements personnels sensibles selon les autorités de protection le CPVP et la CAI

Le CPVP note que « les visages ont été transformés en données électroniques qu'il est désormais possible de regrouper, d'analyser et de classer de façons inédites. Les données d'images du visage sont d'autant plus précieuses et sensibles qu'il s'agit d'une caractéristique de notre corps mesurable de façon unique et d'un élément clé de notre identité »³⁵.

La CAI³⁶ ajoute que « les renseignements biométriques revêtent un caractère particulièrement sensible. Ce sont des caractéristiques permanentes et distinctives, des identifiants uniques composés d'informations intimes ».

« De même, certains de ces renseignements permettent de déduire d'autres informations que l'identité d'une personne. Par exemple, la lecture de l'iris et l'analyse de la démarche peuvent dévoiler une maladie ou un handicap. Les mesures ou les caractéristiques biométriques peuvent également dévoiler une maladie ou un handicap. Les mesures ou les caractéristiques biométriques peuvent également révéler les origines ethniques ».

³⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

³⁵ Commissariat à la protection de la vie privée du Canada, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303

³⁶ Commission d'accès à l'information (CAI), « La biométrie au Québec », Fiche info, Janvier 2016, p.6 : https://www.cai.gouv.qc.ca/documents/CAI_FI_biometrie.pdf

« Enfin, si la confidentialité de ces renseignements est compromise, des conséquences graves peuvent en résulter pour la personne concernée : s'il est possible de remplacer une carte magnétique, un numéro d'identification personnel (NIP) ou un mot de passe, on ne peut pas changer son visage ou ses empreintes digitales. Les risques pour le vol d'identité – entre autres – sont donc particulièrement conséquents ».

Données personnelles sensibles en droit de l'Union européenne

En droit de l'Union européenne, les données biométriques sont qualifiées de données sensibles au sens de l'article 9 du RGPD qui porte sur :

« le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique (...) ».

Les données sensibles sont particulièrement protégées. En principe, de telles données ne peuvent faire l'objet d'un traitement (art. 9.1 du RGPD), sous réserve d'exceptions limitativement énumérées (art. 9.2). Le considérant 51 du RGPD ajoute que « le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique ». Il convient donc de considérer l'usage de ce type de données au cas par cas.

En outre, l'utilisation de la reconnaissance faciale dans l'espace public par les forces de police ne tombe pas sous le coup du RGPD qui s'applique à la matière civile et commerciale mais de la directive 2016/680/UE³⁷ dite directive « police-justice ». Cette directive retient la même définition que le RGPD et encourage aussi une appréciation au cas par cas du traitement des données sensibles en considération des risques. Le considérant 52 précise ainsi que :

« Il convient de déterminer la probabilité et la gravité du risque en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque élevé. On entend par risque élevé un risque particulier de porter atteinte aux droits et aux libertés des personnes concernées ».

³⁷ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

3.3. Exclusions de certaines technologies ou finalités

Le CPVP³⁸ et la CNIL notent que « la reconnaissance faciale ne doit pas être confondue avec la **détection de visage** qui caractérise la présence ou non d'un visage dans une image indépendamment de la personne à qui il appartient »³⁹.

Également, les techniques d'identification à l'aide de la biométrie du visage n'ont aucun lien avec des **techniques de traitement prédictif et de profilage** consistant à analyser les caractéristiques d'une personne pour en déduire des caractéristiques de comportement actuel ou futur⁴⁰.

Enfin, sont aussi exclus les procédés biométriques ayant **d'autres fins que l'identification ou l'authentification des individus**, comme les caméras thermiques, l'analyse de vidéo anonyme (AVA), les bracelets de santé connectés, systèmes de reconnaissance des émotions, etc.

3.4. Détails de la technologie de reconnaissance faciale

L'utilisation de la biométrie du visage comporte trois grandes étapes :

- une phase de captation de l'image du visage ;
- une phase de traitement algorithmique (techniques de biométrie du visage, proprement dites) qui correspond à la représentation numérique du visage ; cette phase s'appuie dans certains cas sur un fichier biométrique ;
- une chaîne opérationnelle comportant analyse et décision, fonction des finalités du processus (identification ou authentification) et de son cadre juridique (ex. enquête judiciaire). La « carte » numérique du visage représenté sur l'image est par exemple comparée avec les images de visages identifiés qui sont enregistrées dans la base de données.

Captation de l'image du visage

La capture de l'image du visage (ou son acquisition) peut se faire sur la voie publique ou dans des lieux privés (commerces, stades...), par photographie ou extraction d'une image d'enregistrements vidéo.

³⁸ Commissariat à la protection de la vie privée du Canada, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Rapport, Mars 2013 : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303

³⁹ Commission Nationale de l'Informatique et des Libertés (CNIL), « Reconnaissance faciale » : <https://www.cnil.fr/fr/definition/reconnaissance-faciale>.

⁴⁰ Voir, par exemple, en droit de l'Union européenne : Groupe de travail « article 29 » sur la protection des données, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, Version révisée et adoptée le 6 février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/wp251_profilage-fr.pdf

Le cadre juridique de cette capture d'image est variable. Il peut s'agir notamment :

- d'une enquête judiciaire (signalisation judiciaire, image d'une vidéo récupérée dans le cadre d'une enquête, photographie de flagrant délit...);
- d'opérations de renseignement effectuées par les services concernés ;
- d'organiser le passage à la frontière.

Technique informatique de biométrie du visage

L'image du visage captée est traitée par un algorithme pour en extraire un gabarit, sorte de signature propre à chaque visage ; ce gabarit est ensuite comparé à un ou plusieurs gabarits issus d'une autre ou de plusieurs autres images du visage.

Cette comparaison ne donne jamais de résultat absolu mais un pourcentage de correspondance, c'est pourquoi l'expression « reconnaissance faciale » est trompeuse. En fonction de la finalité du dispositif et de son environnement humain, **un seuil de correspondance** à partir duquel il sera considéré que les deux images sont susceptibles de correspondre à la même personne devra être déterminé.

Deux grandes distinctions doivent être faites, selon que cette comparaison est réalisée :

- **avec ou sans gabarits** (recherche non ciblée) : avec un seul gabarit (comparaison 1:/1 = authentification) ou bien avec plusieurs gabarits, voire avec les gabarits des personnes figurant dans un fichier (comparaison 1:/N = identification). On peut aussi mener une recherche non ciblée d'analyse systématique d'images de vidéosurveillance pour tenter de retrouver des personnes recherchées recensées dans un fichier (recherche M:/N). On peut aussi appliquer la reconnaissance faciale pour comparer plusieurs images captées *in vivo*, par exemple pour suivre les déplacements d'un agresseur sur des images de vidéosurveillance (traçage 1:/0).
- **en temps réel** (ou « à la volée », par exemple surveillance de grands événements) **ou en temps différé** (par exemple dans le cadre d'une enquête judiciaire ou de la recherche d'une personne disparue).

La comparaison 1:/1 compare une seule personne à une seule image. Tel est par exemple le cas de la personne enrôlée pour bénéficier d'un dispositif d'accès rapide ou figurant dans la puce du passeport en cas d'authentification.

Dans le cas de la comparaison 1:/N, la comparaison concerne une ou plusieurs personnes successivement photographiées dans une foule, avec les personnes figurant dans un fichier de référence comportant de nombreuses personnes. La personne qui fait l'objet de la comparaison n'est pas nécessairement identifiée et pourra l'être si son gabarit « matche » avec une personne identifiée dans un fichier de référence.

Le « match » est la correspondance automatisée alors que le « hit » est la confirmation par un analyste du rapprochement.

La base biométrique à laquelle est confrontée l'image captée est appelée **base de référence**. Il peut s'agir d'une base « positive » (personnes admises, par exemple dans un site protégé) ou bien « négative » (personnes exclues, par exemple pour être recherchées). Techniquement, un même algorithme recherchera des correspondances pour restreindre l'accès à certaines personnes et, au contraire pour faciliter en même temps l'accès d'autres personnes enrôlées volontairement.

Les **bases de référence** constituent un élément essentiel au plan des libertés individuelles puisqu'elles contribuent à décider de l'accès ou du refus des personnes. La définition de ces bases de référence, leur mode de constitution et de mise à jour, dans un objectif d'identification ou d'authentification à l'aide de la biométrie du visage, doivent être conformes à la réglementation provinciale et nationale, selon les finalités et cas d'usage déterminés. En outre, les procédures à suivre en cas de « match » ou de « hit » doivent être encadrées et prédéfinies avec un processus opérationnel de vérification et des conduites à tenir qui pourront différer selon chaque cas d'usage.

Organisation de la chaîne opérationnelle associée

Le nombre de rapprochements effectués sera tributaire des **seuils de correspondance choisis** en amont de la mise en place du processus et des finalités de ce dernier. Si le seuil de correspondance est bas, le risque sera d'avoir des personnes reconnues à tort ou faux matchs (faux positifs ou faux négatifs selon si la base de référence conduit à une décision positive ou négative).

Par exemple, dans le cadre d'un contrôle d'accès, un seuil de correspondance bas conduit à un haut niveau d'acceptation, ce qui peut générer des faux positifs ou association erronée de deux personnes différentes. Au contraire, si le seuil de correspondance est élevé, le niveau d'acceptation sera faible et les faux négatifs plus nombreux, c'est-à-dire l'échec d'association de deux images représentant la même personne.

La prise en charge des faux positifs et faux négatifs commande la mise en place d'une organisation humaine adaptée, la détermination des actions à mettre en œuvre et leurs modalités pratiques.

3.5. Reconnaissance faciale et sécurité intérieure

Dans le cadre des usages possibles de la biométrie du visage en matière de sécurité intérieure, il est nécessaire d'appréhender l'ensemble du processus. Il faut notamment se demander si ces techniques viennent à l'appui d'un processus d'identification sous un contrôle humain ou non.

Si l'humain intervient, la biométrie du visage constitue alors essentiellement une aide à la décision, ce qui confère des garanties de respect des libertés fondamentales. L'utilisation de la biométrie du visage doit toujours s'intégrer dans une chaîne opérationnelle humaine, liée à des cas d'usage stricts. Il ne faut donc pas attendre des économies d'effectifs par le recours à cette technologie.

À l'heure actuelle, peu de situations ne font pas appel à un contrôle humain. On peut toutefois donner l'exemple des contrôles d'accès dans les aéroports qui peuvent se faire à l'aide de la biométrie du visage sans intervention humaine lorsque s'il s'agit de laisser passer les personnes titulaires de passeports ». La décision automatisée est alors positive et il s'agit d'authentification à partir d'un enrôlement volontaire de la personne concernée.

3.6. Notion d'espace public

Par ailleurs, il convient d'avoir une attention particulière sur **l'acquisition d'une image d'un visage dans un espace ouvert au public**. La notion d'espace public s'étend à certains espaces privés ouverts au public comme des stades ou des centres commerciaux, sachant que le fait que la captation de l'image relève d'un acteur privé ou une collectivité publique n'implique pas que l'utilisation de techniques de biométrie du visage relève de ces acteurs.

Sont donc **exclus** de cette définition de l'espace public :

- les processus comportant une **captation d'image de personnes dans un domicile ou un site réservé** (par exemple une entreprise ou une administration) ;
- les enrôlements correspondant à des **usages privés** sur la base du volontariat (tel un accès à un smartphone ou une identification numérique auprès d'une banque).

4. Principaux enjeux sociaux et juridiques de la reconnaissance faciale

4.1. Avantages de la reconnaissance faciale à des fins de sécurité publique

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 société⁴¹ lorsqu'elle est couplée avec la vidéosurveillance. Alors que les villes sont toujours plus denses et peuplées, cette innovation permet de maintenir un niveau de sécurité que les gardiens de la paix ne peuvent plus assurer seuls. D'autres avantages sont mis en avant, tel que le gain de temps ou la simplification du travail des forces de police.

4.2. Questionnements induits par l'usage de la reconnaissance faciale

L'usage de la reconnaissance faciale dans l'espace public à des fins de sécurité suscite toutefois des interrogations et craintes pour les libertés individuelles. Le potentiel liberticide de ce type de technologie ne peut en effet être ignoré.

Chacune des phases du processus d'identification utilisant la biométrie du visage induit un questionnement spécifique dont une première liste indicative figure ci-après :

- **La capture de l'image** d'une personne est-elle autorisée ou doit-elle être consentie ? Peut-elle être imposée dans certains cas ? Quel est le devenir de ces images captées ? Sont-elles conservées ? Si oui combien de temps ? Qui peut y avoir accès et dans quelles conditions ? Cette captation d'image se place-t-elle dans un cadre

⁴¹ European Union agency for fundamental rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019, p.18 : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

judiciaire, de renseignement, de prévention de la délinquance ou de police administrative ?...

- **Le traitement de l'image** qui calcule le gabarit et effectue les rapprochements comporte-t-il des biais posant question au regard de l'égalité entre les personnes ? Ces biais viennent-ils de défauts de conception de l'algorithme, d'une insuffisance de son entraînement, de son évolution autonome (*machine learning* ou *deep learning*) ? Ces biais viennent-ils des données d'entraînement insuffisamment variées et représentatives ? Comment peut-on contrôler en amont ces risques de biais et, conséquemment, de discrimination ? Faut-il mettre en place un système d'audit ou de certification ? Quel est le seuil de correspondance choisi et pourquoi ? Quel est alors le taux admis de fausse acceptation ou de faux refus ? Le respect de ces paramètres est-il contrôlé ? Comment ?...
- Comment est choisie **la base biométrique de référence** à laquelle sont comparés le ou les visages captés ? Cette base de référence est-elle conforme à la réglementation sur les renseignements personnels ? Les accès aux données sont-ils maîtrisés ? S'agit-il d'une base de données existante ou d'une base spécifique établie à partir d'autres fichiers ? Dans ce dernier cas, quel est le critère de sélection ? A quelle finalité obéit le choix de ce fichier et de ses éléments ? ...
- **Comment sont traités les rapprochements trouvés par le traitement ?** En cas de « match », y a-t-il un contrôle humain systématique ? Une supervision à distance ? Y a-t-il une décision humaine pour valider ou non ce résultat ou en tirer des effets prédéterminés (ouverture ou non de porte, contrôle des personnes, accentuation des vérifications, vigilance...) ? L'organisation humaine est-elle adaptée au processus défini et à la performance de l'outil ? Quelle interaction entre le paramétrage de l'outil de biométrie du visage et l'organisation mise en œuvre ? Quels sont les acteurs aux différentes phases du processus ? S'agit-il d'acteurs publics ou privés ? de police municipale, provinciale ou nationale ? ...

4.3. Conditions de capture d'images : le cas de Clearview AI

Gigantesque base de données d'images de personnes sans consentement

Clearview AI a développé une application de reconnaissance faciale qui permet de comparer n'importe quelle photo à une base de données composée de milliards de clichés en accès libre, récupérés depuis sa création en 2016 sur la plupart des réseaux sociaux et des millions de sites Internet. Cette entreprise américaine a constitué une base de données sans équivalent et propose cette technologie essentiellement aux forces de l'ordre. Un algorithme compare rapidement et efficacement un cliché pris à l'aide d'un smartphone avec la base de données de référence de Clearview AI.

L'outil a séduit les forces de l'ordre américaines et canadiennes. La police de l'Indiana est devenue le premier client de la start-up en février 2019 et cette technologie a été utilisée par environ 600 services de police locale aux États-Unis. Les activités de cette entreprise discrète ont été révélés en janvier 2020 par le New York Times⁴².

Mise en demeure par les grandes entreprises technologiques

En février 2020, Google, YouTube et Twitter ont mis en demeure l'entreprise ClearView pour ordonner que Clearview AI cesse d'utiliser des photos de leurs usagers, afin d'entraîner son outil de reconnaissance faciale et de constituer une gigantesque base de données, en violation de leurs politiques de protection de la vie privée⁴³.

Enquêtes des autorités canadiennes de protection des renseignements personnels

L'utilisation de cet outil par certains corps de police au Canada, comme les polices d'Edmonton⁴⁴, de Calgary⁴⁵, Vancouver⁴⁶, de Toronto⁴⁷, d'Halifax⁴⁸ et la Gendarmerie Royale du Canada (GRC)⁴⁹, ont soulevé des craintes⁵⁰ ayant justifié de lancer, en février 2020, une enquête connexe menée par le CPVP en vertu de la *Loi sur la protection des renseignements personnels*⁵¹.

⁴² Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It" (18 Janvier 2020), The New York Times : <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

⁴³ Radio-Canada, "Google, Facebook et Twitter mettent en demeure Clearview AI" (6 Février 2020), Radio-Canada: <https://ici.radio-canada.ca/nouvelle/1509484/clearview-ai-intelligence-artificielle-reconnaissance-faciale>.

⁴⁴ Dylan Short, "Controversial Clearview AI facial recognition program used twice by city police: Privacy commissioner Investigating" (28 Février 2020), Edmonton Journal : <https://edmontonjournal.com/news/local-news/controversial-clearview-ai-facial-recognition-program-used-twice-by-city-police-review-launched>.

⁴⁵ Alanna Smith, "Two Calgary officers tested Clearview AI facial-recognition software" (29 Février 2020), Calgary Herald : <https://calgaryherald.com/news/local-news/two-calgary-officers-tested-clearview-ai-facial-recognition-software>

⁴⁶ Nick Eagland, Lori Culbert, "Vancouver detective used controversial facial-recognition software once" (05 Mars 2020), Vancouver Sun : <https://vancouversun.com/news/vancouver-police-used-controversial-clearview-facial-recognition-software-a-single-time>.

⁴⁷ Kayla Goodfield, "Canadian privacy officials will investigate controversial facial recognition tool used by Toronto police" (21 Février 2020), Toronto CTV News : <https://toronto.ctvnews.ca/canadian-privacy-officials-will-investigate-controversial-facial-recognition-tool-used-by-toronto-police-1.4822198>.

⁴⁸ Alexander Quon, "Halifax police confirm use of controversial Clearview AI facial recognition technology" (28 Février 2020), Global News : <https://globalnews.ca/news/6607993/halifax-police-confirm-clearview-ai-facial-recognition-technology>

⁴⁹ Bryan Carney, Despite Denials, "RCMP Used Facial Recognition Program for 18 Years" (10 Mars 2020), The Tyee : <https://thetyee.ca/News/2020/03/10/RCMP-Admits-To-Using-Clearview-AI-Technology>

⁵⁰ Louis Blouin, Christian Noël, « L'utilisation par la GRC de la reconnaissance faciale fait l'objet d'une enquête » (29 février 2020), Radio-Canada : <https://ici.radio-canada.ca/nouvelle/1641664/grc-clearview-intelligence-artificielle-enquete-commissaire-vie-privee>.; Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It" (18 Janvier 2020), The New York Times : <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

⁵¹ Les quatre autorités de réglementation de la protection de la vie privée examineront si les pratiques de l'organisation sont conformes aux lois canadiennes sur la protection des renseignements personnels. Dans le cas du CPVP, cela comprendrait la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). La CAI enquêtera sur la conformité à la Loi sur la protection des renseignements

Parallèlement, une enquête conjointe est menée par les autorités de protection des renseignements personnels du Canada, de la Colombie-Britannique, du Québec et de l'Alberta, afin d'étudier si ses pratiques sont conformes aux lois canadiennes sur la protection des renseignements personnels⁵². Cette enquête a été initiée à la suite de nombreux reportages dans les médias ayant soulevé des questions et des préoccupations à savoir si l'entreprise recueille et utilise des renseignements personnels sans consentement. Les résultats de l'enquête n'ont pas encore été rendus publics.

Fin des services de Clearview AI

Clearview AI a informé les autorités canadiennes chargées de la protection de la vie privée qu'en réponse à leur enquête conjointe, elle n'offrira plus ses services de reconnaissance faciale au Canada. Elle a aussi suspendu indéfiniment son contrat avec la GRC, son dernier client au Canada⁵³.

Actions en justice contre Clearview AI aux États-Unis

ACLU vs Clearview AI

ACLU (American Civil Liberties Union) et ACLU Illinois ont intenté un procès à Chicago devant la Cour de l'État de l'Illinois contre Clearview le 28 mai 2020 après les révélations du New York Times sur le fondement de l'Illinois Biometric Information Privacy Act (BIPA)⁵⁴.

personnels dans le secteur privé et à la Loi concernant le cadre juridique des technologies de l'information du Québec. Le CIPVP C.-B. enquêtera sur la conformité à la Personal Information Protection Act (Loi sur la protection des renseignements personnels). Le CIPVP Alb. enquêtera sur la conformité à la Personal Information Protection Act (Loi sur la protection des renseignements personnels), voir Commissariat à la protection de la vie privée du Canada, « Le Commissariat lance une enquête sur le recours par la GRC à la technologie de reconnaissance faciale », Annonce, 28 février 2020 : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/an_200228.

⁵² Commission d'accès à l'information du Québec, « Des commissaires lancent une enquête conjointe sur Clearview AI dans un contexte de préoccupations croissantes quant à l'utilisation de la technologie de reconnaissance faciale », 21 février 2020 : <https://www.cai.gouv.qc.ca/commissaires-lancent-enquete-conjointe-clearview-ai-dans-contexte-preoccupations-croissantes-quant-utilisation-technologie-reconnaissance-faciale/>.

⁵³ Commissariat à la protection de la vie privée du Canada, « Clearview AI cesse d'offrir sa technologie de reconnaissance faciale au Canada », Communiqué, 6 juillet 2020 : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/nr-c_200706.

⁵⁴ ACLU, « ACLU v. Clearview AI », 27 Mai 2020 : <https://www.aclu.org/cases/aclu-v-clearview-ai>.

En mars 2020⁵⁵, l'Attorney General Donovan du Vermont poursuit Clearview AI pour violation de la loi sur la protection des consommateurs⁵⁶ et de la loi sur les courtiers de données⁵⁷.

