INTERNATIONAL OBSERVATORY ON THE SOCIETAL IMPACTS OF AI AND DIGITAL TECHNOLOGY

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

Use of facial recognition by police forces in the public space in Quebec and Canada

Elements of comparison with the United States and Europe

English Summary

Report prepared by

Céline Castets-Renard
Professor, Faculty of Law, University of Ottawa

Émilie Guiraud and Jacinthe Avril-Gagnon
Research assistants

November 2020

This report was prepared as a part of the research project of the International Observatory on the societal impacts of AI and digital technology (OBVIA) supported by the Québec Research Funds (FRQ). The production of this report is also supported and funded by the University Research Chair in Accountable AI in a Global Context hold by Professor Céline Castets-Renard.

Written by:

- Céline Castets-Renard, Professor at the Faculty of Law, Civil Section, University of Ottawa, University Research Chair Holder in Accountable AI in a Global Context and co-leader of the *International Relations, Humanitarian Action, Human Rights* OBVIA's research axis.

Prepared by :

- Céline Castets-Renard, Professor at the Faculty of Law, Civil Section, University of Ottawa.
- Émilie Guiraud, Research Assistant at OBVIA and student in Law, Université Laval.
- Jacinthe Avril-Gagnon, Research Assistant and student in Law, University of Ottawa.

Advisor committee :

- Pierre-Luc Déziel, Professor at the Faculty of Law, Université Laval and co-leader of the *Law, cyberjustice and cybersecurity* OBVIA's research axis.
- Benoit Dupont, Professor of Criminology, Université de Montréal, and Scientific Director, Smart Cybersecurity Network (SERENE-RISC).
- Steve Jacob, Professor in the Department of Political Science, Université Laval, holder of the Research chair on public administration in the digital age and co-head of the *Public Policies* function, OBVIA.
- Lyse Langlois, Professor in the Department of Industrial Relations, Université Laval, and Executive director, OBVIA.
- Guillaume Macaux, Scientific Advisor, OBVIA.

ISBN: 978-2-925138-01-3

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

Dépôt légal - Bibliothèque et Archives Canada, 2020.

Table of Content

1. Scope and Objectives of this Report

This document presents the main issues in the use of facial recognition by law enforcement agencies in the public space in Quebec and Canada, in comparison with other provinces, Europe and the United States. In a context where the use of this technology is increasingly in question, it is advisable to conduct a reflection prior to its deployment, in order to eliminate or minimize the risks incurred, in particular for individual rights and freedoms.

The main objectives of the document are then:

1) To enlighten legislators on what this technology is and the risks involved, in particular the risks of infringing on individual rights and freedoms protected by the Charters of Canada and Quebec.

2) To present the solutions already implemented to consider those that minimize the risks and intrusion of this technology on privacy, in order to set the conditions for transparency and better social acceptability.

2. Definitions

The concept of facial recognition is not defined in the texts either in Quebec law or in Canadian law or in any other province. Facial recognition is a technology that combines biometric techniques, artificial intelligence, 3D mapping and machine learning to compare and analyze a person's face in order to identify them. Facial recognition devices are part of biometric technologies and allow to identify or authenticate people from facial images (photos or videos): to authenticate a person, that is to say, to verify that a person is indeed who he or she claims to be (within the framework of an access control); to identify a person, that is to say, to find a person within a group of individuals, in a place, an image or a database.

Qualification of Personal Information

The data extracted to form the facial recognition template is biometric data that can be qualified as personal information.

