Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée

Rapport spécial au Parlement

Le 10 juin 2021

La version html de ce rapport spécial a préséance sur le présent document en cas de divergence.

Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée

Rapport spécial au Parlement sur l'enquête réalisée par le Commissariat à la protection de la vie privée du Canada sur l'utilisation par la GRC de la technologie de Clearview AI et version préliminaire d'un document d'orientation conjoint à l'intention des services de police qui envisagent d'avoir recours à la technologie de reconnaissance faciale

Commissariat à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec) K1A 1H3

Numéro de catalogue : IP54-110/2021F-PDF
ISBN : 978-0-660-39087-1

Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

PAR COURRIEL

Le 10 juin 2021

L'honorable George J. Furey, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport spécial du Commissariat à la protection de la vie privée du Canada intitulé *Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée*. Ce dépôt se fait en vertu de l'article 39(1) de la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Le commissaire,

Document original signé par

Daniel Therrien

30, rue Victoria, 1er étage | 30 Victoria Street, 1st Floor
Gatineau (Québec) K1A 1H3
Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

PAR COURRIEL

Le 10 juin 2021

L'honorable Anthony Rota, député
Président
Chambre des communes
Ottawa (Ontario) K1A 0A6

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport spécial du Commissariat à la protection de la vie privée du Canada intitulé *Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée*. Ce dépôt se fait en vertu de l'article 39(1) de la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Le commissaire,

Document original signé par

Daniel Therrien

30, rue Victoria, 1er étage | 30 Victoria Street, 1st Floor
Gatineau (Québec) K1A 1H3
Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

Table des matières

1. Message du commissaire

La technologie de reconnaissance faciale (RF) constitue désormais un outil puissant, qui est d'un intérêt considérable pour les organismes d'application de la loi et les entités commerciales. Utilisée de manière responsable et dans les bonnes conditions, cette technologie peut apporter d'importants avantages à la société.

Elle peut, à titre d'exemple, contribuer à l'atteinte d'objectifs en matière de sécurité nationale, aider les services de police à résoudre des crimes ou aider les autorités à trouver des personnes disparues.

Facilement adaptable, la technologie est relativement peu coûteuse à utiliser et elle peut être mise en œuvre en complément à une infrastructure de surveillance existante, ce qui pourrait expliquer son attrait grandissant au Canada et à l'étranger, en particulier pour les services de police.

Cependant, la RF peut être une technologie de surveillance très envahissante comportant de nombreux risques.

Des études ont démontré que cette technologie peut produire des résultats biaisés sur le plan de la race et, au vu de l'effet intimidant qu'elle peut avoir sur certaines activités, elle pourrait porter atteinte au droit à la vie privée et miner des droits et libertés de la personne, comme la liberté d'expression et de réunion pacifique. Les dépôts de données obtenues au moyen de la technologie de RF constituent également des cibles fort intéressantes pour les personnes malveillantes et doivent être protégés en conséquence.

La technologie de reconnaissance faciale entraîne la collecte et le traitement de renseignements personnels très sensibles. Les données biométriques du visage sont propres à chaque individu, peu susceptibles de varier de manière significative au fil du temps, et difficiles à modifier dans leurs particularités. Jumelée à des sources contenant de vastes quantités de données, comme Internet, les banques de données gouvernementales ou la télévision en circuit fermé, cette technologie peut constituer un puissant outil de renseignements et de suivi.

Les données visées par la technologie de reconnaissance faciale sont intimement liées à l'identité individuelle et, alors que l'utilisation de la technologie est appelée à s'étendre, tant dans les entités commerciales que les gouvernements, d'importantes questions se posent quant au type de société dans laquelle nous désirons vivre. Le déploiement à très grande échelle de la technologie de reconnaissance faciale justifie que l'on mène un examen attentif pour déterminer si nos lois protègent adéquatement les Canadiens contre d'éventuels usages de celle-ci à mauvais escient. Le présent rapport porte particulièrement sur l'application des lois sur la protection des renseignements personnels dans ce domaine et sur les pratiques exemplaires d'utilisation de la technologie de RF à l'intention des services de police.

Mesures prises par le Commissariat et prochaines étapes

Le présent rapport spécial au Parlement fait état des conclusions de notre enquête sur l'utilisation par la Gendarmerie royale du Canada (GRC) de la technologie de Clearview AI, une entreprise qui a offert des services de technologie de reconnaissance faciale à des organismes d'application de la loi ainsi qu'à certaines organisations privées.