4.4. Principaux risques sociaux et juridiques

Risques d'atteinte aux libertés d'aller et venir, d'expression, association et réunion

Les risques d'atteintes aux libertés individuelles susceptibles d'être induits par ces dispositifs de reconnaissance faciale 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). Dans l'affaire *Greater Vancouver*, la Cour précise que la liberté d'expression protège non seulement l'activité expressive, mais aussi « le droit de l'exercer dans certains lieux publics »⁵⁸. La liberté d'expression et la liberté de réunion pacifique « protègent le droit de s'exprimer sur la voie publique »⁵⁹ et le recours à la reconnaissance faciale peut nuire à la liberté d'expression, d'association et de réunion⁶⁰.

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). Dans l'affaire *Le Puil c. Vacchino Itée*⁶¹, le Tribunal a souligné que le fait de capter des images vidéo dans un endroit public d'une personne identifiable « équivaut à une collecte de renseignements personnels »⁶². La protection accordée par la loi à la vie privée n'est pas limitée géographiquement à l'espace privé et peut donc s'étendre à l'espace public. La protection de la vie privée ne se rattache donc pas au lieu mais à la personne, où qu'elle se

⁵⁵ Office of the Vermont attorney general, "Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law," 10 Mars 2020 : <https://ago.vermont.gov/blog/2020/03/10/attorney-general-donovan-sues-clearview-ai-for-violations-of-consumer-protection-act-and-data-broker-law>.

⁵⁶ Vermont General Assembly, The Vermont Statutes Online, Title 9 : Commerce and Trade, Chapter 63 : Consumer Protection : <https://legislature.vermont.gov/statutes/chapter/09/063>.

⁵⁷ Vermont General Assembly, The Vermont Statutes Online, Title 9 : Commerce and Trade, Chapter 62 : Protection Of Personal Information : <https://legislature.vermont.gov/statutes/chapter/09/062>.

⁵⁸ *Greater Vancouver Transportation Authority c. Fédération canadienne des étudiantes et étudiants*, [2009] 2 R.C.S. 295, par. 27

⁵⁹ *Garbeau c. Montréal (Ville de)*, 2015 QCCS 5246 (CanLII), par. 127

⁶⁰ European Union Agency for Fundamental Rights, "Facial recognition technology : fundamental rights considerations in the context of law enforcement", 27 Novembre 2019 : <https://fra.europa.eu/en/publication/2019/facial-recognition>.

⁶¹ *Le Puil c. Vacchino Itée (Appartements Mozart)*, 2019 QCRDL 28045 (CanLII)

⁶² *Le Puil c. Vacchino Itée*, par. 29.

trouve⁶³. À partir du moment où l'environnement en question revêt une dimension privée pour la personne, ceci relèvera de la vie privée, même s'il s'agit d'un espace public⁶⁴.

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 fondamentales⁶⁵. En ce sens, la Haute Commissaire des Nations Unies aux droits de l'homme a demandé aux États et entreprises de veiller à ce que l'utilisation de ces outils ne vienne pas compromettre « la capacité des personnes d'exercer leurs droits fondamentaux à la liberté de réunion pacifique et à la liberté d'expression, et leur droit de participer aux affaires publiques »⁶⁶.

S'agissant de l'utilisation de ces renseignements et de la reconnaissance faciale par les forces de police, « bien que les citoyennes et les citoyens soient souvent favorables à de telles comparaisons lorsque les services policiers utilisent les empreintes digitales pour localiser des suspects, la même technique peut aussi priver des gens au-dessus de tout soupçon de leur droit de vivre leur vie dans l'anonymat et de ne pas faire l'objet d'une surveillance »⁶⁷. La liberté de se mouvoir anonymement dans l'espace public doit en effet être protégée car il est un lieu où s'exercent de nombreuses libertés individuelles et publiques.

En outre, aucune règle oblige chacun à être identifié ou à s'identifier à chaque seconde où il circule dans l'espace public. S'il existe certains interdits de ce point de vue (interdiction de dissimuler son visage) ou certaines obligations (port de badge dans certains lieux ou obligation de se soumettre aux contrôles, vérifications et relevés d'identité, par exemple), ces dispositifs sont précisément encadrés par la loi et ne remettent aucunement en cause toute possibilité d'anonymat dans les espaces publics⁶⁸. De façon générale, l'utilisation de la reconnaissance faciale par les services de police dans l'espace public peut donc faire craindre à l'instauration d'une surveillance généralisée des individus, manifestement disproportionnée au regard de l'objectif de maintien de l'ordre public. De telles pratiques pourraient en outre permettre un « fichage » des individus et un profilage de certaines communautés en vue de les discriminer. L'oppression des opposants politiques par exemple

⁶³ Université Concordia et Syndicat des employés et employés de soutien de l'Université Concordia (K.S.), 2010 CanLII 102247 (QC SAT), par. 58 à 60.

⁶⁴ Pierre Trudel, « Le droit de la personne sur son image », *Lex Electronica*, Vol. 25, 2020, p.368 : <http://www.canlii.org/t/xjt9>.

⁶⁵ Interview d'Éloïse Gratton dans Tristan Péloquin, « La vie privée menacée: souriez, vous êtes filmés (et reconnus) » (8 février 2020), *La Presse*: <https://www.lapresse.ca/actualites/2020-02-08/la-vie-privee-menacee-souriez-vous-etes-filmes-et-reconnus>.

⁶⁶ Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), « Les nouvelles technologies doivent favoriser et non entraver le droit de manifester pacifiquement », annonce Michelle Bachelet aux États, 25 juin 2020 : <https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=F>. Un rapport a été publié.

⁶⁷ Ibid. voir D. Solove, "The Virtues of Anonymity" (11 Mars 2016), *The New York Times* : <https://www.nytimes.com/roomfordebate/2011/06/21/youre-mad-youre-on-youtube/the-virtues-of-anonymity>.

⁶⁸ Commission Nationale Informatique et Libertés (CNIL), *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, 15 novembre 2019 : https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf.

lors de manifestations pourrait alors être facilitée comme le montre certains exemples étrangers tristement célèbres⁶⁹.

Risques d'atteinte à la protection des renseignements personnels et à la vie privée

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 font l'objet d'une protection spécifique selon plusieurs législations dans le monde.

Ainsi, en droit de l'Union européenne, les données biométriques sont des données sensibles qui bénéficient d'une protection renforcée. En outre, conformément à l'article 35 du RGPD, tout projet de recourir à la reconnaissance faciale devra à tout le moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD)⁷⁰.

Aux États-Unis, il a été relevé que les images recueillies par le biais d'outils de reconnaissance faciale peuvent être liés à divers dossiers contenant des renseignements personnels, tels que les dossiers médicaux, le casier judiciaire, les renseignements sur le crédit⁷¹. La protection des données reste donc un enjeu crucial avec l'usage de technologies de reconnaissance faciale. Plusieurs États ont ainsi pris des mesures législatives renforcées pour protéger les données biométriques comme par exemple l'État de l'Illinois qui a adopté dès 2008 le *Biometric Information Privacy Act* (BIPA)⁷².

Le lieu de stockage des données utilisées dans la base de référence doit aussi être pris en considération. En cas de stockage aux États-Unis, l'accès pourrait être facilité aux autorités américaines sur le fondement du *Cloud Act*⁷³. Les risques d'atteinte à la sécurité des données (fuite, piratage) constituent aussi des enjeux à considérer.

Le cadre légal de la protection des données personnelles sera développé dans les parties 4 et 5.

⁶⁹ Voir, par exemple, l'oppression des manifestants hongkongais par le gouvernement chinois et l'utilisation de la technologie pour ce faire : Human Rights Council, Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/41/35, 2019 ; Paul Mozur, "One Month, 500,000 Face Scans : How China Is Using A.I. to Profile a Minority" (14 Avril 2019), New York Times : <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.

⁷⁰ Commission Nationale de l'Informatique et des Libertés, « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », 22 Octobre 2019 : <https://www.cnil.fr/fr/ce-qu'il-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>.

⁷¹ Meredith Whittaker et al., AI Now Report 2018, p. 14 ; Kate Crawford, « Regulate facial-recognition technology », Nature n°572, 2019 ; CNIL, Reconnaissance Faciale : pour un débat à la hauteur des enjeux, Novembre 2019 : https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf.

⁷² Illinois General Assembly, Civil Liberties, (740 ILCS 14/) Biometric Information Privacy Act : <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%20>.

⁷³ Le *Clarifying Lawful Overseas Use of Data Act* est une loi fédérale des États-Unis adoptée en mars 2018 sur l'accès aux données de communication, notamment opérées dans le Cloud. Il modifie le *Stored Communications Act* et l'*Electronic Communications Privacy Act*.

Risques d'erreur, de biais, de discrimination et atteinte à la dignité des personnes

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. L'exactitude des systèmes de reconnaissance faciale varie grandement selon plusieurs facteurs, dont la qualité des appareils photo, l'éclairage, le type de modèles utilisés, les algorithmes de comparaison et la taille des bases de données de référence. Ainsi, des études faites notamment au MIT Media Lab montrent 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 femmes⁷⁴. Pour les femmes ayant la peau plus foncée, le taux d'erreurs avoisinerait les 35%⁷⁵. Une étude fédérale réalisée aux États-Unis en décembre 2019 confirme l'existence de biais raciaux dans de nombreux systèmes⁷⁶. Selon cette étude, les personnes d'origine asiatiques et afro-américaines ont jusqu'à 100 fois plus de chance d'être mal identifiées que les hommes blancs, selon l'algorithme et le type de recherche. Plus récemment, une étude du National Institute of Standards and Technology (NIST) a confirmé les biais⁷⁷.

Les technologies de reconnaissance faciale d'Idemia, dont l'utilisation est envisagée par la Sûreté du Québec, sont parmi les plus fiables sur le marché, selon des tests publiés en décembre dernier aux États-Unis par le NIST⁷⁸. Un des algorithmes a toutefois montré une probabilité d'erreur de 1 pour 1000 lorsqu'il était en présence de photos de femmes noires, alors que le taux d'erreur était de 1 pour 10 000 dans le cas des visages de femmes blanches.

Une des explications réside dans le fait que certains groupes de la population, par exemple certains groupes ethniques, les jeunes et les personnes handicapées, sont sous-représentés dans les images d'entraînement⁷⁹, lesquelles ne sont donc pas assez représentatives de la

⁷⁴ Voir les travaux de Joy Buolamwini, chercheuse au MIT et fondatrice de l'Algorithmic Justice League : <http://gendershades.org/overview.html>.

⁷⁵ Joy Buolamwini, "Artificial Intelligence Has a Problem With Gender and Racial Bias: Here's How to Solve It" (7 Février 2019), Time : <https://time.com/5520558/artificial-intelligence-racial-gender-bias/>

⁷⁶ Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use" (19 Décembre 2019), The Washington Post : [https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use.](https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/)

⁷⁷ Patrick Grother, Mei Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3 : Demographic Effects, National Institute of Standards and Technology, NISTIR 8280, Décembre 2019 : <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁷⁸ Patrick Grother, Mei Ngan, Kayee Hanaoka, Ongoing Face Recognition Vendor Test (FRVT) Part 2 : Identification, National Institute of Standards and Technology, NISTIR 8238, Novembre 2018 : <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf>.

⁷⁹ Christopher Parsons, « Peut-on encore être un visage dans la foule? », Blogue Savoir Techno CPVP, 17 juillet 2017 : <https://www.priv.gc.ca/fr/blogue/20170717/>.

population sur laquelle ces systèmes seront utilisés. Des systèmes biaisés entraînent des faux positifs et des faux négatifs, ce qui fait peser de lourdes conséquences dans l'identification des suspects par exemple. Les conséquences juridiques, sociales, et psychologiques pour les personnes faussement identifiées pèsent lourd et doivent être prises au sérieux par les gouvernements au moment de choisir et déployer ce type de technologies.

Ce risque porte naturellement atteinte au principe d'égalité et à la non-discrimination, pourtant 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. Le risque de stigmatiser certaines communautés et d'atteinte à la cohésion sociale est particulièrement élevé surtout pour une population très diversifiée au Canada. Dans un contexte d'utilisation de technologie de reconnaissance faciale et face aux risques de discrimination, l'article 15 de la Charte canadienne prône l'égalité réelle selon laquelle il est essentiel que le gouvernement tienne compte de la situation et des éléments factuels pour produire un véritable traitement égalitaire⁸⁰.

La discrimination systémique et le profilage racial sont de nature à porter atteinte à ces dispositions. La discrimination systémique se caractérise par des pratiques qui, par leur effet, provoquent une discrimination comme l'exclusion systématique d'un groupe. L'intention n'est pas ici un critère déterminant. La discrimination est alors dite indirecte en raison de ses effets, en l'absence d'intentionnalité. Le profilage racial est le plus souvent le fait d'une action prise par une personne en situation d'autorité contre un groupe ou des personnes en raison de leur appartenance, par exemple à une communauté raciale⁸¹. S'il advient d'autres formes de discrimination créées par ces dispositifs de surveillance, la Cour suprême dans l'arrêt *Bombardier*⁸² rappelle que le libellé de la Charte permet aux tribunaux de « constater l'existence de nouvelles formes de discrimination au fur et à mesure qu'elles se manifestent dans notre société »⁸³.

Risques d'erreurs judiciaires dans les enquêtes pénales

Il existe également des risques en cas d'utilisation de la reconnaissance faciale dans le cadre d'enquêtes judiciaires. En effet, on constate qu'il y a plus de risques d'erreurs judiciaires dans les causes où l'identité d'un suspect est mise en doute. Dès lors, on peut alors craindre que la technologie souvent vue comme infaillible et crédible auprès des tribunaux

⁸⁰ Christian Brunelle et Mélanie Samson, Chapitre IV, « Les droits et libertés dans le contexte civil », Droit public et administratif, Collection de droit 2020-2021, École du Barreau du Québec, vol. 8, 2020 (en ligne).

⁸¹ Ibid.

⁸² Québec (Commission des droits de la personne et des droits de la jeunesse) c. Bombardier Inc. (Bombardier Aéronautique Centre de formation), 2015 CSC 39 (CanLII), [2015] 2 RCS 789.

⁸³ Bombardier, par. 34

conforte les policiers, les témoins et les juges dans leurs certitudes⁸⁴. Or, les risques d'erreurs existent et les technologies fabriquées par des humains intègrent les risques de préjugés, *a fortiori* si les données d'entraînement sont biaisées. La technologie risque alors de conforter les préjugés sociaux.

Risques d'une faible acceptabilité sociale et dégradation des relations avec les forces de police

Compte tenu des risques précités, l'acceptabilité sociale de cette technologie risque d'être faible. On en veut pour preuve le fait que les géants des technologies IBM, Amazon⁸⁵ et Microsoft ont annoncé en juin 2020, des moratoires sur la vente de logiciels de reconnaissance faciale à des corps policiers, dans la foulée du mouvement Black Lives Matter⁸⁶, en raison du fait que de nombreuses études ont montré que ces technologies, utilisées dans le cadre d'enquêtes criminelles pour identifier rapidement des suspects, font davantage d'erreurs pour traiter des images de personnes à la peau noire que pour celles qui ont la peau blanche.

En ce sens, il faut aussi noter qu'en juillet 2020, l'International Civil Liberties Monitoring Group (ICLMG), OpenMedia, 29 organisations et 46 personnes actives dans la 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 GRC⁸⁷. L'appel invite à une consultation publique sur tous les aspects de la technologie de la reconnaissance faciale au Canada. Il invite aussi à établir des politiques et lois claires et transparentes pour réguler l'usage de la reconnaissance faciale au Canada, y compris la loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Une étude d'opinion réalisée au Royaume-Uni confirme que le public souhaite un encadrement de l'usage de cette technologie⁸⁸. Aux États-Unis, une étude réalisée par le *Pew Research Center* révèle qu'un peu plus de la moitié des Américains

⁸⁴ Voir le biais généré par le logiciel de calcul du risque de récidive COMPAS et révélé par l'étude des journalistes de Propublica : <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

⁸⁵ Les services de police ont été les principaux partisans de la technologie de reconnaissance faciale, arguant qu'elle les aide dans les enquêtes criminelles. Dans le comté de Washington, Oregon, le bureau du shérif a déclaré que le produit Rekognition d'Amazon a « considérablement augmenté la capacité de nos agents de la force publique à agir rapidement et de manière décisive » en réduisant le temps nécessaire pour « identifier les suspects criminels » de deux à trois jours à quelques minutes », voir Amazon Rekognition Customers : <https://aws.amazon.com/fr/rekognition/customers/?ots=1&slotNum=0&imprToken=a0b9ff16-f8c1-97d5-024&tag=curbedcom06-20&linkCode=w50>.

⁸⁶ AFP, « Amazon interdit à la police d'utiliser sa technologie de reconnaissance faciale » (10 Juin 2020), Radio-Canada : <https://ici.radio-canada.ca/nouvelle/1711007/amazon-rekognition-reconnaissance-faciale-police>.

⁸⁷ International civil liberties monitoring group, "Open letter: canadian government must ban use of facial recognition by federal law enforcement, intelligence agencies", 8 Juillet 2020 : <https://iclmg.ca/facial-recognition-letter>.

⁸⁸ Ada Lovelace Institute, "Beyond face value : public attitudes to facial recognition technology", Septembre 2019 : https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf.

seulement font confiance aux services de police dans l'usage de la reconnaissance faciale mais font encore moins confiance aux publicitaires ou entreprises privées⁸⁹.

Bien souvent, lorsque les États cherchent à instaurer des mesures visant à une plus grande sécurité, certaines limitations aux libertés des citoyens sont introduites, sans pour autant omettre la recherche d'un juste équilibre⁹⁰. Cet équilibre est appelé à changer en fonction des menaces, selon leur gravité ou leur imminence⁹¹. La légitimité sociale de ces mesures va s'évaluer en fonction de plusieurs critères comme l'inclusion de la population dans les processus de prise de décision. La prise en considération des aspects individuels, du contexte social et d'un équilibre entre les coûts et les avantages pourraient favoriser une plus grande acceptabilité sociale des mesures de sécurité⁹². Les limitations devront répondre à des objectifs d'intérêt général ou de protection des droits et libertés des individus, tout en restant justifié et proportionné aux droits de l'Homme⁹³.

Dans ce contexte, la légalité mais aussi la légitimité des procédés mis en place sont essentiels pour éviter que les forces de police subissent une perte de confiance de la population. Les exemples sont légion aux États-Unis et la dénonciation des violences policières, ainsi que les débats autour de l'utilisation des caméras corporelles (*body cam*) par les policiers montrent une certaine défiance de la population envers les personnels pourtant chargés de la protéger. C'est ainsi que les images des caméras corporelles ont pu être utilisées pour faire de la reconnaissance faciale plutôt que de servir de preuve et moyen de pacifier les relations entre les forces de l'ordre et la population.

Risques inhérents aux partenariats avec des opérateurs privés

Un autre risque résulte pour les services de police de recourir à des entreprises privées pour mettre en place un dispositif de reconnaissance faciale. Le choix du prestataire suppose des vérifications sur les pratiques de ces acteurs privés, compte tenu des risques d'atteinte aux droits et libertés fondamentaux. 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, ce partenaire privé doit respecter les lois sur la protection des renseignements personnels applicables aux entreprises privées. Rappelons aussi que la loi québécoise sur

⁸⁹ Pew Research Center, "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly", Septembre 2019 : <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly>.

⁹⁰ Mark Neocleous, "Security, Liberty and the Myth of Balance : Towards a Critique of Security Politics, Contemporary Political Theory", London Vol. 6, n°2, Mai 2007, p.131-132

⁹¹ Jeremy Waldron, "Security and Liberty : The Image of Balance", The Journal of Political Philosophy, Vol. 11, n°2, 2003, p.192

⁹² Mathias Bug, Sebastian U. Bukow, "Civil Liberties vs. Security : Why Citizens Accept or Reject Digital Security Measures", German Politics, Vol. 26 Issue 2, Juin 2017, p.293

⁹³ European Union agency for fundamental rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019, p. 21 : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

l'accès aux documents des organismes publics et sur la protection des renseignements personnels s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers (art. 1^{er}). L'exemple de Clearview AI confirme les risques inhérents au choix de partenaires extérieurs. Également, un enjeu de dépendance peut également se poser si les forces de police deviennent dépendantes d'une solution privée qu'elles ne maîtrisent 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. Ce risque est d'autant plus fort qu'il y a enfin un enjeu d'asymétrie d'expertise. Le secteur public ne dispose pas des agents capables d'apprécier dans tous les détails les propositions formulées par les acteurs privés, *a fortiori* s'agissant de technologies complexes comme la reconnaissance faciale.

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. Si les gouvernements canadien et québécois décident d'aller de l'avant dans les projets de déploiement de la reconnaissance faciale à des fins policières et sécuritaires, ils devront prendre en compte ces risques pour la sécurité nationale et devront être très vigilants dans le choix de leurs partenaires privés.

5. Cadre légal de la reconnaissance faciale au Canada et au Québec

5.1. Chartes canadiennes et québécoises des droits et libertés et reconnaissance faciale

Libertés d'aller et venir, de réunion et de manifestation, droit à la vie privée et principe d'égalité

Le recours à des outils de reconnaissance faciale par les services de police dans l'espace public ne doit pas entraver le respect des droits et libertés individuelles garantie par la Charte canadienne et la Charte québécoise. Comme vu précédemment, ce type de technologies peut porter atteinte en particulier à 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). Doivent aussi être respectés le droit à la vie privée (art. 8 de la Charte canadienne des droits et libertés et article 5 de la Charte québécoise des droits et libertés de la personne) et le principe d'égalité et de 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. L'application de l'article 8 de la Charte à la reconnaissance faciale soulève des enjeux notamment en relation au droit à l'anonymat, aux attentes raisonnables à l'égard de son image en public, à l'autorisation légale requise pour effectuer cette surveillance. L'application de l'article 8 mérite une analyse plus poussée qui dépasse les limites du rapport.

