Commission
d'accès à l'information
du Québec

Avis de consultation et appel aux observations - Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement à la reconnaissance faciale

10 juin 2021

Les autorités fédérale, provinciales et territoriales du Canada responsables de la protection de la vie privée, dont la Commission d'accès à l'information, ont conjointement produit un document d'orientation à l'intention des services de police afin de définir les obligations de ces dernières en matière de protection de la vie privée relativement à l'utilisation de la technologie de reconnaissance faciale (RF), afin de garantir que toute utilisation de celle-ci ne contrevient pas à la loi, limite les risques d'atteinte à la vie privée et respecte le droit à la vie privée.

Ce document d'orientation est destiné aux services de police fédéraux, provinciaux, régionaux et municipaux. Il n'est pas destiné aux autres organisations publiques qui mènent des activités d'application de la loi (par exemple le contrôle frontalier) ni aux organisations du secteur privé qui exercent des activités similaires (par exemple la sécurité privée).

La Commission sollicite la rétroaction par écrit des intervenants, tant sur la version préliminaire du document d'orientation que sur le cadre juridique et politique en matière d'utilisation de la RF par les services policiers, de manière plus générale.

Les intervenants ne sont pas tenus de répondre à l'ensemble des questions. En effet, certaines questions peuvent porter précisément sur la façon dont les services de police mettraient en œuvre le document d'orientation en fonction de leurs réalités opérationnelles.

Procédures relatives à la rétroaction

Les observations peuvent être transmises par courriel à l'adresse presidence@cai.gouv.qc.ca **jusqu'au 15 octobre 2021.**

Vos observations ne seront pas publiées sur le site Web de la Commission, mais il est possible qu'un sommaire général de tous les commentaires que nous recevrons y soit publié. Si vous publiez vos observations en ligne, veuillez-nous en avertir et nous fournir le lien. Si vous soumettez des travaux déjà publiés à l'appui de vos observations, veuillez inclure les références et les liens.

Vos observations pourraient également être communiquées aux autres autorités fédérale, provinciales et territoriales du Canada responsables de la protection de la vie privée qui pourraient communiquer avec vous, le cas échéant.

Pour tout renseignement supplémentaire, vous pouvez communiquer avec M. Thomas Forget à l'adresse courriel thomas.forget@cai.gouv.qc.ca ou par téléphone au 418 528-7741, poste 51115.

Observations sur la version préliminaire du document d'orientation

1.	**Le présent document d'orientation aura-t-il l'effet escompté, soit de contribuer à assurer que l'usage que font les services de police de la RF est légal et atténue comme il se doit les risques d'atteinte à la vie privée? Si vous estimez que ce n'est pas le cas, pourquoi?**
2.	**Le présent document d'orientation peut-il être mis en œuvre concrètement?** À quelles pratiques et techniques exemplaires les organismes d'application de la loi pourraient-ils avoir recours pour mettre en pratique le présent document d'orientation? Dans les cas où la mise en application pourrait s'avérer difficile, veuillez en expliquer les raisons et fournir des exemples ainsi que des renseignements détaillés dans la mesure du possible.
3.	**Les recommandations figurant à la section « Exactitude » suffisent-elles pour s'assurer que les services de police s'acquittent de leurs obligations en matière d'exactitude dans les initiatives faisant intervenir la RF?** Dans votre réponse, nous vous invitons à formuler des observations sur les pratiques exemplaires permettant de fixer un seuil approprié pour les correspondances de RF et de déterminer les taux d'erreur acceptables, le cas échéant.
4.	**Les recommandations du document d'orientation portant sur la conservation et la destruction des renseignements personnels recueillis et utilisés dans le cadre d'une initiative de RF peuvent-elles être mises en œuvre de manière appropriée dans un contexte d'application de la loi? Si ce n'est pas le cas, pourquoi?**
5.	**À quelles mesures ou pratiques les services de police peuvent-ils avoir recours pour veiller à ce que toute tierce partie prenant part à une initiative de RF soit légalement autorisée à exercer ses activités?** Par tierces parties, on entend, par exemple, des fournisseurs de logiciels de RF ou ceux qui contrôlent les bases de données d'empreintes faciales que consultent les services de police.
6.	**Anticipez-vous des conséquences négatives découlant des recommandations présentées dans ce document d'orientation et, si c'est le cas, lesquelles?**

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

Il existe actuellement des régimes législatifs exhaustifs encadrant l'utilisation d'autres formes de données biométriques par les organismes d'application de la loi : les empreintes digitales et les photographies en vertu de la *Loi sur l'identification des criminels*, et les profils d'ADN en vertu de la *Loi sur l'identification par les empreintes génétiques*. Compte tenu du caractère sensible de ces données biométriques et des répercussions importantes sur le plan des droits et des libertés des particuliers, leur collecte et leur utilisation se limitent à des circonstances et à des fins bien précises. Des dispositions particulières encadrant leur destruction existent également. Puisque les empreintes faciales constituent une autre forme de données biométriques, nous souhaitons obtenir des observations sur le cadre juridique et de politiques applicable au recours à la RF par les services de police au Canada.

7.	**Le recours à la RF par les services de police est-il encadré de façon appropriée au Canada par les lois existantes? Si ce n'est pas le cas, quelles sont vos préoccupations quant à la façon dont l'utilisation de la RF par les services de police est encadrée aujourd'hui et quelles modifications devraient être apportées au cadre juridique actuel?** Vaudrait-il mieux que ces modifications soient abordées dans un cadre réglementaire distinct qui porte précisément sur l'utilisation de la RF ou dans le contexte de la réforme des lois sur la protection des renseignements personnels (application générale)?
8.	**Quelles mesures de protection devraient être offertes aux personnes dont les renseignements biométriques sont versés dans une base de données contenant des empreintes faciales?** **À titre d'exemples de mesures de protection, citons les suivantes :** • règles législatives liées à l'avis à donner indiquant que les renseignements de particuliers se trouvent dans la base de données; • le droit de demander le retrait et la destruction de son empreinte faciale; ou • le devoir imposé aux services de police (ou à des tierces parties) de détruire automatiquement les empreintes faciales dans certaines situations.
9.	**L'utilisation que font les services de police de la RF, y compris la collecte des empreintes faciales, devrait-elle se limiter à un ensemble déterminé de fins (comme pour les crimes graves ou pour des raisons humanitaires, par exemple dans le cas de personnes disparues)? Les services de police devraient-ils être en mesure d'utiliser ou de conserver des empreintes faciales autres que celles des personnes qui ont été arrêtées ou condamnées?** Existe-t-il des situations dans lesquelles les services de police ne devraient jamais être autorisés à recourir à la RF, ou des applications particulières de la

	RF qui devraient être interdites (c.-à-d. des « zones interdites » telle que le prélèvement systématique des images sur Internet)? Des règles spéciales (ou une interdiction) devraient-elles encadrer l'application de la RF aux jeunes?
10.	**Existe-t-il d'autres enjeux importants en matière de politiques sur lesquels il y aurait lieu de se pencher en rapport avec l'utilisation que font les services de police de la RF?** Sont notamment visés de nouveaux enjeux à caractère juridique, éthique ou social entourant le développement et la mise en œuvre de bases de données d'empreintes faciales par les services de police. Si c'est le cas, quels sont ces enjeux et comment recommanderiez-vous que l'on intervienne à leur égard?

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

Aperçu

1. La reconnaissance faciale (RF) s'est révélée être une puissante technologie qui peut présenter de sérieux risques pour la vie privée. Le but du présent document d'orientation est de définir les obligations des services de police en matière de protection de la vie privée relativement à l'utilisation de la technologie de RF, avec pour objectif de veiller à ce que toute utilisation de celle-ci ne contrevienne pas à la loi, pose des risques limités d'atteinte à la vie privée et respecte le droit à la vie privée.

2. Le présent document d'orientation est publié conjointement par toutes les autorités provinciales et territoriales de protection de la vie privée du Canada et le Commissariat à la protection de la vie privée du Canada.

Portée

3. La présente orientation s'applique aux services de police fédéraux, provinciaux, municipaux et régionaux. Elle n'a pas été rédigée à l'intention des organisations publiques qui sont également chargées de l'application de la loi autres que les services de police (par exemple le contrôle frontalier) et des organisations du secteur privé qui exercent des activités similaires (par exemple la sécurité privée). Cependant, ces organisations doivent continuer à se conformer à toutes les lois applicables, y compris les lois sur la protection des renseignements personnels et les lois sur les droits de la personne. Des sections de ce document d'orientation pourront être utiles à cette fin.

Introduction

4. La technologie de reconnaissance faciale (RF) s'est révélée être un outil d'intérêt considérable pour l'application de la loi. Utilisée de manière responsable et à bon escient, la RF peut aider les services de police à mener à bien divers projets en matière de sécurité publique, notamment les enquêtes sur les actes criminels et la recherche de personnes disparues.

5. Parallèlement, la RF pourrait également devenir une technologie de surveillance portant gravement atteinte à la vie privée.

6. L'utilisation de la RF entraîne la collecte et le traitement de renseignements personnels sensibles : les données biométriques du visage sont uniques à chaque

individu, peu susceptibles de varier de manière significative au fil du temps et dont les caractéristiques intrinsèques sont difficiles à modifier. Ces données constituent le noyau même de l'identité personnelle. La collecte et l'utilisation de celles-ci par un corps policier permettent d'identifier et, éventuellement, de surveiller des personnes.

7. De plus, la technologie de RF s'adapte facilement, est relativement peu coûteuse à utiliser et peut être mise en œuvre en complément d'une infrastructure de surveillance existante. Elle permet d'automatiser l'extraction de renseignements servant à l'identification d'un large éventail de sources, et ce, à partir d'à peu près n'importe quelles sources d'images numériques, qu'elles soient accessibles en ligne ou non.

8. La possibilité que les services de police intègrent la technologie de RF dans leurs activités d'application de la loi laisse entrevoir un risque grave d'atteintes à la vie privée, à moins que des mesures de protection appropriées ne soient mises en place.