The Office of the Privacy Commissioner of Canada (OPC) notes that "biometric systems store personal information about identifiable individuals. This means that their use by the federal government is subject to the Privacy Act. Biometric data may also be collected, used or

disclosed by private sector organizations, which may be subject to the Personal Information Protection and Electronic Documents Act (PIPEDA)."[1]

The CAI (Commission d'accès à l'information du Québec) states that "biometric information is personal information, i.e. information that relates to an individual and makes it possible to identify him or her" within the meaning of section 54 of the Act respecting access to documents held by public bodies and the protection of personal information and section 2 of the Act respecting the protection of personal information in the private sector. They are unique, distinctive and persistent over time.[2]

3. Background: Use of Facial Recognition in Canada by Police Forces

Facial recognition technology was originally developed to help governments with security and law enforcement. In addition, the public sector also operates most databases containing images of identified individuals, such as holders of driver's licenses, passports and people with criminal records. This is the case in Canada, where facial recognition systems are used for public services such as driver's licenses, identification documents such as e-passports, immigration documents and border security tools.

In addition, Clearview AI has developed a facial recognition application that compares any photo against a database of billions of freely available images, which have been retrieved since its inception in 2016 from most social networks and millions of websites. This American company has built up an unparalleled database and offers this technology mainly to law enforcement agencies. An algorithm quickly and efficiently compares a snapshot taken with a smartphone with Clearview AI's reference database.

The tool has attracted both U.S. and Canadian law enforcement agencies. Indiana Police became the start-up's first customer in February 2019, and the technology has been used by approximately 600 local police departments in the United States. The activities of this discreet company were revealed in January 2020 by the New York Times.[3]

[1] 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/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102.

[2] 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

[3] 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.

This tool was implemented by some police departments and the Royal Canadian Mounted Police (RCMP).[4] Elsewhere in Canada, police departments in Edmonton,[5] Calgary,[6] Vancouver,[7] Toronto[8] and Halifax[9] have confirmed the use of this technology. Finally, the Ottawa Police Service (OPS) reported in February 2020 that it had tested a facial recognition system without using it.[10] A three-month pilot project was reportedly conducted in March 2019 with the NeoFace Reveal application. The goal was to study the effectiveness of facial recognition technologies in criminal investigations. Deputy Police Chief Steve Bell says he would not want to implement it without consulting the community to ensure privacy and human rights. He adds that any new technology would be tested in a laboratory before being used, to ensure that it is used in a controlled manner.

In Quebec, little information has been circulated on the use or non-use of facial recognition technologies by the Service de Police de la Ville de Montréal (SPVM). In June 2020, the SPVM confirmed to the Commission de la Sécurité Publique (CSP) at City Hall that it had not used this device.[11] The Director of the SPVM, Mr. Caron, added that "the organization does not exclude, however, in specific and exceptional situations, the use of the services of a third party possessing this type of technology to advance a major investigation, while always ensuring that its operations and investigations are conducted in compliance with all applicable laws.[12] In July 2020, elected municipal officials urged the City of Montreal to create a by-law to regulate the potential use of facial recognition and other surveillance

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] Ibid.

technologies by its police force.[13] In addition, the Commission de la Sécurité Publique (CSP) was mandated to make recommendations in the fall of 2020 on the use of facial recognition.[14]

The Sûreté Québec wants to use this technology in criminal investigations to automatically compare video images to its bank of tens of thousands of descriptive photos. The Sûreté Québec issued a call for tenders and a contract was signed in June 2020 with Idemia for the acquisition of facial recognition and fingerprint technology capable of automatically comparing images of suspects against a bank of tens of thousands of descriptive photos.[15]

The use of Clearview AI's facial recognition tool by some police forces in Canada has raised concerns that have led to the OPC launching a related investigation under the Privacy Act in February 2020.[16] At the same time, a joint investigation is being conducted by the privacy authorities of Canada, British Columbia, Quebec and Alberta to examine whether its practices comply with Canadian privacy laws.[17] This investigation was initiated as a result of numerous media reports that raised questions and concerns about whether the company collects and uses personal information without consent. The results of the investigation have not yet been made public.

Clearview AI has informed Canadian privacy authorities that in response to their joint investigation, it will no longer offer its facial recognition services in Canada. It has also suspended indefinitely its contract with the RCMP, its last customer in Canada.[18]

---

[13] 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.

[14] 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.

[15] Tristan Peloquin, « 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.

[16] 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 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.

