JANVIER 2024

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

La reconnaissance faciale et les bases de données de photos signalétiques : document d'orientation à l'intention des services de police en Ontario

Le présent document d'orientation du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) a pour but de mieux faire comprendre les droits et obligations prévus par les lois ontariennes sur l'accès à l'information et la protection de la vie privée en ce qui concerne l'utilisation par la police de la technologie de reconnaissance faciale associée à des bases de données de photos signalétiques. Il ne saurait se substituer à ces lois et il ne contient pas de conseils juridiques. Il ne lie pas le Tribunal du CIPVP, qui peut être appelé à enquêter et à rendre une décision sur une plainte ou un appel en se fondant sur les circonstances et les faits pertinents. Pour obtenir la version la plus à jour du présent document, visitez www.cipvp.ca.

Remerciements

Le CIPVP a partagé une ébauche du présent document d'orientation avec un certain nombre de parties intéressées, dont les suivantes :

- Universitaires
- Organismes de la société civile et de droits de la personne
- Organismes de défense pénale, d'aide juridique et d'avocats
- Membres du Conseil consultatif stratégique du CIPVP
- Services de police municipaux
- Ministères du gouvernement provincial
- Commissions des domaines de la protection de la vie privée, des droits de la personne et du droit

Le CIPVP remercie ces organismes et particuliers de leurs commentaires judicieux.

Table des matières

Section 1 – Introduction

Contexte

En mai 2022, le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP), de concert avec ses homologues fédéral, provinciaux et territoriaux de l'ensemble du Canada (commissaires FPT), a rendu publique une **déclaration commune** réclamant un cadre juridique clair et complet pour contrer les risques du recours à la technologie de reconnaissance faciale par les services de police pour le droit à la vie privée et d'autres droits fondamentaux au Canada[1]. Entre-temps, les commissaires ont publié un **document d'orientation sur la protection de la vie privée** pour clarifier les obligations des services de police en matière de protection de la vie privée en vertu des lois actuelles et faire en sorte que tout recours à la reconnaissance faciale minimise les risques pour la vie privée et respecte le droit à la vie privée[2].

Les services de police de l'Ontario ont commencé à se servir de la technologie de reconnaissance faciale, entre autres technologies biométriques, pour rehausser l'efficacité de leurs initiatives de sécurité publique. Si elle est utilisée de façon responsable, la technologie de reconnaissance faciale, conjuguée aux bases de données de photos signalétiques (également appelées « photos d'identité judiciaire »), pourrait aider les services de police à trouver des pistes d'enquête.

La **reconnaissance faciale** (RF) est une technologie de l'intelligence artificielle (IA) qui permet de recueillir et de traiter des renseignements personnels délicats pour identifier un particulier ou vérifier son identité. La RF recourt à un système de traitement d'image pour analyser les traits du visage d'une personne, comme la largeur du nez, la longueur de la mâchoire et la distance entre les yeux (p. ex., sur une photo). À partir de ces traits du visage, les **algorithmes de RF** créent une **empreinte faciale**. Le système de reconnaissance faciale peut alors comparer deux empreintes faciales et produire une **cote de similarité** ou jumeler des empreintes faciales à l'issue d'une recherche dans une base de données de référence contenant un grand nombre d'images pour obtenir une liste de candidats possibles dont la cote de similarité est égale ou supérieure à un **seuil** établi.

Les bases de données de photos signalétiques que tiennent les services de police contiennent surtout de telles photos de personnes ayant été accusées de **crimes graves**. L'utilisation de la RF conjuguée à celles de bases de données de photos signalétiques peut permettre aux services de police d'effectuer l'**identification** plus rapidement et à plus grande échelle.

Les systèmes de reconnaissance faciale sont censés présenter des avantages, mais cette technologie soulève d'importants problèmes juridiques, éthiques et de protection de la vie privée, étant donné qu'elle peut donner des résultats biaisés ou inexacts et porter atteinte aux droits et libertés. Partout dans le monde, on s'interroge sur la manière de réglementer l'utilisation de ces systèmes[3].

---

1 Voir la déclaration commune des commissaires fédéral, provinciaux et territoriaux (FPT) à la protection de la vie privée, **Cadre juridique recommandé pour le recours à la reconnaissance faciale par les services de police.**

2 Voir la **Déclaration commune du Commissaire à l'information et à la protection de la vie privée de l'Ontario et de la Commission ontarienne des droits de la personne sur l'utilisation des technologies de l'intelligence artificielle**.

3 Voir le document **To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada** du Citizen Lab, Université de Toronto, International Human Rights Program.

En outre, des membres du public, de la société civile, du gouvernement et du monde universitaire ont exprimé des inquiétudes quant aux risques généraux liés à l'utilisation de la reconnaissance faciale, notamment :

- les risques pour le droit à la vie privée et d'autres droits fondamentaux, y compris le droit à l'égalité et à la non-discrimination, par exemple :
    - les préjugés et les inexactitudes liés au sexe et à la race;
    - des erreurs humaines ou de système pouvant se répercuter sur les particuliers, qui peuvent par exemple faire l'objet d'une surveillance ou de soupçons injustifiés ou excessifs, ou de détentions, d'arrestations ou d'accusations injustifiées;
    - la surveillance policière excessive des communautés à faibles revenus, noires et autochtones, ainsi que d'autres communautés marginalisées;
- un manque de transparence, de reddition de comptes et de surveillance des organisations qui adoptent la RF;
- le risque d'utilisation abusive, de manipulation et d'accès non autorisé aux **données biométriques des particuliers.**

Au moment de la publication du présent document d'orientation, aucun tribunal judiciaire ou administratif ne s'était encore prononcé sur la légalité des programmes de reconnaissance faciale associés à des bases de données de photos signalétiques, et notamment sur leur conformité à la Charte canadienne des droits et libertés (la « Charte »). Par ailleurs, il n'existe pas en Ontario de règles juridiques claires ou exhaustives sur l'utilisation par la police de la technologie de reconnaissance faciale, y compris lorsqu'elle est conjuguée à de telles bases de données. Bien que la Loi sur l'identification des criminels (LIC) permette à la police de photographier des personnes accusées de crimes graves et de compiler des renseignements connexes pour le maintien de l'ordre, cette loi n'aborde pas l'utilisation de la technologie de reconnaissance faciale, de la technologie de l'IA, de la biométrie ou des bases de données biométriques. Elle ne prévoit pas non plus de mesures de précaution ou de contrôle pour faire en sorte que les pratiques des services de police concernant les programmes de RF associés à des bases de données de photos signalétiques soient nécessaires, proportionnées et non discriminatoires. Il y a donc des lacunes dans la législation actuelle qui, si elles ne sont pas comblées, pourraient porter gravement atteinte au droit à la vie privée et à d'autres droits fondamentaux des particuliers.

Portée du présent document

Le présent document d'orientation propre à l'Ontario concernant l'utilisation par les services de police de la reconnaissance faciale associée à des bases de données de photos signalétiques s'appuie sur le document d'orientation FPT de mai 2022. Lors des consultations provinciales sur le document d'orientation FPT proposé, les services de police de l'Ontario et d'autres groupes ont souligné la nécessité de disposer d'une orientation réglementaire plus concrète sur des cas précis d'utilisation de la RF par les services de police. Le présent document d'orientation traite donc spécifiquement de l'utilisation par la police de logiciels de reconnaissance faciale pour identifier des personnes à l'aide d'une base de données de photos signalétiques en Ontario.

Les expressions « programme de reconnaissance faciale associé à une base de données de photos signalétiques », « programme de RF associé à une base de données de photos signalétiques » et « programme » sont utilisées tout au long du présent document pour désigner cette application particulière.

Le présent document d'orientation contient des recommandations visant à réduire des risques précis des programmes de RF associés à des bases de données de photos signalétiques. Il traite de facteurs clés liés à la protection de la vie privée, à la transparence et à la reddition de comptes, pour concevoir, utiliser et gérer ces programmes de manière responsable. Il contient également en annexe un glossaire et des recommendations clés.

Objet du présent document

Le CIPVP a élaboré le présent document d'orientation pour aider les services de police et les commissions des services policiers de l'Ontario (les « services de police »)[4] à respecter leurs obligations aux termes des lois ontariennes sur l'accès à l'information et la protection de la vie privée. Ce document devrait être utilisé par les services de police qui envisagent de mettre en place un programme de reconnaissance faciale associé à une base de données de photos signalétiques, y compris des programmes conjoints. Il s'applique aussi aux services de police qui ont déjà commencé à utiliser la reconnaissance faciale dans le cadre de programmes de ce genre. Le CIPVP recommande aux services de police d'examiner leurs programmes actuels en regard du présent document d'orientation dans les plus brefs délais.

Le présent document d'orientation ne cautionne pas l'utilisation de la technologie de reconnaissance faciale pour améliorer ou accélérer les recherches dans les bases de données de photos signalétiques. Il reconnaît que l'utilisation de cette technologie à cette fin n'est pas sans risque. Le présent document ne peut non plus remplacer la tenue d'un débat plus large sur la mise à jour des lois afin de régir plus efficacement l'utilisation de la reconnaissance faciale par les services de police. Il vise plutôt à alimenter le débat et la prise de décision sur la question de savoir si et comment les services de police peuvent utiliser de manière responsable la reconnaissance faciale associée aux bases de données de photos signalétiques, tout en respectant les droits des particuliers et de divers groupes de la population ontarienne. À l'instar d'autres technologies évoluées de l'IA, l'utilisation de la reconnaissance faciale par le secteur public en Ontario doit être assujettie à des balises claires et contraignantes qui tiennent compte de la sécurité, de la protection de la vie privée, de la reddition de comptes, de la transparence et des droits de la personne[5].

Il est recommandé de suivre les étapes décrites plus loin avant, pendant et après la mise en œuvre d'un programme de RF associé à une base de données de photos signalétiques. Cependant, les services de police pourraient devoir mettre en place des mesures supplémentaires de protection de la vie privée selon la nature, la complexité et la portée des risques que pose leur programme particulier.

4 Dans le présent document, toute mention des commissions des services policiers s'applique également au solliciteur général, dont relève la Police provinciale de l'Ontario.

5 Voir la **Déclaration commune du Commissaire à l'information et à la protection de la vie privée de l'Ontario et de la Commission ontarienne des droits de la personne sur l'utilisation des technologies de l'intelligence artificielle**.

Section 2 – Avant la mise en œuvre : facteurs clés d'ordre stratégique et juridique

Au moment d'envisager l'incidence sur la vie privée d'un programme technologique proposé, comme l'utilisation de la reconnaissance faciale conjuguée à des bases de données de photos signalétiques, les services de police devraient déterminer si les avantages d'un tel programme l'emportent clairement sur ses risques. Ils devraient également se demander si un tel programme est nécessaire et proportionné dans les circonstances avant de déterminer comment utiliser la technologie d'une manière qui respecte la vie privée et les droits de la personne. Voici les principaux facteurs à prendre en compte aux stades de la planification, de l'élaboration et des essais avant de mettre en œuvre un programme de RF associé à une base de données de photos signalétiques.