9. Le droit de vivre et de s'épanouir à l'abri de la surveillance est un droit fondamental. Au Canada, le droit à la vie privée est reconnu comme étant de nature quasi constitutionnelle pour les organisations du secteur public, et certains aspects du droit à la vie privée sont protégés par la *Charte canadienne des droits et libertés* (la *Charte*). En vertu de ce droit, les citoyens peuvent circuler dans les espaces publics, semi-publics et privés sans risquer que leurs activités ne soient systématiquement recensées, suivies et surveillées. Même si certaines atteintes peuvent être justifiées dans des circonstances précises, les citoyens ne renoncent pas à leur droit à la vie privée simplement en interagissant dans le monde d'une manière qui peut révéler leur visage à d'autres ou qui peut permettre à une caméra de saisir leur image.

10. La protection de la vie privée est également nécessaire à l'exercice d'autres droits fondamentaux protégés par la *Charte.* La protection de la vie privée est essentielle à la dignité, à l'autonomie et à l'épanouissement personnel. Elle est une condition préalable à la participation libre et ouverte des citoyens à la vie démocratique. Une surveillance accrue peut dissuader les gens d'exercer ces droits et libertés.

11. La surveillance est également liée à la discrimination systémique, notamment celle que subissent les communautés racialisées. Les préoccupations de longue date concernant les interventions disproportionnées des services de police auprès des communautés racialisées soulèvent de sérieuses questions quant aux répercussions sur la vie privée et les droits de la personne de l'application de la technologie de RF, par exemple, des fichiers de données historiques comme des bases de données contenant des photos signalétiques. Lorsqu'ils examinent l'impact de la technologie de RF sur la vie privée des citoyens, les organismes d'application de la loi doivent aussi tenir compte du fait que tous ont droit à la même protection et au même bénéfice de la loi, indépendamment de toute discrimination.

12. Si elle est utilisée de manière inappropriée, la technologie de RF peut donc avoir des effets durables et sérieux sur la protection de la vie privée et sur d'autres droits fondamentaux. Cela inclut non seulement des préjudices subis par certaines personnes dont les renseignements personnels peuvent être recueillis, utilisés ou communiqués, mais également des préjudices sociétaux plus généraux qui découlent de la capacité accrue des autorités à surveiller les espaces physiques et numériques dans lesquels les citoyens interagissent. Une fois enclenchée, il peut être difficile de limiter cette capacité de surveillance accrue.

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

14. Le processus visant à fixer des limites appropriées à l'utilisation de la RF reste inachevé. Contrairement à d'autres formes de données biométriques recueillies par les organismes d'application de la loi, comme les photographies, les empreintes digitales ou les profils d'ADN, l'utilisation de la RF n'est pas assujettie à un ensemble de règles claires et exhaustives. L'utilisation de cette technologie est plutôt réglementée par un ensemble disparate de lois et de jurisprudences qui, pour la plupart, ne tiennent pas compte des risques propres à la RF. Cette situation crée une incertitude quant aux utilisations acceptables de la RF et quant aux conditions d'utilisation.

15. C'est dans ce contexte que nos organisations publient le présent document d'orientation. Ce dernier vise à clarifier les responsabilités et obligations légales, telles qu'elles existent actuellement, afin de veiller à ce que toute utilisation de la RF par les services de police ne contrevienne pas à la loi, de limiter les risques d'atteinte à la vie privée et de respecter le droit à la vie privée. Ce document d'orientation ne doit pas être considéré comme une justification, une caution ou une approbation de l'utilisation de la RF par les services de police. Il ne remplace pas non plus la nécessité plus générale de se doter d'un cadre réglementaire plus solide en matière de RF.

16. Bien qu'il aborde de nombreuses exigences légales relatives à l'utilisation de la RF, ce document ne les couvre pas nécessairement toutes. Les services de police demeurent responsables de s'assurer que l'utilisation de la RF est conforme à toutes les exigences légales applicables.

Technologie de reconnaissance faciale

17. La technologie de RF est un type de logiciel qui utilise des techniques complexes de traitement de l'image pour détecter et analyser les caractéristiques biométriques du visage d'une personne aux fins d'identification ou d'authentification. Alors que 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, le processus actuel de création d'un modèle facial ou d'une « empreinte faciale » est entièrement automatisé. Grâce à des algorithmes avancés d'« apprentissage profond » formés au moyen de millions d'exemples, la technologie de RF peut générer des empreintes faciales en trois dimensions comprenant près d'une centaine de caractéristiques biométriques à partir d'images en deux dimensions.

Comment est utilisée la reconnaissance faciale?

18. L'identification et l'authentification ont des sens très précis dans le contexte de la RF. L'identification est utilisée dans le cadre d'une enquête visant à déterminer l'identité d'une personne inconnue. Dans ce cas, la RF compare l'image saisie dans le système (ou l'« image de référence ») avec l'ensemble des autres images qui se trouvent dans une base de données d'images faciales préalablement saisies, afin de tenter de connaître l'identité de la personne en cause. Cette méthode est parfois appelée appariement « 1:N ».

19. L'authentification constitue une forme spéciale d'identification. Elle est utilisée principalement pour des raisons de sécurité dans les cas où une identité est déjà associée à l'image de référence. Plutôt que d'utiliser plusieurs images, la RF permet de comparer l'image de référence à la seule image de la base de données qui correspond à la déclaration d'identité. Si ces deux images correspondent, l'identité de la personne en cause est démontrée selon un niveau d'assurance plus élevé. Par opposition à l'identification, l'authentification est parfois appelée appariement « 1:1 ».

20. Le présent document d'orientation porte principalement sur l'utilisation de la RF aux fins d'identification. Même si l'authentification constitue une utilisation courante de la RF de manière générale (p. ex. pour déverrouiller son téléphone), le mandat des organismes d'application de la loi correspond davantage au processus d'identification.

Comment fonctionne la reconnaissance faciale?

21. La RF comporte un certain nombre de composantes qui jouent chacune un rôle pour déterminer son fonctionnement dans un ensemble de circonstances particulières. Selon le système de RF utilisé, certaines composantes peuvent être configurées par l'utilisateur. Cependant, dans les cas où la RF est achetée auprès d'un fournisseur plutôt que conçue à l'interne, la fonctionnalité de certaines

composantes sera intégrée à la programmation du logiciel lui-même et ne pourra être modifiée qu'en changeant de produit ou en obtenant une version mise à jour.

22. La liste suivante fournit une brève description des principales composantes que les services de police devraient connaître lorsqu'ils utilisent la RF dans un contexte d'application de la loi.

23. Données d'entraînement. Les algorithmes de traitement d'images qui alimentent la RF sont générés à l'aide de méthodes d'apprentissage automatique qui utilisent des images étiquetées de visages de personnes comme données d'entrée. Ces données servent de données d'entraînement pour l'algorithme. En paramétrant un modèle statistique à partir de ces données, la RF est capable d'« apprendre » à détecter les caractéristiques distinctives des visages humains, sans que ses concepteurs aient besoin de coder explicitement toutes les règles du programme.

24. Algorithmes. La RF fonctionne en effectuant 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 de confiance déterminé.

25. Base de données d'images faciales. Pour identifier une personne ou vérifier l'identité de celle-ci, la RF doit avoir accès à une base de données d'images de visages identifiées. L'image de la personne à identifier sera comparée aux images contenues dans cette base de données. Habituellement, la base de données d'images faciales est fournie par l'utilisateur dans le cadre d'un projet de RF. Dans le contexte de l'application de la loi, il peut s'agir d'une base de données de photos d'identité judiciaires ou de personnes disparues. Cependant, certains fournisseurs de RF ont tenté de compiler leurs propres bases de données, généralement à partir d'images provenant d'Internet, et d'utiliser celles-ci pour développer et mettre en marché leur produit dont le fondement juridique est contestable[1].

[1] Voir, p. ex. : « Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta », 2 février 2021.

26. **Empreinte faciale.** Après avoir détecté les différentes caractéristiques du visage d'une personne, la RF les mesure et code le résultat dans un vecteur de valeurs numériques appelé « empreinte faciale ». Une empreinte faciale est constituée de caractéristiques biométriques semblables à une empreinte digitale, c'est-à-dire qu'elle représente un ensemble de caractéristiques physiques uniques inhérentes à une personne, lesquelles ne peuvent pas être facilement modifiées. Voici des exemples de caractéristiques biométriques codées dans une empreinte faciale :

    - distance entre les yeux;
    - largeur du nez;
    - distance entre le nez et les lèvres;
    - profondeur des orbites;
    - forme des pommettes;
    - longueur de la mâchoire.

27. **Cote de similarité.** Les visages présentent une grande diversité, tant au niveau de leurs similitudes que de leurs différences. Certains visages peuvent n'avoir pratiquement aucune similitude. D'autres visages peuvent être similaires, voire identiques, à certains égards, mais moins à d'autres ou pas du tout. Un même visage peut avoir un aspect différent selon les circonstances, comme l'éclairage, l'angle d'orientation ou en raison du temps qui s'est écoulé entre les images. 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.

28. **Seuil.** Même si deux empreintes faciales peuvent avoir une cote de similarité élevée, seules celles qui atteignent ou dépassent un seuil donné sont considérées comme des correspondances possibles. Certains systèmes de RF permettent à l'utilisateur de fixer le seuil, d'autres non. La façon dont le seuil est fixé a une incidence directe sur le nombre de résultats obtenus lors d'une recherche donnée, ce qui a des répercussions 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.

29. Parmi les autres composantes ou fonctionnalités de la RF non mentionnées dans la liste ci-dessus figurent l'évaluation de la qualité et la détection de l'usurpation d'identité.

Cadre de protection de la vie privée

30. Comme il a été expliqué dans l'introduction, l'utilisation de la technologie de RF peut présenter des risques extrêmement graves pour la vie privée. Nombre de ces risques peuvent être difficiles à atténuer et peuvent causer des préjudices importants aux personnes et aux collectivités.

31. Lorsque les services de police envisagent d'avoir recours à la technologie de RF, il est essentiel qu'ils s'assurent non seulement que la loi permet l'utilisation proposée, mais aussi qu'ils appliquent des normes de protection de la vie privée proportionnelles aux préjudices possibles. Dans certains cas, les préjudices possibles peuvent être si graves qu'aucune mesure de protection ne permet de réduire suffisamment le risque d'atteinte à la vie privée. Dans d'autres cas, il peut être possible de gérer les risques de manière appropriée grâce à une planification rigoureuse et à une application diligente des mesures de protection de la vie privée.