5.2. Loi fédérale applicable à la reconnaissance faciale et la GRC (secteur public)

Cadre légal de la protection des renseignements personnels dans le secteur public

Seront envisagées ici uniquement les législations du secteur public susceptibles de s'appliquer aux missions des forces de police. Bien que des départements de police au Canada aient commencé à utiliser des technologies de reconnaissance faciale, le gouvernement fédéral n'a pas de politique ni de loi spécifique à la collecte de données biométriques qui constituent des caractéristiques physiques et comportementales pouvant être utilisées pour identifier numériquement les personnes. Dès lors, il n'y a pas de standard minimum de protection de la vie privée, de minimisation des risques ou de transparence

publique spécifiquement applicable à la biométrie ou à la reconnaissance faciale. Il faut donc s'en remettre plus généralement aux lois sur les renseignements personnels.

La loi sur la protection des renseignements personnels⁹⁴ concerne le secteur public et régit les informations personnelles que les entités fédérales peuvent collecter, utiliser, divulguer et conserver. Elle ne vise pas spécifiquement la reconnaissance faciale mais l'article 3 (d) donne la définition des renseignements personnels qui concernent un individu identifiable et notamment ses empreintes digitales. Dès lors, l'ensemble des données biométriques comme la reconnaissance faciale sont incluses dans le champ d'application matériel de la loi, dès lors qu'elles permettront d'identifier un individu.

La loi sur la protection des renseignements personnels a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent (art. 2). Elle ne s'applique donc pas aux forces de police provinciales et municipales qui relèvent des réglementations provinciales. Seule la GRC est sujette à cette loi.

L'article 4 prévoit que les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux ayant un lien direct avec ses programmes ou ses activités. Également, à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution, de même que pour les usages qui sont compatibles avec ces fins (art. 7(a)). La GRC peut donc collecter uniquement les informations directement en lien avec son mandat en tant que force de police nationale du Canada. Enfin, il en est de même de la communication des renseignements personnels (art. 8(a)).

Limites du cadre légal des renseignements personnels dans le secteur public

Le principe de finalité qui encadre ainsi la collecte, l'utilisation et la communication des renseignements personnels s'applique à l'utilisation de la reconnaissance faciale par la GRC dans le cadre de ses actions de police. En dehors de ce principe, aucune autre exigence ne s'applique. On peut légitimement se demander si ce cadre est suffisant aujourd'hui. Il est à noter que la nouvelle concernant l'utilisation de l'outil de reconnaissance faciale de la société Clearview AI par la GRC a été diffusée suite à une fuite d'informations⁹⁵. En vue d'améliorer l'acceptabilité sociale et un meilleur dialogue entre les services de police et la population, une réforme doit établir des politiques et lois claires et transparentes réglementant l'utilisation de cette technologie, y compris des réformes de la loi fédérale. Il pourrait par exemple être

⁹⁴ L.R.C. (1985), ch. P-21.

⁹⁵ Nicolas de Rosa, « La GRC et 34 services policiers canadiens ont utilisé l'application de Clearview AI » (28 février 2020), Radio-Canada : <https://ici.radio-canada.ca/nouvelle/1641195/clearview-ai-canada-police-grc-entreprise-via-rail-liste-client-vol-donnees-intelligence-artificielle-reconnaissance-faciale-logiciel-application-controverse>.

envisagé de créer de nouvelles obligations d'information du public, afin de garantir plus de transparence et redevabilité des forces de police.

Par ailleurs, le CPVP a constaté un risque de violation du principe de finalité. Ainsi, « les renseignements personnels ne doivent être utilisés qu'aux fins pour lesquelles ils ont été recueillis. Dans le domaine de la biométrie, le risque d'utilisations multiples découle du fait que certaines caractéristiques, comme les empreintes digitales, sont relativement permanentes et très distinctives, ce qui en fait un élément d'identification très pratique à la fois constant et universel. Une fois l'élément d'identification saisi et emmagasiné dans une base de données, il est facile d'y avoir accès et de le comparer à des échantillons futurs, même si ceux-ci sont réunis dans des contextes complètement différents »⁹⁶. Il y a là un risque non négligeable de glissement de finalité qui n'est pas suffisamment encadré.

Recommandations du CPVP en cas de projet biométrique dans le secteur public

Le CPVP avertit du fait que plusieurs types de renseignements biométriques, comme les empreintes digitales et les images du visage, peuvent être recueillis à l'insu d'une personne et, à plus forte raison, sans son consentement. Ils peuvent donc servir à surveiller subrepticement les déplacements et le comportement d'une personne. Il invite les organisations gouvernementales à réfléchir avant de proposer des projets qui comprennent la collecte, l'utilisation ou la communication de renseignements biométriques.

Le CPVP a ainsi précisé les conditions de mise en œuvre d'un projet biométrique⁹⁷. Les préoccupations en matière de protection de la vie privée devraient être traitées à toutes les étapes de l'élaboration du projet, de sa conception à sa mise en œuvre en passant par son évaluation et même sa suppression. En particulier, l'évaluation des facteurs relatifs à la vie privée (EFVP) est un processus visant à aider les organisations à tenir compte de l'incidence, sur la vie privée, d'un projet nouveau ou profondément modifié, surtout lorsqu'il implique la collecte de renseignements personnels. Ce processus est obligatoire dans le secteur public. Les organismes fédéraux qui proposent un programme, une politique ou un service ayant des répercussions sur la protection de la vie privée doivent ainsi présenter une évaluation des facteurs relatifs à la vie privée au Commissariat aux fins d'examen⁹⁸. Avant d'établir un

⁹⁶ Commissariat à la protection de la vie privée du Canada, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée », Février 2011 : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102.

⁹⁷ Ibid.

⁹⁸ Par exemple, Passeport Canada a collaboré avec le Commissariat pendant plusieurs années dans le cadre de ses activités visant à déceler et à atténuer les risques pour la vie privée liés à l'utilisation d'un passeport électronique comprenant des renseignements biométriques enregistrés sur une puce électronique. Le processus d'évaluation des facteurs relatifs à la vie privée nous a permis de formuler les recommandations suivantes :

- enregistrer sur la puce uniquement les données essentielles pour les passeports;
- sécuriser les renseignements stockés sur la puce;

nouveau système (notamment de nature biométrique), l'organisation doit justifier clairement les ingérences éventuelles dans la vie privée.

Pour donner une orientation à cette démarche, le Commissariat invite les organisations à appliquer le critère en quatre parties, qui est une adaptation de l'arrêt *R. c. Oakes* rendu en 1986 par la Cour suprême du Canada⁹⁹ (dit test Oakes). Le critère évalue la pertinence d'une mesure qui pourrait porter atteinte à la vie privée en fonction de quatre questions :

1. Est-il démontré que la mesure est nécessaire pour répondre à un besoin précis? (principe de nécessité)
2. Répondra-t-elle vraisemblablement efficacement à ce besoin? (principe d'efficacité)
3. La perte au chapitre de la vie privée serait-elle proportionnelle à l'avantage obtenu? (principe de proportionnalité)
4. Existe-t-il un moyen moins envahissant d'arriver au même but? (recherche de solutions alternatives).

5.3. Lois du Québec applicables à la reconnaissance faciale et les polices (provinciale et municipales) (secteur public)

Seront envisagées ici uniquement les législations du secteur public susceptibles de s'appliquer aux missions des forces de police. Tout comme le Canada, le Québec n'a pas non plus de loi spécifique applicable à la collecte et l'usage des données biométriques ou de la reconnaissance faciale. Il en est de même des autres provinces et territoires du Canada dans lesquels il convient de se reporter aux lois de protection des renseignements personnels du secteur public. Les dispositions pertinentes de ces lois sont détaillées en annexe.

Dès lors, l'utilisation des technologies de reconnaissance faciale est essentiellement encadrée par la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels¹⁰⁰, ainsi que par la loi concernant le cadre juridique des technologies de l'information¹⁰¹.

-
- veiller à leur suppression adéquate;
 - éviter d'établir des bases de données centralisées contenant des renseignements biométriques;
 - sensibiliser les citoyens et obtenir leur consentement dans le cadre de campagnes d'information publique.

⁹⁹ *R. c. Oakes*, [1986] 1 R.C.S. 103.

¹⁰⁰ Chapitre A-2.1 - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels : <http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1>.

¹⁰¹ Chapitre C-1.1 - Loi concernant le cadre juridique des technologies de l'information : <http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/C-1.1>.

Cadre légal de la protection des renseignements personnels (principales dispositions)

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers. Elle s'applique quelle que soit la forme de ces documents: écrite, graphique, sonore, visuelle, informatisée ou autre (art. 1^{er}). Seront concernés les organismes relevant du gouvernement du Québec et les municipalités du Québec. Sont donc visées les services de Sécurité Québec et les services des polices municipales, au premier rang desquelles se trouve le Service de Police de la Ville de Montréal (SPVM). Sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier (art. 54).

Principaux droits des organismes publics

La loi accorde aux organismes publics auxquels appartiennent les services de police certains droits. Ainsi, en principe, un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée, sauf si l'organisme public est chargé, en vertu de la loi, de prévenir, détecter ou réprimer le crime ou les infractions aux lois et si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec (art. 59-3^o). Outre les cas prévus à l'article 59, un organisme public peut également communiquer un renseignement personnel, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence (art. 59.1).

En outre, un corps de police peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à un autre corps de police (art. 61). Plus généralement, un renseignement personnel est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions (art. 62). Enfin, un organisme public peut communiquer des renseignements personnels pour les comparer à un autre fichier détenu par une personne ou un organisme sans avoir besoin que la personne concernée y consente (art. 68.1 al.1).

Enfin, si en principe la personne concernée par une collecte de ses renseignements personnels doit être informée notamment « du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite, de la finalité, des catégories de personnes qui y auront accès, du caractère obligatoire ou facultatif de la demande, (et) des conséquences en cas de refus » (art. 65 al. 1 et 2), ce droit à l'information disparaît en cas d'enquête de nature judiciaire ou d'une enquête ou un constat, faits par un organisme chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois (art. 65 al. 5).

Principales obligations des organismes publics

Les organismes publics doivent toutefois respecter certaines obligations de sécurité, finalité et exactitude des renseignements personnels. Ils doivent ainsi prendre des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support (art. 63.1). Les services de police détiennent par définition de nombreux renseignements personnels sensibles dont ils doivent garantir la sécurité.

Par ailleurs, nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion (art. 64). Si en principe un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli, il peut toutefois être utilisé à une autre fin avec le consentement de la personne concernée ou, sans son consentement, dans certains cas. Il en est ainsi notamment lorsque son utilisation se fait à des fins compatibles avec celles pour lesquelles il a été recueilli (art. 65.1) ou encore lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi (art. 65.3).

Les services de police pourraient se fonder sur de telles circonstances pour justifier un changement de finalité. Mais on peut se demander par exemple si la collecte d'images dans le cadre de certaines finalités comme la délivrance de titres d'identités (passeports, visa, permis de travail, d'étude ou de conduire) pourrait fonder la réutilisation de ces renseignements personnels à d'autres fins comme dans le cadre d'enquêtes judiciaires.

Enfin, un organisme public doit veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés (art. 72). Les dispositifs de reconnaissance faciale sont encore aujourd'hui insuffisamment précis, notamment en raison d'erreurs qui surviennent à l'étape 2 de numérisation des caractéristiques de l'image pour la transformer en donnée biométrique.

On peut là aussi se demander si cette obligation d'exactitude pourrait s'appliquer au procédé et aux données biométriques, ce qui permettrait de fonder une obligation de nature à lutter contre le risque d'erreur.

Fichier confidentiel et restrictions aux droits d'accès et rectification

Par ailleurs le gouvernement peut, par décret, autoriser un organisme public à établir un fichier confidentiel. Un fichier confidentiel est un fichier constitué principalement de renseignements personnels destinés à être utilisés par une personne ou un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois (art. 80). En principe, les personnes concernées par un renseignement personnel ont un droit d'accès (art. 83) et de rectification (art. 89), mais un organisme public peut refuser de

confirmer à une personne l'existence, dans un fichier confidentiel, d'un renseignement personnel la concernant ou de lui en donner communication (art. 86).

Si l'utilisation de la reconnaissance faciale entre dans le cadre de la loi sur la collecte de renseignements personnels, les caractéristiques de cette technologie ne sont pas prises en compte, ce qui limite la protection et témoigne de l'inadaptation de la loi. En outre, l'application de ces règles à la reconnaissance faciale soulève de nombreuses questions d'interprétation, notamment sur les droits accordés aux services de police dans le recours à cette technologie, en particulier s'agissant du changement de finalité. Une clarification et adaptation de la loi s'impose.

Cadre légal des technologies de l'information

Obligations de sécurité du responsable de l'accès aux documents électroniques

La loi concernant le cadre juridique des technologies de l'information (LCJTI) adoptée en 2001 prévoit des mesures de protection. L'article 25 dispose que « la personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder ».

Confidentialité, intégrité et sécurité des documents électroniques confiés à des prestataires de services

Également, l'article 26 al. 1^{er} de la loi dispose que « quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance ». L'alinéa 2 ajoute que « le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document ».

Données biométriques

La loi concernant le cadre juridique des technologies de l'information prévoit des mesures de protection contre les risques que font courir les données biométriques¹⁰². L'article 44 al. 1^{er} pose que « nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance ».

Cette disposition interdit d'exiger, sans le consentement valide et exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Le consentement est donc au cœur du dispositif, ce qui suppose qu'en principe les renseignements biométriques ne peuvent être collectés à l'insu de la personne. En outre, le consentement doit être libre, clair, spécifique et limité dans le temps.

Divulcation préalable à la Commission d'accès à l'information de la constitution d'une banque de données biométriques

La loi concernant le cadre juridique des technologies de l'information confie un large pouvoir à la Commission d'accès à l'information (CAI) à l'égard des banques de données biométriques. L'article 45 al. 1^{er} dispose que la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la CAI. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service. La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne (art. 45 al. 2). Elle peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée (art. 45 al. 3). La CAI met ainsi à disposition en ligne un formulaire de déclaration d'une banque de caractéristiques ou de mesures biométriques¹⁰³. Cette déclaration inclut les outils de reconnaissance faciale.

Exigences de la Commission d'accès à l'information envers les systèmes biométriques

La CAI a publié en juillet 2020 un guide d'accompagnement pour les organismes publics et les entreprises intitulé : « Biométrie : principes à respecter et obligations légales des

¹⁰² Voir Julie M. Gauthier, *Le droit de la biométrie au Québec : sécurité et vie privée*, Éditions Yvon Blais, 2015.

¹⁰³ Commission d'accès à l'information, « Formulaire de déclaration d'une banque de caractéristiques ou de mesures biométriques » : https://www.cai.gouv.qc.ca/documents/CAI_FO_banque_bio.pdf.

organisations »¹⁰⁴. Ce guide s'adresse tant aux organismes publics qu'aux entreprises¹⁰⁵ qui souhaitent utiliser un système biométrique et qui en sont responsables. Il concerne aussi les entreprises qui fournissent ces solutions aux organisations pour les aider à conseiller leurs clients et proposer des produits respectueux de la législation applicable au Québec.

Le guide expose la démarche à accomplir par les organismes publics ou privés souhaitant mettre en œuvre un dispositif biométrique. Elle peut se résumer en trois étapes : faire une analyse préliminaire, déclarer la banque auprès de la CAI, respecter les obligations.

L'**analyse préliminaire** suppose de connaître la législation applicable (telle que rappelée ci-dessus) et de tenir compte du caractère sensible des renseignements personnels biométriques lors de l'évaluation tant de la légalité du projet envisagé que des obligations à respecter lors du déploiement de la solution retenue. Le meilleur moyen de faire cette évaluation est de réaliser une évaluation des facteurs relatifs à la vie privée pour laquelle la CAI a publié un autre guide d'accompagnement intitulé « Évaluation des facteurs relatifs à la vie privée »¹⁰⁶. L'évaluation des facteurs relatifs à la vie privée, ci-après appelée « EFVP » (ou en anglais *privacy impact assessment* « PIA »), est un processus permettant de déterminer si certains projets impliquant l'utilisation de renseignements personnels posent des risques en matière de protection de la vie privée. Les EFVP permettent de détecter ces risques et de proposer des solutions visant à les éliminer ou les minimiser. Elles doivent être réalisées en amont du projet et impliquer toutes les parties prenantes au sein de l'entreprise ou de l'organisme public.

En ce sens, la CAI rappelle qu'avant même de décider la mise en place d'un système biométrique dans une organisation, il convient de respecter le principe essentiel de nécessité. Ce principe implique de se demander s'il est nécessaire de recueillir des renseignements personnels dont des mesures ou des caractéristiques biométriques (art. 64 de la loi sur l'accès). Pour satisfaire ce principe de nécessité, l'objectif poursuivi par la collecte doit être important, légitime et réel pour résoudre une situation problématique.

En outre, la collecte doit être proportionnée à l'objectif poursuivi, en tenant compte des autres moyens à disposition et des conséquences pour les personnes concernées. La nature sensible des renseignements biométriques doit être prise en compte dans l'évaluation, alors même que la collecte de données de cette nature constitue un degré d'intrusion élevé dans la vie privée des individus. Il faut en particulier poser la question de savoir si les avantages de recourir à la biométrie sont plus importants que l'atteinte à la vie privée des personnes concernées. La balance des intérêts doit se faire en documentant les avantages et

¹⁰⁴ Commission d'accès à l'information, « Biométrie : principes à respecter et obligations légales des organisations, Guide d'accompagnement », Juillet 2020 : https://www.cai.gouv.qc.ca/documents/CAI_G_biometrie_principes-application.pdf.

¹⁰⁵ Les entreprises seront soumises à la loi sur la protection des renseignements personnels dans le secteur privé.

¹⁰⁶ Commission d'accès à l'information (CAI), « Évaluation des facteurs relatifs à la vie privée : Savoir détecter et atténuer les risques d'atteinte aux renseignements personnel », Fiche Info, Janvier 2018 : https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf.

inconvenients du système biométrique envisagé. Si la preuve de la nécessité a pu être rapportée, seules doivent être collectées les mesures biométriques essentielles à l'établissement ou vérification de l'identité.

Il est à noter que l'utilisation de la reconnaissance faciale par les services de police au Québec doit satisfaire ces exigences. Néanmoins, compte tenu de la nature de leur mission, la preuve de la nécessité devrait pouvoir être rapportée selon les cas d'usage considérés, comme par exemple en cas d'enquête judiciaire.

À la suite de cette analyse préliminaire, l'organisation doit **déclarer à la CAI** la banque de caractéristiques ou mesures biométriques. La CAI peut interdire la mise en service ou rendre une ordonnance obligeant à des modifications du projet ou ordonner la destruction de la banque.

Enfin, lors de la **mise en place d'un système biométrique**, il convient d'obtenir le consentement exprès des personnes concernées ou de prévoir un autre moyen d'identification en cas de refus. En effet, rappelons que l'article 44 de la loi concernant le cadre juridique des technologies de l'information interdit d'exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Un formulaire de consentement est disponible sur le site internet de la Commission d'accès à l'information¹⁰⁷. Enfin, des mesures fortes de sécurité et de confidentialité doivent être mises en place, qu'il s'agisse de la sécurité physique, informatique, logique et organisationnelle. En ce sens, doit aussi être considéré le lieu de stockage des données, afin de privilégier un prestataire de services infonuagiques situé sur le territoire québécois.

Par ailleurs, lorsque l'objectif associé à la collecte des caractéristiques ou des mesures biométriques a été accompli, la CAI souligne la nécessité de détruire ces données. En outre, tout tiers qui fournit des services impliquant l'accès à la banque doit aussi procéder à la destruction.

Questionnements sur l'application aux forces de police des obligations liées à l'utilisation de la biométrie

En résumé, il existe déjà au Québec une législation qui a vocation à encadrer les technologies fondées sur la biométrie. Il convient cependant aujourd'hui de vérifier si cette législation encadre toujours adéquatement le déploiement des technologies fondées sur la biométrie¹⁰⁸, en particulier dans le cadre de son utilisation par les forces de police dans l'espace public. Le respect des droits fondamentaux doit être garanti comme le rappelle la CAI dans son guide,

¹⁰⁷ Commission d'accès à l'information (CAI), Exemple de formulaire de consentement sur la cueillette, l'usage et la conservation de caractéristiques ou de mesures biométriques : https://www.cai.gouv.qc.ca/documents/CAI_FO_consentement_bio.pdf.

¹⁰⁸ Pierre Trudel, « Reconnaissance faciale : de San Francisco à Montréal » (21 Mai 2019), Le Devoir : <https://www.ledevoir.com/opinion/chroniques/554765/reconnaissance-faciale-de-san-francisco-a-montreal>.

en particulier par la mise en balance des intérêts et le respect des principes de nécessité et proportionnalité.

La mise en œuvre de l'article 44 de la loi concernant le cadre juridique des technologies de l'information et le principe du consentement de la personne concernée pose un certain nombre de questions s'agissant des forces de police et de la finalité de la collecte de ces données. Si, en principe, la collecte doit avoir lieu avec le consentement des personnes concernées, un tel consentement ne pourra par hypothèse être obtenu, dans le cadre d'une enquête. En revanche, lorsqu'il s'agit par exemple de recueillir les images et empreintes digitales pour établir un passeport électronique, le consentement sera aisément obtenu et permettra de constituer légalement une banque de données après déclaration à la CAI et sous réserve du respect des exigences légales. Dès lors, une telle base de données pourrait-elle être utilisée à d'autres fins, notamment pour des motifs de sécurité intérieure ? La question du glissement de finalité est à nouveau posée.