Facteur clé 1 : autorisation légale et utilisation légale

L'identification des personnes raisonnablement soupçonnées d'avoir commis une infraction grave est un objectif légitime aux fins de l'exécution de la loi. Cela dit, les programmes de RF associés à une base de données de photos signalétiques ont une incidence sur les attentes raisonnables en matière de vie privée des particuliers, particulièrement ceux dont les services de police conservent les photos signalétiques et les versent dans une telle base de données après que les accusations portées contre eux ont été rejetées ou retirées.

Dans ce contexte, on peut s'interroger sur la source et l'étendue des pouvoirs des services de police en matière de création, de stockage et d'utilisation d'empreintes faciales biométriques dans les bases de données de photos signalétiques, ainsi que sur l'absence de mesures de précaution et de contrôle adéquates. Pour mériter la confiance du public, il est donc nécessaire d'adopter une approche prudente, progressive, transparente et responsable de l'utilisation de la reconnaissance faciale. Il est particulièrement important de renseigner le public sur la source et la portée de l'autorisation légale d'agir lorsqu'il existe une incertitude juridique et des préoccupations importantes quant au caractère adéquat des mesures de précaution et de contrôle.

Les services de police ont le devoir de s'assurer qu'ils disposent d'une autorisation légale et qu'ils agissent conformément à la loi. Pour s'assurer qu'ils ont l'autorisation légale de concevoir et de gérer un programme de RF associé à une base de données de photos signalétiques en Ontario, les services de police doivent tenir compte des facteurs clés suivants :

- Un programme de reconnaissance faciale associé à une base de données de photos signalétiques comporte la collecte, la conservation, l'utilisation et la divulgation de renseignements personnels et doit être conforme à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP).
- La création d'empreintes faciales suppose généralement la collecte de nouvelles données biométriques personnelles à caractère délicat, qui se distinguent des photos utilisées pour créer ces données biométriques[6].

6 Voir l'**enquête PC-010005-1** du CIPVP sur l'utilisation par la Commission des alcools et des jeux de l'Ontario de la technologie de reconnaissance faciale dans les casinos de l'Ontario; le **rapport d'enquête F12-01** du commissaire à l'information et à la protection de la vie privée de Colombie-Britannique (B.C.I.P.C.) sur l'utilisation de la technologie de reconnaissance faciale par l'Insurance Corporation of British Columbia; les **conclusions en vertu de la LPRPDE no 2020-004** à l'issue de l'enquête sur Cadillac Fairview; les **conclusions en vertu de la LPRPDE no 2021-001** concernant

- La LAIPVP et la LAIMPVP autorisent les services de police à recueillir, à conserver et à utiliser des renseignements personnels et à se divulguer ces renseignements à des fins légitimes d'exécution de la loi. Toutefois, lorsque la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels suscite des attentes raisonnables en matière de vie privée, elle doit faire l'objet d'une autorisation distincte en vertu de la common law ou d'une loi[7]. En outre, les services de police ne sont généralement pas autorisés à recueillir, à conserver ou à utiliser des renseignements personnels qui ont été recueillis ou compilés contrairement à la loi par un autre organisme chargé de l'application de la loi, une institution ou un fournisseur de services tiers[8].
- Les tribunaux canadiens ont statué que la collecte, la conservation, l'utilisation et la divulgation de dossiers de non-condamnation en vertu de la *Loi sur l'identification des criminels* (LIC), et notamment de photos signalétiques et d'empreintes digitales, font l'objet d'attentes réduites, mais raisonnables, en matière de vie privée en vertu de l'article 8 de la Charte[9].
- Un programme de reconnaissance faciale associé à une base de données de photos signalétiques doit être conforme au Code des droits de la personne de l'Ontario et à la Charte, y compris au droit à la privée protégé par les articles 7 et 8 et au droit à l'égalité protégé par l'article 15. Les analyses de la Charte et des droits de la personne devraient tenir compte des préoccupations de longue date concernant les pratiques policières disproportionnées envers les communautés autochtones et racialisées et d'autres communautés marginalisées, ainsi que de la façon dont ces communautés peuvent être surreprésentées dans la collecte d'empreintes faciales, leur conservation et leur utilisation dans les bases de données de photos signalétiques[10]. Une analyse de la nécessité et de la proportionnalité d'un programme de reconnaissance faciale associé à une base de données de photos signalétiques est également pertinente en vertu de l'article 1 de la Charte.
- La LIC permet l'identification de certains particuliers en utilisant les « mensurations et autres opérations de dactyloscopie, de palmiscopie et de photographie ». Cependant, la LIC ne mentionne pas explicitement la reconnaissance faciale ou l'utilisation de bases de données conjuguée à la reconnaissance faciale. Il est conseillé aux services de police qui supposent que la LIC autorise la création et la comparaison d'empreintes faciales dans des bases de données biométriques d'examiner attentivement la portée de leur autorisation légale et de s'assurer qu'ils ont mis en place des mesures de précaution et de contrôle rigoureuses[11].

---

l'enquête sur Clearview AI; le **rapport d'enquête 23-02** du B.C.I.P.C. sur l'utilisation par les détaillants associés de Canadian Tire de la technologie de reconnaissance faciale.

7 Voir **R. v. Orlandis-Habsburgo**, 2017 ONCA 649 (CanLII); **R. c. Spencer**, 2014 CSC 43, [2014] 2 RCS 212; **R. v. El-Azrak**, 2018 ONSC 4450 (CanLII); **R. v. Otto**, 2019 ONSC 2514 (CanLII); **R. c. Marakah**, 2017 CSC 59 (CanLII), [2017] 2 RCS 608; **R. c. Jones**, 2017 CSC 60 (CanLII), [2017] 2 RCS 696.

8 Voir les décisions **MO-2225** et **PO-2826** du CIPVP et le rapport spécial du Commissariat à la protection de la vie privée du Canada intitulé **Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée** sur l'enquête réalisée concernant l'utilisation par la GRC de la technologie de Clearview AI.

9 Voir **R. c. Beare; R. c. Higgins**, 1988 CanLII 126 (CSC); R. v. Doré, [2002] O.J. No. 2845 (OCA); Lin v. Toronto Police Services Board, [2004] O.J. No. 170 (Ont. Sup. Ct.); **R. v. Strickland**, 2017 BCPC 1 (CanLII); **R. v. Strickland**, 2017 BCPC 211 (CanLII)**; R. v M.O.**, 2017 ONSC 1213 (CanLII); **R. v. Fogah-Pierre**, [2023] O.J. No. 1999 (ONSC)**.**

10 Voir par exemple **R. c. Le**, 2019 CSC 34 (CanLII); le deuxième rapport provisoire de la Commission ontarienne des droits de la personne, **Un impact disparate** et son rapport final, **From Impact to Action**; les renseignements sur la **collecte de données fondées sur la race et l'identité** du Service de police de Toronto et l'**article du Toronto Star** du 26 août 2022 sur les données relatives à la disproportionnalité provenant de la Police de la région de Peel.

11 Soulignons que dans Beare, la Cour suprême du Canada a statué que la LIC ne confère pas « le pouvoir illimité de recourir à n'importe quelle méthode d'identification. Seuls les procédés sanctionnés par le gouverneur en conseil sont autorisés. » De plus, la Cour a observé que la LIC prévoit « la publication des fiches, à titre de renseignements à l'usage

- Même si un tribunal judiciaire ou administratif établit que la LIC ou une autre loi autorise la création et la comparaison d'empreintes faciales dans des bases de données biométriques, l'autorisation conférée par la LIC de recueillir des photos signalétiques se limite aux personnes accusées de crimes graves et celle qu'elle confère de conserver ces photos est limitée à ce qui est nécessaire et proportionné.
- Les ententes entre les services de police et les fournisseurs tiers ou les fournisseurs de services commerciaux de technologie de reconnaissance faciale doivent prévoir des modalités qui garantissent le respect des lois s'appliquant aux services de police de l'Ontario, y compris des restrictions concernant la collecte, la conservation, l'utilisation et la divulgation subséquente de renseignements personnels ainsi que l'accès à ces renseignements. Les fournisseurs tiers ou les fournisseurs de services commerciaux et leurs produits doivent également être conformes aux lois sur la protection de la vie privée s'appliquant au secteur privé, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

Recommandations

1.1 S'assurer d'avoir l'autorisation légale de recourir à un programme de reconnaissance faciale associé à une base de données de photos signalétiques et de la documenter clairement avant le lancement du programme. Si un programme est déjà en place, réévaluer l'autorisation légale dès que possible.

1.2 Veiller à ce que la conception et le fonctionnement du programme, y compris le recours à des fournisseurs de services tiers, répondent à toutes les exigences légales et prévoient des mesures de précaution et de contrôle rigoureuses en matière de protection de la vie privée et de transparence.

1.3 S'il existe des lacunes sur le plan de l'autorisation légale, du respect de la loi ou de la protection des droits, il faut modifier la portée du programme de RF associé à une base de données de photos signalétiques afin de garantir le respect de la loi et la protection des droits fondamentaux.

Facteur clé 2 : principes directeurs

Pour garantir la confiance du public, les services de police devraient élaborer et communiquer au public les principes qui orienteront leurs décisions et leurs démarches lors de l'utilisation de la technologie de reconnaissance faciale associée à une base de données de photos signalétiques. Pour que le public accorde cette confiance et que la collectivité accepte ce programme, les principes directeurs doivent faire preuve de transparence et traduire l'engagement de la police de les respecter et de les appliquer.

À tout le moins, la déclaration de principes devrait s'engager à utiliser la reconnaissance faciale d'une manière qui :

- est nécessaire et proportionnée compte tenu des objets du programme;
- respecte les droits de la personne et fait de la dignité humaine une valeur fondamentale;

---

des responsables de l'exécution ou de l'application de la loi, mais je ne pense pas qu'il autorise leur conservation inconstitutionnelle. »

- respecte les droits des particuliers en matière de protection de la vie privée et d'accès à l'information;
- évite de causer des préjudices aux particuliers et groupes;
- est transparente et comptable au public;
- est toujours assujettie à une surveillance humaine, les résultats étant interprétés par des opérateurs qualifiés;
- considère toutes les correspondances possibles uniquement comme des pistes d'enquête;
- évalue le rendement du système et élimine les inexactitudes et les biais dans toute la mesure du possible;
- préserve l'intégrité du système de justice pénale et de l'administration de la justice;
- permet d'atteindre des objectifs de sécurité communautaire qui l'emportent sur le risque de préjudice.

Recommandations

2.1 Rédiger et rendre publique une déclaration de principes directeurs pour l'utilisation de la RF associée à une base de données de photos signalétiques, qui prévoit la prestation juste, efficace et équitable de services policiers d'une manière qui protège et valorise la vie privée, la transparence, la reddition de comptes et les droits de la personne.

2.2 Respecter ces principes et y souscrire à tous les stades de l'élaboration et de l'utilisation d'un programme de reconnaissance faciale associé à une base de données de photos signalétiques.