32. Le cadre décrit ci-dessous a pour but d'aider les services de police à s'assurer que l'utilisation de la RF est légale et assortie de normes de protection de la vie privée proportionnelles aux risques de préjudices en cause. Il repose sur l'application de principes acceptés mondialement en matière de protection de la vie privée, dont un grand nombre sont repris dans les lois sur la protection des renseignements personnels. Même si les obligations légales précises peuvent varier d'une province ou d'un territoire à l'autre, nous nous attendons à ce que tous les services de police respectent la loi et nous recommandons qu'ils se conforment aux pratiques exemplaires figurant dans le présent cadre, étant donné le risque élevé de préjudice qui peut résulter d'une utilisation inappropriée de la technologie de RF.

33. Ultimement, il incombe aux services de police de s'assurer que toute utilisation de la technologie de RF est autorisée par la loi et que les risques d'atteinte à la vie privée sont gérés de manière appropriée. Le présent document d'orientation constitue un point de départ à partir duquel il est possible d'intégrer des mesures de protection de la vie privée dans les projets de RF. Les services de police pourraient avoir besoin de mettre en place des mesures de protection de la vie privée supplémentaires en fonction de la nature et de la portée des risques pour la vie privée introduits par un projet en particulier.

Conformité à la loi

34. Les services de police doivent s'assurer que la loi leur permet d'utiliser la RF et ils doivent l'utiliser d'une manière qui respecte le droit à la vie privée des Canadiens. La présente section traite des sources possibles de fondement juridique pour l'utilisation de la RF par les services de police, ainsi que des limites de ces utilisations possibles.

35. Pour établir s'ils ont l'autorité de mettre en œuvre et d'exploiter un programme de RF proposé et si le programme respecte adéquatement les droits des personnes, les services de police devraient obtenir un avis juridique. Le programme proposé pourrait ne pas pouvoir être mis en œuvre vu les conclusions de l'avis juridique.

36. Les provinces et les territoires canadiens n'ont pas encore adopté de loi traitant précisément de la technologie de RF, à l'exception du Québec, qui dispose d'un régime encadrant la collecte et l'utilisation des renseignements biométriques[2].

37. Comme la RF entraîne la collecte et l'utilisation de renseignements personnels, elle est assujettie aux lois applicables sur la protection des renseignements personnels. Les organismes d'application de la loi doivent également établir si la RF est conforme à la *Charte* ainsi qu'aux lois relatives aux droits de la personne[3]. La mesure dans laquelle ces lois s'appliqueront à l'utilisation de la RF par les services de police est à déterminer.

Sources de fondement juridique

38. Il n'existe pas de cadre juridique précis pour l'utilisation de la RF au Canada. Le cadre juridique prend plutôt la forme d'un ensemble disparate faisant intervenir des lois et la common law. Les lois fédérales et provinciales sur la protection des renseignements personnels constituent un point de départ pour comprendre le cadre existant, dans la mesure où elles exigent que les services de police – ou quiconque agissant en leur nom – s'assurent que la loi leur permet de recueillir et d'utiliser les renseignements personnels.

39. Comme il a été décrit dans la section précédente, la RF requiert la collecte et l'utilisation de renseignements personnels à de multiples étapes, telles que : l'entraînement d'un algorithme de RF, la création d'une base de données d'images faciales, la collecte des images à comparer à cette base de données, et parfois à d'autres étapes. Il doit exister une assise juridique pour toutes les étapes qui entraînent la collecte de renseignements personnels. En outre, lorsque les services de police ont recours à des fournisseurs ou à des tierces parties pour fournir des services de RF, dont des bases de données de RF, ils doivent s'assurer que la loi permet à ces fournisseurs de recueillir et d'utiliser les renseignements personnels qui composent leurs services.

40. Les sources de fondement juridique peuvent comprendre à la fois les lois, mais également la common law. Veuillez noter que la section suivante sert principalement à illustrer un propos. Elle ne doit en aucun cas être considérée comme un avis sur la validité ou la portée des fondements juridiques possibles.

Autorisation judiciaire

41. Les services de police peuvent demander et obtenir l'autorisation judiciaire de recueillir et d'utiliser des empreintes faciales dans les situations qui justifient une telle intervention. Le *Code criminel* prévoit la délivrance de mandats qui autorisent une intrusion dans la vie privée d'une personne lorsqu'un juge est convaincu : qu'il

---

[2] *Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1.* Cet encadrement pourrait être mis à jour par le projet de loi nº 64.

[3] *Charte canadienne des droits et libertés,* partie I de la *Loi constitutionnelle de 1982*, Annexe B de la *Loi de 1982 sur le Canada* (R-U), 1982, c 11 [*Charte*], art. 8.

existe des motifs raisonnables de croire qu'une infraction a été ou sera commise et que des renseignements relatifs à l'infraction seront obtenus grâce à une telle utilisation ou à l'accomplissement d'un tel acte; que la délivrance du mandat servirait au mieux l'administration de la justice d'agir; et dans les situations pour lesquelles il n'existe aucun fondement juridique permettant d'intervenir en ce sens[4]. Ces autorisations sont assujetties aux conditions habituelles pour l'obtention d'un mandat, ainsi qu'à toute condition ou limitation supplémentaire imposée par les tribunaux lorsqu'ils les accordent.

Pouvoirs conférés par la loi

42. La *Loi sur l'identification des criminels* permet aux services de police de prélever des empreintes digitales ou de photographier les personnes accusées ou déclarées coupables de certains crimes[5]. Elle permet d'utiliser ces éléments d'identification dans le but d'identifier les criminels et de fournir de l'information aux policiers et à d'autres personnes chargées d'appliquer et d'exécuter la loi. La *Loi sur l'identification des criminels* n'autorise cependant pas la collecte arbitraire de photographies d'autres personnes au sein de la population en général. Un avis juridique serait nécessaire pour établir si – et dans quelles circonstances – cette loi constitue un fondement juridique pour une utilisation précise de la RF, lequel s'appliquerait aux bases de données existantes de photos signalétiques selon les pouvoirs conférés par cette loi.

Pouvoirs conférés par la common law

43. Les services de police jouent un rôle crucial dans la promotion de l'intérêt public tels que le maintien de la paix, la prévention des crimes et l'administration de la justice[6]. La common law, tout comme les pouvoirs conférés par la loi, peuvent permettre des interventions policières qui portent atteinte aux libertés des personnes pour la poursuite de ces objectifs sociétaux. Le terme « liberté » utilisé dans les discussions sur les pouvoirs conférés aux services de police par la common law englobe les droits et libertés constitutionnels comme la vie privée abordés ci-dessous[7].

44. Les tribunaux canadiens ont limité les pouvoirs des services de police conférés par la common law[8]. Pour qu'une intervention policière soit autorisée par la common law, elle doit :

    1. s'inscrire dans la portée générale du devoir de la police prévu par la loi ou la common law;

---

[4] *Code criminel, L.R.C. (1985), ch. C-46,* art. 487.01.
[5] *Loi sur l'identification des criminels,* L.R.C. (1985), ch. I-1.
[6] Voir par exemple la *Loi sur la Gendarmerie royale du Canada*, L.R.C. (1985), ch. R-10, à l'art. 18.
[7] *R. c. Clayton, 2007* CSC 32 au paragraphe 46.
[8] *R. c. Waterfield,* [1963] 3 All E.R. 659*, R. c. Stenning,* 1970 CanLII 12 (CSC), [1970] RCS 631*, Fleming c. Ontario,* 2019 CSC 45.

2. entraîner un exercice justifiable des pouvoirs de la police liés au devoir susmentionné[9].

45. La seconde exigence consiste à évaluer si l'intervention de la police « est raisonnablement nécessaire pour l'accomplissement du devoir ». De plus, elle permet de prendre en compte trois facteurs, soit :

    1. l'importance de l'accomplissement du devoir pour l'intérêt public;
    2. la nécessité de l'entrave à la liberté des personnes pour l'accomplissement du devoir;
    3. l'étendue de l'entrave à la liberté des personnes[10].

46. Découlant des facteurs susmentionnés, l'entrave à la liberté doit-être considérée comme nécessaire considérant l'étendue du risque et de la liberté en jeu, et elle ne doit pas entraver la liberté plus que ce qui est raisonnablement nécessaire pour faire face au risque[11].

47. L'examen judiciaire de l'utilisation de la RF par les services de police demeure limité jusqu'à présent et les tribunaux canadiens n'ont pas eu l'occasion d'établir si l'utilisation de la RF est autorisée par la common law[12]. Si l'utilisation de la RF contrecarre les attentes raisonnables en matière de vie privée d'une personne et que celle-ci n'est pas autorisée par une loi ou la common law, une autorisation prévue à l'article 487.01 du *Code criminel* sera généralement requise pour y avoir recours.

Respect des droits des Canadiens

48. Même si les services de police ont besoin d'une assise juridique pour mettre en œuvre un programme de RF, ils doivent également protéger les droits des personnes. La *Charte,* ainsi que les lois fédérales et provinciales sur la protection des renseignements personnels, prévoient des mesures de protection.

Lois sur la protection des renseignements personnels

49. Les lois sur la protection des renseignements personnels définissent les conditions dans lesquelles les organismes publics peuvent recueillir, utiliser, communiquer et conserver les renseignements personnels. Les institutions publiques, y compris les services de police, sont généralement autorisées par les lois sur la protection des renseignements personnels à recueillir des renseignements personnels à des fins légitimes. À titre d'exemple, certaines lois provinciales en matière de protection des renseignements personnels dans le secteur public autorisent la

[9] *Fleming c. Ontario*, *ibid*, paragraphe 46.
[10] *Ibid* au paragraphe 47.
[11] Voir *Clayton*, précité à la note 8 au paragraphe 21.
[12] Voir p. ex. *R. c. Voong*, 2018 ONCJ 352, qui ne traite pas de la question des pouvoirs policiers au titre de la common law, mais qui représente la jurisprudence canadienne extrêmement limitée sur le thème de l'utilisation de la RF par les services de police.

collecte de renseignements personnels à des fins d'« application de la loi »[13]. Les services de police devraient établir si la collecte de renseignements personnels au moyen de la RF s'inscrit dans le cadre de l'« application de la loi », ou si elle est autrement autorisée par l'une des autres fins autorisées pour la collecte de renseignements personnels énoncées dans la loi. Au niveau de la législation fédérale, la collecte de renseignements personnels doit être directement liée à un programme ou à une activité de l'institution fédérale qui recueille les renseignements personnels[14]. Cela signifie que les institutions fédérales doivent s'assurer qu'elles ont l'autorité parlementaire pour le programme ou l'activité pour lequel les renseignements sont recueillis[15].