En outre, l'affaire Clearview AI pose une autre question en matière de cadre légal applicable à la reconnaissance faciale utilisée par les forces de police. Dans ces circonstances, la base de données d'images associant des procédés de reconnaissance faciale est constituée par Clearview qui met son outil à la disposition des forces de police. Même s'il n'apparaît pas à ce stade que les services de police du Québec aient pu utiliser ce service, la base de données a été principalement constituée à partir d'images captées sur les réseaux sociaux sans le consentement de ces opérateurs privés ni des personnes concernées. L'enquête des autorités de protection des renseignements personnels est en cours mais il ne semble pas que la banque de données biométriques ait été légalement constituée. Dès lors, son usage par les services de police est-il automatiquement illégal ? Faut-il distinguer la situation du prestataire qui constitue la base de celle qui l'utilise ? Faut-il considérer des règles spéciales à des fins de sécurité intérieure pour permettre la collecte de données biométriques moyennant des garanties pour protéger les droits et libertés individuelles ? L'exigence du consentement est-elle aujourd'hui toujours adaptée ? Autant de questions qui montrent la nécessité d'une réflexion sur l'adaptation des lois québécoises face aux évolutions technologiques, en particulier l'adéquation des réglementations sur la protection des renseignements personnels mais aussi plus largement le cadre légal spécifique de la reconnaissance faciale.

5.4. Projet de réforme de la loi du Québec sur la protection des renseignements personnels (projet de loi n° 64)

Un projet de loi visant à moderniser les dispositions protégeant les renseignements personnels (projet de loi n° 64) a été présenté en juin 2020 par Madame Sonia LeBel, Ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information. Il sera à l'étude à la reprise des travaux parlementaires à l'automne 2020. Bien que la réforme envisage de modifier largement les législations des renseignements

personnels du secteur public et du secteur privé¹⁰⁹, seront uniquement présentées ici les principales mesures envisagées, susceptibles de s'appliquer à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public.

Renforcement du consentement

Le projet de loi envisage d'insérer, après l'article 53, un nouvel article 53.1, afin de préciser les conditions d'expression du consentement. Ce dernier doit être « manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé ». En outre, « le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé ». Il est sans effet s'il n'est pas donné conformément à la loi. Également, s'agissant des renseignements personnels sensibles, le consentement doit être manifesté de façon expresse (art. 59 modifié).

Le projet de loi envisage les conditions d'obtention du consentement du mineur : « le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale. Le consentement du mineur de 14 ans et plus est donné par le mineur ou par le titulaire de l'autorité parentale ».

Ces dispositions auront toutefois peu d'incidence sur l'utilisation des renseignements personnels par les services de police puisque la loi les autorise à le faire sans le consentement des personnes concernées, dès lors qu'ils sont chargés, en vertu de la loi, de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Reconnaissance de renseignements personnels « sensibles »

L'article 59.3., tel que proposé par le projet de loi n° 64 prévoit de reconnaître une nouvelle catégorie de renseignements personnels « sensibles », lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, le renseignement « suscite un haut degré d'attente raisonnable en matière de vie privée ».

Compte tenu à la fois de la nature biométrique des renseignements associés à l'utilisation des outils de reconnaissance faciale et du contexte de leur application par les forces de police dans l'espace public, cette qualification devrait s'appliquer aux types de renseignements et usages dans le contexte de cette étude. Cette interprétation est d'ailleurs confirmée par le CPVP et la CAI¹¹⁰ qui considèrent que les renseignements biométriques sont sensibles.

¹⁰⁹ Chapitre P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé : <http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1>.

¹¹⁰ Commission d'accès à l'information (CAI), « La biométrie au Québec », Fiche Info, Janvier 2016 : https://www.cai.gouv.qc.ca/documents/CAI_FL_biometrie.pdf.

Cette définition a l'avantage de permettre une souplesse et rend possible les évolutions, tout en tenant compte des cas d'usage. Elle pourrait toutefois susciter des problèmes d'interprétation lors de son application. En comparaison, l'Union européenne a fait le choix depuis la directive de 1995/46/CE du 25 octobre 1995, d'énumérer les données sensibles ce qui est confirmé par le RGPD dont la liste a été élargi. Cette méthode présente donc l'inconvénient de devoir susciter une intervention législative à chaque avancée technologique ou sociétale mais a l'avantage de la clarté et de la sécurité juridique.

Transparence et gouvernance des renseignements personnels

Le nouvel article 63.3, tel que proposé par le projet de loi, prévoit que : « un organisme public doit publier sur son site Internet des règles encadrant sa gouvernance à l'égard des renseignements personnels. Ces règles doivent être approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels. Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles incluent une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels ».

Ces dispositions de transparence et gouvernance des renseignements personnels sont bienvenues et de nature à informer le public, spécialement en cas d'usage des dispositifs de reconnaissance faciale souvent ignorés du grand public.

Publication d'une politique de confidentialité

En outre, le nouvel article 63.4., issu du projet de loi, prévoit que « un organisme public qui recueille par un moyen technologique des renseignements personnels doit publier sur son site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Il fait de même pour l'avis dont toute modification à cette politique doit faire l'objet. Un règlement du gouvernement peut déterminer le contenu et les modalités de cette politique et de cet avis ».

Le recours à un dispositif de reconnaissance faciale par un organisme public suppose par définition la collecte de renseignements personnels par un moyen technologique. Ces dispositions ont donc vocation à s'appliquer en cas d'usage par les forces de l'ordre dans l'espace public et renforcent aussi la transparence, la confiance et la minimisation des risques.

Évaluation des facteurs relatifs à la vie privée (EFVP) de tout projet de système d'information

Le nouvel article 63.5 du projet de loi ajoute que « un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Aux fins de cette évaluation, l'organisme public doit consulter, dès le début du projet, son comité sur l'accès à l'information et la protection des renseignements personnels. Cet organisme public doit également s'assurer que ce projet permet qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé ».

L'évaluation des facteurs relatifs à la vie privée, telle que recommandée par la CAI en matière biométrique, est désormais rendue obligatoire par la loi. Cette dernière conforte donc les recommandations de la Commission. Ces dispositions vont dans le sens d'une étude préalable d'impact des dispositifs de reconnaissance faciale sur la vie privée ce qui permettra de vérifier en amont les principes de nécessité, efficacité et proportionnalité. Ces mesures vont aussi dans le sens de la reconnaissance d'une protection de la vie privée dès la conception.

Rôle du comité sur l'accès à l'information et mesures de protection des renseignements personnels

Le projet de loi prévoit la mise en œuvre, au sein des organismes publics, d'un comité sur l'accès à l'information et la protection des renseignements personnels. Ce comité est chargé de soutenir ces organismes dans l'exercice de leurs responsabilités et dans l'exécution de leurs obligations en vertu de la loi (art. 8 du projet de loi).

L'article 63.6., prévu par le projet de loi, dispose que : « Le comité peut, à toute étape d'un projet visé à l'article 63.5, suggérer des mesures de protection des renseignements personnels applicables à ce projet, telles que : 1^o la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels; 2^o des mesures de protection des renseignements personnels dans tout document relatif au projet, tel un cahier des charges ou un contrat; 3^o une description des responsabilités des participants au projet en matière de protection des renseignements personnels; 4^o la tenue d'activités de formation sur la protection des renseignements personnels pour les participants au projet ».

Ce comité devrait donc être au centre du respect de la loi, en particulier dans la mise en œuvre d'un dispositif de reconnaissance faciale dans l'espace public par les services de police.

Incident de confidentialité et notification à la Commission et aux personnes concernées

Par ailleurs, l'article 63.7 prévoit que « un organisme public qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser la Commission. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Il peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication ». Cependant, « une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article ».

On entend par « incident de confidentialité » : 1° l'accès non autorisé par la loi à un renseignement personnel; 2° l'utilisation non autorisée par la loi d'un renseignement personnel; 3° la communication non autorisée par la loi d'un renseignement personnel; 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement (art. 63.8).

En dépit des mesures de sécurité que doivent prendre les organismes publics envers les renseignements personnels, des failles de sécurité sont toujours possibles et il convient alors de tout mettre en œuvre pour minimiser les risques inhérents aux fuites. Les mesures à prendre dépendront des risques de préjudice pour les personnes concernées. « Lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, un organisme public doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. L'organisme doit également consulter son responsable de la protection des renseignements personnels » (nouvel article 63.9). « Un organisme public doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre. Sur demande de la Commission, une copie de ce registre lui est transmise » (nouvel article 63.10).

Information en cas d'usage de technologies d'identification, localisation et profilage

Par ailleurs, en plus des informations devant être fournies suivant l'article 65, le nouvel article 65.0.1. prévoit une obligation d'information supplémentaire : « quiconque recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci doit, au préalable, l'informer :

- 1° du recours à une telle technologie;
- 2° des moyens offerts, le cas échéant, pour désactiver les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne ».

Ces dispositions peuvent tendre à remettre en cause l'utilisation de la reconnaissance faciale qui peut conduire au profilage. Toutefois, lorsque ce type de technologies est utilisé par les services de police dans le cadre d'une enquête par exemple, il reste à définir les conditions de mise en œuvre de cette information et éventuellement admettre une exception à cette information qui paraît contredire l'efficacité d'une enquête.

Exceptions au principe de finalité et au consentement

Le projet de loi prévoit de modifier ainsi les deux premiers alinéas de l'article 65.1 de la loi sur l'accès : « Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible. L'organisme public peut toutefois utiliser un renseignement personnel à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants :

- 1° lorsque son utilisation est à des fins compatibles avec celles auxquelles il a été recueilli ;
- 2° lorsque son utilisation est manifestement au bénéfice de la personne concernée ;
- 3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
- 4° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé ».

En tout état de cause, ce régime d'exceptions va permettre aux organismes publics de se libérer du principe de finalité et de la recherche d'un consentement de la personne

concernée. Si on envisage la question posée précédemment de la réutilisation des données biométriques pour d'autres finalités, par exemple l'utilisation des images collectées pour la délivrance de titres d'identité ou d'immigration dans le cadre d'un dispositif de reconnaissance faciale par les services de police dans le cadre d'une enquête, une telle réutilisation pourrait être couverte par la 3^{ème} exception. Il faudrait alors qu'une loi du Québec justifie une telle utilisation même en l'absence d'une autorisation expresse et il paraît souhaitable dans ce cadre de faire adopter une loi dédiée pour le permettre expressément et prévoir des garanties pour les droits et libertés.

Communication de renseignements personnels d'un organisme public à toute personne ou organisme

En ce sens, le nouvel article 67 proposé par le projet de loi dispose que « un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme lorsque cette communication est nécessaire à l'application d'une loi au Québec et lorsque cette communication :

1° est prévue expressément par la loi;

2° n'est pas prévue expressément par la loi, est ponctuelle et, s'il y a aussi communication de renseignements personnels concernant toute autre personne, lorsque ces renseignements n'en concernent qu'un nombre restreint;

ou 3° n'est pas prévue expressément par la loi et s'effectue conformément aux deuxième, troisième et quatrième alinéas de l'article 68 ».

Il y a donc bien là aussi des moyens pour les forces de police d'obtenir des informations et en particulier des images détenues par d'autres services et organismes publics à l'occasion de l'accomplissement d'autres missions.

Notons que d'autres dispositions permettent la communication de renseignements personnelles à des fins d'étude, de recherche ou de production de statistiques. L'utilisation des dispositifs de reconnaissance faciale par les forces de police ne devrait *a priori* pas tomber sous le coup de ces exceptions.

Information en cas de décision fondée sur un traitement automatisé

Le projet de loi prévoit d'ajouter un article 65.2. à la loi sur l'accès particulièrement intéressant. Il dispose que : « Un organisme public qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit, au moment de la décision ou avant, en informer la personne concernée. Il doit aussi, à la demande de la personne concernée, l'informer :

1° des renseignements personnels utilisés pour rendre la décision;

2° des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;

3° de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision ».

Les organismes publics prennent de plus en plus de décisions au moyen de logiciels ou procédés automatiques¹¹¹. La plupart des procédés sont des aides à la décision comme par exemple en matière d'immigration¹¹² mais pourrait devenir des moyens pour prendre exclusivement les décisions, c'est-à-dire sans contrôle humain. La loi impose alors une obligation d'information qui porte non seulement sur les renseignements personnels utilisés mais aussi sur les raisons facteurs et paramètres ayant mené la décision.

Cette disposition n'est pas sans rappeler le droit de l'Union européenne et l'article 13.2. f) du RGPD mais il faut saluer ici le fait que l'information porte sur la décision individuelle et non pas sur les procédés ou critères utilisés de façon globale. Le RGPD évoque pour sa part la divulgation des « informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». En revanche, le projet de loi ne va pas jusqu'à accorder le droit de ne pas faire l'objet d'une telle prise de décision automatisée exclusive, contrairement à ce que permet l'article 22 du RGPD.

Désignation d'un gestionnaire de renseignements personnels

Le projet de loi prévoit d'ajouter un nouvel article 70.3 à la loi sur l'accès pour permettre au gouvernement après consultation de la Commission, de « désigner un ou plusieurs organismes publics pour exercer la fonction de gestionnaire de renseignements personnels lorsqu'il juge que cela est dans l'intérêt public ou au bénéfice des personnes concernées. Un gestionnaire de renseignements personnels recueille, utilise ou communique des renseignements personnels lorsque cela est nécessaire à l'une ou l'autre des fins suivantes : 1° la prestation par plus d'un organisme public de services communs ou la réalisation de missions communes à plus d'un organisme public; 2° l'accomplissement d'un mandat ou d'une initiative à portée gouvernementale; 3° la vérification de l'admissibilité d'une personne à un programme ou à une mesure; 4° la planification, la gestion, l'évaluation ou le contrôle de ressources, de programmes ou de services gouvernementaux ».

De telles circonstances ne visent pas spécifiquement l'utilisation de dispositifs de reconnaissance faciale par les services de police, sauf lorsqu'une telle prestation est accomplie par plusieurs organismes publics de police.

¹¹¹ Voir au fédéral la Directive du Conseil du trésor du Canada sur la prise de décision automatique, Février 2019 : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592>.

¹¹² International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto), "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System", 2018 : <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>

Modification de l'article 45 de la loi concernant le cadre juridique des technologies de l'information

Le projet de loi 64 envisage de modifier ainsi l'article 45 de la Loi concernant le cadre juridique des technologies de l'information : « La création d'une banque de caractéristiques ou de mesures biométriques doit être divulguée à la Commission d'accès à l'information avec diligence, au plus tard 60 jours avant sa mise en service ».

L'obligation de divulgation à la CAI n'est actuellement pas assortie d'un délai, aussi cette disposition va-t-elle dans le sens d'une meilleure protection dans le cadre de l'utilisation de la reconnaissance faciale par les forces de police.

Conclusion sur le projet de loi 64

Le projet de loi 64 prévoit des dispositions de nature à renforcer la protection des québécoises et québécois dans la collecte et l'utilisation de leurs renseignements personnels et en particulier des renseignements personnels sensibles dont les données biométriques. Cette réforme va donc dans le bon sens et doit être menée. Toutefois, elle ne permet pas de considérer et minimiser tous les risques inhérents à l'utilisation des technologies de reconnaissance faciale, aussi est-il souhaitable de la compléter par une autre loi spécifique.

Conclusion sur la reconnaissance faciale confrontée aux lois fédérales et provinciales : insuffisance du cadre légal

En résumé, si la plupart des lois provinciales (voir en annexe) qualifient implicitement ou explicitement les données biométriques de « renseignements personnels » ou « personal informations », aucune disposition législative spécifique n'est prévue pour protéger davantage ce type de données à risques. Autrement dit, les renseignements biométriques sont visés sans entraîner de conséquences juridiques particulières. Aucun régime juridique n'est associé. Si on ajoute le fait que la plupart des lois ont été adoptées depuis plusieurs années et ne tiennent pas compte des évolutions technologiques, l'insuffisance du cadre légal est flagrante aujourd'hui. Elle 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 qui a notamment lancé une consultation publique pour renforcer les lois¹¹³. Ces lois actuelles ne réglementant pas la biométrie, y compris la reconnaissance faciale par les forces de police, la technologie est alors déployée par certains services à travers le pays sans règles claires ni surveillance. Il n'y a ainsi pas de standard minimum de protection de la vie privée, de minimisation des risques ou de transparence publique.

¹¹³ Commissariat à la protection de la vie privée du Canada, « Consultation sur l'intelligence artificielle », Janvier 2020 : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-ai>.

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.

6. Comparaison avec le cadre légal applicable à la reconnaissance faciale en Europe et aux États-Unis

6.1. Droit de l'Union européenne concernant l'usage par les forces de police de la reconnaissance faciale

Directive 2016/680/UE pour la protection des données personnelles en matière de « police et justice » et données biométriques

La directive 2016/680/UE dite « Police-Justice »¹¹⁴ concerne la protection des données personnelles en matière pénale et s'applique au traitement des données personnelles par les services de police. L'objet de ce texte est d'établir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (art. 1.1). L'utilisation des outils de reconnaissance faciale par les forces de police entre clairement dans le champ d'application du texte. Ce texte organise le libre-échange des données personnelles à des fins de police et justice entre les États membres de l'Union européenne (art. 1.2) et n'empêche pas ces derniers de prendre des mesures plus protectrices des données personnelles, ce qui en fait un texte d'harmonisation minimale (art. 1.3.).

Données biométriques sensibles

L'article 10 prévoit des dispositions spécifiques concernant le traitement de « données sensibles », dont les données biométriques aux fins d'identifier une personne physique de manière unique. Ce traitement est autorisé à condition d'une « nécessité absolue » et sous réserve de « garanties appropriées pour les droits et libertés de la personne concernée » et uniquement dans trois cas limitativement énumérés :

- a) lorsque le traitement est autorisé par le droit de l'Union ou le droit d'un État membre ;
- b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou

¹¹⁴ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil :

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.FRA.

- c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

Le traitement de données biométriques à des fins de police correspond à la première hypothèse et suppose le recours à une loi ou un décret pour l'autoriser.

Traitements automatisés et profilage appliqués à la reconnaissance faciale

L'article 11.1 pose des mesures en matière de « décision individuelle automatisée ». Les États membres doivent prévoir que « toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite ».

Par exception, une telle décision pourra toutefois être possible, si elle est autorisée par le droit de l'Union ou le droit national et que ce droit fournit des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties doivent être au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. De telles décisions ne doivent toutefois pas être fondées sur des données sensibles, sauf si des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée sont en place (art. 11.2). Enfin, tout profilage qui entraînerait une discrimination à l'égard des personnes physiques sur la base des données sensibles est interdit, conformément au droit de l'Union (art. 11.3).

Dispositions applicables à la reconnaissance faciale

En résumé, si on applique ces dispositions à la reconnaissance faciale utilisée par les forces de police, on peut considérer que :

- le traitement de données biométriques est possible s'il y a à la fois une nécessité absolue, des garanties pour les droits et libertés des personnes concernées et si son usage est prévu par un texte (droit de l'Union ou droit national) :
- une décision automatisée, y compris le profilage, utilisant des données biométriques et produisant des effets négatifs sur la personne, pourra par exception être autorisée, si le droit national ou de l'union l'autorise et si des garanties appropriées sont prévues (tenant au minimum à une intervention humaine), ainsi que des mesures de protection des libertés et intérêts légitimes de la personne concernée, à condition toutefois de ne pas aboutir à une discrimination.

Ces deux mesures reposent essentiellement sur l'autorisation de la loi et les garanties de protection des droits fondamentaux. Une balance des intérêts est établie ici entre, d'une part, le recours à des dispositifs biométriques et décisions automatisées qui par nature entravent la protection de la vie privée et des données personnelles (art. 7 et 8 de la Charte

des droits fondamentaux de l'Union européenne) et, d'autre part, les garanties à apporter aux droits et libertés fondamentaux qu'il faudra expliciter.

Principes directeurs du traitement applicables à la reconnaissance faciale

Par ailleurs, si on comprend bien l'intérêt des services de police à recourir à ces dispositifs, notamment dans le cadre des enquêtes, l'usage de données personnelles doit en outre répondre aux exigences des principes directeurs de la protection de ces données posées plus généralement par l'article 4 de la directive, selon lequel les données à caractère personnel doivent être traitées de manière :

- licite et loyale, collectées (principe de licéité) ;
- pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités (principe de finalité) ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées (principe de nécessité et proportionnalité) ;
- exactes et, si nécessaire, tenues à jour (principe d'exactitude) et toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (principe de rectification et d'effacement) ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (principe de sécurité).

Droits de la personne concernée et ses limites dans l'usage de la reconnaissance faciale

Quant aux droits de la personne concernée, les articles 12 à 18 ont vocation à les concilier avec les besoins de l'action pénale. Les articles 12 et 13 organisent un droit à l'information et indiquent, la nature des informations à fournir tenant notamment aux finalités du traitement, à la base juridique du traitement et à la durée de conservation (art 13.1 et art. 13.2). Cependant, la directive autorise les États membres à adopter des mesures législatives visant à retarder, limiter ou ne pas fournir ces informations, afin de ne pas gêner les enquêtes et recherches ou ne pas nuire à la prévention ou à la détection d'infractions pénales, à condition qu'une telle mesure soit nécessaire et proportionnée dans une société démocratique et tienne compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée (art. 13.3).

Autrement dit, l'utilisation de la reconnaissance faciale peut être un outil de collecte des données mis en œuvre dans le cadre d'enquêtes ou pour prévenir ou détecter une infraction. Dans ce cas, les besoins de l'enquête primeront sur le droit à l'information mais, là encore, le législateur tente de poser des critères pour une balance des intérêts. Les mêmes limites

s'appliquent au droit d'accès aux informations personnelles (art. 14) et au droit de rectification et d'effacement (art. 16). Par ailleurs, la directive prévoit que les droits puissent être exercés indirectement par l'intermédiaire des autorités de contrôle (art. 17).