Facteur clé 3 : bases de données de photos signalétiques et politiques connexes

Afin que votre programme de RF associé à une base de données de photos signalétiques soit conçu et utilisé de manière responsable, il doit être structuré et régi de manière à tenir compte de l'environnement informationnel sous-jacent dans lequel il sera mis en œuvre.

Les responsables des services de police devraient prendre en considération les données probantes de plus en plus nombreuses selon lesquelles les dossiers d'arrestation versés dans une base de données de photos signalétiques peuvent être associés à des pratiques policières discriminatoires ou disproportionnées[12] et continuer à faire leur part pour renverser les effets de ces pratiques policières historiques et actuelles. Lorsqu'ils utilisent ou envisagent de mettre en place un programme de RF associé à une base de données de photos signalétiques, les services de police devraient déterminer dans quelle mesure les pratiques d'enquête et le contenu de la base de données reflètent des pratiques discriminatoires en matière d'enquête, d'arrestation et

12 Voir par exemple **R. c. Le**, 2019 CSC 34 (CanLII); le deuxième rapport provisoire de la Commission ontarienne des droits de la personne, **Un impact disparate** et son rapport final, **From Impact to Action**; les renseignements sur la **collecte de données fondées sur la race et l'identité** du Service de police de Toronto et l'**article du Toronto Star** du 26 août 2022 sur les données relatives à la disproportionnalité provenant de la Police de la région de Peel.

d'inculpation. Un volet essentiel de ce travail consiste à établir des exigences appropriées en matière de conservation et de destruction des dossiers contenus dans cette base de données.

Sauf exceptions limitées et circonscrites, il n'existe pas d'exigences légales quant à la conservation ou à la destruction des renseignements personnels recueillis aux termes de la LIC[13]. L'établissement de règles et d'exigences à cet égard est laissé à la discrétion des responsables de l'établissement de calendriers de conservation des documents, en l'occurrence les commissions des services policiers.

Dans l'exercice de leurs fonctions relatives à la mise en place de règles et d'exigences en matière de conservation et de destruction de documents, les commissions des services policiers doivent veiller à ce que les services de police ne conservent les photos signalétiques qu'aussi longtemps que cela est nécessaire et proportionné compte tenu des circonstances. Ces règles, exigences et procédures doivent au minimum reconnaître et protéger le droit à la vie privée et à l'égalité des jeunes, des personnes racialisées et autochtones ainsi que d'autres personnes et communautés vulnérables.

En outre, les personnes qui n'ont jamais été condamnées pour un crime grave et qui ne font l'objet d'aucune accusation ou instance en cours devraient être protégées contre la conservation et l'utilisation excessives de leurs renseignements personnels, en particulier ceux qui sont compilés dans des bases de données de photos signalétiques consultables. Pour ce faire, les services de police doivent mettre à jour leurs bases de données de photos signalétiques afin de s'assurer qu'elles rendent compte fidèlement des décisions définitives quant aux accusations criminelles[14] et suppriment de ces bases de données :

- les dossiers de non-condamnation;
- les dossiers d'arrestation pour infractions punissables sur déclaration sommaire de culpabilité, y compris les infractions mixtes[15] après que la Couronne a décidé de procéder par voie de procédure sommaire;
- les dossiers d'arrestation de personnes visées la *Loi sur le système de justice pénale pour les adolescents* (LSJPA), après l'expiration des périodes d'accès prévues aux termes de cette loi[16].

La suppression des dossiers des bases de données de photos signalétiques doit être effectuée dès que possible, en tenant compte de la nécessité de conserver les dossiers liés à des affaires ou à des appels. Les exceptions à ces exigences de suppression devraient être autorisées uniquement dans des situations très limitées, que les services de police devraient définir clairement dans leurs politiques, procédures, calendriers de conservation et autres directives. Les critères ou facteurs employés pour définir ces situations doivent être conformes aux lois susmentionnées au **facteur clé 1.** Lorsque ces critères sont appliqués à un cas particulier, la décision prise devrait être documentée et examinée dans le cadre de **vérifications annuelles de la conformité**.

---

13 La seule exception à cette règle réside dans les dispositions des articles 4 et 5 de la Loi sur l'identification des criminels, qui prévoient la destruction des empreintes digitales et des photographies pour les infractions qualifiées de contraventions en vertu de la Loi sur les contraventions et de la Loi sur le cannabis.

14 Voir **Shanthakumar v. CBSA**, 2023 ONSC 3180 (CanLII).

15 Pour des précisions sur les infractions mixtes et les infractions punissables par voie de déclaration sommaire de culpabilité, voir la définition de crime grave dans le glossaire du présent document.

16 Voir **R. v. Fogah-Pierre**, [2023] O.J. No. 1999 (ONSC), qui précise que les dossiers concernant des adolescents doivent être détruits systématiquement ou à tout le moins restreints afin que personne, y compris les services de police, ne puisse y accéder après l'expiration de la période d'accès énoncée à l'article 119 de la Loi sur le système de justice pénale pour les adolescents.

Recommandations

3.1 Avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, examiner les politiques concernant les dossiers d'arrestation et les calendriers de conservation, notamment ceux qui s'appliquent aux bases de données de photos signalétiques, pour s'assurer qu'ils ne permettent pas la conservation et l'utilisation excessives, discriminatoires, inconstitutionnelles ou autrement illégitimes des photos signalétiques.

3.2 Avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, et chaque année par la suite, supprimer de la base de données les dossiers qui reflètent ou pourraient favoriser des pratiques policières excessives, discriminatoires ou illégales, notamment :

- les dossiers de non-condamnation;
- les dossiers d'arrestation pour infractions punissables sur déclaration sommaire de culpabilité, y compris les infractions mixtes après que la Couronne a décidé de procéder par voie de procédure sommaire;
- les dossiers d'arrestation de personnes visées la *Loi sur le système de justice pénale pour les adolescents* (LSJPA), après l'expiration des périodes d'accès prévues aux termes de cette loi.

3.3 Si un programme de RF associé à une base de données de photos signalétiques a été mis en œuvre, examiner et supprimer les dossiers conformément aux recommandations 3.1 et 3.2, dès que possible et au plus tard un an après la publication du présent document d'orientation, puis chaque année au moins par la suite.

Facteur clé 4 : évaluations de l'incidence sur la vie privée

Les programmes de reconnaissance faciale associés à des bases de données de photos signalétiques présentent des risques élevés pour la vie privée en raison de la façon dont les données biométriques faciales et d'autres renseignements personnels peuvent être recueillis, utilisés, divulgués et conservés. Ces risques comprennent l'utilisation éventuellement abusive des renseignements personnels, des biais et inexactitudes et des erreurs technologiques ou humaines qui pourraient entraîner des reconnaissances fausses, des arrestations injustifiées et des enquêtes intrusives.

Vous devriez évaluer, réduire et surveiller ces risques et d'autres encore tout au long du cycle de vie de votre programme. Des mesures de précaution et de contrôle visant à assurer la protection de la vie privée doivent être mises en place dès le début de la conception et de l'élaboration de votre programme afin de protéger les renseignements personnels, y compris les **données d'entraînement**, les empreintes faciales biométriques, les images de référence, les bases de données de photos signalétiques et les renseignements recueillis lors de recherches par RF.

Généralement reconnue comme une pratique exemplaire, l'évaluation de l'incidence sur la vie privée (EIVP) est un outil de gestion des risques qui aide les institutions à évaluer les risques

possibles pour la vie privée d'un programme ou d'une activité[17]. L'EIVP peut également permettre de déterminer le fondement et la portée de votre autorisation légale, de rehausser la transparence et de respecter vos obligations en matière de protection de la vie privée en vertu de la loi. Pour mieux comprendre les risques pour la vie privée, vos obligations et les mesures d'atténuation des risques, consultez des experts en protection de la vie privée au début du processus d'EIVP.

Votre processus d'EIVP devrait être documenté dans un rapport d'EIVP, lequel devrait énumérer tous les risques pour la vie privée et expliquer les stratégies visant à les atténuer, notamment pour protéger le droit à la vie privée des particuliers et communautés dont les renseignements personnels pourraient être recueillis, conservés, utilisés ou divulgués dans les images de référence et dossiers de bases de données de photos signalétiques. Les stratégies d'atténuation des risques devraient comprendre :

- des politiques et procédures documentées visant à limiter les fins des recherches par reconnaissance faciale;
- la consignation de toutes les utilisations et divulgations de renseignements personnels;
- l'assignation de rôles et responsabilités clairs à un membre du personnel supérieur en ce qui concerne la surveillance des risques pour la vie privée et la vérification de la conformité.

Les EIVP devraient également tenir compte du fait que les programmes de RF associés à des bases de données de photos signalétiques :

- comprennent la collecte de données biométriques personnelles qui sont nouvelles et délicates, en plus des photos utilisées pour créer ces données biométriques[18];
- avoir une incidence sur la vie privée de tous les particuliers dont les renseignements personnels pourraient être utilisés aux fins de l'utilisation d'un système de reconnaissance faciale, et non seulement de ceux dont le système établit que les images pourraient constituer une correspondance éventuelle;
- font partie d'un système de dossiers d'arrestation que les services de police accumulent depuis de longues années, y compris des dossiers de non-condamnation;
- représentent une application de la technologie de RF qui est utilisée à l'insu ou sans le consentement des particuliers concernés;
- sont utilisés pour générer des pistes d'enquête qui pourraient notamment donner lieu à une surveillance injustifiée et à la consignation de données inutiles ou excessives (dans les dossiers d'enquêtes criminelles);
- pourraient faciliter la divulgation de renseignements personnels à des services de police de l'Ontario et à d'autres organismes d'exécution de la loi du Canada ou de pays étrangers.

Vous devrez probablement aussi procéder à d'autres évaluations des risques pour identifier et atténuer les menaces pour la sécurité, les préoccupations en matière de droits de la personne et les risques inhérents à la technologie de l'IA, y compris ceux liés aux logiciels et aux fournisseurs

17 Pour des précisions sur les EIVP, consultez **Planifier pour réussir : Guide d'évaluation de l'incidence sur la vie privée** du CIPVP.

18 Voir l'**enquête PC-010005-1** du CIPVP sur l'utilisation de la technologie de reconnaissance faciale par la Commission des alcools et des jeux de l'Ontario dans les casinos de la province; le **rapport d'enquête F12-01** du commissaire à l'information et à la protection de la vie privée de Colombie-Britannique (B.C.I.P.C.) sur l'utilisation de la technologie de reconnaissance faciale par l'Insurance Corporation of British Columbia; les **conclusions en vertu de la LPRPDE no 2020-004** à l'issue de l'enquête sur Cadillac Fairview; les **conclusions en vertu de la LPRPDE no 2021-001** concernant l'enquête sur Clearview AI; le **rapport d'enquête 23-02** du B.C.I.P.C. sur l'utilisation par les détaillants associés de Canadian Tire de la technologie de reconnaissance faciale.

de services tiers. Cela pourrait nécessiter la consultation d'experts compétents. Ces évaluations devraient être combinées ou coordonnées avec votre EIVP.