50. Même si les critères permettant d'établir la validité d'une collecte de renseignements personnels varient selon les provinces et les territoires, les principes de protection de la vie privée abordés ci-dessous figurent dans de nombreuses lois sur la protection des renseignements personnels applicables. Une fois les renseignements personnels recueillis, les services de police ne peuvent généralement les utiliser qu'aux fins pour lesquelles ils ont été recueillis ou compilés, ou pour une utilisation compatible avec cette fin, sauf autorisation contraire. Toutefois, le respect des lois sur la protection des renseignements personnels ne permet pas nécessairement de remédier à tout vice juridique qui pourrait exister au titre de la *Charte*[16].

La *Charte canadienne des droits et libertés*

51. Outre l'intérêt général de ne pas subir l'ingérence de la police et d'être à l'abri de l'ingérence de celle-ci[17], la *Charte* confère aux personnes le droit d'être protégées contre les fouilles et les saisies abusives effectuées par les services de police[18].

52. Pour établir si une intervention policière constitue une fouille déraisonnable, un tribunal doit, dans un premier temps, déterminer si une fouille a eu lieu. Cette conclusion dépend de l'attente raisonnable d'une personne à ce que sa vie privée soit protégée dans le contexte de la fouille et de l'ensemble des circonstances. L'analyse qui consiste à établir s'il y a bel et bien eu fouille se fonde sur un certain nombre de facteurs interreliés tels que l'objet même de la fouille et la nature des intérêts en matière de protection de la vie privée de la personne par rapport à celle-ci. Sont ainsi visés non seulement les photographies et les empreintes faciales en elles-mêmes, mais également des renseignements supplémentaires concernant les gestes posés par une personne et sa localisation qui peuvent être révélés par

[13] Par exemple, voir la *Freedom of Information and Protection of Privacy Act* de l'Alberta, alinéa 33 *b)*.
[14] *Loi sur la protection des renseignements personnels*, LRC 1985, c. P-21, art. 4.
[15] Secrétariat du Conseil du Trésor, *Directive sur les pratiques relatives à la protection de la vie privée,* section 6.2.6.
[16] Ministère de la Justice, « Chartepédia – Article 8 – Fouilles, perquisitions et saisies » (consulté le 13 mai 2021).
[17] *Hunter c. Southam Inc, [1984] 2 RCS 145.*
[18] *Charte*, précitée à la note 2 à l'article 8.

le croisement de renseignements relatifs à l'identité, des images vidéo et des métadonnées, comme une indication de la date et de l'heure, et d'autres renseignements d'identification[19]. L'existence d'une attente raisonnable en matière de vie privée est également tributaire du contexte dans lequel survient l'utilisation de la RF. Selon le contexte, une personne pourrait, d'un point de vue subjectif, s'attendre raisonnablement à ce que sa vie privée soit protégée. De surcroît, le tribunal tente d'établir si cette attente raisonnable en matière de vie privée est objectivement raisonnable, en tenant compte du niveau de protection de la vie privée auquel devrait s'attendre toute personne dans une société libre et ouverte, en soulignant le fait que, fondamentalement, les attentes relatives à la protection de la vie privée sont non seulement descriptives, mais également normatives[20].

53. Même si les attentes raisonnables des citoyens concernant l'utilisation de la RF n'ont pas encore été clairement définies, il est évident que la RF utilise des renseignements personnels sensibles qui, en général, ne peuvent être modifiés et qui peuvent servir à identifier des personnes dans le cadre de situations très sensibles du point de vue du droit à la vie privée. Nous supposons donc que le recours à la RF suscitera généralement des attentes raisonnables en matière de vie privée, même si les visages sont publiquement visibles, que ce soit en ligne ou en personne. En effet, les personnes ne s'attendent pas à faire l'objet d'une surveillance lorsqu'elles vaquent à leurs occupations normales et légitimes, et conservent généralement certaines attentes raisonnables en matière de vie privée même dans les espaces publics[21]. Inversement, même si une personne peut s'attendre à ce que la RF soit utilisée, une plus grande atteinte à la vie privée ne devient pas socialement acceptable simplement en raison des progrès technologiques ou parce que les pratiques des services de police ont changé[22].

54. Si une fouille a lieu dans un contexte où la personne visée a une attente raisonnable en matière de vie privée, un tribunal établira alors si la fouille était raisonnable. Pour qu'une fouille soit raisonnable, elle doit être autorisée par une loi et effectuée d'une manière qui n'est pas abusive. Lorsqu'une intervention policière est jugée autorisée selon la common law, elle sera généralement considérée comme conforme à la *Charte,* puisque les tests de conformité à la common law et à la *Charte* sont similaires[23].

Nécessité et proportionnalité

55. Les principes de nécessité et de proportionnalité garantissent que les pratiques portant atteinte à la vie privée sont mises en œuvre pour un objectif suffisamment important et qu'elles sont rigoureusement adaptées afin de ne pas porter atteinte au droit à la vie privée autrement que si cela est nécessaire. Dans le cas de

[19] *R. c. Spencer,* 2014, 2 CSC 212.
[20] *R. c. Jarvis,* 2019 CSC 10, au paragraphe 68, *R. c. Wise,* [1992] 1 RCS 527.
[21] *Jarvis*, *ibid*.
[22] *R. c. Tessling,* 2004 CSC 67, au paragraphe 42.
[23] *Fleming* précité à la note 9 au paragraphe 111.

l'application de la loi, deux principes entrent en contradiction, soit l'intérêt public d'assurer la sécurité publique et la protection du droit fondamental des personnes à la vie privée. Même si le droit à la vie privée n'est pas absolu, la quête de la sécurité publique ne peut justifier quelconques formes de violations des droits. Par conséquent, les services de police ne peuvent utiliser que des moyens justifiables dans une société libre et démocratique.

56. Comme il a été mentionné précédemment, la nécessité et la proportionnalité existent à divers degrés dans les lois sur la protection des renseignements personnels, la common law et la *Charte*[24]. Conclure à la nécessité et à la proportionnalité du recours à la FR exigera de manière générale une évaluation des éléments qui suivent.

57. **Nécessaire pour répondre à un objectif précis :** Les droits ne sont pas absolus et peuvent être restreints si cela est nécessaire pour atteindre un objectif suffisamment important[25]. Le terme « nécessaire » signifie bien entendu plus que simplement « utile ». Il est important de définir l'objectif d'un programme de RF avec précision. Il ne suffit pas de s'appuyer sur des objectifs généraux de sécurité publique pour justifier l'utilisation d'une technologie aussi intrusive que la RF. Les services de police doivent démontrer la nature urgente et importante de l'objectif en question par des preuves. En outre, l'étendue des renseignements personnels recueillis ne devrait pas être trop vaste; elle devrait être adaptée et nécessaire pour atteindre l'objectif en question.

58. **Efficacité :** Les services de police doivent être en mesure de démontrer que la collecte de renseignements personnels sert réellement à atteindre l'objectif poursuivi. Les services de police devraient fournir des preuves qui attestent que l'utilisation précise de la RF proposée permettra d'atteindre les objectifs précis du programme. Cette démonstration d'efficacité devrait tenir compte de tout problème connu en matière d'exactitude associés à l'utilisation précise.

59. **Atteinte minimale :** L'intrusion des services de police dans la vie privée des personnes ne doit pas aller au-delà de ce qui est raisonnablement nécessaire pour atteindre l'objectif légitime de l'État[26]. La portée d'un programme devrait être aussi restreinte que possible. En cas d'utilisation de la RF, les services de police devraient être en mesure de démontrer qu'il n'existe aucun autre moyen moins intrusif pour la vie privée permettant d'atteindre l'objectif de manière raisonnable[27] et de justifier la non-utilisation de mesures portant moins atteinte à la vie privée[28].

---

[24] Par exemple, le critère Oakes est utilisé principalement pour vérifier la constitutionnalité de la loi. Il a également été utilisé pour tester le comportement de la police dans le contexte des pouvoirs conférés par la common law : *R. c. Clayton*, précité à la note 8.
[25] *Canada (AG) c. JTI-Macdonald Corp,* 2007 CSC 30 au paragraphe 36.
[26] *Frank c. Canada (Procureur général),* 2019 CSC 1, au para. 66.
[27] *R c. KJR,* 2016 CSC 31 au paragraphe 70.
[28] *Thomson Newspapers Co c. Canada (Procureur général),* [1998] 1 RCS 877.

60. **Proportionnalité :** Cette étape nécessite d'évaluer si l'atteinte à la vie privée engendrée par le programme est proportionnelle à l'avantage obtenu[29]. Les services de police devraient déterminer les répercussions qu'aura l'utilisation de la RF sur la protection de la vie privée des personnes, en tenant compte des facteurs généraux tels que ceux mentionnés dans l'introduction du présent document et des répercussions propres à l'utilisation prévue de la RF, par exemple sur certains groupes. Ensuite, les services de police devraient établir si ces atteintes à la vie privée sont justifiées par les avantages liés au recours à la RF. Un aspect inhérent à cette étape tient à considérer le fait que tous les objectifs n'ont pas le même poids. À titre d'exemple, empêcher un complot terroriste connu justifierait une intrusion dans la vie privée plus importante que celle qui serait associée à la capture d'une personne ayant commis un acte de vandalisme mineur. Pour examiner cet aspect, les organismes d'application de la loi doivent être conscients du fait que, dans une société libre et démocratique, l'utilisation d'un système de RF proposé ayant une incidence importante sur la vie privée (comme dans le cas d'une surveillance de masse) pourrait ne jamais être proportionnelle aux avantages obtenus. Lorsque l'incidence est importante, les organismes d'application de la loi doivent se montrer particulièrement prudents avant de recourir à la RF en l'absence de contrôles et de mesures de protection légales clairs et exhaustifs permettant de protéger la vie privée et les droits de la personne de la population en général. Le fait de demander un mandat et une autorisation au tribunal pourrait contribuer à faire en sorte qu'une utilisation proposée de la technologie de la RF respecte le critère de proportionnalité.