Obligations des responsables de traitement (services de police) et sous-traitants (organisations publiques ou privées) appliquées à la reconnaissance faciale

La directive prévoit toutefois aussi des obligations à la charge du responsable de traitement (art. 19) ou des responsables conjoints (art. 21), ainsi qu'envers les sous-traitants (art. 22) qui agiraient au nom et pour le compte du ou des responsables de traitement. Le sous-traitant ne doit traiter les données personnelles que sur instruction du responsable du traitement (art. 23). Pour sa part, le responsable de traitement est celui qui décide des moyens et finalités du traitement, ce qui sera en principe le cas d'un service de police. Le sous-traitant pourra être un partenaire privé ou public, avec lequel les relations contractuelles sont encadrées par la loi. Il doit prendre les mesures techniques et organisationnelles appropriées pour que le traitement soit conforme à la directive.

L'article 20 prévoit aussi l'obligation de protéger les données dès la conception et protection des données par défaut, en respectant en particulier le principe de minimisation de la collecte des données eu égard à la finalité du traitement. En outre, l'article 29 prévoit explicitement une obligation de sécurité des données à la charge du responsable du traitement et du sous-traitant qui doivent mettre en œuvre les mesures techniques et organisationnelles appropriées, afin de garantir un niveau de sécurité adapté au risque. Par ailleurs, la violation de données personnelles doit faire l'objet d'une notification à l'autorité de contrôle dans les meilleurs délais et, si possible, dans un délai de 72 heures au plus tard après en avoir pris connaissance, sauf si la violation n'engendre pas de risques pour les droits et les libertés d'une personne physique (art. 30). Si, au contraire, ce risque est élevé pour cette dernière, elle doit aussi faire l'objet d'une notification (art. 31).

Enfin, le responsable du traitement doit désigner un délégué à la protection des données (art. 32) qui doit notamment s'assurer du respect de la directive et coopérer avec l'autorité de contrôle (art. 34).

Outils de redevabilité des responsables de traitement et sous-traitants

La directive impose aux responsables de traitement et sous-traitants de mettre en œuvre des outils de contrôle, tels le registre des activités de traitements (art. 24) et la journalisation (art. 25). Le registre de traitement indique notamment les catégories de données utilisées, si bien que l'on doit pouvoir notamment savoir s'il est fait usage de données biométriques, ainsi que du profilage, pour quelle finalité et quelles sont les catégories de destinataires de ces informations. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification

de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel.

Coopération et pouvoirs des autorités de contrôle

Le responsable du traitement et le sous-traitant doivent coopérer avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions (art. 26) et même la consulter préalablement au traitement dans certains cas à risque pour les droits et libertés des individus (art. 27). Les autorités de contrôle (art. 41 et 44) sont indépendantes (art. 42). Parmi les missions qui leur sont confiées (art. 46), elles exercent les contrôles, traitent les plaintes et effectuent des enquêtes. Chaque autorité de contrôle doit pouvoir disposer de pouvoirs d'enquêtes effectifs (art. 47) et toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle unique (art. 52). En outre, un mécanisme d'assistance mutuelle entre autorités de contrôle des États membres permet de renforcer leur efficacité dans l'Union européenne (art. 50).

Analyse d'impact en matière de reconnaissance faciale et consultation préalable de l'autorité de contrôle

L'article 27.1 prévoit que « lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ». La reconnaissance faciale est une nouvelle technologie qui engendre un risque élevé pour les droits et libertés des individus, aussi une analyse d'impact devra-t-elle être réalisée¹¹⁵.

L'analyse d'impact relative à la protection des données personnelles (AIDP) est comparable dans la démarche à l'évaluation des effets sur la vie privée en droit québécois et canadien (EFVP).

Cette analyse d'impact doit contenir au moins : une description générale des opérations de traitement envisagées ; une évaluation des risques pour les droits et libertés des personnes concernées ; les mesures envisagées pour faire face à ces risques ; les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la directive, compte tenu des droits et intérêts légitimes des personnes concernées et des autres personnes touchées.

¹¹⁵ Cette obligation a été rappelée par plusieurs autorités nationales de protection comme par exemple en France avec la CNIL dans CNIL, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », qui intègre les traitements biométriques : <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf>.

En outre, si à l'issue de l'analyse d'impact, un risque élevé est révélé, le responsable du traitement ou le sous-traitant doit consulter l'autorité de contrôle préalablement au traitement. Une telle consultation doit aussi se faire lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées. Tel sera là encore le cas de la reconnaissance faciale. Si l'autorité de contrôle est d'avis que le traitement prévu constituerait une violation de la directive, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant.

Voies de recours, responsabilité et sanctions

Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, sans préjudice de tout autre recours administratif et judiciaire (art. 52). Elle a également un droit à un recours juridictionnel effectif contre ladite autorité (art. 53), ainsi qu'un droit contre un responsable du traitement ou un sous-traitant (art. 54). L'article 55 confère aux personnes concernées la possibilité de se faire représenter en confiant un mandat d'agir et d'exercer ses droits en son nom à un organisme, une organisation ou une association à but non lucratif, d'intérêt public et actif dans le domaine de la protection des droits et libertés. L'article 56 confère à toute personne ayant subi un dommage matériel ou un préjudice moral du fait d'une opération de traitement illicite en violation de la directive, le droit d'obtenir réparation du préjudice subi.

S'agissant des sanctions applicables en cas de violation, la directive n'en fixe pas le montant et laisse les États membres en déterminer le montant, le régime et prendre toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions doivent être effectives, proportionnées et dissuasives (art. 57). Il est logique que la détermination de ces mesures législatives soit laissée aux États puisque la matière pénale relève de leur compétence. L'efficacité de ces mesures dépendra donc fortement de la volonté et capacité des États à les faire respecter.

Absence de législation spécifique : directive 2016/680/UE et Charte des droits fondamentaux de l'UE dans le Livre Blanc sur l'IA

Pas de moratoire ou interdiction de la reconnaissance faciale en Europe

Bien que certaines voix se soient élevées pour encourager la Commission européenne à prendre parti en faveur de l'interdiction de la reconnaissance faciale, les forces de police des différents États membres se sont opposés à une prise de position aussi radicale. En conséquence, alors qu'une version précédente du Livre Blanc sur l'IA en janvier prévoyait une

telle interdiction¹¹⁶, la version finale publiée le 19 février 2020 ne comporte aucune disposition interdisant l'usage de cette technologie¹¹⁷. La Commission distingue les risques élevés pour les droits et libertés individuelles des risques faibles et considère que l'utilisation d'applications d'intelligence artificielle à des fins d'identification biométrique à distance et pour d'autres technologies de surveillance intrusive serait toujours considérée comme étant « à haut risque », ce qui devrait impliquer le respect d'exigences légales que l'Union européenne devrait poser à l'avenir.

Usage de la reconnaissance faciale considéré à « haut risque »

La Commission européenne reconnaît que la collecte et l'utilisation de données biométriques à des fins d'identification à distance, au moyen du déploiement de la reconnaissance faciale dans des lieux publics, comportent des risques particuliers en termes de droits fondamentaux. L'utilisation de systèmes d'IA pour l'identification biométrique à distance a des incidences sur les droits fondamentaux qui peuvent considérablement varier selon sa finalité, son contexte et sa portée.

Ainsi, les règles de l'UE en matière de protection des données interdisent en principe le traitement de données biométriques aux fins d'identifier une personne physique de manière unique, sauf dans des conditions précises telles que posées à l'article 10 de la directive 2016/680/UE. Rappelons que le traitement doit être strictement nécessaire, il doit être en principe autorisé par le droit de l'Union ou le droit d'un État membre et être assorti de garanties adéquates. Étant donné que tout traitement de données biométriques aux fins d'identifier une personne physique de manière unique constituerait une exception à une interdiction prévue par le droit de l'Union, il serait soumis à la charte des droits fondamentaux de l'UE. Dès lors, l'IA ne peut être utilisée à des fins d'identification biométrique à distance que lorsque cette utilisation est dûment justifiée, proportionnée et assortie de garanties adéquates.

Conclusion sur l'encadrement de la reconnaissance faciale en droit de l'Union européenne

Controverses et vaste débat public à venir sur la reconnaissance faciale

La Commission européenne n'a pas imposé une interdiction ou un moratoire sur la reconnaissance faciale mais veut cependant lancer un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi

¹¹⁶ Eric Weiss, "European Union Considers Temporary Ban on Facial Recognition" (17 Janvier 2020), Find Biometrics : <https://findbiometrics.com/biometrics-news-european-union-considers-temporary-ban-facial-recognition-011709/> ; Elena Sánchez Nicolás, "EU backtracks on plans to ban facial recognition" (20 Février 2020), EU Observer : <https://euobserver.com/science/147500>.

¹¹⁷ Commission européenne, Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance, Livre Blanc, COM(2020) 65 final, 19 Février 2020 : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf.

que sur les garanties communes à mettre en place. La position actuelle de la Commission européenne ne fait en effet par l'unanimité. Dès 2019, l'Agence de l'Union européenne pour les droits fondamentaux souligne les risques et enjeux de la technologie pour lesdits droits¹¹⁸. Le contrôleur européen de la protection des données (*European Data Protection Board*), Wojciech Wiewiórowski, se positionne en octobre 2019 et conçoit que de tels outils de reconnaissance faciale soient utilisés dans certains contextes comme un contrôle d'identité au niveau des frontières mais dès lors que l'utilisation vise à identifier un individu en comparant l'image prise dans l'espace public à un nombre élevé d'autres images, il considère que cela se rapproche davantage d'une intrusion¹¹⁹. En outre, le contrôleur a adopté en janvier 2020 des lignes directrices sur le traitement de données personnelles par des outils de vidéo¹²⁰ dans lesquelles il rappelle l'obligation de respecter les principes de légalité, nécessité, proportionnalité et minimisation des données. En outre, est aussi rappelée la nécessité de faire une étude d'impact préalable sur les droits et libertés fondamentales et enfin de considérer la méthode la moins intrusive possible pour atteindre l'objectif légitime du traitement.

Demande de moratoire du Contrôleur européen et de la Commission des libertés civiles du Parlement européen

Enfin, en juin 2020, dans son opinion 4/2020 sur le Livre Blanc¹²¹, le contrôleur a finalement appelé la Commission européenne à mettre en place une interdiction provisoire de tout logiciel qui permette de capturer non seulement les images, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, les frappes et autres signaux biométriques ou comportementaux dans les espaces publics.

Le contrôleur européen à la protection des données espère convaincre la Commission européenne qu'un tel moratoire est nécessaire, afin qu'un débat informé et démocratique puisse avoir lieu. Le Commissaire est d'avis d'avoir ce moratoire tant que la technologie n'est pas assez mature et que l'UE et les États membres ne disposeront pas de toutes les garanties appropriées, y compris un cadre juridique complet pour garantir la proportionnalité des technologies et systèmes respectifs pour le cas d'utilisation spécifique.

¹¹⁸ European Union Agency for Fundamental Rights, "Facial recognition technology : fundamental rights considerations in the context of law enforcement", 27 Novembre 2019 : <https://fra.europa.eu/en/publication/2019/facial-recognition>.

¹¹⁹ Wojciech Wiewiórowski, "Facial recognition: A solution in search of a problem?", European Data Protection Supervisor, 28 Octobre 2019, https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

¹²⁰ European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

¹²¹ European Data Protection Supervisor, "Opinion 4/2020 EDPS on the European Commission's White Paper on Artificial Intelligence" – A European approach to excellence and trust, 29 juin 2020 : https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.

Dans le même sens, la Commission des libertés civiles du Parlement européen a approuvé le 2 juillet 2020 un moratoire sur les outils de « reconnaissance faciale à des fins répressives » dans les espaces publics¹²². L'interdiction est également appelée de ses vœux par les groupes de défense des droits comme le European Digital Rights¹²³. La Haut-Commissaire aux droits de l'homme des Nations Unies, Michelle Bachelet, a également exprimé son inquiétude quant à l'utilisation d'armes non-létales contre les manifestants. Elle a également appelé à un moratoire sur l'utilisation de la technologie de la reconnaissance faciale, spécialement dans le cadre de manifestations pacifiques, jusqu'à ce que les États remplissent certaines conditions, notamment la transparence, la surveillance et le respect des droits de l'homme avant de la déployer¹²⁴.

Les dispositions de la directive 2016/680/UE constituent le cadre général de protection des données personnelles en matière de police et justice, applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'Union européenne. Puisque la matière pénale demeure de la compétence des États membres, il convient de rechercher aussi les mesures applicables dans les droits nationaux.

6.2. État des lieux de la reconnaissance faciale dans l'espace public en France et au Royaume-Uni

Absence de législation spécifique sur la reconnaissance faciale dans les États européens

À l'heure actuelle, aucun État européen n'a adopté de législation spécifique en matière de reconnaissance faciale¹²⁵, aussi faut-il s'en remettre à la directive 2016/680/UE sur la protection des données personnelles en matière de police et justice, ainsi qu'à ses déclinaisons nationales.

Expérimentations de systèmes de reconnaissance faciale dans l'espace public en Europe

Bien qu'aucune réglementation spécifique sur la reconnaissance faciale n'ait été adoptée en Europe, force est de constater que les technologies de reconnaissance faciale sont déjà

¹²² Elena Sánchez Nicolás, "Facial-recognition moratorium back on EU agenda", EUobserver : <https://eKonuobserver.com/science/148839>.

¹²³ EDRI, "Ban Biometric Mass Surveillance : A set of fundamental rights demands for the European Commission and EU Member States", Mai 2020 : <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>.

¹²⁴ UN News, "Digital tools being used to track people as never before, warns UN rights chief", 25 Juin 2020 : <https://news.un.org/en/story/2020/06/1067112>.

¹²⁵ Notons qu'en Belgique, le 16 juin 2020, a été déposée une Proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (déposée par M. Gilles Vanden Burre, Mme Jessika Soors et M. François De Smet) : <https://www.lachambre.be/doc/flwb/pdf/55/1349/55k1349001.pdf>.

utilisées en Europe¹²⁶. Des expérimentations ciblées de la reconnaissance faciale ont pu être mises en œuvre dans des espaces publics comme la rue¹²⁷ et en particulier aussi sur des lieux de transport où de nombreuses personnes en transit affluent dans des zones névralgiques, comme les aéroports, les gares ou encore les stations de métro¹²⁸. Les risques pour la sécurité des personnes paraissent alors significatifs, spécialement la menace terroriste après les attentats de Londres, Bruxelles, Paris et Nice.

Exemple de la France

Reconnaissance faciale et passage aux frontières des aéroports

Après les attentats du 11 septembre, le gouvernement américain a poussé les autres États à renforcer les mesures de sécurité dans les aéroports. Ainsi, la France utilise depuis 2009 le système PARAFE (Passage automatisé rapide des frontières extérieures) pour le contrôle aux frontières extérieures de l'espace Schengen, mis en place dans plusieurs aéroports stratégiques comme Orly et Charles de Gaulle. En 2016, la Commission Nationale Informatique et Libertés (CNIL) a approuvé ce dispositif¹²⁹. Elle relève qu'il ne nécessite pas la constitution d'une base de données centralisée et les images recueillies dans le sas sont effacées dès la comparaison effectuée avec l'image numérisée stockée dans le passeport suivant un procédé d'authentification et non d'identification. En outre, cette fonctionnalité repose sur le volontariat des passagers. Le dispositif a été confirmé par décret¹³⁰ et est pérennisé.

Prise de position de la CNIL sur la reconnaissance faciale

Au-delà du cas particulier du système PARAFE, en novembre 2019, la CNIL a appelé à un débat sur les enjeux de la reconnaissance faciale¹³¹. Elle pose trois exigences aux expérimentations de la reconnaissance faciale : tracer des lignes rouges avant même tout usage expérimental ;

¹²⁶ Notons que l'autorité suédoise de protection des données a autorisé en octobre 2019 l'utilisation de la reconnaissance faciale par la police pour aider à identifier les suspects en matière criminelle et permettre à la police de comparer des images faciales des séquences de télévision en circuit fermé à une liste de surveillance contenant plus de 40 000 images, Datainspektionen, "Polisen får använda ansiktsgenkänning för att utreda brott" (24 Octobre 2019) : <https://www.datainspektionen.se/nyheter/2019/polisen-far-anvanda-ansiktsgenkanning-for-att-utreda-brott/> ; NewEurope, « Sweden authorises the use of facial recognition technology by the police » (28 Octobre 2019) : <https://www.neweurope.eu/article/sweden-authorises-the-use-of-facial-recognition-technology-by-the-police>.

¹²⁷ Voir par exemple le bilan d'une expérimentation pour le carnaval de Nice en France : <https://www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html>.

¹²⁸ Pour une étude des expérimentations menées en Europe, voir le rapport réalisé par la Fablex DL4T, Dir. C. Lesquesne Roth, La reconnaissance faciale dans l'espace public : une cartographie juridique européenne, Avril 2020 : <https://dl4t.org/la-reconnaissance-faciale-dans-lespace-publique>.

¹²⁹ CNIL, « Délibération n°2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE » : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372514&categorieLien=id>

¹³⁰ Décret publié au Journal Officiel le 8 avril 2016.

¹³¹ Commission Nationale Informatique et Libertés (CNIL), Reconnaissance Faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019 : https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf.

placer le respect des personnes au cœur de la démarche ; adopter une démarche sincèrement expérimentale. Cela implique notamment une limitation dans le temps et dans l'espace de tels dispositifs, une identification exacte des objectifs poursuivis par ces expérimentations et de leurs critères de réussite. La définition précise de leurs modalités d'évaluation, qui doit être rigoureuse, contradictoire, pluridisciplinaire et menée dans des délais raisonnables, ainsi que la détermination des autorités chargées de celle-ci, constituent des dimensions essentielles. Elle ajoute qu'une telle démarche ne peut avoir éthiquement pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive.

Décision judiciaire sur l'utilisation de la reconnaissance faciale dans un établissement scolaire

Le Tribunal administratif de Marseille s'est prononcé le 27 février 2020¹³² sur un système de reconnaissance faciale expérimenté pour un contrôle d'accès virtuel dans deux lycées à Marseille et à Nice. La région Provence-Alpes-Côte d'Azur (PACA) se prévaut de poursuivre des finalités de fluidification et sécurisation des contrôles à l'entrée des lycées concernés. Sur le fondement des réglementations européennes et nationales de protection des données personnelles, le juge annule le recours à cet outil en estimant que ces finalités ne constituent pas un motif d'intérêt public. En outre, la région n'a pas démontré que lesdites finalités pourraient être atteintes de manière suffisamment efficace par des contrôles par badge, assortis, le cas échéant, de l'usage de la vidéosurveillance. Dès lors, le traitement de données biométriques ainsi institué ne satisfait pas aux exigences prévues par le point a) de l'article 9.1 du règlement général sur la protection des données (RGPD) qui protège les données sensibles. Cet usage n'entre au demeurant dans aucune des exceptions énumérées par le point 2 de l'article 9 du RGPD. Ajoutant par ailleurs que le consentement des lycéens n'a pas été collecté de manière libre et éclairée par la seule signature d'un formulaire, alors que le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés et en l'absence de garanties suffisantes. Le Tribunal administratif de Marseille a donc annulé la décision de recourir à ce système de reconnaissance faciale sur le fondement des articles 4 et 9 du RGPD et de l'article 6 de la loi 78-17 du 6 janvier 1978 modifiée dite loi informatique et libertés.

Exemple du Royaume-Uni

Prise de position de l'ICO, du Surveillance Camera Commissioner et du Biometric Commissioner sur la reconnaissance faciale en temps réel

Au Royaume-Uni, la police de Londres (Metropolitan Police Service (MPS)) a testé une technologie pour identifier la population en temps réel grâce à des caméras de surveillance

¹³² TA Marseille, 27 février 2020, n°1901249 : <https://www.doctrine.fr/d/TA/Marseille/2020/UC5C992ECBF9E9E4A1D82>.

implantées dans la rue ou technologie Live Facial Recognition (LFR)¹³³. La police du sud du Pays de Galles (South Wales Police (SWP)) en a aussi fait utilisation lors d'événements majeurs¹³⁴ dans le cadre d'un projet pilote appelé "AFR Locate". Elle utilise des caméras de surveillance pour capturer des images numériques de membres du public qui sont ensuite traitées et comparées aux images numériques de personnes figurant sur les listes de surveillance de la SWP.

Le 31 octobre 2019, l'autorité de protection des données (Information Commissioner's Office) (ICO) a délivré une opinion sur ces pratiques¹³⁵. La Commissaire Elizabeth Denham est d'avis que la combinaison du droit et de la pratique peut être rendue plus claire, plus précise et plus prévisible afin que les personnes puissent mieux comprendre quand leurs données biométriques peuvent être traitées par LFR. La Commissaire s'attend à ce que, pour donner confiance au public dans l'utilisation des LFR par la police, il soit nécessaire de fournir plus de détails dans les évaluations d'impact sur la protection des données (DPIA). Un point essentiel, selon la Commissaire, est que l'exigence de "stricte nécessité" de l'article 35(5) de la loi sur la protection des données (*Data Protection Act* de 2018), qui est la clé de l'utilisation des LFR dans les espaces publics, exige un examen plus détaillé de la part de la police et des autorités chargées de l'application de la loi quant à la proportionnalité de l'utilisation des LFR par rapport à l'intrusion qui se produit. Les LFR peuvent être plus susceptibles de répondre aux exigences de stricte nécessité et de proportionnalité lorsqu'ils sont déployés sur une base ciblée ou à plus petite échelle et dans un but étroitement défini. En d'autres termes, il sera probablement moins difficile de justifier un traitement sensible lorsqu'il s'agit d'un déploiement de LFR : ciblé ; mené par le renseignement ; limité dans le temps. Le responsable de traitement doit pouvoir expliquer clairement pourquoi l'utilisation de LFR, qui est une tactique intrusive, est strictement nécessaire lorsque d'autres options moins intrusives peuvent être disponibles.