Recommandations

4.1 Effectuer une EIVP exhaustive et la documenter dans un rapport d'EIVP avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, y compris avant la tenue d'un projet pilote, et chaque fois que des changements importants sont apportés à un programme existant.

4.2 Indiquer dans le rapport d'EIVP les risques pour la vie privée de l'utilisation de la technologie de reconnaissance faciale conjuguée à une base de données de photos signalétiques (comme il est décrit plus haut) et prévoir des mesures de précaution et de contrôle pouvant être intégrées dans les politiques et procédures du programme afin d'atténuer ces risques.

4.3 Faire part des résultats de l'EIVP à la commission des services policiers et publier le rapport intégral ou un résumé par souci de transparence et de reddition de comptes.

4.4 Effectuer au besoin d'autres évaluations des risques, notamment pour la sécurité et les droits de la personne, et des évaluations de l'incidence algorithmique, et veiller à les combiner ou à les coordonner avec votre EIVP.

Facteur clé 5 : portée, objet et politiques du programme

Portée et objet du programme

Pour gérer de façon responsable votre programme de RF associé à une base de données de photos signalétiques, vous devriez en définir et en limiter la portée et l'objet. Ainsi, vous pourrez assurer que les principes de protection de la vie privée que sont le caractère raisonnable, la nécessité et la proportionnalité[19] permettent de réduire les risques pour la vie privée. Bien définir la portée et l'objet du programme peut également permettre d'éviter que sa portée ne s'élargisse, par exemple par l'ajout de fonctions de reconnaissance faciale à d'autres technologies de surveillance policière.

Un programme raisonnable, nécessaire et proportionné devrait avoir pour but de trouver des pistes d'enquête en vue d'identifier des personnes dont on soupçonne qu'elles ont commis une infraction grave.

Politiques et procédures du programme

Après avoir clairement défini la portée et l'objet de votre programme, vous devriez élaborer et approuver des politiques et procédures exhaustives qui sont conformes aux recommandations énoncées dans le présent document d'orientation. En incluant un glossaire de définitions et de termes clés relatifs à votre programme dans vos politiques et procédures, vous ferez en sorte que tous les membres de votre personnel interprètent de la même façon les éléments techniques et les processus.

19 Pour des précisions sur ces principes concernant la protection de la vie privée dans le contexte de l'utilisation de la reconnaissance faciale par les services de police, voir le document conjoint des commissaires FPT à la protection de la vie privée, **Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale**.

Recommandations

5.1 Établir et limiter la portée et l'objet du programme de RF associé à une base de données de photos signalétiques dès le départ, en se concentrant sur la production de pistes d'enquête dans le but d'identifier des personnes dont on soupçonne qu'elles ont commis une infraction grave. Veiller à ce que cette portée et cet objet soient tenus à jour et conformes à la législation applicable et aux principes de protection de la vie privée que sont le caractère raisonnable, la nécessité et la proportionnalité.

5.2 Élaborer et approuver, pour le programme de RF associé à une base de données de photos signalétiques, des politiques et procédures exhaustives qui sont conformes aux recommandations énoncées dans le présent document d'orientation.

Facteur clé 6 : mobilisation du public

Les activités de mobilisation du public devraient commencer dès les premières étapes de l'élaboration du programme, y compris avant la mise en place d'un programme pilote. Ces activités doivent être opportunes, informatives et prévoir des possibilités de dialogue sur les questions de protection de la vie privée et d'équité avec des membres de la communauté et des experts en la matière. Vous devriez également consulter les communautés concernées et les parties intéressées, en particulier les groupes faisant l'objet d'une surveillance policière excessive, comme les personnes appartenant à des communautés autochtones ou racialisées et à d'autres communautés marginalisées.

Vous devriez consulter le public sur la manière dont vous utiliserez la RF et protégerez les droits fondamentaux, y compris ceux des personnes dont les renseignements personnels pourraient être contenus dans les bases de données de photos signalétiques et la composition démographique de ces bases de données. Pour être pertinente, la mobilisation du public peut exiger plusieurs étapes, notamment le partage d'informations et de mises à jour importantes, la sollicitation de commentaires, la réponse à des questions et un dialogue critique. Dans le cas de programmes actuels ou en cours, vous devez procéder à des consultations publiques même si vous n'avez pas entamé ce travail de mobilisation au cours des premières étapes de l'élaboration de votre programme.

Enfin, consulter les communautés concernées et les parties intéressées et montrer publiquement que vous avez prévu et évalué les questions plus générales touchant la protection de la vie privée et les droits de la personne soulevées par la reconnaissance faciale *avant* de mettre en place votre programme favorisera la reddition de comptes et la transparence.

Recommandations

6.1 Mener des consultations publiques pertinentes auprès des communautés touchées et des parties intéressées au sujet du programme avant de le mettre en place. Il faut également procéder à des consultations publiques sur les programmes actuels ou en cours.

6.2 Lors des consultations publiques, s'assurer de prendre en compte les préoccupations en matière de protection de la vie privée et d'équité des communautés marginalisées, y compris celles qui sont touchées de manière

disproportionnée par la discrimination systémique et une surveillance policière excessive.

Facteur clé 7 : transparence

Bien avant de mettre en œuvre un programme de RF associé à une base de données de photos signalétiques, vous devez faire preuve de transparence envers le public quant à vos projets et à la nature évolutive du programme. Faire preuve de transparence dès le départ contribuera à gagner la confiance du public, y compris celle des communautés qui sont vulnérables et qui font l'objet d'une surveillance policière excessive. Les questions de transparence sont soulevées tout au long de ce document et ne se limitent pas à la présente section.

Recommandations

7.1 Publier des renseignements à jour, faciles d'accès et en langage clair concernant le programme sur les sites Web de la commission des services policiers et du service de police afin de favoriser une transparence continue.

Ces renseignements publics devraient comprendre :

- la version la plus récente des politiques et procédures du programme;
- l'EIVP et d'autres évaluations des risques ou, à tout le moins, des résumés de ces évaluations;
- une explication en langage simple du fonctionnement du programme, notamment sa portée et son objet, l'autorisation légale et les mesures de précaution et de contrôle;
- des précisions sur les consultations publiques qui ont eu lieu, y compris une description générale des parties consultées, la nature de la consultation (groupes de discussion, réunions, sondages) et un résumé général des observations reçues;
- des renseignements sur l'acquisition du système de reconnaissance faciale, y compris sur les fournisseurs de services tiers et leur respect de leurs obligations en matière de protection de la vie privée;
- les résultats des essais effectués afin de déterminer l'exactitude du système ou les biais, le cas échéant, y compris une description générale de la méthodologie;
- des statistiques sur l'efficacité globale du programme;
- des renseignements sur la marche à suivre pour les particuliers afin de demander l'accès à leurs renseignements personnels et leur rectification.

Facteur clé 8 : programmes pilotes

Si vous décidez de mettre en place un programme de RF associé à une base de données de photos signalétiques, vous devriez mener un programme pilote d'une durée limitée, assorti de buts et d'objectifs clairs, avant de procéder à la mise en œuvre complète de la technologie. L'évaluation des résultats du programme pilote vous aidera à apporter les modifications

nécessaires aux éléments clés de votre programme, y compris l'EIVP et les politiques et procédures.

Un programme pilote de RF associé à une base de données de photos signalétiques devrait à tout le moins permettre de déterminer :

- si les avantages escomptés du système ont été obtenus et si des risques ou préjudices imprévus se sont manifestés;
- si les demandes et les procédures de recherche du RF sont suivies correctement, et notamment si les résultats des recherches sont bien documentés (voir le **facteur clé 11** pour des précisions sur la documentation);
- si le personnel qui utilise le système de RF a reçu une formation adéquate pour interpréter les correspondances signalées par le système à la suite d'une recherche et pour comprendre les capacités et les limites du système;
- si les paramètres du système, comme les seuils minimums pour une correspondance, sont réglés de manière appropriée ou doivent être modifiés, par exemple pour éviter les **faux positifs** et favoriser l'évaluation du programme;
- s'il existe des signes d'erreur, d'inexactitude ou de biais dans les résultats du système ou dans l'interprétation de ces résultats par le personnel ou les agents.

Après l'évaluation du programme pilote, les parties consultées devraient être informées de ses principales conclusions dans le cadre d'un processus pertinent de mobilisation du public.

Recommandations

8.1 Mener un programme pilote d'une durée limitée, assorti de buts et d'objectifs clairs, avant de mettre intégralement en œuvre la technologie. Ce programme pilote doit consister à mettre le programme à l'essai pour s'assurer qu'il permet d'atteindre les résultats escomptés, à repérer et à résoudre tout problème ou conséquence imprévus et à atténuer les risques pour la vie privée et les droits de la personne.

8.2 Évaluer les résultats du programme pilote et en rendre compte publiquement avant la mise en œuvre, en communiquant ses principales conclusions aux communautés concernées et aux parties intéressées dans le cadre d'un processus pertinent de mobilisation du public.

Section 3 – Facteurs clés d'ordre opérationnel

Facteur clé 9 : qualité des images de référence

Les services de police recueillent souvent des images de référence dans le cadre d'enquêtes criminelles. La qualité de ces images peut varier. Pour favoriser l'utilisation légale et rigoureuse de la RF, réduire les risques d'erreurs d'identification et faciliter l'examen et l'évaluation du programme, il y a lieu d'établir des normes minimales de qualité des images de référence. Plus précisément :

- Fixer des normes concernant la densité des pixels, l'éclairage, le pourcentage du visage qui est visible et tout autre facteur susceptible d'avoir une incidence importante sur l'exactitude des résultats des recherches effectuées au moyen du système de reconnaissance faciale. Ces normes devraient servir à appuyer les opérateurs qualifiés, mais ceux-ci devraient quand même se fonder sur leur jugement. En outre, ces normes devraient être employées pour favoriser l'examen et l'évaluation efficaces et objectifs du programme de RF associé à une base de données de photos signalétiques.
- Éviter d'utiliser des dessins d'artistes, des portraits-robots ou des photos de personnes ressemblantes comme images de référence. Des études ont montré que les systèmes de reconnaissance faciale sont peu performants à l'analyse de portraits-robots, ce qui pose un risque accru d'erreurs d'identification et de résultats de recherche médiocres[20].
- Éviter de modifier numériquement les images de référence. S'il est justifié de modifier une image (p. ex., lorsqu'il faut flouter ou supprimer les visages d'autres personnes en arrière-plan pour protéger leur vie privée), documenter toutes les mesures prises pour la modifier.

Recommandation

9.1 Pour favoriser l'utilisation légale et précise de la reconnaissance faciale, il y a lieu de fixer et d'appliquer des normes claires pour que les images de référence répondent à des critères minimums de qualité, conformément aux normes recommandées dans le présent document d'orientation.