61. Rappelons que les principes susmentionnés de protection de la vie privée se répètent et se recoupent avec les fondements juridiques ainsi qu'avec le droit à la vie privée des personnes. Ces thèmes récurrents confirment la nécessité pour les services de police de respecter les limites des pouvoirs d'application de la loi et de s'assurer que les objectifs parallèles de sécurité publique et de respect de la vie privée sont atteints en même temps.

Protection de la vie privée dès la conception

62. Il est important d'intégrer des mesures de protection de la vie privée dès la conception d'un projet. Ce concept est communément appelé la « protection de la vie privée dès la conception ». Suivre une approche de protection de la vie privée dès la conception aide à s'assurer que la protection de la vie privée est une composante essentielle de tout projet ou de tout système de RF. Pour être le plus efficaces possible, ces mesures de protection doivent être intégrées de la conception et au tout début de la planification jusqu'au déploiement et à la mise en œuvre à long terme du projet.

63. Tenir compte de la protection de la vie privée dès la conception signifie que les services de police doivent intégrer officiellement les mesures de protection de la vie privée **avant** de s'engager dans toute utilisation de la technologie de RF. Les

[29] *R c. KJR,* précité à la note 26 au paragraphe 77.

mesures de protection de la vie privée doivent également être conçues de manière à protéger **tous** les renseignements personnels associés à un projet donné, y compris les données de formation, les empreintes faciales, les images sources, les bases des données d'images faciales ainsi que les renseignements tirés des recherches par RF, en plus de tout autre renseignement personnel susceptible d'être recueilli, utilisé, communiqué ou conservé.

Évaluations des facteurs relatifs à la vie privée

64. Un élément essentiel de la mise en pratique du concept de la protection de la vie privée dès la conception est la réalisation d'une évaluation des facteurs relatifs à la vie privée (EFVP). L'EFVP est un outil largement reconnu qui est utilisé pour analyser et prendre en compte les répercussions des projets sur la vie privée. Lorsqu'elles sont utilisées correctement, les EFVP permettent de s'assurer que les programmes et les activités répondent aux exigences légales et atténuent les risques d'atteinte à la vie privée.

65. Les services de police devraient réaliser une EFVP avant de mettre en œuvre des projets qui entraînent la collecte, l'utilisation ou la communication de renseignements personnels, notamment des projets pilotes, ou d'apporter d'importantes modifications à de tels projets. Dans certaines provinces et certains territoires canadiens, les institutions gouvernementales sont tenues par la législation ou par les politiques de réaliser des EFVP.

66. Au moment de réaliser une EFVP, les services de police sont tenus de faire ce qui suit :

    - Mener l'EFVP conformément aux exigences législatives et aux politiques applicables;
    - Suivre toute directive fournie par le commissaire à la protection de la vie privée compétent sur le processus d'EFVP[30];
        - En l'absence de telles directives, les services de police peuvent consulter l'organisme de surveillance de leur province ou de leur territoire.
    - Consigner le processus relatif à l'EFVP dans un rapport sur l'EFVP;
    - Atténuer tous les risques soulevés dans l'EFVP et désigner une personne responsable de la gestion des risques résiduels;
    - Publier un résumé du rapport final sur l'EFVP avant de mettre en œuvre la RF, et mettre à jour ce rapport selon l'évolution de la planification et de la mise en œuvre du projet;
    - Effectuer une nouvelle EFVP (ou, le cas échéant, modifier l'EFVP existante) si des changements majeurs qui pourraient avoir une incidence

[30] Gouvernement fédéral : Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée.
Ontario : Planning for Success: Privacy Impact Assessment Guide (en anglais seulement).
Alberta : Privacy Impact Assessments (en anglais seulement).
Québec : Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée.

sur la collecte, l'utilisation, la communication ou la conservation des renseignements personnels sont apportés au projet.

67. Lorsque les services de police évaluent les risques d'atteinte à la vie privée au moyen du processus relatif à l'EFVP, ils devraient tenir compte de tous les risques relatifs à la vie privée pertinents. Cette démarche comprend l'évaluation des répercussions possibles du projet sur :

    - les personnes;
    - les communautés dans lesquelles la RF peut être mise en œuvre;
    - les groupes qui peuvent être touchés de manière disproportionnée par les atteintes à la vie privée;
    - la confiance du public à l'égard de la collecte et de l'utilisation des renseignements personnels par les organismes d'application de la loi;
    - les droits de la personne et les droits démocratiques, y compris le droit à la vie privée, à l'égalité, aux réunions pacifiques et à la liberté d'expression.

68. Après avoir évalué les répercussions possibles susmentionnées, les services de police ne devraient pas poursuivre la planification et la mise en œuvre du projet, à moins de pouvoir expliquer clairement :

    1) la raison pour laquelle l'utilisation proposée de la RF est nécessaire pour répondre à un besoin précis qui a un lien logique avec un objectif public urgent ou substantiel;
    2) les avantages attendus du projet et la mesure dans laquelle ils sont proportionnels aux risques encourus;
    3) la raison pour laquelle d'autres moyens moins intrusifs ne sont pas suffisants;
    4) la manière dont les risques encourus seront réduits au minimum pendant la mise en œuvre du projet.

69. Les services de police devraient consigner leurs explications sur les points susmentionnés ainsi que leur évaluation des risques dans le rapport sur l'EFVP. Pour y parvenir efficacement, les services de police devraient :

    - s'entretenir avec les intervenants et des experts en protection de la vie privée compétents au sujet des répercussions possibles du projet proposé sur la vie privée;
    - consulter leur commissariat à la protection de la vie privée dès le début de la planification du projet, dans les provinces et les territoires où ces commissariats offrent des services-conseils;
    - consulter leur commissariat aux droits de la personne au moment de la planification du projet, compte tenu du lien étroit entre le droit à la vie privée et les droits de la personne plus étendus, parmi lesquels figure le droit à la protection contre la discrimination;
    - s'assurer que l'EFVP est effectuée par des personnes ayant les compétences appropriées pour cerner et analyser les risques d'atteinte à

la vie privée. Les principales parties concernées par le projet devraient participer au processus, notamment :

- les conseillers juridiques;
- le personnel chargé de la protection de la vie privée;
- le personnel responsable du programme (les personnes qui géreront le projet);
- les groupes d'intervenants (les personnes qui pourraient être touchées par le projet);
- les experts techniques;
- la direction;
- les tiers qui participent au projet.

Surveillance et réévaluation

70. L'analyse des risques d'atteinte à la vie privée est un processus continu qui ne prend pas fin au moment de réaliser l'EFVP ou avec le déploiement d'un projet. Les EFVP doivent être mises à jour périodiquement. De plus, elles peuvent aider à assurer la gestion continue des risques d'atteinte à la vie privée dans le cadre de la stratégie globale de gestion des risques d'un service de police.

71. Les services de police devraient surveiller et réévaluer les risques d'atteinte potentiels à la vie privée et l'efficacité des mesures de protection de la vie privée. Pour ce faire, ils peuvent mettre en œuvre les meilleures pratiques suivantes au fur et à mesure que les projets de RF sont déployés :

- Effectuer des audits périodiques du projet.
  - Les audits devraient porter à la fois sur la conformité du projet aux exigences légales et sur le respect par les exploitants du système des politiques et des procédures établies pour le projet (voir aussi les recommandations formulées dans la section « Responsabilité » ci-dessous).
  - Les audits devraient également porter sur le respect par les tiers des conditions prévues aux ententes d'échange de renseignements personnels et des ententes de services.
- Effectuer des examens périodiques (par exemple, chaque année) de l'efficacité du programme.
  - Les examens devraient servir à évaluer dans quelle mesure les activités du programme permettent d'atteindre les objectifs du projet, en utilisant des critères démontrables (par exemple, le nombre d'arrestations ou de condamnations résultant du programme, etc.).
- Examiner et mettre à jour les mesures de sécurité, les politiques et les procédures, au besoin, pour assurer le respect continu des responsabilités en matière de protection de la vie privée.
  - Par exemple, les services de police peuvent avoir besoin d'adapter leurs politiques à la lumière des audits, des examens de programmes, des atteintes, des réformes législatives, des nouvelles directives ou des progrès technologiques.

- Examiner et, s'il y a lieu, mettre à jour les ententes de partage de renseignements et de services avec des tiers.
- Examiner et mettre à jour les procédures relatives à la formation, au besoin.
    - S'assurer que les modifications apportées aux politiques et aux procédures sont communiquées rapidement au personnel concerné.
- Surveiller régulièrement les fonds de renseignements (par exemple, les fichiers de renseignements personnels) pour s'assurer que les dossiers sont conservés et détruits conformément aux politiques et aux procédures en vigueur.
- Consigner toute modification apportée au programme dans l'EFVP.
- Collaborer avec les intervenants externes tout au long du déploiement (par exemple, les experts en protection de la vie privée, les groupes communautaires, les organisations de la société civile).
    - Les intervenants peuvent être une source précieuse de rétroaction sur les répercussions des projets sur la vie privée.

Exactitude

72. Les services de police doivent s'assurer que les renseignements personnels recueillis et utilisés dans le cadre d'un projet de RF sont suffisamment exacts et à jour. La précision des logiciels de RF ne peut pas être considérée comme acquise, étant donné les risques sérieux que la collecte et l'utilisation de renseignements inexacts font peser sur les droits des personnes.

73. Afin de respecter les obligations relatives à la précision dans le cadre d'un projet de RF, il faut tenir compte du système de RF *dans son ensemble*. La RF est composée d'un certain nombre d'éléments, lesquels soulèvent tous des préoccupations particulières. Ce n'est que lorsque les éléments constitutifs d'un système de RF traitent les renseignements personnels avec précision et équité que l'on peut dire que le système dans son ensemble fait de même.