[17] 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/.

[18] 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.

4. Advantages of Facial Recognition

Facial recognition devices are increasingly used by police forces in public spaces for surveillance and public safety purposes. These tools are intended to be effective, particularly in complex investigations, such as when a violent crime occurs on the street. This technology is also used to detect potential criminals and terrorists among spectators at large events, such as stadiums or concert halls. These systems have been particularly deployed in high-risk areas in the United States to monitor criminal activity. Facial recognition systems are also heavily deployed in airports, particularly in the United States. They have captured and stored the facial data of more than half of U.S. citizens. Facial recognition thus makes it possible to increase the level of security in society when it is coupled with video surveillance. Other benefits are highlighted, such as saving time or simplifying the work of police forces.

5. Social Risks of Facial Recognition

However, the risks of infringements on individual liberties likely to be induced by these facial recognition devices used by police services in the public space are considerable, including in particular the mobility rights (art. 6 of the Canadian Charter of Rights and Freedoms), the freedom of thought (art. 2 (b) of the Canadian Charter of Rights and Freedoms), the freedom of peaceful assembly and the freedom of association (art. 2 (c) and (d) of the Canadian Charter of Rights and Freedoms and art. 3 of the Quebec Charter of Human Rights and Freedoms) as well as the right to liberty (art. 7 of the Canadian Charter of Rights and Freedoms and art 1 of the Quebec Charter of Human Rights and Freedoms). The use of facial recognition may interfere with freedom of expression, association and assembly. The right to privacy is also threatened (art. 8 of the Canadian Charter of Rights and Freedoms, art. 5 of the Québec Charter of Human Rights and Freedoms and art. 3, 35 to 37 of the Civil Code of Québec). The risk of surveillance by these devices is then to lead to a form of self-censorship on the part of citizens, particularly with respect to their participation in public life and more broadly the exercise of their fundamental freedoms. Moreover, the risks of data protection breaches are obvious, since this technology relies on the use of personal data, particularly biometric data, which is sensitive data that is subject to specific protection under several legislations around the world.

Facial recognition technology can undermine the dignity of individuals and also have repercussions on the right to non-discrimination. It can affect the rights of special groups, such as children, the elderly and the disabled. In addition, while facial recognition technology is developing, the error rate remains high, especially for certain categories of populations. Numerous studies prove that facial recognition technology is more effective in detecting

fair-skinned people and men than dark-skinned people and women.[19] A federal study conducted in the United States in December 2019 confirms the existence of racial bias in many systems.[20] According to this study, people of Asian and African-American origin are up to 100 times more likely to be misidentified than white males, depending on the algorithm and type of search. More recently, a study by the National Institute of Standards and Technology (NIST) confirmed such biases.[21] One explanation is that certain groups of the population, such as certain ethnic groups, youth and people with disabilities, are under-represented in the training images[22] and therefore not sufficiently representative of the population on which these systems will be used. Biased systems lead to false positives and false negatives, with serious consequences in the identification of suspects, for example. The legal, social, and psychological consequences for those falsely identified weigh heavily and must be taken seriously by governments when choosing and deploying such technologies. This risk naturally violates the principle of equality and non-discrimination, protected in section 15 of the Canadian Charter of Rights and Freedoms and section 10 of the Quebec Charter of Human Rights and Freedoms.

Systemic discrimination and racial profiling are likely to undermine these provisions. Systemic discrimination is characterized by practices that, by their effect, result in discrimination such as the systematic exclusion of a group. Intent is not the determining factor here. Discrimination is then said to be indirect because of its effects, in the absence of intentionality. Racial profiling is most often the result of an action taken by a person in a position of authority against a group or individuals because of their membership, for example, in a racial community.[23] If other forms of discrimination are created by these surveillance devices, the Supreme Court in the Bombardier decision noted that the wording of the Charter allows the courts to "recognize the existence of new forms of discrimination as they arise in our society.[24]

There are also risks if facial recognition is used in criminal investigations. Indeed, there is a greater risk of miscarriages of justice in cases where the identity of a suspect is in doubt. Consequently, there is a fear that the technology, often seen as infallible and credible in

---

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

[20] 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.