Facteur clé 10 : conservation des images de référence

Pour minimiser les atteintes au droit à la vie privée, vous devriez vous assurer que votre programme de RF associé à une base de données de photos signalétiques n'enregistre pas, ne stocke pas ou ne conserve pas automatiquement les images de référence après une recherche par reconnaissance faciale. Ne conservez l'image de référence que le temps nécessaire, par exemple, s'il s'agit d'un élément de preuve dans le cadre d'une instance pénale. Les images de référence qui deviennent des éléments de preuve dans une telle instance peuvent être soumises à des exigences de conservation supplémentaires en vertu des règles de preuve, lesquelles dépassent la portée du présent document d'orientation.

Certaines images de référence ne donneront pas lieu à une correspondance lors d'une recherche dans une base de données de photos signalétiques. On les appelle des images de référence non identifiées. Elles non plus ne doivent pas être conservées plus longtemps que nécessaire. À moins que leur conservation ne soit exigée par la loi ou pour la bonne administration de la justice, les images de référence non identifiées doivent être détruites :

- si la personne n'est plus un suspect dans le cadre de l'enquête criminelle en question;
- si l'image de référence non identifiée n'est plus pertinente dans le cadre de l'enquête criminelle;
- dans les 30 jours suivant la fin de l'enquête criminelle;
- dans les 30 jours suivant une décision définitive selon laquelle l'image de référence non identifiée a été recueillie illégalement;

20 Voir le document **Garbage In, Garbage Out. Face Recognition on Flawed Data** du Georgetown Law Center on Privacy and Technology.

- si les règles de conservation des dossiers de la commission des services de police exigent leur destruction;
- si leur destruction est requise en vertu de loi (p. ex., selon une ordonnance judiciaire définitive).

Vous pourriez devoir conserver des images de référence (y compris des images de référence non identifiées) pendant une période plus longue que celle qui serait normalement appropriée pour soumettre votre système de RF à des essais de rendement. Toute conservation d'images de référence à des fins d'essai doit être limitée à ce qui est strictement nécessaire pour répondre aux exigences de précision ou à d'autres exigences de rendement de votre programme. Les images conservées pour les essais doivent être détruites dès que ceux-ci sont terminés.

Recommandations

10.1 Établir des règles et des processus clairs concernant la durée de conservation des images de référence (y compris les images de référence non identifiées) et le moment où elles doivent être détruites de façon sécurisée. Ces règles et processus doivent être compatibles avec les circonstances décrites dans le présent document d'orientation.

10.2 Mettre en place un processus de surveillance approprié pour confirmer régulièrement le respect des règles de conservation et de destruction s'appliquant aux images de référence (y compris les images de référence non identifiées).

Facteur clé 11 : exactitude, examen et surveillance humaine des résultats

Pour garantir l'exactitude, l'équité et l'absence de biais dans la prestation des services, ainsi que l'efficacité générale de votre programme, vous devriez documenter et expliquer comment vous interpréterez les résultats des recherches effectuées au moyen de la RF et comment vous y donnerez suite. Il est essentiel de soumettre ces programmes à des essais et à une surveillance humaine pour éviter de trop s'en remettre à des algorithmes éventuellement défaillants. Si l'on n'examine pas avec soin les résultats de la recherche ou si l'on y accorde trop de crédibilité, on risque de soumettre une personne à une enquête inutile ou injuste.

Exactitude

Vous ne devriez pas présumer de l'exactitude du logiciel de RF et des résultats que produit votre système de RF. La qualité, la fiabilité et les taux de précision des systèmes de RF varient. Des recherches ont montré que les personnes racialisées et les femmes sont plus susceptibles d'être incorrectement identifiées par la technologie de reconnaissance faciale[21]. En outre, le rendement des systèmes de RF a tendance à se dégrader lorsque les images datent de plus de cinq ans[22].

Vous devrez prendre des mesures pour minimiser les inexactitudes et les biais que présente votre système de RF. Il s'agit notamment d'évaluer à l'interne si les paramètres du système, comme le

21 Voir le document **To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada** du Citizen Lab, Université de Toronto, International Human Rights Program.

22 Voir l'article de New Scientist intitulé **Face recognition struggles to recognize us after five years of ageing**.

seuil minimum pour une correspondance, sont correctement réglés ou s'ils doivent être modifiés, par exemple, pour éviter les faux positifs et favoriser l'évaluation du programme.

La correspondance entre une image de référence et une empreinte faciale contenue dans une base de données de photos signalétiques est généralement évaluée en fonction d'un seuil préétabli (p. ex., une cote de similarité précise, ou un nombre prédéterminé de correspondances possibles). Le seuil à établir repose sur la nature et la portée de votre programme. Pour fixer un seuil approprié, vous devez relever les risques pour les droits et libertés des particuliers, y compris ceux qui appartiennent à des groupes pour qui les taux de faux positifs sont élevés, en tenir compte et les atténuer.

Opérateurs qualifiés

Seuls les membres du personnel des services de police qui sont des opérateurs qualifiés du système de RF et qui respectent les politiques et procédures prescrites devraient pouvoir effectuer des recherches et des examens au moyen de ce système et des examens pour le compte des enquêteurs qui en font la demande.

Un opérateur qualifié doit déterminer s'il existe une possibilité raisonnable de correspondance entre une image de référence et une photo signalétique. L'opérateur doit pouvoir déroger aux résultats de recherche générés par le système de RF selon des pratiques exemplaires visant à réduire les erreurs et à minimiser les biais et les inexactitudes[23].

Même s'il est très probable qu'une correspondance générée par le système de RF soit exacte, les résultats doivent toujours être examinés par des opérateurs qualifiés, à titre de précaution. **Toute correspondance résultante doit être considérée uniquement comme une piste d'enquête et non comme l'identification certaine d'une personne.**

Contrôle des résultats

Les opérateurs qualifiés et le personnel dirigeant qui sont responsables du système de RF devraient être comptables de leurs décisions et actions lorsqu'ils recourent à la reconnaissance faciale. Ils devraient s'efforcer de réduire le risque global de résultats inexacts et biaisés et expliquer comment ils s'y prennent pour ce faire.

Recommandations

11.1 Prendre régulièrement des mesures pour minimiser les inexactitudes et les biais que présente le système de RF. Il s'agit notamment d'évaluer à l'interne si les paramètres du système, comme le seuil minimum pour une correspondance, sont correctement réglés ou s'ils doivent être modifiés, par exemple, pour éviter les faux positifs et favoriser l'évaluation du programme.

11.2 Définir et suivre des procédures transparentes pour l'examen humain et les contrôles d'exactitude du programme. Ces procédures devraient préciser qui est responsable de l'examen, comment les opérateurs qualifiés interprètent et expliquent les résultats des recherches effectuées au moyen de la RF et quelles sont les exigences en matière de formation pour ce travail. Les opérateurs qualifiés doivent se fonder

23 Pour des précisions sur les aspects touchant l'exactitude, voir le document conjoint des commissaires FPT à la protection de la vie privée, **Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale**.

sur des critères précis et être en mesure d'expliquer clairement les étapes et les processus suivis pour générer des pistes d'enquête.

11.3 Définir et respecter des exigences en matière de documentation de toutes les recherches effectuées au moyen de la RF et de tous les résultats d'évaluation. Cette documentation doit porter sur l'image de référence et le seuil de correspondance utilisés, la probabilité de correspondance, le résultat obtenu par le système de RF, l'opérateur qualifié qui a effectué la recherche, la décision prise par l'opérateur à l'issue de l'évaluation de traiter ou non une correspondance éventuelle comme un faux positif ou comme une piste d'enquête possible, ainsi que tout autre renseignement pertinent.

Facteur clé 12 : limites à la collecte, à la conservation, à l'utilisation ou à la divulgation de renseignements personnels et mesures de précaution raisonnables

Vos politiques et procédures devraient faire en sorte que toute collecte, conservation, utilisation ou divulgation de documents liés à votre programme de RF associé à une base de données de photos signalétiques soit limitée et conforme à la loi[24].

Comme il est indiqué au **facteur clé 1**, les services de police de l'Ontario peuvent recueillir, conserver, utiliser ou divulguer des renseignements personnels uniquement en conformité aux dispositions de la LAIPVP et de la LAIMPVP qui s'appliquent à eux. La collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels qui suscite une attente raisonnable en matière de vie privée doit faire l'objet d'une autorisation indépendante en vertu de la common law ou d'une loi et nécessite une évaluation de son autorisation légale. Il faut veiller tout particulièrement à limiter la collecte, la conservation, l'utilisation ou la divulgation de données biométriques, compte tenu du fait qu'elles sont plus délicates que d'autres types de renseignements personnels.

En outre, vous devez prendre des mesures de sécurité raisonnables pour protéger les renseignements personnels dont vous avez la garde ou le contrôle. Ces mesures doivent comprendre des contrôles administratifs, techniques et physiques complets et des mesures de précaution pour la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels.

Recommandations

12.1 Veiller à ce que la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels se limite à ce qui est nécessaire et proportionné pour réaliser l'objet déclaré du programme de RF associé à une base de données de photos signalétiques.

12.2 S'assurer que les exigences relatives à la collecte, à la conservation, à l'utilisation ou à la divulgation des renseignements personnels sont bien documentées dans les politiques et procédures connexes et qu'elles tiennent compte des

24 Selon l'article 2 de la LAIPVP et de la LAIMPVP, « document » s'entend d'un « document qui reproduit des renseignements sans égard à leur mode de transcription, que ce soit sous forme imprimée, sur film, au moyen de dispositifs électroniques ou autrement ».

différents éléments du programme de RF (p. ex., les bases de données de photos signalétiques, les images de référence et les données d'entraînement).

12.3 Mettre en place des contrôles et des mesures de précaution d'ordre administratif, technique et physique pour la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels dans le cadre du programme, y compris des mesures de précaution visant à protéger les données biométriques.

Facteur clé 13 : droits en matière d'accès aux renseignements personnels et de rectification et suppression de ces renseignements

Sauf exceptions limitées et précises, les particuliers dont vous avez la garde ou le contrôle des renseignements personnels ont le droit d'accéder à ces renseignements et de les rectifier en vertu de l'article 47 de la LAIPVP et de l'article 36 de la LAIMPVP. Le grand public, les groupes de la société civile, les journalistes et d'autres entités jouissent également d'un droit général d'accès à l'information en vertu de l'article 10 de la LAIPVP et de l'article 4 de la LAIMPVP. Vous devez donc mettre en place des procédures pour répondre aux demandes d'accès et aider les particuliers ou leurs représentants à exercer leurs droits en la matière, tout en respectant les exigences relatives à la protection de la vie privée.

De plus, les personnes accusées d'une infraction criminelle ont le droit, en vertu de la common law, de demander que leur photo signalétique et d'autres documents relatifs à leur arrestation soient supprimés lorsque les accusations ont donné lieu à une décision de non-condamnation. Sauf circonstances exceptionnelles bien définies et justifiables, la police doit faire droit à ces demandes de suppression.

Recommandations

13.1 Veiller à ce que les politiques et les procédures soient conformes aux droits d'accès, de rectification et de suppression et à ce qu'elles en tiennent compte.