74. En ce qui concerne les données d'entraînement, l'une des principales considérations est le rôle qu'elles peuvent jouer en contribuant à la présence de biais dans le système de RF. Si les données d'entraînement utilisées pour générer un algorithme de RF ne représentent pas suffisamment les visages de certains groupes démographiques, la précision de l'algorithme sera probablement inégale selon les groupes de personnes. Il est possible qu'un algorithme de RF produise des résultats erronés, tout particulièrement lorsqu'il a été formé en s'appuyant sur des données non représentatives ou biaisées. Des études révèlent que les algorithmes de RF présentent des taux d'erreur très variables pour les visages de personnes de différentes origines ethniques et de différents genres[31]. D'autres

[31] Voir Patrick Grother, Mei Ngan, et Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Rapport interagence 8280, National Institute of Standards and Technology, décembre 2019 (en anglais seulement).

recherches démontrent que le manque de données d'entraînement diversifiées et de haute qualité constitue la principale cause de ces différences[32].

75. Trois éléments clés sont à prendre en compte en ce qui concerne la précision de l'algorithme de RF. Le premier élément dont il faut tenir compte est le fait que la précision est interprétée *de manière statistique*. Le résultat d'un algorithme de RF est une inférence probabiliste quant à la probabilité que deux images représentent la même personne. Il ne s'agit pas d'un fait vérifié concernant la personne. Ainsi, la précision n'est pas une mesure binaire comme « vrai ou faux », elle est plutôt calculée sur la base des taux d'erreur observés de l'algorithme au cours des recherches. Deux types d'erreurs sont à prendre en compte :

    1. Les faux positifs (également connus sous le nom d'erreurs de « type I ») où l'algorithme trouve une correspondance potentielle dans la base de données d'images faciales qui ne correspond pas à celle de la personne sur l'image de référence;
    2. Les faux négatifs (également connus sous le nom d'erreurs de « type II ») où l'algorithme ne parvient pas à trouver une correspondance authentique dans la base de données d'images faciales, alors que l'image de celle-ci s'y trouve pourtant.

76. Le deuxième élément à prendre en compte est qu'il existe généralement un équilibre entre les taux de faux positifs et de faux négatifs d'un algorithme de RF. Ce phénomène s'explique par le seuil de correspondance probable. En fonction du niveau du seuil (élevé ou bas), un algorithme de RF générera plus ou moins de correspondances potentielles. Toutefois, le nombre de résultats fournis par l'algorithme a des répercussions sur son taux d'erreur. Ainsi, un seuil plus élevé fournira uniquement les correspondances présentant une probabilité plus élevée et réduira le nombre de faux positifs, mais il fera en sorte que l'algorithme sera plus susceptible de ne pas détecter les correspondances à faible probabilité, ce qui entraînera possiblement un plus grand nombre de faux négatifs.

77. Enfin, il importe de tenir compte du fait que la détermination d'un seuil approprié dépendra de la nature, de la portée, du contexte et de l'objet du projet en matière de RF, en tenant compte des risques pour les droits et les libertés des personnes. À proprement parler, il n'existe aucun seuil approprié unique. Il s'agit de donner la priorité à la réduction de certains types d'erreurs en fonction de la nature et de la gravité des risques qu'ils posent aux personnes, tout en assurant l'efficacité globale du système de RF.

78. La base de données d'images faciales est un autre élément qui soulève des questions importantes concernant la précision et l'équité. Il faut tenir compte de la qualité ou de l'ancienneté des images qu'elle contient et des effets possibles de celles-ci sur la précision du système de RF. Par exemple, des études ont révélé que le temps écoulé entre deux images d'une même personne augmente la

[32] Voir Jan Lunter. Beating the bias in facial recognition technology. *Biometric Technology Today*. 2020; 2020(9):5-7. doi:10.1016/S0969-4765(20)30122-3.

probabilité que les résultats soient de faux négatifs[33]. Cependant, il est également important de prendre en compte les caractéristiques démographiques des *personnes figurant dans la base de données* d'images faciales et de se demander si la représentation disproportionnée de certains groupes peut avoir des effets négatifs. Un système de RF peut être exposé à un « effet de rétroaction » selon lequel la constitution des personnes figurant dans une base de données d'images faciales conduit la police à soupçonner ces personnes ainsi que leurs associés ou leur communauté de manière répétée, augmentant ainsi le caractère disproportionné de leur représentation démographique au fil du temps.

79. Le dernier élément à mentionner est l'intervention humaine. Même si l'intervention humaine constitue une mesure d'atténuation importante pour réduire les risques d'inexactitude et de préjugés, elle peut aussi, par inadvertance, réintroduire ces mêmes risques dans le système de RF. Contrairement aux ordinateurs, les humains peuvent se sentir dépassés lorsqu'une quantité excessive de renseignements leur est présentée. Pour que l'intervention humaine soit efficace, il faut que les personnes chargées de l'intervention soient formées sur la modération de contenu et qu'elles disposent d'un délai raisonnable, proportionnel au nombre de correspondances potentielles qu'elles sont censées évaluer. Cependant, même avec une formation et un délai suffisant, l'intervention humaine peut être influencée de façon excessive par le niveau de précision statistique du système de RF. Il est important d'éviter les « partialités relatives à l'automatisation » ou la tendance à trop se fier aux systèmes automatisés lors de décisions prises par une personne. Le fait que le système de RF s'appuie sur des calculs mathématiques ne signifie pas nécessairement que ses prévisions sont exactes ou justes.

80. Compte tenu de ce qui précède, il est impératif que les services de police prennent des mesures pour réduire les inexactitudes et les préjugés dans tout déploiement de la technologie de RF. Ces mesures devraient inclure les meilleures pratiques suivantes :

81. Les services de police devraient exiger des fournisseurs de RF qu'ils :

- rendent accessibles leurs algorithmes de RF pour des essais externes indépendants :
    - Les essais devraient comprendre une évaluation de la précision de l'algorithme ainsi que de l'efficacité de celui-ci dans les populations sociodémographiques distinctes (par exemple des groupes en fonction de la race, du genre et de l'âge).
- précisent, dans les résultats de chaque recherche par RF, la cote de similarité, c'est-à-dire une estimation de la probabilité qu'une correspondance donnée soit exacte (par exemple, sous forme de pourcentage).

[33] Voir Patrick Grother, Mei Ngan, et Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 2: Identification. Rapport interagence 8280, *National Institute of Standards and Technology*, décembre 2019 (en anglais seulement).

82. Les services de police devraient également :

- Fixer un seuil approprié afin de donner la priorité à la réduction de certains types d'erreurs en fonction de la nature et de la gravité des risques encourus par les personnes concernées, tout en garantissant l'efficacité globale du système de RF.
- Effectuer des tests à l'interne pour détecter les préjugés et les inexactitudes relatifs à l'efficacité du système de RF dans son ensemble avant le déploiement, puis de façon périodique pendant son déploiement.
- S'assurer que les essais sont effectués par des personnes ou des organisations qualifiées pour évaluer de manière indépendante l'efficacité des systèmes de RF.
- Préciser la cote de similarité, comme celle-ci est indiquée dans les résultats des recherches par RF, au moment de l'enregistrement ou de la communication de renseignements au sujet d'une correspondance.
- Cesser d'utiliser la RF si les essais internes ou externes révèlent :
    - une précision statistique insuffisante dans le système de RF, ou
    - une variation significative des taux d'erreur selon les populations socio-démographiques.

83. Les services de police ne devraient pas :

- Automatiser entièrement les décisions administratives ou juridiques fondées sur les résultats des procédures de mise en correspondance de la RF.
    - En d'autres termes, les décisions qui touchent aux droits, privilèges ou intérêts légaux devraient être prises par des humains, y compris, par exemple, les décisions touchant la détention ou l'accusation d'individus dans le cadre d'un crime ou les enquêtes.
- Agir à partir d'une correspondance de RF, à moins que cette correspondance n'ait été examinée dans un délai approprié par un agent formé sur les procédures et les limites de l'identification par RF.

Minimisation des données

84. Les services de police doivent limiter la collecte de renseignements personnels à ceux directement liés et nécessaires aux objectifs précis d'un projet de RF.

85. Pour ce faire, les services de police devraient mettre en œuvre les pratiques suivantes de minimisation des données :

- Réduire au minimum la quantité de renseignements personnels recueillis et utilisés pour effectuer chaque tâche, en fonction de la quantité de renseignements personnels nécessaires pour effectuer la tâche.
    - Les images utilisées pour effectuer une recherche par RF devraient être recadrées afin d'empêcher l'identification de personnes figurant sur l'image qui ne sont pas visées par la recherche.

- Éliminer rapidement et définitivement les renseignements personnels qui ne relèvent pas de la portée du projet, y compris les renseignements personnels recueillis par inadvertance au cours du projet.
- Inclure un cadre politique soutenu par des mécanismes permettant de vérifier systématiquement que la loi permet de recueillir des données dans le cadre du projet.

86. Dans les projets de RF, au moment de la collecte et du stockage des renseignements personnels, les services de police devraient :

    - Ne pas croiser les informations de RF avec les renseignements personnels contenus dans d'autres bases de données, sauf dans la mesure où cela est nécessaire pour atteindre les objectifs licites du projet.
    - Autant que possible, stocker les informations de RF dans des bases de données distinctes des autres renseignements personnels et isoler ces bases de données des autres réseaux.

Principe de finalité

87. Les services de police doivent s'assurer que les renseignements personnels ne sont utilisés que pour l'objectif pour lequel ils ont été recueillis, ou à des fins compatibles avec cet objectif. Ils doivent également s'assurer que chaque utilisation des renseignements personnels relève des pouvoirs juridiques octroyés dans le cadre du projet.

88. Pour les aider à respecter les exigences susmentionnées, les services de police devraient mettre en place un ensemble complet de contrôles administratifs, techniques et physiques visant à gérer l'accès aux données et aux logiciels utilisés dans des projets de RF et l'utilisation de ceux-ci.