[21] 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.

[22] 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/.

[23] Ibid.

[24] Québec (Commission des droits de la personne et des droits de la jeunesse) c. Bombardier Inc. (Bombardier Aéronautique Centre de formation), 2015-07-03, [2015] 2 RCS 789, par. 34.

court, will reinforce the certainty of police officers, witnesses and judges.[25] However, the risk of error exists and human-made technologies incorporate the risk of bias, especially if the training data is biased. The technology then risks reinforcing social prejudices.

Given these risks and in this context, the social acceptability of this technology is likely to be low. In July 2020, privacy, human rights and civil liberties NGOs and associations sent an open letter calling on the Canadian federal government to adopt an immediate ban on the use of facial recognition by federal law enforcement and intelligence agencies, including the RCMP.[26] It also calls for clear and transparent policies and legislation to regulate the use of facial recognition in Canada, including the Personal Information Protection and Electronic Documents Act (PIPEDA).

Finally, there is a further risk that police services may use private companies to implement facial recognition. Since these players are performing a public service mission, police services must be vigilant and verify their good practices. Moreover, the possible choice of foreign private operators poses the risk of losing control of State sovereignty, which is particularly worrying.

6. Legal Framework for Facial Recognition in Canada and Quebec

Federal Public Sector Privacy Law

Only public sector legislation that may apply to law enforcement agencies will be considered here. Although police departments in Canada have begun to use facial recognition technologies, the federal government has no specific policy or legislation for the collection of biometric data, which are physical and behavioural characteristics that can be used to digitally identify individuals. As a result, there is no minimum standard of privacy protection, risk minimization or public transparency specifically applicable to biometrics or facial recognition. It is therefore necessary to rely more generally on personal information laws.

The Privacy Act applies to the public sector and regulates the personal information that federal entities may collect, use, disclose and retain. It does not specifically address facial recognition, but Article 3 (d) defines personal information about an identifiable individual, including fingerprints. Consequently, all biometric data such as facial recognition are

[25] 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.

[26] 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.

included in the material scope of the law, as long as they will allow an individual to be identified.

The purpose of the Privacy Act is to complement Canadian legislation on the protection of personal information under the control of federal institutions and the right of access by individuals to personal information about themselves (s. 2). It therefore does not apply to provincial and municipal police forces that are subject to provincial regulations. Only the RCMP is subject to this Privacy Act.

Article 4 provides that the only personal information that may be collected by a government institution is information that relates directly to an operating program or activity of the institution. Also, without the consent of the individual, personal information under the control of a government institution may be used only for the purpose for which it was collected or prepared by the institution and for a use consistent with that purpose (s. 7(a)). The RCMP may therefore only collect information directly related to its mandate as Canada's national police force. Finally, the same applies to the disclosure of personal information (article 8 (a)).

Limitations of the Federal Legal Framework for Personal Information in the Public Sector

The purpose principle that governs the collection, use and disclosure of personal information applies to the RCMP's use of facial recognition in policing. Other than this principle, no other requirements apply. There are legitimate questions as to whether this framework is sufficient today. It should be noted that the news regarding the RCMP's use of Clearview AI's facial recognition tool was released as a result of an information leak. In order to improve social acceptability and better dialogue between police services and the public, reform must establish clear and transparent policies and legislation regulating the use of this technology, including reforms to federal law. For example, consideration could be given to creating new public information obligations to ensure greater transparency and accountability of police forces.

In addition, the OPC has identified a potential violation of the purpose principle. For instance, "personal information shall be used only for the purpose for which it was collected. In the area of biometrics, the risk of multiple uses arises from the fact that some features, such as fingerprints, are relatively permanent and highly distinctive, making them a very convenient identifier that is both consistent and universal. Once the identifier is captured and stored in a database, it is easy to access and compare it to future samples, even if the samples are collected in completely different contexts.[27] There is a significant risk of purpose creep that is not sufficiently controlled.