Clearview AI a elle-même déjà fait l'objet d'une enquête menée par le Commissariat, dont les résultats ont été publiés en février 2021.

Le présent rapport spécial contient également une version préliminaire du document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale. Élaboré conjointement avec nos homologues provinciaux et territoriaux au Canada, ce document d'orientation préliminaire a pour objectif de préciser les obligations des services de police en matière de protection de la vie privée relativement à l'utilisation de la technologie de RF, afin d'assurer que l'utilisation de celle-ci soit conforme aux lois actuelles et limite les risques d'atteintes à la vie privée.

Dans les semaines et les mois à venir, nous consulterons les corps policiers et divers intervenants en rapport avec ce document d'orientation. Il importe de tenir des discussions publiques sur la façon dont cette technologie potentiellement utile, mais qui comporte également des risques très importants, devrait être utilisée.

Notre travail actuel s'ajoute à l'enquête que nous avons menée sur Cadillac Fairview – une société immobilière commerciale qui a intégré des caméras à des bornes d'orientation numérique situées dans des centres commerciaux afin d'estimer le sexe et l'âge des clients, à leur insu et sans leur consentement. Nous espérons que l'ensemble de notre travail contribuera aux importantes discussions qui ont lieu à l'heure actuelle sur la réglementation de technologies potentiellement perturbatrices, comme la technologie de reconnaissance faciale.

Nous voyons d'un bon œil que les parlementaires se saisissent actuellement de la question. Le mois dernier, j'ai été invité à comparaître devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique à la Chambre des communes afin de discuter des préoccupations que soulève cette technologie sur le plan de la vie privée. Les membres du Comité ont d'ailleurs manifesté un vif intérêt à l'égard de nos enquêtes sur l'utilisation de la technologie de RF dans le contexte de l'application de la loi.

Il convient, selon nous, de communiquer sans délai aux Canadiens les résultats de notre enquête sur l'utilisation par la GRC de la technologie de reconnaissance faciale de Clearview AI. Ne pas le faire serait de mal servir les Canadiens. L'occasion est d'autant plus opportune que le gouvernement souhaite actuellement moderniser le régime canadien de protection de la vie privée.

Aperçu de l'enquête sur l'utilisation par la GRC de la technologie de Clearview AI

Notre enquête sur l'utilisation par la GRC de la technologie de reconnaissance faciale, qui figure intégralement dans le présent rapport, est liée à une enquête distincte sur Clearview AI.

Dans cette enquête, nous avons constaté que la technologie de Clearview AI avait permis à des corps policiers et à des organisations commerciales de faire une recherche dans la banque de données de l'entreprise à partir d'une photographie d'une personne. Cette banque de données renfermait plus de 3 milliards d'images prélevées de sites Internet sans le consentement des utilisateurs.

Résultat : des milliards de personnes se sont retrouvées tous les jours, 24 heures sur 24, dans une parade d'identification policière. Nous avons conclu que cela représentait une surveillance de masse et une violation manifeste de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui s'applique au secteur privé au Canada.

Dans le cadre de notre enquête sur la GRC, nous avons conclu que le service de police national du Canada avait contrevenu à la *Loi sur la protection des renseignements personnels*, qui s'applique aux institutions fédérales, lorsqu'il a recueilli des renseignements personnels auprès de Clearview AI. En l'espèce, une institution fédérale ne peut recueillir de renseignements personnels auprès d'un tiers si celui-ci les a recueillis illégalement.

La GRC nous avait tout d'abord indiqué, à tort, qu'elle n'avait pas recours à la technologie de Clearview AI, ce que nous avons trouvé préoccupant. Lorsqu'elle a plus tard reconnu avoir eu recours à la technologie de cette entreprise, la GRC a affirmé publiquement qu'elle l'avait seulement utilisée de manière limitée, principalement pour identifier, retrouver et sauver des enfants exploités sexuellement sur Internet.

Or, d'après notre enquête, la GRC n'a pas été en mesure de rendre compte de manière satisfaisante de la grande majorité des recherches qu'elle a effectuées.