13.2 Veiller à publier les politiques et les procédures ainsi que des renseignements en langage simple sur les droits d'accès, de rectification et de suppression.

Facteur clé 14 : demandes d'autres services de police

Il peut arriver que l'on vous demande d'effectuer une recherche par reconnaissance faciale avec une image de référence pour le compte d'un autre service de police afin de vérifier si un suspect inconnu peut être identifié au moyen de votre base de données de photos signalétiques. Pour assurer la reddition de comptes dans ces situations, vous devriez créer un formulaire standard à l'usage du service de police demandeur, qui décrit les conditions à remplir avant que vous ne décidiez d'approuver ou non la demande, y compris les suivantes :

- la demande de recherche d'image de référence doit être présentée par écrit (p. ex., un formulaire précisant le nom de l'agent, son numéro matricule et ses coordonnées, le service de police, la date, des précisions sur les renseignements demandés et le numéro d'enquête);

- la demande doit avoir une fin compatible avec la portée de votre programme (p. ex., avoir trait à une enquête sur un crime grave);
- l'image de référence doit être d'une qualité suffisante pour répondre à vos normes minimales (voir le **facteur clé 9**);
- les renseignements dont vous ferez part au service de police demandeur ne serviront que de pistes d'enquête et ne seront pas communiqués sans votre accord exprès;
- le service de police demandeur détruira définitivement, supprimera ou vous rendra les renseignements communiqués dès que l'une ou l'autre des situations suivantes s'appliquera :
    - les renseignements ne sont plus nécessaires à l'enquête, conformément aux critères de destruction des images de référence non identifiées établis au **facteur clé 10**; ou
    - les documents associés à la photo signalétique devraient être supprimés selon les critères énoncés dans la **recommandation 3.2**.

Vous devez tenir des registres détaillés de toutes les demandes émanant d'autres services de police et de vos réponses à ces demandes. Cela permettra d'assurer la reddition de comptes et la surveillance, notamment à des fins de vérification et d'établissement de rapports publics.

Recommandations

14.1 Définir et appliquer des politiques et des procédures claires pour le traitement des demandes de RF émanant d'autres services de police, y compris pour :

- recevoir et traiter les demandes de tels services visant à effectuer des recherches de RF dans sa base de données de photos signalétiques;
- communiquer les résultats de toute correspondance possible au service de police demandeur;
- tenir des registres et des journaux détaillés de tous les accès à des renseignements personnels et de toutes les divulgations de tels renseignements, comme les demandes de recherche de RF reçues, si elles ont été traitées et comment, leurs résultats et les renseignements fournis au service de police demandeur, s'il y a lieu.

Facteur clé 15 : programmes conjoints de reconnaissance faciale associés à des bases de données de photos signalétiques

Certains services de police de l'Ontario envisagent de combiner leurs bases de données de photos signalétiques avec celles d'autres services afin d'améliorer leur capacité collective à utiliser la RF pour générer des pistes d'enquête. Cela donnerait lieu à un programme conjoint de reconnaissance faciale associé à des bases de données de photos signalétiques. Le présent document d'orientation s'applique à tout programme conjoint actuel ou éventuel.

La combinaison de bases de données de photos signalétiques à des fins de RF doit être envisagée avec une prudence accrue, car elle peut aggraver les risques pour la vie privée et les droits de la personne que comportent les programmes autonomes. Consultez vos experts en la

matière, les services juridiques et le public pour déterminer si la mise en place d'un programme commun est nécessaire et proportionnée.

À supposer que vous ayez l'autorisation légale de procéder, toute initiative visant à combiner des bases de données de photos signalétiques devrait se limiter à des services de police de l'Ontario, du moins jusqu'à ce que la RF fasse l'objet d'un cadre juridique clair et complet au Canada.

Après avoir réalisé une EIVP commune et les autres évaluations des risques qui s'imposent, les commissions des services policiers et les services de police devraient collaborer à l'élaboration de cadres de gouvernance équivalents pour toutes les parties à un programme conjoint, en se fondant sur le présent document d'orientation. Ce cadre devrait comprendre des ententes officielles d'échange de renseignements ainsi que des politiques, procédures et exigences connexes liant les parties. Ces ententes devraient limiter explicitement l'utilisation par les services de police des photos signalétiques partagées aux seules fins d'un programme raisonnable, nécessaire et de portée adéquate, à la réalisation de vérifications régulières du programme conjoint, à la préparation d'un rapport exigé par l'entente ou à des fins exigées par la loi.

Recommandations

15.1 Chaque service de police participant à un programme conjoint de RF associé à une base de données de photos signalétiques devrait déterminer s'il a l'autorisation légale requise et suivre tous les facteurs et recommandations figurant dans le présent document d'orientation, notamment :

- réaliser une EIVP commune et les autres évaluations des risques qui s'imposent;
- conclure une entente officielle d'échange de renseignements;
- établir des politiques, des procédures et des exigences connexes liant toutes les parties au programme conjoint et leur imposant des normes et mesures de précaution équivalentes, conformément au présent document d'orientation.

15.2 L'entente d'échange de renseignements devrait limiter explicitement l'utilisation des photos signalétiques partagées aux fins suivantes :

- mise en œuvre d'un programme raisonnable, nécessaire et de portée adéquate (qui vise uniquement à générer des pistes d'enquête sur des crimes graves);
- essais, vérifications et examens réguliers du programme conjoint et rapports connexes;
- établissement du rapport exigé aux termes de l'entente;
- autres fins que la loi exige.

15.3 Avant de combiner leurs bases de données de photos signalétiques, les services de police devraient revoir leurs politiques en matière de dossiers d'arrestation, leurs calendriers de conservation des documents et leurs bases de données, et supprimer les dossiers qui reflètent des pratiques de conservation excessives, discriminatoires ou illégales, y compris les dossiers de non-condamnation, comme indiqué au facteur clé 3.

15.4 Chaque commission des services policiers concernée devrait soumettre régulièrement tout programme conjoint à des vérifications et à des évaluations de son efficacité et de sa pertinence, et rendre publics les rapports de vérification et les évaluations.

Section 4 – Examen et évaluation du programme

Facteur clé 16 : surveillance et réévaluation continues

Comme d'autres technologies de l'IA, la reconnaissance faciale utilisée en lien avec des bases de données de photos signalétiques présente de nouvelles possibilités pour les forces de l'ordre, et pose de nouveaux défis qui requièrent des mesures de contrôle et de réévaluation pour faire en sorte que la technologie soit exploitée de la manière la plus digne de confiance et la plus sécuritaire possible tout au long de son cycle de vie[25]. Si vous mettez en place un programme de RF associé à une base de données de photos signalétiques, vous devriez assurer l'évaluation régulière du rendement du système de RF et des risques qu'il présente pour la vie privée, et vous tenir au fait des avancées sur le plan de l'utilisation de la technologie de RF. Vous devriez adapter vos pratiques en fonction des résultats de votre évaluation et de tout nouvel élément d'information, des risques émergents et des pratiques exemplaires. Ce faisant, vous pouvez atténuer et limiter les préjudices liés aux erreurs ou biais potentiels du système, les erreurs d'identification, les lacunes du programme, les menaces pour la sécurité ou l'utilisation abusive ou le traitement inapproprié de données biométriques délicates, qui pourraient vous obliger à réévaluer et à mettre à jour la conception et l'utilisation de votre programme ou de votre système de RF[26].

Vous devriez également revoir votre EIVP et toute autre évaluation des risques que vous avez réalisée afin de confirmer que les risques ont été effectivement réduits et qu'aucune répercussion imprévue n'est survenue. En cas de nouvelles répercussions ou de nouveaux risques, il y a lieu de mettre à jour ou de réévaluer en conséquence l'EIVP ainsi que les politiques et les procédures du programme. Vous devriez également envisager de consulter le CIPVP si de nouvelles répercussions ou de nouveaux risques importants se présentent.

Recommandations

16.1 Lorsque le programme de RF associé à une base de données de photos signalétiques a été mis en œuvre, surveiller et réévaluer régulièrement le rendement du système et ses risques pour la vie privée en se fondant sur les renseignements à disposition, les risques émergents, les pratiques exemplaires et les avancées générales sur le plan de l'utilisation de la technologie de reconnaissance faciale.

16.2 Déterminer s'il y a lieu de réévaluer et de mettre à jour les évaluations des risques, y compris l'EIVP, ainsi que les politiques, les procédures, la conception d'ensemble et le fonctionnement du programme ou système de RF.

16.3 Envisager de consulter le CIPVP en cas de nouvelles répercussions ou de nouveaux risques importants.

25 Voir le rapport du Forum économique mondial intitulé **A policy framework for responsible limits on Facial Recognition. Use Case: Law Enforcement Investigations**.

26 Voir le chapitre **Paysage technique de l'IA** de l'ouvrage de l'Organisation de coopération et de développement économiques (OCDE) intitulé L'intelligence artificielle dans la société.

Facteur clé 17 : reddition de comptes

Afin de démontrer la conformité de votre programme de RF associé à une base de données de photos signalétiques et d'assurer la reddition de comptes au public, des experts internes ou externes devraient effectuer chaque année une vérification de la conformité[27]. Une telle vérification devrait évaluer à tout le moins :

- la conformité à l'autorisation légale et à d'autres exigences juridiques;
- la conformité aux politiques et procédures de votre programme;
- la pertinence et la fréquence des mises à jour des politiques et procédures de votre programme, y compris des informations publiques et des rapports à son sujet;
- les méthodes d'examen du contenu des bases de données de photos signalétiques afin de réduire les biais et de maintenir des pratiques de suppression régulière conformes aux règles et exigences en matière de conservation;
- les plaintes éventuelles du public concernant votre programme et leur traitement;
- les atteintes à la vie privée qui sont survenues, le cas échéant, et les mesures prises;
- la conformité des tiers aux obligations de votre programme en matière de protection de la vie privée.

Les services de police, par l'intermédiaire de leurs commissions des services policiers, devraient également procéder à un examen annuel du programme de RF associé à une base de données de photos signalétiques afin d'en mesurer l'efficacité globale, et notamment de déterminer s'il atteint l'objectif établi et s'il respecte les principes directeurs. Cet examen devrait s'appuyer sur des critères précis, comme des statistiques clés. Ces statistiques annuelles devraient comprendre au moins :

- des précisions sur la taille et la composition démographique des bases de données concernées, y compris en ce qui concerne les catégories de documents décrites à la section 3.2 (dossiers de non-condamnation, dossiers d'arrestation pour infractions punissables sur déclaration sommaire de culpabilité, dossiers d'arrestation de personnes visées par la Loi sur le système de justice pénale pour les adolescents);
- le nombre et la nature des recherches de RF effectuées au cours de l'année écoulée, y compris les demandes formulées par d'autres services de police;
- des indicateurs sur l'efficacité du programme, comme le nombre de pistes d'enquête générées grâce à la RF associée à des bases de données de photos signalétiques, ainsi que le nombre d'accusations et de condamnations associées à ces pistes.