[27] 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-

OPC Recommendations for Biometrics Projects in the Public Sector

The OPC cautions that many types of biometric information, such as fingerprints and facial images, can be collected without an individual's knowledge, let alone consent. They can therefore be used to surreptitiously monitor an individual's movements and behaviour. It encourages government organizations to think carefully before proposing projects that involve the collection, use or disclosure of biometric information.

For example, the OPC has set out the conditions under which a biometric project can be implemented.[28] Privacy concerns should be addressed at all stages of project development, from conception, to evaluation, to implementation and even termination. In particular, a Privacy Impact Assessment (PIA) is a process designed to help organizations consider the privacy impact of a new or substantially altered project, especially when it involves the collection of personal information. This process is mandatory in the public sector. Federal organizations proposing a program, policy or service that has privacy implications must submit a Privacy Impact Assessment to our Office for review.[29] Before establishing a new system (including biometrics), the organization must clearly justify any potential privacy intrusions.

To provide guidance in this process, the OPC encourages organizations to apply the four-part test, which is adapted from the 1986 Supreme Court of Canada decision in *R. v. Oakes* (the Oakes test).[30] The test assesses the appropriateness of a potentially privacy-invasive measure based on four questions:

1. Is the measure demonstrably necessary to meet a specific need? (necessity principle)
2. Is it likely to be effective in meeting this need? (principle of effectiveness)
3. Would the loss of privacy be proportional to the benefit gained? (principle of proportionality)

protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102.

[28] Ibid.

[29] 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;
- 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.

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

4. Is there a less intrusive way to achieve the same goal? (search for alternative solutions).

Québec Laws applicable to Facial Recognition and Policing (Provincial and Municipal): Legal Framework for the Protection of Personal Information

(Public Sector - Main Provisions)

The use of facial recognition technologies is essentially governed by the law on access to documents of public bodies and on the protection of personal information, as well as by the law on the legal framework of information technology. The Act respecting access to documents held by public bodies and the protection of personal information applies to documents held by a public body in the performance of its duties, whether they are kept by the public body or by a third party. The Act applies regardless of the form of such documents: written, graphic, sound, visual, computerized or other (art. 1). It applies to organizations under the jurisdiction of the Government of Québec and Québec municipalities. This includes the services of Sécurité Québec and municipal police departments, first and foremost the Service de Police de la Ville de Montréal (SPVM). Personal information is information that relates to a natural person and allows that person to be identified (art. 54).

Only public sector legislation that may apply to police missions will be considered here. Like Canada, Quebec also has no specific legislation applicable to the collection and use of biometric data or facial recognition. The same is true of the other provinces and territories of Canada in which it is appropriate to refer to public sector privacy legislation. The relevant provisions of these Acts are detailed in the appendix.

Therefore, the use of facial recognition technologies is essentially governed by the Act respecting access to documents held by public bodies and the protection of personal information,[31] as well as by the Act respecting the legal framework for information technology (loi concernant le cadre juridique des technologies de l'information)(LCJTI).[32]

The law gives public bodies to which police services belong certain rights. Thus, in principle, a public body may not communicate personal information without the consent of the person concerned, unless the public body is responsible under the law for preventing, detecting or punishing crime or offences against the law and the information is necessary for the purposes of a prosecution for an offence under a law applicable in Québec (art. 59-3°). In addition to the cases provided for in section 59, a public body may also disclose personal information, without the consent of the persons concerned, for the purpose of preventing an

[31] 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.

[32] 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.

act of violence, including suicide, where there are reasonable grounds to believe that there is a serious risk of death or serious injury to an identifiable person or group of persons and the nature of the threat inspires a sense of urgency (art. 59.1).