La commissaire est enfin préoccupée par le risque de biais technique inhérent au fonctionnement de la technologie LFR. Elle a développé sa méthodologie interne d'audit des algorithmes¹³⁶, afin, entre autres, de fournir une assurance supplémentaire que les utilisateurs de ces technologies et les fournisseurs de technologies LFR tiennent compte de la partialité en faisant notamment une étude d'impact sur l'égalité (Equality Impact Assessment).

¹³³ National Physical Laboratory, « Metropolitan Police Service, Metropolitan Police Service Live Facial Recognition Trials », Février 2020 : <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf>.

¹³⁴ Automated Facial Recognition (AFR) : <http://afr.south-wales.police.uk/>.

¹³⁵ Information Commissioner's Opinion, "The use of live facial recognition technology by law enforcement in public places", 31 octobre 2019 : <https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf>.

¹³⁶ Information Commissioner's Opinion, Guidance on the AI auditing framework, Draft guidance for consultation : <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf>.

Plus généralement, la commissaire invite le gouvernement à encourager le débat public et à introduire dans les plus brefs délais un code de pratique juridiquement contraignant afin de fournir des garanties supplémentaires qui répondent aux problèmes spécifiques découlant de l'utilisation de technologies biométriques telles que les LFR.

Cette politique du Metropolitan Police Service et de la South Wales Police a également été dénoncée ensemble par le Commissaire à la biométrie (Biometrics Commissioner)¹³⁷ et par le Surveillance Camera Commissioner (SCC). Créés en vertu du Protection of Freedoms Act (POFA) (2012), le Biometrics Commissioner surveille la conservation et l'utilisation par la police d'échantillons d'ADN, de profils d'ADN et d'empreintes digitales, alors que le Surveillance Camera Commissioner réglemente la vidéosurveillance¹³⁸ et encourage le respect du Code de bonnes pratiques des caméras de surveillance¹³⁹ par les autorités compétentes. Par ailleurs, les positions de ces institutions ont aussi été reprises par le Center for Data Ethics and Innovation dans un rapport rendu en mai 2020 sur les enjeux de la reconnaissance faciale¹⁴⁰.

Décision judiciaire sur l'utilisation de la reconnaissance faciale par les forces de police

Cette expérimentation des services de police du Royaume-Uni et en particulier à la South Wales Police (SWP) a fait l'objet d'un recours judiciaire. En septembre 2019, dans une affaire *Bridge v. The Chief Constable of South Wales Police*¹⁴¹, la Haute Cour de Cardiff devait juger le fait qu'un membre du public craignait que son image n'ait été capturée sur LFR à partir d'un fourgon de police, alors qu'il faisait des courses dans le centre de Cardiff. La Cour était invitée à décider si le régime juridique actuel du Royaume-Uni est adéquat pour garantir l'utilisation appropriée et non arbitraire de la reconnaissance faciale automatisée (AFR) dans une société libre et civilisée.

C'est la première fois qu'un tribunal au monde prenait en compte la reconnaissance faciale automatisée par les forces de police. La décision portait spécifiquement sur la manière dont la technologie avait été utilisée par la police du sud du Pays de Galles (SWP), dans le cadre d'un projet pilote appelé "AFR Locate" et son adéquation au cadre juridique actuel, concernant les droits de l'homme, la protection des données et la législation sur l'égalité. Le

¹³⁷ Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 Janvier 2020 : <https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition>.

¹³⁸ Surveillance Camera Commissioner, "Police use of automated facial recognition technology with surveillance camera systems", 15 Mars 2020 : <https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems>.

¹³⁹ Surveillance Camera Code of Practice, Juin 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

¹⁴⁰ Center for Data Ethics and Innovation, "Facial Recognition Technology", Snapshot Paper, Mai 2020 : <https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology>.

¹⁴¹ Judiciary of England and Wales, "The Queen on the application of Edward Bridges and Chief constable of South Wales police and others" EWHC 2341 (Admin), Press Summary, 4 Septembre 2019 : <https://www.judiciary.uk/wp-content/uploads/2019/09/Press-Summary-Bridges-v-Cheif-Constable-South-Wales-Police-CO-4085-2018FINAL-1.pdf>.

tribunal de première instance a rejeté la demande de contrôle juridictionnel pour tous les motifs et a validé l'usage de cette technologie.

Mais cette décision a fait l'objet d'un appel et a été infirmée. Dans sa décision rendue le 11 août 2020 dans l'affaire *R (Bridges) -v- CC South Wales*¹⁴², La Cour d'appel a estimé que bien que le cadre juridique comprenne la législation primaire (Data Protection Act, 2018), la législation secondaire (le code de pratique des caméras de surveillance) et les politiques locales publiées par SWP, il n'y avait pas d'indications claires sur les endroits où AFR Locate pouvait être utilisé et sur les personnes pouvant être mises sur une liste de surveillance. La Cour a estimé que cette latitude était trop large pour que les policiers puissent satisfaire à la norme requise par l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme qui protège le droit à la vie privée. La Cour d'appel décide aussi que la Cour a eu tort de considérer que SWP a fourni une évaluation adéquate de l'impact sur la protection des données (DPIA), comme l'exige l'article 64 de la DPA 2018. La Cour d'appel a estimé que, comme le DPIA a été rédigée sur la base du fait que l'article 8 n'a pas été enfreint, alors qu'il l'était, ce qui rend le DPI déficient. Enfin, la Cour d'appel considère que la Cour de Cardiff a eu tort de considérer que l'analyse sur la discrimination n'était pas défailante.

Le Metropolitan Police Service s'appuyait sur la décision de première instance pour annoncer le début du déploiement de la reconnaissance faciale en direct (Live Facial Recognition (LFR) technology) en affirmant garantir la sauvegarde des droits fondamentaux et de la vie privée¹⁴³. Son annulation par la Cour d'appel devrait remettre en cause cette politique mais il a annoncé ne pas vouloir faire appel.

Conclusion sur l'encadrement de la reconnaissance faciale en France et au Royaume-Uni

La France et le Royaume-Uni sont actuellement les deux seuls États en Europe à avoir jugé du recours à la reconnaissance faciale. Si les deux contextes sont très différents, les juges se sont tous deux montrés défavorables à un tel usage et ont sanctionné le recours à cette technologie. Ils ont en outre posé les conditions d'un encadrement plus strict du recours à cette technologie, sans pour autant vouloir l'interdire. Il est fort probable que les conditions ainsi posées, fondées sur les réglementations de protection des données personnelles et la Charte des droits fondamentaux de l'Union européenne, soient reprises à l'avenir par d'autres juridictions. Cependant, il serait souhaitable que les conditions de recours à la reconnaissance faciale soient posées dans une loi pour donner plus de garanties et assurer une meilleure sécurité juridique. Il serait aussi nécessaire que ce futur cadre légal soit adopté au niveau de l'Union européenne, pour permettre une harmonisation plus large du recours à

¹⁴²R (Bridges) -v- CC South Wales, [2020] EWCA Civ 1058, Case No : C1/2019/2670, in the Court of Appeal (civil division) on appeal from the High Court of Justice Queen's Bench Division (administrative court) : <https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales>.

¹⁴³ Biometrics Commissioner, "Response to announcement on Live Facial Recognition", 24 Janvier 2020 : <https://www.gov.uk/government/news/response-to-announcement-on-live-facial-recognition>.

cette technologie, d'autant que les principales normes actuellement applicables sont issues du droit de l'Union.

6.3. Règlementations aux États-Unis propres aux données biométriques et à la reconnaissance faciale

Après les attentats du 11 septembre 2001, la reconnaissance faciale a été déployée par plusieurs départements de police aux États-Unis et utilisée dans des milliers d'enquêtes criminelles¹⁴⁴. Par ailleurs, dans la mesure où trente et un États autorisent les recherches de la police dans les bases de données du Department of Motor Vehicles (DMV), plus de la moitié des adultes américains peuvent être identifiés par la reconnaissance faciale de la police par le simple fait d'avoir un permis de conduire¹⁴⁵. Les faiblesses de cette technologie ont aussi été pointées du doigt dans un rapport rendu en 2016 par le Government Accountability Office sur l'utilisation de la reconnaissance faciale par le FBI¹⁴⁶. Ce rapport a formulé des recommandations pour accroître la transparence, renforcer la protection de la vie privée et mieux tester la précision des systèmes, afin de se prémunir contre les erreurs d'identification.

Après notamment la révélation de l'affaire Clearview AI et la publication de nombreux articles académiques révélant des taux d'erreur élevés inhérents à la plupart des systèmes de reconnaissance faciale, plusieurs sociétés privées américaines comme IBM et Amazon se sont provisoirement retirées du marché¹⁴⁷. En outre, les réactions de rejet de la reconnaissance faciale par la société civile ont conduit le gouvernement fédéral, ainsi que les gouvernements étatiques et municipaux à prendre ou envisager des mesures d'encadrement de cette technologie. AINow a publié en septembre 2020 un rapport sur les données biométriques dont une des études porte sur une taxonomie sur les approches législatives de la reconnaissance faciale aux États-Unis¹⁴⁸.

¹⁴⁴ Pinellas County Sheriff's Office, Florida's Facial Recognition Network (Mar. 26, 2014) : <https://drive.google.com/file/d/0B-MxWJP0ZmePX1QwTjltQkdVX0U/view>.

¹⁴⁵ Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law devant the U.S. House of Representatives Committee on Oversight and Reform (22 Mai 2019), 5 : <https://docs.house.gov/meetings/GO/G000/20190522/109521/HHRG-116-G000-Wstate-GarvieC-20190522.pdf>.

¹⁴⁶ Government Accountability Office (GAO), « Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy », Mai 2016: <https://www.gao.gov/assets/680/677098.pdf>.

¹⁴⁷ AFP, « Amazon interdit temporairement à la police d'utiliser sa technologie de reconnaissance faciale » (10 juin 2020), Le Journal de Montréal : <https://www.journaldemontreal.com/2020/06/10/amazon-interdit-temporairement-a-la-police-dutiliser-sa-technologie-de-reconnaissance-faciale>.

¹⁴⁸ Jameson Spivack & Clare Garvie (Georgetown Center on Privacy and Technology), "A Taxonomy of Legislative Approaches to Face Recognition in the United States," in "Regulation Biometrics: Global Approaches and Urgent Questions", ed. Amba Kak, AINow, Sept. 2020.

Projet de loi fédérale : Ethical Use of Facial Recognition Act (2020)

Au niveau fédéral, deux projets de lois sont à relever dont un seul concerne les forces de l'ordre. Le premier projet de loi intitulé *Commercial Facial Recognition Privacy Act* (S.847), introduit au Sénat le 14 mars 2019¹⁴⁹, vise à interdire à certaines entités d'utiliser la technologie de reconnaissance faciale pour identifier ou suivre un utilisateur final sans obtenir le consentement affirmatif de ce dernier et à d'autres fins. Ce projet de loi n'a toutefois pas encore été adopté et exclut explicitement de son champ d'application les agents de sécurité : (i) le Gouvernement Fédéral ou toute autre administration locale ou étatique ; (ii) une agence répressive ; (iii) une agence de sécurité nationale ; ou (iv) une agence de renseignement.

Le second projet de loi, introduit au Sénat le 12 février 2020 et intitulé *Ethical Use of Facial Recognition Act*¹⁵⁰, est plus directement en lien avec l'utilisation de la reconnaissance faciale par les forces de police. Il s'appuie sur les constats suivants (section 2) : (1) la reconnaissance faciale est une technologie qui est de plus en plus utilisée et commercialisée auprès des forces de l'ordre à travers les États-Unis sans débat approprié ni considération de ses impacts ; (2) il a été démontré que la reconnaissance faciale a un impact disproportionné sur les communautés de couleur, les activistes, les immigrants et d'autres groupes qui sont souvent déjà injustement ciblés ; (3) la reconnaissance faciale a toujours été inexacte, en particulier pour les femmes, les jeunes, les Afro-Américains et d'autres groupes ethniques ; (4) il est prouvé que la reconnaissance faciale a été utilisée lors de manifestations et de rassemblements, ce qui pourrait refroidir la parole ; (5) il est essentiel que la reconnaissance faciale ne soit pas utilisée pour supprimer des activités liées au Premier Amendement, violer la vie privée ou avoir un impact négatif sur les droits et libertés civiles des individus.

Considérant le rappel de ces risques, le projet de loi vise à créer un moratoire sur l'utilisation gouvernementale de la technologie de la reconnaissance faciale jusqu'à ce qu'une Commission recommande des lignes directrices appropriées et limitations de l'utilisation de ladite technologie¹⁵¹. Concrètement, le projet de loi interdit à tout agent, employé ou

¹⁴⁹ S.847 - Commercial Facial Recognition Privacy Act of 2019 : <https://www.congress.gov/bill/116th-congress/senate-bill/847>.

¹⁵⁰ S.3284 - Ethical Use of Facial Recognition Act of 2020 : <https://www.congress.gov/bill/116th-congress/senate-bill/3284>.

¹⁵¹ Ladite Commission comportera 13 membres et aura pour mission (section 6(c)) :

(1) d'envisager et de créer des lignes directrices et des limitations pour l'utilisation de la technologie de reconnaissance faciale aux États-Unis afin de garantir que l'utilisation de cette technologie ne...

(A) créer un état constant de surveillance des individus aux États-Unis qui ne permet pas un niveau d'anonymat raisonnable ;

(B) produire des résultats biaisés ou inexacts ;

(C) avoir un impact disproportionné sur un groupe racial, ethnique, d'origine nationale ou sur une autre catégorie protégée d'individus ;

(D) empiètent sur la vie privée, la liberté d'expression ou les droits à une procédure régulière des individus aux États-Unis ; ou

(E) limiter la capacité des agents de la force publique à retrouver les enfants disparus et exploités et les victimes de la traite

contractant d'une agence fédérale de s'engager dans des activités spécifiées concernant la technologie de reconnaissance faciale sans mandat jusqu'à ce qu'une commission du Congrès, établie par ce projet de loi, recommande des règles régissant l'utilisation et les limites de l'utilisation gouvernementale et commerciale de cette technologie (section 4).

Le projet de loi permet à une personne lésée d'intenter une action civile en vue d'obtenir une injonction ou une déclaration devant le tribunal de district américain compétent des États-Unis (section 5 (a)). Par ailleurs, aucun fonds fédéral ne peut être utilisé par un État ou une administration locale pour investir dans un logiciel de reconnaissance faciale, acheter des services de technologie de reconnaissance faciale ou acquérir des images pour les utiliser dans des systèmes de technologie de reconnaissance faciale (section 5 (b)).

Au plus tard 18 mois après la date de promulgation de la loi, la Commission présentera au Congrès un rapport (section 6 (d)) contenant : (1) les lignes directrices qui doivent être créées en vertu du point c) ; (2) les recommandations pour la mise en œuvre de ces lignes directrices ; et (3) toute opinion minoritaire ou recommandation de la Commission.

Au plus tard 90 jours après la date à laquelle ce rapport est soumis au Congrès, ce dernier doit préparer un texte législatif pour mettre en œuvre les recommandations contenues dans ce rapport.

Ce projet de loi n'a pas encore été discuté au Congrès américain.

Règlementations municipales

Dans certaines villes américaines, les décisions d'acquérir et utiliser les dispositifs de reconnaissance faciale ont été prises par les services de police sans avoir au préalable

(2) examiner et recommander les règles appropriées pour régir l'utilisation et les limites de l'utilisation tant gouvernementale que commerciale de la technologie de reconnaissance faciale, y compris

- (A) s'il existe des utilisations appropriées de la technologie de reconnaissance faciale sans mandat par des fonctionnaires dans un espace privé ou public ;
- (B) quelles sont les utilisations appropriées et les limites de l'utilisation commerciale, y compris les droits que les personnes devraient avoir en ce qui concerne les données produites et l'utilisation de leur ressemblance dans la technologie de reconnaissance faciale ;
- (C) dans quelles circonstances, le cas échéant, les fonctionnaires devraient être autorisés à utiliser la reconnaissance faciale sans mandat ;
- (D) quelles règles devraient régir comment et où les images peuvent être acquises par la technologie de reconnaissance faciale, en tenant compte des attentes raisonnables des individus en matière de vie privée ou d'anonymat ;
- (E) dans quelles situations les individus devraient pouvoir refuser ou être obligés d'accepter l'utilisation de la technologie de reconnaissance faciale ;
- (F) quelles garanties doivent être mises en place pour prévenir les abus de la technologie de reconnaissance faciale ;
- (G) quels sont les recours appropriés en cas d'utilisation abusive de la technologie de reconnaissance faciale ; et
- (H) quels sont les droits des personnes en ce qui concerne les données produites et l'utilisation de leur ressemblance dans la technologie de reconnaissance faciale.

informé et consulté ni le public ni les élus¹⁵². La prolifération de l'utilisation des technologies de surveillance par les services de police locaux présente des menaces importantes pour les droits civils et les libertés civiles qui ont un impact disproportionné sur les communautés de couleur et les communautés à faible revenu¹⁵³.

C'est dans ce contexte que la campagne Contrôle communautaire de la surveillance policière (Community control over police surveillance (CCOPS)) a été lancée le 21 septembre 2016 par l'American Civil Liberties Union (ACLU)¹⁵⁴. L'objectif principal de cette campagne est d'adopter des lois sur le CCOPS qui garantissent que les résidents locaux, par l'intermédiaire des représentants de leur conseil municipal, sont habilités à décider si et comment les technologies de surveillance sont utilisées - un objectif qu'elle atteint en maximisant l'influence du public sur ces décisions.

En l'absence de loi fédérale applicable à la reconnaissance faciale, plusieurs villes aux États-Unis ont alors réagi pour interdire ou encadrer l'utilisation de la reconnaissance faciale par les services municipaux auxquelles appartiennent les autorités policières, ce qui peut s'expliquer par la proximité avec les citoyens et la nécessité plus immédiate de leur rendre compte. À ce jour, les lois du CCOPS ont été adoptées dans plus d'une quinzaine de juridictions¹⁵⁵, comme Seattle (Washington), Alameda (Californie)¹⁵⁶, Davis (Californie), Berkeley (Californie), Oakland (Californie), San Francisco (Californie), Palo Alto (Californie), Comté de Santa Clara (Californie), Nashville (Tennessee), Yellow Springs (Ohio), Lawrence (Massachusetts), Cambridge (Massachusetts), Somerville (Massachusetts), Boston (Massachusetts), Brookline (Massachusetts), Northampton (Massachusetts), Springfield (Massachusetts), New York (New York). Notons que si la plupart de ces législations ont été présentées dans les médias comme interdisant le recours à la reconnaissance faciale, il apparaît à la lecture de la plupart de ces textes que tout usage de cette technologie n'est pas

¹⁵² American Civil Liberties Union (ACLU), Community control over police surveillance : <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance>.

¹⁵³ American Civil Liberties Union (ACLU), Community control over police surveillance : <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance#map>.

¹⁵⁴ Ibid. Depuis le lancement de la campagne, ACLU estime que le besoin de lois CCOPS s'est considérablement accru en raison de deux moments de transformation. Tout d'abord, le CCOPS est devenu encore plus urgent le 8 novembre 2016, lorsque Donald Trump a été élu président sur un programme qui prévoyait d'identifier et d'expulser des millions d'immigrants sans papiers, de traquer les musulmans, et de contrôler encore plus agressivement les communautés de couleur. Les lois du CCOPS étaient nécessaires pour permettre aux conseils municipaux de dire "non" à ces efforts de surveillance accrus et au partage secret des données de surveillance avec des agences fédérales comme l'ICE. Le besoin de lois CCOPS s'est encore accru en 2020 après la mort de George Floyd, alors que les mouvements de définancement et de désinvestissement de la police nationale prenaient de l'ampleur. Les lois CCOPS sont essentielles pour garantir que les forces de police moins bien financées ne passent tout simplement pas d'un maintien de l'ordre humain plus coûteux et à caractère racial à un maintien de l'ordre de haute technologie moins coûteux et à caractère racial.

¹⁵⁵ Voir le modèle de loi élaboré par ACLU : <https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf>

¹⁵⁶ File # 2019-7533, Adoption of Resolution Establishing a Privacy Policy, Data Management Policy, and Prohibiting the Use of Face Recognition Technology. 17 Déc. 2019 : <https://alameda.legistar.com/LegislationDetail.aspx?ID=4273393&GUID=F515A75C-2EB6-4CF8-A0A1-749610C379F8&Options=&Search=>.

systématiquement interdit mais repose sur des conditions désormais posées par la loi. Nous préférons donc considérer que ces législations encadrent plutôt qu'interdisent la reconnaissance faciale, sous réserve de certaines lois particulières ci-dessous indiquées.

Villes californiennes : exemples du Comté de Santa Clara, Berkeley, San Francisco, Oakland pour encadrer l'utilisation des technologies et de la reconnaissance faciale

Le 21 juin 2016, le comté de Santa Clara a été le premier à adopter une ordonnance pour mettre fin à la surveillance secrète et discriminatoire¹⁵⁷. Cette ordonnance ajoute une division relative à l'exigence d'approbation du conseil d'administration pour l'acquisition et l'exploitation d'équipements de surveillance, y compris les technologies de reconnaissance faciale, et pour une politique d'utilisation de la surveillance connexe. Les principales dispositions de la nouvelle ordonnance sur les technologies de surveillance du comté de Santa Clara prévoient : un débat public éclairé et l'approbation du conseil d'administration dès les premières étapes du processus ; détermination par le Conseil que les avantages l'emportent sur les coûts (droits fiscaux et civils) et les préoccupations ; approbation par le Conseil d'une politique robuste d'utilisation de la surveillance robuste ; l'approbation du Conseil d'une politique d'utilisation de la surveillance avec des garanties solides en matière de droits civils, de libertés civiles et de sécurité pour toutes les technologies de surveillance existantes et nouvelles ; une surveillance continue et une responsabilité.