Cela illustre bien ce que notre enquête a permis de révéler de manière plus détaillée, c'est-à-dire que les politiques et les systèmes de la GRC présentent des lacunes graves et systémiques au chapitre du suivi, de l'identification, de l'examen et du contrôle des nouvelles collectes de renseignements personnels. De telles mesures sont essentielles pour veiller à ce que la GRC se conforme à la loi lorsqu'elle a recours à de nouvelles technologies, comme la technologie de RF, et de nouvelles sources, comme des bases de données privées.

Après l'annonce de notre enquête, la GRC a émis à l'intention de son personnel une directive interne imposant des limites à la collecte de renseignements personnels au moyen de la technologie de Clearview et a mis sur pied un projet pilote, soit le « Programme national d'intégration des technologies » [traduction], pour examiner de manière systématique la conformité de nouvelles techniques d'enquête à la *Loi sur la protection des renseignements personnels* et à la *Charte canadienne des droits et libertés*.

La GRC n'a plus recours à la technologie de Clearview AI puisque l'entreprise a cessé d'offrir ses services au Canada en juillet 2020, dans la foulée de notre enquête qui était alors en cours. Cependant, nous demeurons préoccupés par le fait que la GRC n'a pas souscrit à notre conclusion, selon laquelle nous estimons qu'elle avait contrevenu à la *Loi sur la protection des renseignements personnels*. La GRC a fait valoir que l'article 4 de cette loi n'impose pas expressément le devoir de confirmer le fondement juridique de la collecte de données personnelles par ses partenaires du secteur privé. Exiger de la GRC qu'elle s'assure de la conformité des pratiques d'un tiers à la LPRPDE lui imposerait, a-t-elle affirmé, une obligation déraisonnable.

La GRC a néanmoins accepté de mettre en œuvre nos recommandations l'enjoignant à améliorer ses politiques, ses systèmes et sa formation. À ce titre, elle sera notamment appelée à réaliser des évaluations complètes des pratiques de collecte de données par des tiers afin de veiller à ce que tout renseignement personnel soit recueilli ou utilisé conformément à ce que prévoit la législation canadienne en matière de protection des renseignements personnels.

Les activités des institutions fédérales doivent se limiter à celles que la loi leur permet de mener et elles doivent respecter le principe de la primauté du droit. Nous incitons le Parlement à modifier la *Loi sur la protection des renseignements personnels* afin de préciser que la GRC est tenue de s'assurer que les tiers auprès desquels elle recueille des renseignements personnels ont agi conformément à la loi.

Qui plus est, la common law fixe clairement des limites aux pouvoirs de collecte de la GRC en tant que corps policier. Nous sommes d'avis que le recours par la GRC à la technologie de RF pour effectuer des recherches dans d'énormes dépôts de données sur des Canadiens nullement soupçonnés d'actes criminels constitue une importante atteinte à la vie privée et justifie clairement un examen attentif à la lumière des limites susmentionnées.

Pour être efficace, un tel examen doit se fonder sur une compréhension nuancée des enjeux de vie privée en cause.

Document d'orientation préliminaire à l'intention des services de police

De concert avec nos homologues des autorités de protection de la vie privée au pays, nous avons produit une version préliminaire d'un document d'orientation à l'intention des services de police afin de préciser les circonstances et les conditions dans lesquelles l'utilisation de la technologie de RF pourrait être acceptable.

Nous n'en sommes pas encore arrivés à une prise de position définitive sur les conditions d'utilisation de la technologie de RF. Nous comptons consulter divers intervenants au sujet de nos recommandations avant d'en arrêter la version définitive. Dans le document d'orientation préliminaire, on met l'accent sur le fait que les services de police doivent s'assurer que la loi leur permet de faire l'utilisation proposée de la technologie, et sur l'importance d'appliquer des normes de protection de la vie privée qui soient proportionnelles aux préjudices possibles.

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 plus que cela n'est nécessaire.

En d'autres termes, les services de police ne devraient pas avoir recours à la technologie de RF tout simplement parce que l'on estime qu'elle est « utile » pour l'application de la loi de manière générale. Les services de police doivent avoir un motif précis de faire appel à cette technologie et ce motif doit être fondé sur des éléments probants. Il ne suffit pas de s'appuyer sur des objectifs généraux en matière de sécurité publique pour justifier l'utilisation d'une technologie aussi intrusive. Le caractère urgent et important de l'objectif en question devrait être démontrable par des éléments probants.