89. Ces contrôles devraient comprendre :

    - Un mécanisme permettant aux agents d'informer la haute direction des nouveaux outils d'enquête pouvant entraîner la collecte ou l'utilisation de renseignements biométriques.
        - Même si l'approbation de la direction est nécessaire avant toute utilisation de nouveaux outils d'enquête, cette approbation ne remplace pas les exigences applicables en matière de protection de la vie privée, y compris la réalisation d'une EFVP.
    - Un système de gestion des accès permettant d'autoriser des personnes à accéder aux logiciels et aux bases de données de RF et à utiliser ceux-ci uniquement dans la mesure où cela est nécessaire pour atteindre les objectifs du projet.
    - Des directives précisant les conditions dans lesquelles les agents sont autorisés à effectuer une recherche par RF.
    - Un registre des décisions autorisant le recours à la recherche par RF.

- Des procédures d'utilisation normalisées offrant des balises à la réalisation d'une recherche par RF, y compris des instructions précisant quelles données peuvent être utilisées et comment la recherche doit être effectuée.
- Un mécanisme qui tient les personnes autorisées réellement responsables de toute utilisation abusive des logiciels ou des données connexes de RF, qu'elle soit intentionnelle ou accidentelle.

90. Ces contrôles devraient empêcher :

- L'accès aux logiciels et aux données de RF par des personnes non autorisées.
- L'utilisation des logiciels ou des données de RF à des fins non autorisées.
- L'utilisation de tout logiciel de RF hors du cadre d'un projet licite approuvé et supervisé par la haute direction.
- L'expérimentation de nouvelles technologies biométriques sur des données réelles, hors du cadre de projets licites approuvés et supervisés par la haute direction.

91. Les services de police doivent également s'assurer que les tierces parties qui interviennent en leur nom ne se servent pas des renseignements personnels qui leur ont été transférés dans le cadre d'un projet à des fins autres que celles qui cadrent avec l'objet initial de la collecte. Par exemple, si un service de police transfère une image à un fournisseur de logiciels de RF tiers à des fins d'identification, le service de police doit prendre des mesures raisonnables pour s'assurer que le fournisseur ne se serve pas de l'image (ou des données des empreintes faciales connexes) à titre de données d'entraînement de l'algorithme ou qu'il ne saisisse pas ces données dans une base de données d'images faciales à des fins de comparaison au cours de recherches ultérieures.

92. Pour leur permettre de respecter ces exigences, les services de police devraient recourir à des ententes d'échange de renseignements personnels pour définir les limites de l'utilisation des renseignements personnels communiqués à des tiers au cours d'un projet, ainsi que toutes autres mesures de protection de la vie privée[34]. Il peut s'agir de la communication aux fournisseurs de logiciels de RF d'images à comparer, ainsi que de la communication à toute autre organisation (par exemple, d'autres organismes d'application de la loi) d'images, de bases de données ou d'autres renseignements personnels.

[34] Les ententes d'échange de renseignements personnels sont des protocoles d'entente écrits qui décrivent les conditions selon lesquelles les renseignements personnels seront échangés entre les parties en question. Ces ententes peuvent prendre diverses formes, notamment des lettres d'entente, des protocoles d'entente, des conditions d'engagement ou d'autres mécanismes semblables. Les parties concluent souvent des ententes d'échange de renseignements personnels dans le cadre d'une entente de service plus large. Pour plus de précisions à ce sujet, consulter le Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels du Secrétariat du Conseil du Trésor du Canada.

93. Sous réserve des exigences légales propres à chaque province et territoire, les ententes d'échange de renseignements personnels devraient préciser, au minimum, ce qui suit :

    - les fondements juridiques selon lesquels les renseignements peuvent être communiqués;
    - les renseignements personnels précis qui seront communiqués;
    - les fins précises visées par la communication;
    - les limites d'une utilisation et d'un transfert ultérieurs;
    - les mesures de protection précises qui doivent être appliquées;
    - les exigences en matière de localisation de données, le cas échéant;
    - les procédures à suivre en cas d'atteinte à la protection des données;
    - les obligations en matière de conservation et de destruction des données;
    - les mesures qui doivent être mises en place en matière de responsabilité, y compris ce qui concerne le contrôle de la conformité.

Sécurité des données

94. Les renseignements personnels doivent être protégés par des mesures de sécurité appropriées en fonction du caractère sensible des renseignements ayant été recueillis.

95. Étant donné la nature extrêmement sensible des données biométriques du visage, les services de police sont tenus de mettre en place des mesures de sécurité très strictes dans le cadre des projets de RF. Ces mesures devraient inclure au minimum ce qui suit, bien que cela puisse ne pas être suffisant dans tous les cas de figure :

    - Utiliser le chiffrement des données et d'autres outils de protection numérique pour sécuriser les données lorsqu'elles sont stockées et lorsqu'elles circulent entre les bases de données, les serveurs et les appareils des utilisateurs.
    - S'assurer que les dossiers et les équipements, y compris les disques durs, les serveurs et les appareils des utilisateurs, sont utilisés et stockés uniquement dans des lieux physiques sécurisés.
    - Tenir un journal de tous les accès et de toutes les utilisations des logiciels et des bases de données de RF.
    - Réévaluer et mettre à jour régulièrement les mesures de sécurité pour faire face aux nouvelles menaces et vulnérabilités en matière de sécurité.
    - Utiliser les ententes d'échange de renseignements personnels pour veiller à ce que les tierces parties participant au projet se conforment aux pratiques exemplaires pertinentes en matière de sécurité des données.

96. Les exigences en matière de sécurité de données peuvent aussi exiger que les renseignements personnels recueillis ou créés par un service de police au cours d'un projet de RF soient stockés au Canada. Dans certaines administrations canadiennes, les services de police sont explicitement tenus de procéder ainsi

selon la loi ou les instruments de politique[35]. Dans d'autres administrations canadiennes, ils doivent d'abord s'assurer que les renseignements personnels communiqués à l'extérieur de leur territoire profiteront d'une protection équivalente[36].

Conservation

97. Les services de police ne devraient pas conserver tout renseignement personnel plus longtemps que nécessaire afin d'atteindre les objectifs d'un projet.

98. Compte tenu de la nature extrêmement sensible des données biométriques du visage, il est particulièrement important que les services de police détruisent rapidement et de manière sécuritaire tous les renseignements personnels qui n'ont pas besoin d'être conservés.

99. Dans les projets en matière de RF, il se peut que certains renseignements personnels doivent être conservés plus longtemps que d'autres. Par exemple, les périodes de conservation peuvent varier pour :

    - le support à partir duquel les données faciales ont été recueillies initialement (par exemple une image ou une vidéo numérique);
    - les empreintes faciales créées par le logiciel de RF pendant l'analyse d'une image;
    - les renseignements déduits à partir des résultats de l'analyse de la RF.

100. Les périodes de conservation appropriées peuvent également varier en fonction du contexte d'utilisation de la RF. Par exemple, il peut parfois être nécessaire de conserver les images ou les empreintes faciales des personnes considérées d'intérêt pour la police, mais les images et les empreintes faciales recueillies auprès de l'ensemble de la population devraient être détruites rapidement, à moins qu'elles ne soient conservées à des fins précises et légales ou en raison d'autres exigences légales. De même, il peut parfois être nécessaire de conserver des empreintes faciales ou des données de surveillance vidéo pour la durée du processus d'enquête jusqu'à la décision finale. Toutefois, les empreintes faciales ou les données de surveillance vidéo qui ne sont pas utiles dans le cadre d'une enquête devraient être détruites.

101. Afin de s'assurer que les renseignements personnels ne sont pas conservés plus longtemps que l'exige le projet de RF, les services de police devraient :

---

[35] Par exemple, la *Freedom of Information and Protection of Privacy Act* [Loi sur l'accès à l'information et la protection de la vie privée] de la Colombie-Britannique comporte des dispositions sur la localisation des données qui exigent que tous les organismes publics, y compris les services de police, n'accèdent aux renseignements personnels et ne les stockent qu'au Canada.

[36] Par exemple, voir art. 70.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* du Québec.

- Déterminer les périodes de conservation applicables aux renseignements personnels dès leur collecte.
- Appliquer différentes périodes de conservation aux différentes catégories de renseignements personnels, en fonction de l'objectif de la collecte.
- Procéder à des examens périodiques des fonds de données afin de repérer les renseignements personnels susceptibles d'avoir été conservés inutilement.
- Établir des directives pour s'assurer que les renseignements personnels sont détruits de manière sécuritaire et rapide à l'expiration de la période de conservation applicable.
- Utiliser les ententes d'échange de renseignements personnels pour veiller à ce que les tierces parties participant au projet détruisent rapidement et de manière sécuritaire les renseignements personnels à la fin de la période de conservation applicable.
- Établir des directives de réduction progressive pour détruire les renseignements personnels si le projet est annulé ou interrompu.

Ouverture, transparence et accès aux renseignements personnels

102. Lorsque cela est possible, les personnes concernées et le public doivent être informés de l'objectif de la collecte de leurs renseignements personnels, y compris l'information permettant de savoir comment les renseignements peuvent être utilisés.

103. En général, lorsqu'une technologie de RF est utilisée, les personnes devraient être informées, au moment de la collecte de leur image, que celle-ci peut être recueillie et conservée dans une base de données d'images faciales. Parallèlement, les personnes devraient être informées des fins pour lesquelles leur image est recueillie. De telles mesures de transparence sont importantes, en partie parce qu'elles contribuent à renforcer l'exercice du droit des personnes à demander l'accès à leurs renseignements personnels.

104. Les services de police devraient mettre en œuvre des politiques et des procédures pour répondre aux demandes d'accès dans la mesure du possible, y compris chaque fois que des empreintes faciales sont recueillies auprès du grand public.

105. Cependant, dans le cadre des projets des services de police, il n'est pas toujours possible de permettre aux personnes d'accéder à des renseignements exhaustifs portant sur la collecte de leurs renseignements personnels, par exemple lorsque les personnes font l'objet d'une enquête en cours.

106. Compte tenu de la nature sensible des données biométriques du visage et des risques pour la vie privée liés à l'utilisation de la RF, il est particulièrement important que les services de police mettent en œuvre des mesures de transparence au niveau du programme pour les projets de RF. Ces mesures permettront d'informer le public des projets de RF et d'accroître la confiance du

public à l'égard du fait que de tels projets sont mis en œuvre de manière responsable.