Le conseil municipal de Berkeley, en Californie, tente d'endiguer par la loi la surveillance policière. Le 27 mars 2018, il a adopté à l'unanimité une ordonnance qui couvre largement l'acquisition et l'utilisation des technologies de surveillance par la ville¹⁵⁸. L'ordonnance exige que l'utilisation par la ville de technologies de surveillance, telles que les caméras de surveillance, les lecteurs de plaques d'immatriculation et les traqueurs de téléphones portables soient approuvés par le conseil municipal et soumis à la surveillance des citoyens. Le 15 octobre 2019, une autre ordonnance a été adoptée pour modifier le chapitre 2.99 du Code municipal de Berkeley pour encadrer l'utilisation la technologie de la reconnaissance faciale¹⁵⁹.

Le 6 mai 2019, San Francisco fut ainsi la première ville de taille significative aux États-Unis à encadrer l'utilisation de la reconnaissance faciale par les agences gouvernementales de la

¹⁵⁷ Ordinance no. ns.300.897 : an ordinance of the board of supervisors of the county of Santa Clara adding division a4o of the county of Santa Clara ordinance code relating to surveillance technology and community safety : <https://www.aclunc.org/blog/santa-clara-county-passes-landmark-law-shut-down-secret-surveillance>.

¹⁵⁸ Ordinance 7592 : <https://www.berkeleyside.com/wp-content/uploads/2018/03/2018-03-27-Item-02-Ordinance-7592.pdf>.

¹⁵⁹ Berkeley - Ordinance no. 7676 : https://www.cityofberkeley.info/Clerk/City_Council/2019/10_Oct/Documents/2019-10-29_Item_01_Ordinance_7676.aspx.

ville¹⁶⁰. Par voie d'ordonnance¹⁶¹, la ville a modifié le code administratif dans le but d'encadrer l'utilisation des technologies de surveillance qui incluent les logiciels ou technologies biométriques, y compris les logiciels et bases de données de reconnaissance faciale, vocale, de l'iris et de la démarche. La réforme exige ainsi que les services municipaux qui acquièrent une technologie de surveillance, ou qui concluent des accords pour recevoir des informations provenant d'une technologie de surveillance n'appartenant pas à la ville, soumettent à l'approbation du Conseil des superviseurs une ordonnance sur la politique en matière de technologie de surveillance. Des garanties juridiquement exécutoires, y compris des mesures de transparence, de surveillance et de responsabilité solides, doivent être mises en place pour protéger les droits civils et les libertés civiles avant le déploiement de toute technologie de surveillance. Si une technologie de surveillance est approuvée, des mesures de communication des données doivent être adoptées pour permettre au conseil des autorités de surveillance et au public de vérifier que les garanties obligatoires en matière de droits civils et de libertés civiles ont été strictement respectées.

Le 16 juillet 2019, Oakland¹⁶² fut la troisième ville à l'interdire aussi en modifiant le chapitre 9.64 du code municipal concernant l'encadrement l'acquisition et l'utilisation des technologies de surveillance par la ville.

Villes du Massachusetts : exemples de Boston, Cambridge, Somerville, Brookline, Northampton, Springfield

D'autres ordonnances prévoyant des restrictions à la reconnaissance faciale ont été prises dans des villes du Massachusetts. Le 24 juin 2020, Boston a adopté une ordonnance interdisant l'utilisation de la technologie de reconnaissance faciale¹⁶³. L'interdiction vise la police de Boston et autres services municipaux, dès lors qu'il est prouvé que les systèmes existants identifient mal les personnes de couleur à un taux d'erreur élevé¹⁶⁴. L'alinéa (b)(2) prévoit quelques exceptions. Notamment, l'interdiction d'usage prévue à (b)(1) ne prive pas la ville de Boston ou ses officiers d'utiliser des preuves relatives aux investigations de certains

¹⁶⁰ Colin Lecher, "San Francisco becomes the first US city to ban facial recognition by government agencies" (14 Mai 2019), The Verge : <https://www.theverge.com/2019/5/14/18623013/san-francisco-facial-recognition-ban-vote-city-agencies>.

¹⁶¹ File 190110, Ordinance amending the Administrative Code :

<https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A>.

¹⁶² Chapter 9.64 - Regulations on city's acquisition and use of surveillance technology : https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACU_SSUTE ; Caroline Haskins, "Oakland Becomes Third U.S. City to Ban Facial Recognition" (17 Juillet 2019), Vice : https://www.vice.com/en_U.S./article/zmpaex/oakland-becomes-third-U.S.-city-to-ban-facial-recognition-xz.

¹⁶³ Docket #0683 : <https://assets.documentcloud.org/documents/6956465/Boston-City-Council-face-surveillance-ban.pdf>; Nik DeCosta-Klipa, Boston City Council unanimously passes ban on facial recognition technology (24 Juin 2020), Boston News : <https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban>.

¹⁶⁴ Larry Hardesty, "Study finds gender and skin-type bias in commercial artificial-intelligence systems" (11 Février 2018), MIT News : <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212> ; Natasha Singer and Cade Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study" (December 19, 2019), The New York Times : <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>.

crimes spécifiques prises par des systèmes de reconnaissance faciale, du moment que ces systèmes ne leur appartiennent pas et n'ont pas été mis en place à leur demande. Au final, on peut donc considérer qu'il s'agit davantage d'un encadrement plutôt que d'une interdiction, en dépit du titre de la loi.

Cambridge¹⁶⁵, Somerville¹⁶⁶, Brookline¹⁶⁷, Northampton¹⁶⁸, Springfield¹⁶⁹ ont adopté des ordonnances similaires encadrant l'usage de cette technologie.

New York City : divulgation des technologies de surveillance utilisées par NYPD

Le 15 juillet 2020, la plus grande ville et force de police du pays, la ville et la police de New York (NYPD), a adopté une loi intitulée Public Oversight of Surveillance Technology (POST) Act¹⁷⁰ ou dans son titre complet *Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of New York city police department surveillance technologies*¹⁷¹. La loi exige la déclaration et l'évaluation des technologies de surveillance utilisées par la police de New York. Le ministère sera tenu de publier une politique d'impact et d'utilisation de la surveillance concernant ces technologies. Cette politique comprendra des informations sur les technologies de surveillance telles que la description et les capacités, les règles, les processus et les directives, ainsi que toutes les mesures de sauvegarde et de sécurité destinées à protéger les informations recueillies. Dès la publication du projet de politique sur l'impact et l'utilisation de la surveillance, le public disposera d'un délai pour soumettre ses commentaires. Le commissaire du département examine les commentaires et fournit la version finale de la politique en matière d'impact et d'utilisation de la surveillance au Conseil, au maire et l'affiche sur le site web du département. L'inspecteur général de la police de New York vérifie l'impact de la surveillance et la politique d'utilisation pour s'assurer du respect de ses conditions. La législation a été élaborée à partir des réactions des groupes de défense des droits civils et des libertés civiles préoccupés par le manque de contrôle de l'utilisation par le NYPD (New York Police Department) des outils de surveillance du public. Le NYPD a accès à des simulateurs de sites cellulaires pour saisir des

¹⁶⁵ Nik DeCosta-Klipa, "Cambridge becomes the largest Massachusetts city to ban facial recognition" (January 14, 2020), Boston News : <https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition>.

¹⁶⁶ Sarah Wu, "Somerville City Council passes facial recognition ban" (June 27, 2019), Boston Globe : <https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html>.

¹⁶⁷ Nik DeCosta-Klipa, "Brookline becomes 2nd Massachusetts community to ban facial recognition" (12 Décembre 2019), Boston News : <https://www.boston.com/news/local-news/2019/12/12/brookline-facial-recognition>.

¹⁶⁸ Jackson Cote, "Northampton bans facial recognition technology, becoming third community in Massachusetts to do so" (27 février 2020), Mass Live : <https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html>.

¹⁶⁹ Jackson Cote, "Springfield City Council passes facial recognition moratorium" (February 25, 2020), Mass Live : <https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html>.

¹⁷⁰ New York City Council, "City Council Plans Vote on POST Act, Creating Civilian Oversight of Police Surveillance", 16 juin 2020 : <https://council.nyc.gov/press/2020/06/16/1984>.

¹⁷¹ New York City Council, Int 0487-2018.

informations sur les téléphones portables, à la technologie de reconnaissance faciale, aux lecteurs de plaques d'immatriculation et aux camionnettes à rayons X, mais le public n'a guère été informé des capacités de ces outils et de la manière dont le NYPD utilise les informations privées qu'il collecte. En outre, le public n'a aucun moyen de savoir quels autres outils de surveillance la police de New York utilise. La loi devrait essentiellement permettre d'améliorer l'information, sans pour autant encadrer étroitement l'usage de la technologie.

Règlementations étatiques

Plusieurs États ont adopté ou considèrent la possibilité d'adopter des lois sur les données biométriques, comme le Nebraska¹⁷², ou sur la reconnaissance faciale associée à une autre technologie ou plus spécifiquement sur la reconnaissance faciale même.

Illinois : protection des données biométriques

La loi de l'Illinois sur la protection des informations biométriques de 2008 (Illinois Biometric Information Privacy Act (BIPA))¹⁷³ est l'une des plus anciennes et importantes mesures de protection de la vie privée aux États-Unis pour protéger les citoyens contre les sociétés qui veulent collecter et monétiser leurs informations personnelles. Cette loi exige un consentement explicite pour collecter des données biométriques et prévoit un droit d'action privé, ce qui peut toutefois en limiter l'efficacité¹⁷⁴.

Oregon : interdiction de la reconnaissance faciale en combinaison avec les caméras corporelles

Dès 2015, la loi de l'Oregon interdit¹⁷⁵ l'utilisation de la technologie de la reconnaissance faciale en combinaison avec les caméras corporelles des policiers (section 1(b)(D))¹⁷⁶. La loi du 5 mai 2015 oblige les services répressifs à établir des politiques et des procédures pour l'utilisation et la conservation des enregistrements des caméras portées sur la personne des policiers, afin d'enregistrer les interactions des policiers avec les membres du public.

¹⁷² Nebraska, LB1091, Adopt the Face Surveillance Privacy Act, projet introduit en Janvier 2020 et non encore adopté : https://www.nebraskalegislature.gov/bills/view_bill.php?DocumentID=41387.

¹⁷³ Illinois General Assembly, Civil liabilities (740 ILCS 14/) Biometric Information Privacy Act : <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>.

¹⁷⁴ Woodrow Hartzog, "BIPA: The Most Important Biometric Privacy Law in the US?", in "Regulation Biometrics: Global Approaches and Urgent Questions", ed. Amba Kak, AINow, Sept. 2020

¹⁷⁵ Section 1(b)(D): "A prohibition on the use of facial recognition or other biometric matching technology to analyze recordings obtained through the use of the camera".

¹⁷⁶ Oregon, House Bill 2571, An Act relating to video cameras worn upon police officer's person, 78th Oregon Legislative Assembly, Reg Sess, 2015 : <https://olis.oregonlegislature.gov/liz/2015R1/Measures/Overview/HB2571>.

Californie : interdiction de la reconnaissance faciale en combinaison avec les caméras corporelles

La loi *Law enforcement: facial recognition and other biometric surveillance* a été adoptée le 8 octobre 2019¹⁷⁷. La Californie empêchera les policiers d'inclure la technologie de reconnaissance faciale dans leurs caméras corporelles, interdisant aux forces de l'ordre d'utiliser tout "système de surveillance biométrique"¹⁷⁸. La loi permet aux personnes d'engager des poursuites judiciaires contre les officiers qui violent la loi.

Un projet de loi 2261 a été présenté à l'assemblée le 12 février 2020¹⁷⁹. Ce projet n'interdit pas l'utilisation de la reconnaissance faciale, mais fournit un cadre dans lequel les entreprises et les agences gouvernementales pourraient légalement l'utiliser, si elles en donnent une information préalable. Cela pourrait étendre l'utilisation de la reconnaissance faciale dans l'État, y compris à des fins répressives¹⁸⁰. L'article 1798.300 précise que, si l'utilisation de services de la reconnaissance faciale peut présenter des risques pour la vie privée, il existe de nombreux avantages pour la société comme l'amélioration de la sécurité, la localisation des personnes disparues ou handicapées, l'identification des victimes d'actes criminels, etc.¹⁸¹.

New York State : interdiction de la reconnaissance faciale en combinaison avec les drones

Le 31 janvier 2019, une loi de l'État de New York¹⁸² interdit l'usage de la reconnaissance faciale en lien avec l'utilisation des drones¹⁸³.

New York State : interdiction de la reconnaissance faciale dans les écoles

Une autre loi adoptée en juillet 2020 pose l'interdiction d'utiliser la biométrie identifiante dans les écoles¹⁸⁴. Les écoles élémentaires et secondaires publiques et non publiques, (y compris les *charter schools*) ont l'interdiction de fournir et utiliser des technologies biométriques identifiante quel que soit l'objectif, incluant l'objectif de sécurité des écoles, jusqu'au 1^{er} juillet 2022 ou jusqu'à ce que le commissaire autorise un tel achat ou utilisation.

¹⁷⁷ California, Assembly Bill 1215, Chapter 579, An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement : https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

¹⁷⁸ "This bill would prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera".

¹⁷⁹ California, AB-2261, An Act relating to facial recognition technology, 2019-2020, Reg Sess, 2020.

¹⁸⁰ Russel Brandom, "California's statehouse is considering a controversial facial recognition bill" (June 3 2020), The Verge : <https://www.theverge.com/2020/6/3/21279539/california-facial-recognition-ab2261-law-privacy-regulation>.

¹⁸¹ California, AB-2261 Facial recognition technology, amended in assembly may 12, 2020 : https://leginfo.ca.gov/faces/billtextclient.xhtml?bill_id=201920200ab2261.

¹⁸² New York State, A4030, Assembly Bill on Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof, 2019 : <https://www.nysenate.gov/legislation/bills/2019/A4030>.

¹⁸³ "Neither facial recognition nor other biometric matching technology shall be used on non-target data".

¹⁸⁴ New York State, A6787-D, Assembly Bill Relates to the use of biometric identifying technology, 2019 : <https://legislation.nysenate.gov/pdf/bills/2019/A6787D>.

Michigan : moratoire sur l'utilisation de la reconnaissance faciale

Dans le Michigan par exemple, le projet de loi déposé le 10 juillet 2019 portant sur l'utilisation de la reconnaissance faciale par les forces de l'ordre¹⁸⁵ modifie le code de procédure criminelle pour introduire le moratoire suivant : « jusqu'à l'expiration d'un délai de 5 ans à compter de la date d'entrée en vigueur de l'acte modificatif qui a ajouté cette section au présent chapitre, un agent des services répressifs ne peut obtenir, accéder ou utiliser une technologie de reconnaissance faciale ou toute information obtenue par l'utilisation d'une technologie de reconnaissance faciale pour faire appliquer les lois du présent État ou une subdivision politique de cet État ».

Cette interdiction comprend, sans s'y limiter, l'utilisation de la technologie de reconnaissance des visages en liaison avec les caméras de surveillance, les aéronefs sans pilote, les caméras portées sur le corps, les feux des rues et les feux de circulation. Les éléments de preuve obtenus et les mandats d'arrêt et de perquisition délivrés en raison d'une violation de ces dispositions sont soumis aux règles d'exclusion, comme si les éléments de preuve, le mandat d'arrêt ou le mandat de perquisition avaient été obtenus en violation de l'amendement IV de la Constitution des États-Unis et de la section 11 de l'article I de la Constitution de l'État de 1963.

Washington : moratoire sur l'utilisation de la reconnaissance faciale

Dans l'État de Washington, a été votée le 31 mars 2020 une loi concernant l'acquisition et l'utilisation de la technologie de reconnaissance faciale par des entités gouvernementales dans l'État de Washington et les droits à la vie privée relatifs à la technologie de reconnaissance faciale¹⁸⁶. Elle oblige toutes les entités gouvernementales à suivre la loi de l'État réglementant la collecte et l'utilisation des données biométriques par les agences de l'État jusqu'à ce que certaines conditions soient remplies. Elle interdit l'utilisation par les pouvoirs publics de systèmes de reconnaissance faciale pour surveiller les espaces publics sans raison valable, ou pour analyser des images obtenues à partir d'une caméra portée par un corps de police.

Massachusetts : moratoire sur l'utilisation des systèmes biométriques

L'État du Massachusetts a adopté en 2020 une loi instituant un moratoire sur la reconnaissance des visages et autres systèmes de surveillance biométrique à distance¹⁸⁷.

¹⁸⁵ Michigan, House Bill 4810 : <http://legislature.mi.gov/doc.aspx?2019-HB-4810>.

¹⁸⁶ Washington, H.B. 1654, Bill concerning the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology, 2019-2020, Reg Sess, 2019 : <http://lawfilesexext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729>.

¹⁸⁷ Massachusetts, S.1385, An Act establishing a moratorium on face recognition and other remote biometric surveillance systems, Mai 2020 : <https://malegislature.gov/Bills/191/S1385>.

Cette loi pose que, en l'absence d'autorisation légale expresse, il est illégal pour le Commonwealth du Massachusetts ou pour tout fonctionnaire du gouvernement du Massachusetts d'acquérir, de posséder, d'accéder ou d'utiliser tout système de surveillance biométrique, ou d'acquérir, de posséder, d'accéder ou d'utiliser des informations dérivées d'un système de surveillance biométrique exploité par une autre entité.

Conclusion sur la réglementation en Europe et aux 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 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 Massachusetts. Cependant, les dispositions prévoient majoritairement d'encadrer l'usage de cette technologie plutôt que de l'interdire. Les 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.

L'avènement de la législation est allé de pair avec les usages mais aussi les plaintes et revendications de la société civile et des associations de défenses des droits civils. Au cours de l'année écoulée, les États-Unis ont pris un tournant important dans leur approche de la reconnaissance faciale. Il est désormais largement admis qu'une réglementation est nécessaire, même si les législateurs, les défenseurs, les services répressifs et les autres parties prenantes, incluant les législateurs républicains et démocrates, ainsi que les vendeurs de reconnaissance faciale et les responsables de l'application de la loi. Toutes ces parties prenantes peuvent cependant ne pas être d'accord sur ce qu'il conviendrait de faire. Le statu quo dans l'utilisation de la reconnaissance faciale en mode expansif, non réglementé et secret n'est plus acceptable¹⁸⁸.

¹⁸⁸ Jameson Spivack & Clare Garvie (Georgetown Center on Privacy and Technology), "A Taxonomy of Legislative Approaches to Face Recognition in the United States," in "Regulation Biometrics: Global Approaches and Urgent Questions", ed. Amba Kak, AINow, Sept. 2020.

7. 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.

Annexes

Lois provinciales applicables aux renseignements personnels du secteur public

Alberta

La *Freedom of Information and Protection of Privacy Act* (FOIP)¹⁸⁹ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de l'Alberta. L'article 1(n) de la loi définit la notion de "personal information" qui signifie « recorded information about an identifiable individual ».

Cette définition inclut les informations personnelles sensibles : « (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations ».

S'agissant des données biométriques, l'article 1(n) FOIP cite explicitement ces données comme étant des « informations personnelles » :

« (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics ».

En outre, l'article 1(b.1) définit les informations biométriques comme étant : « information derived from an individual's unique measurable characteristics ».

Au-delà de ces définitions, l'Alberta n'a pas adopté de standards ou lignes directrices sur l'utilisation de la biométrie¹⁹⁰ ou reconnaissance faciale.

Colombie-Britannique

La *Freedom of Information and Protection of Privacy Act* (FIPPA)¹⁹¹ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de la Colombie-Britannique. Le Schedule 1 donne la définition de "Personal identity information" qui signifie : "any personal information of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual". En outre, la notion de "personal information" est définie comme : "recorded information about an identifiable individual other than contact information".

¹⁸⁹ Province of Alberta, *Freedom of information and protection of privacy act*, Revised Statutes of Alberta 2000 Chapter F-25, Current as of November 22, 2019 : <https://www.qp.alberta.ca/documents/Acts/F25.pdf>

¹⁹⁰ Scott MacDormand, Biometrics Privacy Impact Assessment Checklist for Public Educational Institutions in Alberta, 28 Novembre 2010, p.2 : <https://concordia.ab.ca/wp-content/uploads/2017/04/2011MacDormand.pdf>

¹⁹¹ Victoria, British Columbia, Canada, *Freedom of information and protection of privacy act* [rsbc 1996] chapter 165 : https://www.bclaws.ca/civix/document/id/complete/statreg/96165_00.

Le lendemain des émeutes survenues à Vancouver en juin 2011 après la finale de la Coupe Stanley, l'Insurance Corporation of British Columbia (ICBC) a offert d'aider la police à identifier les casseurs en analysant les images de l'émeute au moyen d'un logiciel de reconnaissance faciale et en comparant les suspects avec les images stockées dans sa base de données de titulaires de permis de conduire. D'après le rapport d'investigation F12-01 de l'Office of the Information & Privacy Commissioner for British Columbia publié en février 2012 sur l'utilisation de la technologie de la reconnaissance faciale par l'Insurance Corporation of British Columbia (ICBC)¹⁹², 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. L'Office conclut que l'ICBC doit immédiatement cesser de répondre aux demandes de la police d'utiliser la base de données de reconnaissance faciale aux fins d'identifier des personnes pour la police, en l'absence d'une citation à comparaître, d'un mandat ou d'une décision judiciaire.

Île-du-Prince-Édouard

La *Freedom of Information and Protection of Privacy Act* (FIPPA)¹⁹³ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de l'Île-du-Prince-Édouard. L'article 1.1(i) définit les "personal information" comme étant "recorded information about an identifiable individual, including:

- (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics".