Dans certains cas, les préjudices possibles peuvent être si graves qu'aucune mesure de protection ne réduit suffisamment le risque d'atteinte à la vie privée. Dans d'autres cas, il peut être possible de gérer les risques associés à la technologie de RF de manière appropriée grâce à une planification rigoureuse et à une application diligente des mesures de protection de la vie privée.

Les principes d'exactitude, de minimisation des données, de responsabilité et de transparence sont d'autres principes essentiels dont les services de police doivent tenir compte avant d'utiliser la technologie de RF.

La question de l'exactitude est une préoccupation partagée par plusieurs étant donné que la technologie de RF a tendance à identifier de manière erronée certains genres et groupes raciaux. C'est pourquoi les décisions prises au sujet des individus ne doivent pas reposer uniquement sur la technologie de RF. Cela signifie que des agents de police doivent passer manuellement en revue les correspondances de la RF avant que quelque décision que ce soit ne soit prise pour détenir quelqu'un, mener une enquête sur une personne ou déposer des accusations à l'égard d'une personne.

Les mesures de minimisation des données peuvent contribuer à réduire le risque de collecte trop vaste et la gravité d'une atteinte à la sécurité des données dans l'éventualité où une telle situation se produirait.

Le principe de responsabilité permet de s'assurer que les services de police savent quelles données sont recueillies, comment, par qui et à quelles fins, et de quelle façon elles sont protégées. Ce principe permet, en définitive, de s'assurer que les organisations sont en mesure de démontrer leur conformité avec les exigences juridiques lorsqu'elles sont invitées à le faire.

Les mesures de transparence, quant à elles, permettent à ceux qui sont susceptibles d'être visés par la technologie de RF d'être bien informés de son utilisation.

En plus des lois sur la protection des renseignements personnels, la *Charte canadienne des droits et libertés* protège aussi certains aspects du droit à la vie privée, comme le droit d'être protégé contre les fouilles, les perquisitions ou les saisies abusives par l'État. Certaines atteintes à ce droit peuvent toutefois être justifiées dans des circonstances précises.

À titre d'exemple, 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 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. Le fait de demander un mandat et une autorisation du tribunal pourrait contribuer à faire en sorte qu'une utilisation proposée de la technologie de RF respecte le critère de proportionnalité.

Il est également utile de souligner que les acteurs du secteur privé ne jouissent pas des mêmes pouvoirs en matière de collecte que les services de police. Les fournisseurs commerciaux de technologie de RF alimentent souvent leurs propres bases de données, généralement avec des images provenant d'Internet. Comme nous l'avons souligné dans notre document d'orientation, si les services de police ont recours à des tiers pour fournir des services de reconnaissance faciale, ils doivent s'assurer que la loi permet à ceux-ci de recueillir et d'utiliser les

renseignements personnels qui se trouvent dans leurs bases de données, et qu'ils n'ont pas utilisé à d'autres fins les données qui leur ont été communiquées par les services de police.

Réforme législative et autres facteurs à considérer

Le gouvernement envisage actuellement de moderniser le régime de protection de la vie privée et des données du Canada, et il y a des questions importantes relativement à la technologie de RF dont il faudrait tenir compte dans ce contexte.

Les lois canadiennes sur la protection des renseignements personnels ont été conçues de manière à être neutres sur le plan technologique, ce qui est une bonne chose, compte tenu du rythme des changements technologiques par rapport au rythme des travaux nécessaires pour moderniser des lois.

Toutefois, les risques que présente la technologie de RF sont tels que des règles particulières pourraient s'avérer justifiées en raison du caractère inaltérable de l'information en cause. C'est déjà le cas pour d'autres formes de données biométriques recueillies par les organismes d'application de la loi, comme les empreintes digitales et les profils d'ADN.

À ce jour, le Québec est la seule administration au Canada qui soit dotée d'une loi qui traite précisément des données biométriques, lesquelles englobent celles que visent la technologie de RF. La *Loi concernant le cadre juridique des technologies de l'information* du Québec exige que la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. Cette autorité peut par la suite interdire la mise en service d'une telle banque, ordonner que des changements y soient apportés ou en ordonner la destruction. De plus, tout autre renseignement concernant une personne qui pourrait être découvert à partir des caractéristiques ou mesures biométriques ne peut servir à fonder une décision à son égard.