Par souci de reddition de comptes et de transparence, vous devriez publier ces statistiques annuelles afin de renseigner le public sur votre programme et lui permettre de constater que la technologie de reconnaissance faciale est employée de façon responsable.

Recommandations

17.1 Définir et appliquer des mesures permanentes de reddition de comptes, comprenant des vérifications annuelles de la conformité, afin d'évaluer la conformité du programme aux exigences légales, règles, politiques et procédures, et notamment

27 Le service de police ou sa commission des services policiers pourrait envisager de confier la vérification de conformité à un tiers indépendant.

la conformité des tiers participant au programme et des examens annuels du programme afin de déterminer si ce dernier atteint l'objectif établi et respecte les principes directeurs.

17.2 Évaluer les résultats des vérifications annuelles de la conformité et des examens du programme et en rendre compte publiquement, notamment en fournissant au public des statistiques et des informations annuelles relatives à la conformité, à l'efficacité et à la pertinence du programme.

Annexe

Annexe A : Recommandations

Vous trouverez ci-dessous des recommandations clés, à titre de référence uniquement.

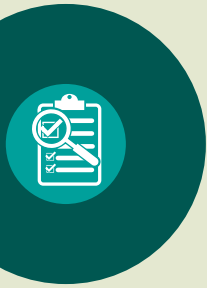
Le CIPVP formule les recommandations suivantes aux commissions des services policiers et aux services de police pour la conception et l'utilisation d'un programme de reconnaissance faciale associé à une base de données de photos signalétiques en Ontario :

Facteur clé 1 : autorisation légale et utilisation légale

1.1. S'assurer d'avoir l'autorisation légale de recourir à un programme de reconnaissance faciale associé à une base de données de photos signalétiques et de la documenter clairement avant le lancement du programme. Si un programme est déjà en place, réévaluer l'autorisation légale dès que possible.

1.2. Veiller à ce que la conception et le fonctionnement du programme, y compris le recours à des fournisseurs de services tiers, répondent à toutes les exigences légales et prévoient des mesures de précaution et de contrôle rigoureuses en matière de protection de la vie privée et de transparence.

1.3. S'il existe des lacunes sur le plan de l'autorisation légale, du respect de la loi ou de la protection des droits, il faut modifier la portée du programme de RF associé à une base de données de photos signalétiques afin de garantir le respect de la loi et la protection des droits fondamentaux.



Facteur clé 2 : principes directeurs

2.1. Rédiger et rendre publique une déclaration de principes directeurs pour l'utilisation de la RF associée à une base de données de photos

signalétiques, qui prévoit la prestation juste, efficace et équitable de services policiers d'une manière qui protège et valorise la vie privée, la transparence, la reddition de comptes et les droits de la personne.

2.2. Respecter ces principes et y souscrire à tous les stades de l'élaboration et de l'utilisation d'un programme de reconnaissance faciale associé à une base de données de photos signalétiques.

Facteur clé 3 : bases de données de photos signalétiques et politiques connexes

3.1 Avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, examiner les politiques concernant les dossiers d'arrestation et les calendriers de conservation, notamment ceux qui s'appliquent aux bases de données de photos signalétiques, pour s'assurer qu'ils ne permettent pas la conservation et l'utilisation excessives, discriminatoires, inconstitutionnelles ou autrement illégitimes des photos signalétiques.

3.2. Avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, et chaque année par la suite, supprimer de la base de données les dossiers qui reflètent ou pourraient favoriser des pratiques policières excessives, discriminatoires ou illégales, notamment :

- les dossiers de non-condamnation;
- les dossiers d'arrestation pour infractions punissables sur déclaration sommaire de culpabilité, y compris les infractions mixtes après que la Couronne a décidé de procéder par voie de procédure sommaire;
- les dossiers d'arrestation de personnes visées la *Loi sur le système de justice pénale pour les adolescents* (LSJPA), après l'expiration des périodes d'accès prévues aux termes de cette loi.

3.3 Si un programme de RF associé à une base de données de photos signalétiques a été mis en œuvre, examiner et supprimer les dossiers

conformément aux recommandations 3.1 et 3.2, dès que possible et au plus tard un an après la publication du présent document d'orientation, puis chaque année au moins par la suite.

Facteur clé 4 : évaluations de l'incidence sur la vie privée

4.1. Effectuer une EIVP exhaustive et la documenter dans un rapport d'EIVP avant de mettre en place un programme de RF associé à une base de données de photos signalétiques, y compris avant la tenue d'un projet pilote, et chaque fois que des changements importants sont apportés à un programme existant.

4.2. Indiquer dans le rapport d'EIVP les risques pour la vie privée de l'utilisation de la technologie de reconnaissance faciale conjuguée à une base de données de photos signalétiques (comme il est décrit plus haut) et prévoir des mesures de précaution et de contrôle pouvant être intégrées dans les politiques et procédures du programme afin d'atténuer ces risques.

4.3. Faire part des résultats de l'EIVP à la commission des services policiers et publier le rapport intégral ou un résumé par souci de transparence et de reddition de comptes.

4.4. Effectuer au besoin d'autres évaluations des risques, notamment pour la sécurité et les droits de la personne, et des évaluations de l'incidence algorithmique, et veiller à les combiner ou à les coordonner avec votre EIVP.

Facteur clé 5 : portée, objet et politiques du programme

5.1. Établir et limiter la portée et l'objet du programme de RF associé à une base de données de photos signalétiques dès le départ, en se concentrant sur la production de pistes d'enquête dans le but d'identifier des personnes dont on soupçonne qu'elles ont commis une infraction grave. Veiller à ce que cette portée et cet objet soient tenus à jour et conformes à la législation applicable et aux principes de

protection de la vie privée que sont le caractère raisonnable, la nécessité et la proportionnalité.

5.2. Élaborer et approuver, pour le programme de RF associé à une base de données de photos signalétiques, des politiques et procédures exhaustives qui sont conformes aux recommandations énoncées dans le présent document d'orientation.

Facteur clé 6 : mobilisation du public

6.1. Mener des consultations publiques pertinentes auprès des communautés touchées et des parties intéressées au sujet du programme avant de le mettre en place. Il faut également procéder à des consultations publiques sur les programmes actuels ou en cours.

6.2. Lors des consultations publiques, s'assurer de prendre en compte les préoccupations en matière de protection de la vie privée et d'équité des communautés marginalisées, y compris celles qui sont touchées de manière disproportionnée par la discrimination systémique et une surveillance policière excessive.

Facteur clé 7 : transparence

7.1. Publier des renseignements à jour, faciles d'accès et en langage clair concernant le programme sur les sites Web de la commission des services policiers et du service de police afin de favoriser une transparence continue.

Ces renseignements publics devraient comprendre :

- la version la plus récente des politiques et procédures du programme;
- l'EIVP et d'autres évaluations des risques ou, à tout le moins, des résumés de ces évaluations;
- une explication en langage simple du fonctionnement du programme, notamment

sa portée et son objet, l'autorisation légale et les mesures de précaution et de contrôle;

- des précisions sur les consultations publiques qui ont eu lieu, y compris une description générale des parties consultées, la nature de la consultation (groupes de discussion, réunions, sondages) et un résumé général des observations reçues;
- des renseignements sur l'acquisition du système de reconnaissance faciale, y compris sur les fournisseurs de services tiers et leur respect de leurs obligations en matière de protection de la vie privée;
- les résultats des essais effectués afin de déterminer l'exactitude du système ou les biais, le cas échéant, y compris une description générale de la méthodologie;
- des statistiques sur l'efficacité globale du programme;
- des renseignements sur la marche à suivre pour les particuliers afin de demander l'accès à leurs renseignements personnels et leur rectification.

Facteur clé 8 : programmes pilotes

8.1. Mener un programme pilote d'une durée limitée, assorti de buts et d'objectifs clairs, avant de mettre intégralement en œuvre la technologie. Ce programme pilote doit consister à mettre le programme à l'essai pour s'assurer qu'il permet d'atteindre les résultats escomptés, à repérer et à résoudre tout problème ou conséquence imprévus et à atténuer les risques pour la vie privée et les droits de la personne.

8.2. Évaluer les résultats du programme pilote et en rendre compte publiquement avant la mise en œuvre, en communiquant ses principales conclusions aux communautés concernées et aux parties intéressées dans le cadre d'un processus pertinent de mobilisation du public.

Facteur clé 9 : qualité des images de référence

9.1. Pour favoriser l'utilisation légale et précise de la reconnaissance faciale, il y a lieu de fixer et d'appliquer des normes claires pour que les images de référence répondent à des critères minimums de qualité, conformément aux normes recommandées dans le présent document d'orientation.

Facteur clé 10 : conservation des images de référence

10.1. Établir des règles et des processus clairs concernant la durée de conservation des images de référence (y compris les images de référence non identifiées) et le moment où elles doivent être détruites de façon sécurisée. Ces règles et processus doivent être compatibles avec les circonstances décrites dans le présent document d'orientation.

10.2. Mettre en place un processus de surveillance approprié pour confirmer régulièrement le respect des règles de conservation et de destruction s'appliquant aux images de référence (y compris les images de référence non identifiées).

Facteur clé 11 : exactitude, examen et surveillance humaine des résultats

11.1. Prendre régulièrement des mesures pour minimiser les inexactitudes et les biais que présente le système de RF. Il s'agit notamment d'évaluer à l'interne si les paramètres du système, comme le seuil minimum pour une correspondance, sont correctement réglés ou s'ils doivent être modifiés, par exemple, pour éviter les faux positifs et favoriser l'évaluation du programme.

11.2. Définir et suivre des procédures transparentes pour l'examen humain et les contrôles d'exactitude du programme. Ces procédures devraient préciser

qui est responsable de l'examen, comment les opérateurs qualifiés interprètent et expliquent les résultats des recherches effectuées au moyen de la RF et quelles sont les exigences en matière de formation pour ce travail. Les opérateurs qualifiés doivent se fonder sur des critères précis et être en mesure d'expliquer clairement les étapes et les processus suivis pour générer des pistes d'enquête.

11.3. Définir et respecter des exigences en matière de documentation de toutes les recherches effectuées au moyen de la RF et de tous les résultats d'évaluation. Cette documentation doit porter sur l'image de référence et le seuil de correspondance utilisés, la probabilité de correspondance, le résultat obtenu par le système de RF, l'opérateur qualifié qui a effectué la recherche, la décision prise par l'opérateur à l'issue de l'évaluation de traiter ou non une correspondance éventuelle comme un faux positif ou comme une piste d'enquête possible, ainsi que tout autre renseignement pertinent.

Facteur clé 12 : limites à la collecte, à la conservation, à l'utilisation ou à la divulgation de renseignements personnels et mesures de précaution raisonnables

12.1 Veiller à ce que la collecte, la conservation, l'utilisation ou la divulgation de renseignements personnels se limite à ce qui est nécessaire et proportionné pour réaliser l'objet déclaré du programme de RF associé à une base de données de photos signalétiques.