In addition, a police force may, without the consent of the person concerned, disclose personal information to another police force (art. 61). More generally, personal information is accessible, without the consent of the person concerned, to any person who is entitled to receive it within a public body when the information is necessary for the performance of his or her duties (art. 62). A public body may disclose personal information for the purpose of comparing it with another file held by a person or body without the consent of the person concerned (art. 68.1, paragraph 1).

Finally, while in principle the person concerned by a collection of his or her personal information must be informed of, among other things, "the name and address of the public body on whose behalf the collection is being made, the purpose, the categories of persons who will have access to it, whether the request is mandatory or optional, (and) the consequences of refusal" (art. 65 paras. 1 and 2), this right to information disappears in the event of an investigation of a judicial nature or an inquiry or report made by a body responsible for preventing, detecting or punishing crime or infringements of the law (art. 65 par. 5).

While the use of facial recognition falls within the scope of personal information collection law, the characteristics of this technology are not taken into account, which limits protection and demonstrates the inadequacy of the law. In addition, the application of these rules to facial recognition raises many questions of interpretation, including the rights granted to police agencies in the use of this technology, particularly with respect to the change of purpose. Clarification and adaptation of the law is required.

Furthermore, the law concerning the legal framework for information technology (LCJTI) adopted in 2001 provides for protection measures and terms of data security and integrity. This Law provides for protective measures against the risks posed by biometric data. Article 44(1) states that "no one may require, without the express consent of the person, that the verification or confirmation of his or her identity be carried out by means of a process for capturing biometric characteristics or measures. The identity of the person can then only be established by using the minimum number of characteristics or measures that can be linked to the action he or she is taking and only among those that cannot be captured without his or her knowledge".

This law gives the Commission d'accès à l'information (CAI) broad powers with respect to biometric databases. Article 45(1) provides that the creation of a bank of biometric characteristics or measures must first be disclosed to the CAI. Likewise, the existence of such a bank, whether or not it is in operation, must be disclosed. The Commission may issue any order concerning such banks in order to determine their creation, use, consultation, communication and conservation, including the archiving or destruction of the measures or

characteristics taken to establish the identity of a person (art. 45, para. 2). It may also suspend or prohibit the operation of such a bank or order its destruction, if it does not comply with its orders or if it otherwise violates privacy (Art. 45, para. 3).

The CAI thus makes available online a form for declaring a bank of biometric characteristics or measures.[33] This declaration includes facial recognition tools. In July 2020, the CAI published an accompanying guide for public bodies and companies entitled: "Biometrics: principles to be respected and legal obligations of organizations".[34] This guide is intended for both public bodies and companies[35] that wish to use a biometric system and are responsible for it. It also concerns companies that provide these solutions to organizations to help them advise their clients and offer products that comply with the legislation applicable in Québec. The guide sets out the steps to be taken by public or private organizations wishing to implement a biometric device. It can be summarized in three steps: conduct a preliminary analysis, declare the bank to the CAI, and comply with the obligations.

In summary, legislation already exists in Quebec to regulate biometrics-based technologies. However, it is now necessary to verify whether this legislation still provides an adequate framework for the deployment of biometric-based technologies, particularly in the context of their use by police forces in the public space. Quebec's laws, especially with respect to the protection of personal information, are insufficient.

The inadequacy of the legal framework (federal and provincial) is flagrant today and is regularly denounced in Canada by personal data protection authorities such as the Office of the Privacy Commissioner of Canada.[36] Moreover, current laws do not specifically regulate the use of facial recognition by police forces. Thus, there is no minimum standard of privacy protection, risk minimization or public transparency. A reform on all these aspects is needed. In Quebec, Bill 64 is a step in the right direction, but certain points of vigilance will have to be considered during parliamentary debates. In addition, facial recognition presents risks other than those related to the use of personal information.

Legislative Models in the European Union and the United States

As far as we know, no legislation specific to facial recognition has been adopted in Europe. Nevertheless, the European Union law, in particular the General Data Protection Regulation (GDPR) and the "police-justice" directive, which govern the protection of personal data,

[33] 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.