107. Les services de police devraient mettre en œuvre les mesures de transparence suivantes dans le cadre des projets de RF :

- Révéler le projet sur le site Web public du service de police en expliquant le projet et ses objectifs et en fournissant un lien vers le résumé d'EFVP.
- Mettre à jour régulièrement les renseignements publics sur le projet lorsque celui-ci passe de la planification et de l'élaboration à la mise en œuvre.
- Publier des rapports périodiques sur les activités tenues dans le cadre du programme.
    - Ces rapports devraient contenir :
        - des statistiques sur le nombre de recherches effectuées au cours d'une période donnée;
        - les fins pour lesquelles ces recherches ont été effectuées;
        - les statistiques concernant l'efficacité du projet par rapport aux objectifs de celui-ci;
        - les résultats de tout test pour détecter les biais et les erreurs de calibrage du système de RF effectué par le service de police, avec une justification de tout écart entre les groupes.
- Rendre accessibles les données sur l'utilisation du système de RF aux fins de l'audit et du contrôle, y compris les données de recherche.

Responsabilité

108. Les services de police sont responsables des renseignements personnels qu'ils détiennent, et ils devraient être en mesure de démontrer qu'ils se conforment aux exigences légales.

109. Un service de police responsable devrait disposer d'un programme de gestion de la protection de la vie privée, avec une organisation, des politiques, des procédures et des systèmes clairs pour établir le partage des responsabilités en matière de protection de la vie privée, coordonner le travail dans ce domaine, gérer les risques liés à la protection de la vie privée et assurer la conformité aux lois sur la protection des renseignements personnels.

110. Afin de favoriser la responsabilité à l'égard des projets de RF, les services de police devraient mettre en œuvre les mesures ci-après. Ces mesures devraient être considérées comme un minimum requis pour aborder la question de la responsabilité à l'égard du programme, plutôt que comme une liste de contrôle exhaustive :

- Disposer de politiques et de procédures pour le traitement des renseignements personnels qui sont recueillis, utilisés, créés, communiqués et conservés au cours d'un projet.

    - Au besoin, les politiques et les procédures propres aux projets de RF devraient être intégrées au programme global de gestion de la protection de la vie privée du service de police.
- Établir une structure hiérarchique claire pour le projet en désignant une personne chargée de superviser le respect des obligations en matière de protection de la vie privée.
- Mettre en place un programme de formation spécialisée pour les personnes autorisées à utiliser des logiciels de RF.
    - Avoir terminé le programme de formation devrait être un préalable obligatoire à l'autorisation d'accéder aux logiciels de RF et aux bases de données connexes et d'utiliser ceux-ci.
- Tenir un journal de toutes les utilisations des logiciels de RF, y compris de toutes les recherches effectuées et des authentifiants des personnes qui les ont faites.
    - La procédure de journalisation devrait être automatisée et hors du contrôle des personnes qui accèdent au système et utilisent celui-ci pour effectuer des recherches par RF.
    - La journalisation des utilisations de la RF est un moyen essentiel facilitant les activités de surveillance des organismes publics. À ce titre, les registres devraient être mis à la disposition des organismes de surveillance sur demande.
- Tenir un registre de toutes les communications de renseignements personnels, en précisant : l'autorité selon laquelle les renseignements ont été communiqués (y compris une référence à l'entente d'échange de renseignements personnels qui les régit); le nom de la personne ou de l'organisation à qui les renseignements ont été communiqués; les moyens de communication utilisés, le détail de toute condition liée à la communication; l'identité de l'administrateur du programme qui a autorisé la communication.
- Procéder à des audits périodiques de l'activité de programme, y compris l'évaluation de la conformité aux exigences relatives à la protection de la vie privée et de l'efficacité du projet en ce qui concerne l'atteinte des objectifs du programme.
- Établir des directives claires pour remédier à tout manquement aux politiques et aux procédures définies dans le projet.
- Mettre à jour l'EFVP si des changements majeurs qui pourraient avoir une incidence sur la collecte, l'utilisation ou la conservation des renseignements personnels sont apportés au projet.

111. De plus, les services de police devraient offrir une formation appropriée à toutes les personnes ayant accès aux logiciels de RF et aux bases de données connexes, y compris une formation sur les politiques et les procédures pour le traitement des données de RF. La prestation d'une telle formation permet de s'assurer que les administrateurs du programme respectent les politiques et les procédures relatives au projet en matière de collecte, de stockage, d'utilisation et de communication des renseignements personnels.

112. Dans le cadre de ladite formation, les services de police devraient demander aux administrateurs du programme de comprendre et d'analyser les risques d'atteinte à la vie privée liés au projet, y compris les limites de la technologie de RF, notamment :

- le risque de biais dans les procédures de correspondance de RF fondés sur la race, le genre et d'autres caractéristiques démographiques pertinentes;
- le risque d'erreurs générées par l'utilisation d'images de référence de mauvaise qualité ou les erreurs commises par le passé dans la base de données d'images faciales;
- l'importance de l'intervention humaine au chapitre des correspondances de la RF pour éviter une partialité relative à l'automatisation.

113. Les services de police devraient mettre à jour la formation, au besoin, pour s'assurer que les administrateurs du programme possèdent toujours les connaissances, les compétences et l'expérience suffisantes pour s'acquitter de leurs fonctions dans le respect des exigences légales.

Conclusion

114. Compte tenu des risques importants que pose la technologie de RF, nous nous attendons d'une part, à ce que les services de police évaluent les risques liés à toute utilisation envisagée de la RF et d'autre part, à ce qu'ils atténuent les préjudices éventuels en intégrant à la conception des projets proposés des mécanismes appropriés de protection de la vie privée. Si les services de police se tournent vers la RF, ils doivent s'assurer de protéger la vie privée durant toute la durée du projet.

115. Par-dessus tout, les services de police doivent s'assurer que l'utilisation de la RF est conforme à la loi. Même si les exigences légales déterminées varient d'une administration à l'autre, les recommandations que l'on retrouve dans le présent document d'orientation peuvent contribuer à faire en sorte que les utilisations proposées de la RF respectent les exigences légales, minimisent les risques sur le plan de la protection de la vie privée et respectent le droit fondamental des Canadiens à la vie privée.

Résumé des recommandations

Voici un résumé abrégé des principales recommandations formulées dans le présent document d'orientation. Ce résumé est présenté à des fins de référence seulement; veuillez-vous référer au document d'orientation pour y retrouver la version complète des recommandations.

Lorsqu'ils proposent, élaborent et mettent en œuvre des projets faisant appel à l'utilisation de la technologie de RF, nous recommandons aux services de police[37] de :

- S'assurer qu'il existe une assise juridique pour chaque collecte, utilisation, conservation et communication de renseignements personnels.
  - Une assise juridique doit exister pour appuyer chacune des étapes de l'utilisation de la RF, y compris pour la phase d'entraînement d'un algorithme de RF, de la création d'une base de données d'images faciales et de la collecte d'images de référence.
  - S'assurer que toutes les tierces parties participant à la collecte ou à l'utilisation des renseignements personnels se conforment à la loi.

- Protection de la vie privée dès la conception
  - Intégrer les mesures de protection de la vie privée aux projets proposés avant de faire appel à la technologie de RF.
  - Mener des EFVP pour s'assurer que les systèmes de RF répondent aux exigences légales et atténuent les risques d'atteinte à la vie privée.
  - Surveiller et réévaluer en continu les risques d'atteinte à la vie privée et l'efficacité des mesures de protection de la vie privée.

- S'assurer que les renseignements personnels sont exacts et à jour.
  - Mettre à l'essai les données et les systèmes comme il se doit afin de relever et de réduire les inexactitudes et les biais.
  - Veiller à ce qu'un « intervenant humain » participe à l'examen des correspondances issues de la RF.

- Limiter la collecte de renseignements personnels à ceux directement liés et nécessaires aux objectifs précis d'un projet.

- S'assurer que les renseignements personnels ne sont utilisés que pour l'objectif pour lequel ils ont été recueillis, ou à des fins qui s'inscrivent dans cet objectif.
  - Mettre en œuvre des contrôles administratifs, techniques et physiques visant à gérer l'accès aux données et aux logiciels de RF et l'utilisation de ceux-ci.

[37] Selon le territoire ou la province, il se pourrait que certaines de ces recommandations soient des exigences légales, alors que d'autres constitueraient des pratiques exemplaires. Les services de police sont responsables d'assurer que tout projet faisant appel à la RF est conforme à toutes les exigences légales de son territoire ou de sa province.

    - Recourir à des ententes d'échange de renseignements personnels pour limiter l'utilisation de tels renseignements à des tiers.

- Protéger les renseignements personnels en ayant recours à des mesures de protection qui sont appropriées compte tenu du caractère sensible de ces renseignements, et avoir recours à des ententes d'échange de renseignements personnels pour veiller à ce que les tierces parties soient tenues de faire de même.

- Ne pas conserver les renseignements personnels plus longtemps que nécessaire à l'atteinte des objectifs d'un projet (à moins que la loi ne l'exige).
    - Les périodes de conservation appropriées peuvent varier en fonction du contexte d'utilisation.

- Mettre en œuvre des mesures s'articulant autour de l'ouverture et de la transparence, selon le cas, pour permettre aux particuliers et à la population d'être au fait du projet.
    - Mettre en œuvre des politiques et des procédures pour répondre aux demandes d'accès dans la mesure du possible.

- Mettre en œuvre des mesures de responsabilisation efficaces.
    - Disposer d'un programme de gestion de la protection de la vie privée, avec une organisation, des politiques, des procédures et des systèmes clairs pour établir le partage des responsabilités en matière de protection de la vie privée, coordonner le travail dans ce domaine, gérer les risques liés à la protection de la vie privée et assurer la conformité aux lois sur la protection des renseignements personnels.
    - Tenir un journal de toutes les utilisations de la RF, y compris de toute communication de renseignements personnels à l'extérieur de l'organisation.
    - Veiller à ce que tout le personnel ayant accès à des systèmes de RF ait reçu la formation appropriée.