12.2 S'assurer que les exigences relatives à la collecte, à la conservation, à l'utilisation ou à la divulgation des renseignements personnels sont bien documentées dans les politiques et procédures connexes et qu'elles tiennent compte des différents éléments du programme de RF (p. ex., les bases de données de photos signalétiques, les images de référence et les données d'entraînement).

12.3 Mettre en place des contrôles et des mesures de précaution d'ordre administratif, technique et physique pour la collecte, la conservation, l'utilisation ou la divulgation de renseignements

personnels dans le cadre du programme, y compris des mesures de précaution visant à protéger les données biométriques.

Facteur clé 13 : droits en matière d'accès aux renseignements personnels et de rectification et suppression de ces renseignements

13.1. Veiller à ce que les politiques et les procédures soient conformes aux droits d'accès, de rectification et de suppression et à ce qu'elles en tiennent compte.

13.2. Veiller à publier les politiques et les procédures ainsi que des renseignements en langage simple sur les droits d'accès, de rectification et de suppression.

Facteur clé 14 : demandes d'autres services de police

14.1. Définir et appliquer des politiques et des procédures claires pour le traitement des demandes de RF émanant d'autres services de police, y compris pour :

- recevoir et traiter les demandes de tels services visant à effectuer des recherches de RF dans sa base de données de photos signalétiques;
- communiquer les résultats de toute correspondance possible au service de police demandeur;
- tenir des registres et des journaux détaillés de tous les accès à des renseignements personnels et de toutes les divulgations de tels renseignements, comme les demandes de recherche de RF reçues, si elles ont été traitées et comment, leurs résultats et les renseignements fournis au service de police demandeur, s'il y a lieu.

Facteur clé 15 : joint reconnaissance faciale base de données de photos signalétiques programs

15.1. Chaque service de police participant à un programme conjoint de RF associé à une base de données de photos signalétiques devrait déterminer s'il a l'autorisation légale requise et suivre tous les facteurs et recommandations figurant dans le présent document d'orientation, notamment :

- réaliser une EIVP commune et les autres évaluations des risques qui s'imposent;
- conclure une entente officielle d'échange de renseignements;
- établir des politiques, des procédures et des exigences connexes liant toutes les parties au programme conjoint et leur imposant des normes et mesures de précaution équivalentes, conformément au présent document d'orientation.

15.2. L'entente d'échange de renseignements devrait limiter explicitement l'utilisation des photos signalétiques partagées aux fins suivantes :

- mise en œuvre d'un programme raisonnable, nécessaire et de portée adéquate (qui vise uniquement à générer des pistes d'enquête sur des crimes graves);
- essais, vérifications et examens réguliers du programme conjoint et rapports connexes;
- établissement du rapport exigé aux termes de l'entente;
- autres fins que la loi exige.

15.3. Avant de combiner leurs bases de données de photos signalétiques, les services de police devraient revoir leurs politiques en matière de dossiers d'arrestation, leurs calendriers de conservation des documents et leurs bases de données, et supprimer les dossiers qui reflètent des pratiques de conservation excessives, discriminatoires ou illégales, y compris les dossiers de non-condamnation, comme indiqué au facteur clé 3.

15.4. Chaque commission des services policiers concernée devrait soumettre régulièrement tout programme conjoint à des vérifications et à des évaluations de son efficacité et de sa pertinence, et rendre publics les rapports de vérification et les évaluations.

Facteur clé 16 : surveillance et réévaluation continues

16.1. Lorsque le programme de RF associé à une base de données de photos signalétiques a été mis en œuvre, surveiller et réévaluer régulièrement le rendement du système et ses risques pour la vie privée en se fondant sur les renseignements à disposition, les risques émergents, les pratiques exemplaires et les avancées générales sur le plan de l'utilisation de la technologie de reconnaissance faciale.

16.2. Déterminer s'il y a lieu de réévaluer et de mettre à jour les évaluations des risques, y compris l'EIVP, ainsi que les politiques, les procédures, la conception d'ensemble et le fonctionnement du programme ou système de RF.

16.3. Envisager de consulter le CIPVP en cas de nouvelles répercussions ou de nouveaux risques importants.

Facteur clé 17 : reddition de comptes

17.1. Définir et appliquer des mesures permanentes de reddition de comptes, comprenant des vérifications annuelles de la conformité, afin d'évaluer la conformité du programme aux exigences légales, règles, politiques et procédures, et notamment la conformité des tiers participant au programme

et des examens annuels du programme afin de déterminer si ce dernier atteint l'objectif établi et respecte les principes directeurs.

17.2. Évaluer les résultats des vérifications annuelles de la conformité et des examens du programme et en rendre compte publiquement, notamment en fournissant au public des statistiques et des informations annuelles relatives à la conformité, à l'efficacité et à la pertinence du programme.

Annexe B : Glossaire

Algorithme de reconnaissance faciale : La reconnaissance faciale consiste en une série de tâches distinctes. Il existe quatre tâches principales à connaître. Chacune de ces tâches est automatisée à l'aide d'un algorithme. Cependant, dans leur ensemble, ces tâches forment un algorithme global qui s'applique au système. Ces tâches peuvent être définies comme suit :

- Un *détecteur de visage* balaie l'image et repère les visages qu'elle contient.
- Un *générateur d'empreintes faciales* prend l'image d'un visage et génère une empreinte faciale à partir de celle-ci.
- Un *comparateur d'empreintes faciales* compare deux empreintes faciales et génère une cote de similarité.
- Un *programme de correspondance d'empreintes faciales* lance une recherche dans une base de données d'empreintes faciales et (en utilisant un comparateur d'empreintes faciales) génère une liste de candidats dont la cote de similarité est égale ou supérieure à un seuil déterminé.

Cote de similarité : Pour illustrer les différentes façons dont les visages peuvent être similaires ou différents, la RF calcule une « cote de similarité », parfois appelée « cote de confiance ». Il s'agit d'une valeur numérique représentant le degré de similarité entre deux empreintes faciales en fonction des caractéristiques biométriques qu'elles contiennent. Une valeur faible indique une similarité moindre et une valeur élevée, une plus grande similarité.

Crime grave : Dans le présent document, s'entend d'un acte criminel ou d'une infraction hybride en vertu d'une loi fédérale comme le Code criminel du Canada. Cette définition est conforme à la Loi sur l'identification des criminels, qui permet aux services de police de prendre des photos signalétiques uniquement des personnes :

- accusées d'un acte criminel ou d'une infraction mixte, ou visées par une citation à comparaître, une promesse, une sommation ou une ordonnance liée à un acte criminel ou à une infraction mixte;
- accusées d'infractions à la *Loi sur la protection de l'information*;
- arrêtées en application de la *Loi sur l'extradition*;
- sous garde légale conformément à l'article 83.3 du *Code criminel*.

Les actes criminels sont les infractions les plus graves en vertu du Code criminel. Ils comprennent le vol de biens de plus de 5 000 $, l'agression sexuelle grave et le meurtre.

Une infraction mixte est un crime à l'égard duquel le procureur de la Couronne peut procéder par voie de mise en accusation ou de déclaration sommaire de culpabilité, selon la gravité des faits allégués. Soulignons que les services de police ne sont pas autorisés à prendre des photos signalétiques de personnes accusées d'infractions punissables sur déclaration sommaire de culpabilité.

Données biométriques : Renseignements personnels résultant d'un traitement technique spécifique, relatifs aux caractéristiques physiques d'une personne, qui permettent de confirmer son identité.

Données d'entraînement: Les algorithmes de traitement d'images qui alimentent la RF sont générés à l'aide de méthodes d'apprentissage automatique qui nécessitent un grand nombre d'images étiquetées de visages de personnes aux fins d'entraînement. Cet ensemble d'exemples d'images étiquetées est appelé « données d'entraînement » de l'algorithme.

Dossier de non-condamnation : Dossier d'arrestation portant sur une personne qui a été accusée d'un acte criminel si l'accusation a été rejetée, retirée ou suspendue, ou a donné lieu à une suspension d'instance ou à un acquittement.

Empreinte faciale : Modèle des caractéristiques biométriques du visage d'une personne. Elle contient un ensemble de caractéristiques physiques uniques et inhérentes à une personne, lesquelles ne peuvent pas être facilement modifiées. Les caractéristiques biométriques codées dans une empreinte faciale peuvent comprendre la distance entre les yeux, la largeur du nez, la forme des pommettes et la longueur de la mâchoire.

Faux négatif : Erreur qui se produit lorsque l'algorithme de RF ne parvient pas à trouver une correspondance réelle dans la base de données, alors qu'une telle correspondance s'y trouve.

Faux positif : Erreur qui se produit lorsque l'algorithme de RF trouve dans la base de données une image donnant une correspondance potentielle qui n'est pas celle de la personne sur l'image de référence.

Identification : Fait de déterminer l'identité d'une personne inconnue. Dans le contexte d'un programme de RF associé à une base de données de photos signalétiques, la reconnaissance faciale compare l'image saisie à l'ensemble des autres images qui se trouvent dans une base de données d'images faciales afin de tenter de connaître l'identité de la personne en cause. Cette méthode est parfois appelée appariement

« 1:N ».

Image de référence : Les systèmes de reconnaissance faciale ont recours à une ou plusieurs images de personnes afin de les identifier ou de vérifier leur identité. Ces images sont connues sous le nom d'images de référence. La manière dont une image de référence est saisie dans un système de reconnaissance faciale à des fins d'identification peut varier.

Seuil : Même si deux empreintes faciales peuvent avoir une cote de similarité élevée, seules celles qui atteignent ou dépassent un seuil donné (p. ex., une cote de similarité précise ou un nombre préétabli de correspondances possibles) sont considérées comme

des correspondances possibles. Certains systèmes de RF permettent à l'utilisateur de fixer le seuil, d'autres pas. La façon dont le seuil est fixé a une incidence directe sur le nombre de résultats obtenus lors d'une recherche donnée, ce qui influe sur la précision, y compris sur les taux d'erreur, de l'algorithme de RF. Selon les circonstances, certaines applications peuvent nécessiter des seuils plus élevés que d'autres.

Technologie de reconnaissance faciale : Technologie utilisant un logiciel de traitement de l'image pour détecter et analyser les caractéristiques du visage d'une personne afin de l'identifier ou de vérifier son identité. Les premières versions de ces logiciels s'appuyaient sur l'intervention humaine pour sélectionner et mesurer manuellement les points de repère du visage d'une personne, alors que le processus actuel consistant à créer un modèle du visage ou une empreinte faciale est entièrement automatisé. Grâce à des algorithmes avancés d'« apprentissage profond » entraînés au moyen de millions d'exemples, la technologie de reconnaissance faciale peut générer des empreintes faciales en trois dimensions comprenant près d'une centaine de caractéristiques biométriques à partir d'images en deux dimensions.

La reconnaissance faciale et les bases de données de photos signalétiques : document d'orientation à l'intention des services de police en Ontario

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2, rue Bloor Est,
Bureau 1400
Toronto, ON
M4W 1A8

cipvp.ca
416-326-3333
info-fr@ipc.on.ca

Janvier 2024