L'article 2(a.2) ajoute que les informations biométriques "means information derived from an individual's unique measurable characteristics". La définition des informations personnelles intègre donc explicitement les données sensibles et les données biométriques.

En outre, l'Office of the Information & Privacy Commissioner for Prince Edward Island (OIPC) a publié des « Facts about Facial Recognition » communs avec l'Ombudsman du Nouveau-Brunswick, l'Office of the Information & Privacy Commissioner (OIPC) Nova Scotia et l'OIPC de la Nouvelle-Écosse¹⁹⁴. Selon ces « faits » : "Facial recognition is the process by which a

¹⁹² Elizabeth Denham, Information and Privacy Commissioner, Office of the information and privacy Commissioner for British Columbia, Investigation report f12-01, Investigation into the use of facial recognition technology by the insurance corporation of British Columbia, 16 Février 2012 : <http://www.oipc.bc.ca/investigation-reports/1245>.

¹⁹³ Prince Edward Island, *Freedom of information and protection of privacy act*, Avril 2019 : https://www.princeedwardisland.ca/sites/default/files/legislation/f-15-01-freedom_of_information_and_protection_of_privacy_act.pdf

¹⁹⁴ OMBUD, « Les faits au sujet de la reconnaissance faciale » : <https://www.ombudnb.ca/site/fr/dernieres-nouvelles/les-faits-au-sujet-de-la-reconnaissance-faciale>

person can be identified or otherwise recognized from a digital image. Facial recognition is one form of biometric identification; others include fingerprints, voice recognition and retinal scans”¹⁹⁵.

Ce document pose par ailleurs la question de l’exactitude de cette technologie. Si l’utilisation d’images 3D a amélioré la précision des systèmes de reconnaissance faciale, le risque de faux positifs (une mauvaise personne est identifiée) ou de faux négatifs (une personne qui aurait dû être identifiée ne l’est pas) demeure. La précision de la correspondance peut être influencée par des éléments tels que la qualité de l’image, les changements qui surviennent sur les visages au fil du temps et la qualité de l’algorithme utilisé. Ce document relève aussi que, de par sa nature, la reconnaissance faciale porte atteinte à la vie privée ; elle a la capacité d’identifier des personnes et de les relier à d’autres fonds d’informations. En outre, une image recueillie dans un but précis peut être utilisée dans un autre but sans que la personne concernée en soit informée ou y consente, comme en témoigne l’utilisation de cette technologie en 2011 par l’ICBC.

Par ailleurs, le document considère aussi l’utilisation de la reconnaissance faciale au Canada atlantique pour les permis de conduire et les cartes d’identité. Cette technologie est utilisée par les gouvernements provinciaux pour confirmer l’identité des personnes qui demandent un permis de conduire ou une carte d’identité avec photo délivrée par le gouvernement. Une fois la photo prise, le logiciel de reconnaissance faciale compare la photo de l’individu avec celle qui figure dans le dossier, et recherche d’autres correspondances pour vérifier l’identité de l’individu. Ces mesures visent à réduire le risque d’usurpation d’identité et de fraude et à empêcher les conducteurs suspendus ou les fraudeurs d’obtenir un permis de conduire ou une carte d’identité avec photo. Les commissaires à l’information et à la protection de la vie privée de la Nouvelle-Écosse, de l’Île-du-Prince-Édouard, du Nouveau-Brunswick et de Terre-Neuve-et-Labrador ont chacun interrogé leur gouvernement respectif sur la nécessité d’une telle technologie ainsi que sur les garanties nécessaires pour protéger ces informations contre toute utilisation abusive. Ils se sont tous engagés à surveiller et à traiter toute nouvelle expansion de ces programmes. D’autres provinces canadiennes, notamment en Ontario, en Colombie-Britannique et au Manitoba, utilisent aussi la reconnaissance faciale pour détecter l’usurpation d’identité et la fraude, par exemple pour repérer les individus qui demandent des permis sous différents noms.

¹⁹⁵ Office of the information and privacy commissioner for Prince Edward Island, “The Facts About Facial Recognition”, Janvier 2020 : <https://www.assembly.pe.ca/sites/www.assembly.pe.ca/files/OIPC%20NEws/Facial%20Recognition%20Background%202020.pdf>.

Manitoba

La *Freedom of Information and Protection of Privacy Act* (FIPPA)¹⁹⁶ est la loi sur la protection des renseignements personnels qui s'applique au secteur public du Manitoba. L'article 1(1) définit les "personal information" comme étant les "recorded information about an identifiable individual, including: (g) the individual's blood type, fingerprints or *other hereditary characteristics*; (n) an identifying number, symbol or other particular assigned to the individual". Les données biométriques sont donc spécifiquement qualifiées « d'informations personnelles ».

Nouveau-Brunswick

La *Right to Information and Protection of Privacy Act*¹⁹⁷ est la loi sur la protection des renseignements personnels qui s'applique au secteur public du Nouveau-Brunswick. L'article 1^{er} prévoit que les « personal information » sont les « recorded information about an identifiable individual, including but not limited to »

(c) information about the individual's age, gender, sexual orientation, marital status or family status

(d) information about the individual's ancestry, race, colour, nationality or national or ethnic origin,

(g) the individual's blood type, fingerprints or other hereditary characteristics". Sont donc aussi explicitement désignées les données personnelles sensibles et les données biométriques.

Par ailleurs, l'Ombudsman du Nouveau-Brunswick a publié des « faits au sujet de la reconnaissance faciale » communs avec l'Ombudsman du Nouveau-Brunswick, l'OIPC de l'Île-du-Prince-Édouard, l'Office of the Information & Privacy Commissioner (OIPC) Nova Scotia et l'OIPC de la Nouvelle-Écosse¹⁹⁸.

Nouvelle-Écosse

La *Freedom of Information and Protection of Privacy Act*¹⁹⁹ est la loi sur la protection des renseignements personnels qui s'appliquent au secteur public de la Nouvelle-Écosse. L'article 4(i) définit ainsi la notion de "personal information" : recorded information about an identifiable individual, including:

¹⁹⁶ Manitoba Laws, C.C.S.M. c. F175, *The Freedom of Information and Protection of Privacy Act* : <https://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php>.

¹⁹⁷ New Brunswick, *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6 : <https://www.canlii.org/en/nb/laws/stat/snb-2009-c-r-10.6/latest/snb-2009-c-r-10.6.html>.

¹⁹⁸ OMBUD, « Les faits au sujet de la reconnaissance faciale » : <https://www.ombudnb.ca/site/fr/dernieres-nouvelles/les-faits-au-sujet-de-la-reconnaissance-faciale>

¹⁹⁹ Nova Scotia, *Freedom of Information and Protection of Privacy Act*, Chapter 5 of the acts of 1993, 2018: <https://nslegislature.ca/sites/default/files/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf>.

- (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- (iv) an identifying number, symbol or other particular assigned to the individual,
- (v) the individual's fingerprints, blood type or inheritable characteristics".

On retrouve ainsi des définitions identiques des données biométriques dans les lois de Nouvelle-Écosse, du Nouveau-Brunswick, Manitoba, l'Île-du-Prince-Édouard.

Également, l'Office of the Information & Privacy Commissioner (OIPC) Nova Scotia a publié des "Facts about Facial Recognition" communs avec l'Ombudsman du Nouveau-Brunswick, l'OIPC de l'Île-du-Prince-Édouard et l'OIPC de la Nouvelle-Écosse²⁰⁰.

Ontario

La Loi sur l'accès à l'information et la protection de la vie privée²⁰¹ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de l'Ontario. En outre, la Loi sur l'accès à l'information municipale et la protection de la vie privée²⁰² s'applique au secteur public municipal de l'Ontario.

De nombreux casinos canadiens utilisent la reconnaissance faciale pour repérer les criminels et les tricheurs connus. En outre, dans le cadre des programmes d'auto-exclusion volontaire en vigueur dans plusieurs provinces, notamment en Ontario et en Colombie-Britannique, on a recours à la reconnaissance faciale dans les casinos exploités par les provinces pour interdire l'accès aux personnes ayant fait une demande en ce sens aux casinos, par exemple dans le but de les aider à s'affranchir de leur dépendance au jeu. En Ontario, des caméras associées à des logiciels de reconnaissance faciale examinent le visage des individus entrant dans les casinos. Elles les comparent avec les images de joueurs ayant demandé leur auto-exclusion qui sont stockées dans une base de données. Ce programme entièrement volontaire permet de reconnaître uniquement les individus ayant donné un consentement explicite. La commissaire à l'information et à la protection de la vie privée de l'Ontario a approuvé le programme²⁰³ parce qu'il possède des caractéristiques qui rehaussent la protection de la vie privée. Les images qui ne correspondent à aucune image stockée dans la base de données sont détruites. En outre, la base de données renfermant les images du visage des joueurs compulsifs est sécurisée au moyen d'un procédé de chiffrement

²⁰⁰ Nova Scotia, Office of the Information and privacy commissioner, "The Facts About Facial Recognition": <https://oipc.novascotia.ca/sites/default/files/publications/Data-Privacy-Day/Facial%20Recognition%20Backgrounder%20NS%202020%2001%2028.pdf>.

²⁰¹ Ontario, *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, Chapitre F.31 : <https://www.ontario.ca/fr/lois/loi/90f31>

²⁰² Ontario, *Loi sur l'accès à l'information municipale et la protection de la vie privée*, L.R.O. 1990, Chapitre m.56 : <https://www.ontario.ca/fr/lois/loi/90m56>

²⁰³ Ontario (*Alcohol and Gaming Commission*) (Re), 2001 CanLII 26269 (ON IPC) : <https://www.canlii.org/en/on/onipc/doc/2001/2001canlii26269/2001canlii26269.html?searchUrlHash=AAAAAQATZmFjaWFsIHJlY29nbmI0aW9uAAAAAB&resultIndex=1>.

biométrique, si bien qu'il est possible d'avoir accès aux renseignements se rapportant à un individu uniquement lorsque celui-ci est présent en personne.

En septembre 1999, le Commissaire à l'information et à la protection de la vie privée de l'Ontario a publié un guide intitulé « Privacy and Biometrics »²⁰⁴. Il est précisé notamment que « La menace pour la vie privée ne provient pas de l'identification positive que la biométrie offre, mais de la capacité des tiers à accéder à ces données sous une forme identifiable et à les relier à d'autres informations, ce qui entraîne des utilisations secondaires des informations, sans le consentement de la personne concernée. Cela a pour effet d'éroder le contrôle personnel d'un individu sur l'utilisation de ses informations ».

Terre-Neuve et Labrador

L'*Access to Information and Protection of Privacy Act*²⁰⁵ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de Terre-Neuve-et-Labrador. L'article 2 (u) définit les "personal information" comme étant les « recorded information about an identifiable individual, including:

- (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- (iii) the individual's age, sex, sexual orientation, marital status or family status,
- (iv) an identifying number, symbol or other particular assigned to the individual,
- (v) the individual's fingerprints, blood type or inheritable characteristics".

On retrouve la définition commune des autres provinces des maritimes. Également, l'Office of the Information & Privacy Commissioner de Terre-Neuve et Labrador a publié des "Facts about Facial Recognition" identiques à ceux précités de l'Ombudsman du Nouveau-Brunswick, de l'OIPC de l'Île-du Prince-Édouard et de OIPC de la Nouvelle-Écosse²⁰⁶. Par ailleurs, ces commissaires à l'information et à la protection de la vie privée (CIP) de l'Atlantique ont également décidé conjointement d'attirer l'attention des citoyens de la région sur les conséquences de la technologie de reconnaissance faciale sur la vie privée à l'occasion de la Journée de la protection des données le 28 janvier 2020²⁰⁷.

²⁰⁴ Ann Cavoukian, Commissioner, "Information and privacy Commissionner Ontario, Privacy and Biometrics", Septembre 1999 : <https://www.ipc.on.ca/wp-content/uploads/Resources/pri-biom.pdf>

²⁰⁵ St. John's, Newfoundland and Labrador, *Chapter a-1.2, an act to provide the public with access to information and protection of privacy*: <https://assembly.nl.ca/Legislation/sr/statutes/a01-2.html>.

²⁰⁶ Nova Scotia, Office of the Information and privacy commissioner, "The Facts About Facial Recognition": <https://oipc.novascotia.ca/sites/default/files/publications/Data-Privacy-Day/Facial%20Recognition%20Backgrounder%20NS%202020%2001%2028.pdf>.

²⁰⁷ Les CIP de l'Atlantique ont remarqué l'utilisation croissante de la technologie de reconnaissance faciale par les organismes publics et les entreprises privées dans les pays du monde entier. Si l'utilisation de cette technologie par les organismes publics canadiens a été relativement limitée jusqu'à présent, son application aux États-Unis, en Europe et en Asie dans des milieux tels que les écoles et les lieux publics semble se répandre rapidement. Au fur et à mesure que cette technologie continue à mûrir et que de nouvelles applications sont développées, il ne fait guère de doute que les organismes publics canadiens exploreront son utilisation pour améliorer leur prestation de biens et de services. Les CIP de l'Atlantique estiment que, dans chaque cas, les organismes publics

Saskatchewan

La *Freedom of Information and Protection of Privacy Act*²⁰⁸ est la loi sur la protection des renseignements personnels qui s'applique au secteur public de la Saskatchewan. L'article 24 (1) définit les "personal information" comme étant les "personal information about an identifiable individual that is recorded in any form, and includes:

- (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual."

Yukon

La loi sur l'accès à l'information et la protection de la vie privée²⁰⁹ est la loi sur la protection des renseignements personnels qui s'applique au secteur public du Yukon. L'article 3 définit les « renseignements personnels » comme étant « les enseignements consignés ayant trait à un particulier identifiable, notamment :

- b) sa race, son origine nationale ou ethnique, sa couleur, ses croyances ou affiliations politiques ou religieuses;
- d) tout numéro ou symbole, ou autre indication identificatrice, qui lui est propre;
- e) ses empreintes digitales, son groupe sanguin ou autre trait héréditaire ».

On retrouve encore les énumérations données par les provinces maritimes concernant les données biométriques.

Nunavut

La loi sur l'accès à l'information et la protection de la vie privée²¹⁰ est la loi sur la protection des renseignements personnels qui s'applique au secteur public du Nunavut. L'article 2

doivent examiner attentivement les conséquences de l'utilisation de cette technologie sur la vie privée et les mettre en balance avec les avantages potentiels. En effet, les Canadiens de la région atlantique doivent être conscients des implications en matière de protection de la vie privée et les examiner attentivement. Les CIP de la région atlantique sont d'avis qu'il incombe aux organismes publics d'éduquer et de consulter le public. Dans cet esprit, les CIP de la région de l'Atlantique ont fourni la fiche d'information ci-jointe afin de fournir aux résidents de la région de l'Atlantique quelques informations de base sur la reconnaissance faciale. Voir New Foundland Labrador, Office of the Information and Privacy Commissioner, "Atlantic Information and Privacy Commissioners highlight implications of facial recognition technology", 28 janvier 2020: <https://www.gov.nl.ca/releases/2020/oipc/0128n02>.

²⁰⁸ Saskatchewan, *The Freedom of Information and Protection of Privacy Act, Chapter f-22.01*, An Act respecting a right of access to documents of the Government of Saskatchewan and a right of privacy with respect to personal information held by the Government of Saskatchewan : <https://pubsaskdev.blob.core.windows.net/pubsask-prod/694/F22-01.pdf>.

²⁰⁹ Yukon, *Loi sur l'accès à l'information et la protection de la vie privée* : http://www.gov.yk.ca/legislation/acts/atipp_c.pdf.

²¹⁰ Nunavut, *Consolidation of access to information and protection of privacy act* S.N.W.T. 1994, c.20 : <https://atipp-nu.ca/wp-content/uploads/2018/04/consolidation-of-access-to-information-and-protection-of-privacy-act.pdf>.

donne une définition des informations personnelles comme Étant les informations « about an identifiable individual, including:

- (b) the individual's race, colour, national or ethnic origin or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics”.

Cette approche est conforme aux définitions données par de nombreuses autres provinces qui désignent explicitement les données biométriques.

Territoires du Nord-Ouest

La Loi sur l'accès à l'information et la protection de la vie privée²¹¹ est la loi sur la protection des renseignements personnels qui s'applique au secteur public des Territoires du Nord-Ouest. La même définition des « renseignements personnels » est consacrée à l'article 2 et inclut les données biométriques. Il s'agit des « renseignements concernant un individu identifiable, notamment :

- b) sa race, sa couleur, son origine nationale ou ethnique et ses croyances ou appartenances religieuses ou politiques;
- d) tout numéro ou symbole, ou toute autre indication identificatrice qui lui est propre;
- e) ses empreintes digitales, son groupe sanguin ou ses traits héréditaires ».

²¹¹ Territoires du Nord-Ouest, *Loi sur l'accès à l'information et la protection de la vie privée*, L.T.N.-O. 1994, ch. 20 : <https://atipp-nt.ca/wp-content/uploads/2016/03/Access-to-Information-and-Protection-of-Privacy-Act.pdf>.

Tableau synthétique du droit de l'UE et de quelques lois applicables en Europe

	Union européenne	États membres (ex. France et Royaume-Uni)
Lois spécifiques sur la reconnaissance faciale	Aucune législation dédiée à ce jour	Aucune législation dédiée à ce jour (aucun État membre de l'UE)
Législation sur la protection des données personnelles	Règlement 2016/679/UE dit RGPD et Directive 2016/680/UE + art. 7 (vie privée) et art. 8 (données personnelles) de la Charte des droits fondamentaux de l'UE Définition : Art. 4 RGPD : définition des données sensibles dont les données biométriques Régime des données sensibles : • Art. 9 RGPD • Art. 10 directive : traitement des données sensibles possible si : - Nécessité absolue - Garanties pour les droits et libertés - Loi de l'UE ou de l'État le prévoit (principe de légalité) • Art. 11 directive : décision automatisée y compris profilage possible si : - Autorisation du droit de l'UE ou droit national - Garanties appropriées (minimum intervention humaine) - Protection des libertés et intérêts légitimes de la personne concernée - Ne pas aboutir à une discrimination	Transposition de la directive dans les lois nationales : - France : loi 78-17 du 6 janvier 1978 dite informatique et libertés (LIL) modifiée par la loi du 20 juin 2018 - Royaume-Uni : Data Protection Act (2018)
Décisions de justice sur la reconnaissance faciale (RF)	Aucune décision de la CJUE à ce jour Notons que la Convention européenne des droits de l'homme (art. 8 sur la vie privée qui englobe la protection des données personnelles : CEDH, <i>S. et Marper c. Royaume-Uni</i>, 4 déc. 2008) et la jurisprudence de la Cour EDH peuvent être utiles.	• France : Tribunal administratif de Marseille, 27 février 2020, n°1901249 / annulation d'un système de RF dans un établissement scolaire. <u>Fondements :</u> art. 4 & 9 du RGPD et art. 6 loi informatique et libertés • Royaume-Uni : Court of Appeal, 11 août 2020, <i>R (Bridges)-v- CC South Wales</i>, [2020] EWCA Civ 1058, Case No : C1/2019/2670 / annulation d'un système de RF en temps réel mis en place dans la rue par la police du sud du pays de Galles (SWP) <u>Fondements :</u> article 8 de la Convention européenne des droits de l'homme + article 64 du Data Protection Act
Documents des autorités nationales de protection des données sur la reconnaissance faciale		• France : Commission Nationale Informatique et Libertés (CNIL), Reconnaissance Faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019 : https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf • Royaume-Uni : Information Commissioner's Opinion, The use of live facial recognition technology by law enforcement in public places, 31 Octobre 2019 : https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

Tableau synthétique des principales lois applicables aux États-Unis (non exhaustif)

	Interdiction	Encadrement
Technologies de surveillance		Santa Clara - Ordinance no. ns.300.897 du 21 juin 2016 Berkeley - Ordinance no. 7592 du 27 mars 2018 San Francisco - File 190110: Ordinance amending the Administrative Code du 6 mai 2019 Oakland - Ord. No. 13563 du 16 juillet 2019 New-York City Council, Int 0487-2018 du 15 juillet 2020 (information et contrôle)
Biométrie		Illinois - Illinois Biometric Information Privacy Act (BIPA) du 3 octobre 2008 Massachusetts - Senate Bill 1385 du 21 mai 2020, An Act establishing a moratorium on face recognition and other remote biometric surveillance systems
Reconnaissance faciale	Alameda - File # 2019-7533 - Adoption of Resolution Establishing a Privacy Policy, Data Management Policy, and Prohibiting the Use of Face Recognition Technology. 17 Déc. 2019 Nebraska - LB1091 - Adopt the Face Surveillance Privacy Act, projet introduit en Janvier 2020 et non encore adopté	Niveau fédéral - S.3284 - Ethical Use of Facial Recognition Act of 2020 du 12 février 2020 (projet) Berkeley - Ordinance no. 7676 to prohibit city use of face recognition technology, 15 octobre 2019 Boston - Docket #0683, ordinance banning facial recognition technology du 24 juin 2020 Michigan - HB 4810 on use of facial recognition technology by law enforcement officials, Juillet 2019 (projet) Californie - AB 2261 <i>An Act relating to facial recognition technology</i>, 12 février 2020 (projet) Washington - HB 1654 concerning the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology, 31 mars 2020
Reconnaissance faciale associée à une autre technologie (drone, caméras corporelles)	Oregon - HB 2571 du 5 mai 2015 Californie - AB-1215 Law enforcement: facial recognition and other biometric surveillance du 8 octobre 2019 Etat de New-York - A4030, Assembly Bill on Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof	
Données biométriques utilisées dans certains lieux	Etat de New-York - A6787-D, Assembly Bill Relates to the use of biometric identifying technology (interdiction des données biométriques dont la reconnaissance faciale dans les écoles)	