[34] 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.

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

[36] 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.

contain specific provisions on biometrics applicable to facial recognition. This legislation does not, however, make it possible to deal with all the risks associated with this technology. Moreover, in Europe, surveillance technologies are mainly the subject of targeted experiments, especially in airports and train stations. In addition, while no national legislation specific to facial recognition has been passed by the European Union member states, a few court decisions based on personal data protection and the EU Charter of Fundamental Rights are beginning to outline the contours of protection.

In comparison, technology deployment is much greater in the United States. At the same time, several laws dedicated to the use of surveillance technologies by law enforcement agencies in the public space, including facial recognition, have been adopted by certain cities or states, mainly in California and Massachusetts. However, most of the provisions provide for the use of this technology to be regulated rather than prohibited. The few prohibition laws have a limited scope of application and aim to prohibit the use of facial recognition when it is associated with technologies such as drones or police body cameras.

7. Recommendations

The tension between the social risks of the use of facial recognition by law enforcement agencies in the public space and the inadequacy of Quebec and Canadian laws leads to three recommendations:

Recommendation 1: Establish a Cost-Benefit Balance: Balance of Freedom/Security Interests

The use of facial recognition in public spaces for policing purposes has undeniable advantages for improving public safety. However, this technology raises questions and fears because of its potential for freedom and the completion of a surveillance society.

It is therefore advisable to look for the points of vigilance to legally and pertinently frame its use by police forces in the public space. To do so, it is necessary to determine the appropriate uses of this technology, to ensure their legality and social acceptability in order to guarantee their legitimacy.

Privacy is not an absolute right. Data protection legislation in Canada, as in other jurisdictions, balances the privacy rights of individuals with broader societal concerns. If a

balance of interests between privacy, liberty and security can be established, the criteria for doing so need to be clarified and a collective decision needs to be made as to where the cost/benefit balance should be struck.

Recommendation 2: Strengthen Privacy Laws in Quebec and Canada

Privacy and personal information protection laws must also be strong enough on their own to ensure a minimum level of protection. However, Canadian and Quebec laws date back 20 years and are far from being adapted to today's technology, a fortiori with respect to intrusive technologies such as facial recognition in the public space, which can lead to widespread surveillance and loss of anonymity.

Bill 64, which aims to strengthen privacy legislation in Quebec, is a step in the right direction, but there is still a need to strengthen protection when biometric data is used, as well as control over its use by the public sector. The risk of a shift in purpose must also be considered. As well, privacy impact assessment (PIA) should be broadly understood and should also integrate the assessment of risks to other fundamental rights.

Recommendation 3: Adopt Specific Restrictive Legislation if Law Enforcement Agencies are to be Conditionally Authorized to use Facial Recognition in Quebec and Canada

Whenever a balance must be struck between the needs of individuals and those of society, legislation is the best way to achieve that balance, especially when it comes to the means made available to law enforcement and the use of technologies that are particularly intrusive to rights and freedoms.

Consequently, the use of facial recognition by police forces must be provided for by law and regulated. Its use must be made public for the sake of transparency. In addition, an independent commission must authorize and control the use of facial recognition and compliance with the framework. This commission must be given sufficient powers, including significant powers to impose sanctions.

Annexes

Summary Table of EU Laws and Some Laws Applicable in 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, *S. et Marper c. Royaume-Uni*, 4 déc. 2008) et la jurisprudence de la Cour EDH peuvent être utile.	• **France :** Tribunal administratif de Marseille, 27 février 2020, n°1901249 / annulation d'un système de RF dans un établissement scolaire. Fondements : art. 4 & 9 du RGPD et art. 6 loi informatique et libertés • **Royaume-Uni :** Court of Appeal, 11 août 2020, *R (Bridges) -v- CC South Wales*, [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) Fondements: 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.

Summary Table of the Main Applicable Laws in the United States (Not Exhaustive)

	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 **Massachussetts** – 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 *An Act relating to facial recognition technology,* 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)	