Aux États-Unis, certaines administrations sont allées aussi loin que d'interdire l'utilisation de la technologie de RF par les services de police ou d'autres organismes publics. Le contrôleur européen de la protection des données a également réclamé que l'utilisation de la technologie de RF soit tout simplement interdite dans l'espace public, la qualifiant d'« intrusion profonde et non démocratique dans la vie privée des gens » [traduction].

Bien que la Commission européenne ne soit pas allée aussi loin que d'ordonner une telle interdiction, elle est intervenue pour encadrer la technologie. En effet, dans un nouveau règlement proposé en avril 2021 sur l'intelligence artificielle, la Commission européenne vise à restreindre l'utilisation de la reconnaissance faciale en temps réel dans les espaces publics, par les organismes d'application de la loi, aux cas relatifs au terrorisme et à la criminalité grave ainsi qu'aux recherches ciblées pour aider des victimes d'actes criminels et retrouver des enfants disparus.

Selon cette proposition, une telle utilisation de la technologie de RF serait assujettie à une autorisation judiciaire. Parmi les principales utilisations interdites, soulignons l'utilisation subliminale de la technologie afin de manipuler le comportement d'une personne d'une manière susceptible de lui porter préjudice, laquelle devrait faire l'objet de restrictions. Le seuil fixé dans la loi est le suivant : « susceptible de causer un préjudice physique ou psychologique » [traduction].

Par ailleurs, toujours selon cette proposition, toutes les autres techniques d'identification biométrique à distance, dont celles auxquelles ont recours les organisations commerciales, seraient considérées comme présentant un « niveau de risque élevé ». Un certain nombre d'obligations seraient alors imposées : évaluations du risque et de la qualité, consignation et conservation des données à des fins de traçabilité, supervision humaine et responsabilité démontrable, entre autres.

Nous avons constaté que les partenariats public-privé et les relations contractuelles où on a recours aux technologies numériques, comme la technologie de RF, peuvent présenter des complications et des risques supplémentaires sur le plan de la vie privée. L'adoption de principes de protection de la vie privée, communs aux lois applicables au secteur public et au secteur privé, permettraient de combler les lacunes sur le plan de la responsabilité là où il y a une interaction entre ces deux secteurs. Ces principes permettraient également d'intervenir pour régler les problèmes d'interopérabilité et d'harmonisation entre nos lois fédérales sur la protection des renseignements personnels et celles d'autres administrations au Canada et ailleurs dans le monde.

À cette fin, les lois fédérales canadiennes sur la protection des renseignements personnels devraient être fondées sur les droits. Ces lois devraient comporter des dispositions sur la prise de décision automatisée, notamment une définition, le droit à une explication valable et le droit de demander une intervention humaine à l'égard de son utilisation. Elles devraient également préciser que le concept de renseignements personnels auxquels le public a accès ne s'applique pas aux renseignements à l'égard desquels un individu a une attente raisonnable en matière de protection de la vie privée. Cela est d'autant plus essentiel dans le cas de la technologie de RF, qui s'appuie sur d'énormes bases de données d'images.

Il faudrait également renforcer les dispositions sur la responsabilité dans les lois canadiennes pour exiger de la part des organisations des preuves de conformité sur le plan de la protection de la vie privée à la demande de l'autorité de réglementation. Ces dispositions devraient faire en sorte que des mesures de protection de la vie privée soient intégrées à tout nouveau produit ou service et que les risques soient examinés et les mesures d'atténuation mises en place avant le lancement du produit ou service en question.

Conclusion

La vie privée n'est rien de moins qu'une condition préalable à la liberté : la liberté de vivre et de se développer de façon autonome, à l'abri de la surveillance de l'État ou d'entreprises commerciales.

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

Les Canadiens doivent être libres de participer volontairement et activement aux activités courantes d'une société moderne, qui sont de plus en plus numériques. Ils doivent être en mesure de 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 à ce droit peuvent être justifiées dans des circonstances précises, les gens ne renoncent pas à leur droit à la vie privée simplement en évoluant dans le monde d'une manière qui peut révéler leur visage à d'autres personnes, ou qui peut permettre à une caméra de capter leur portrait. La protection de la vie privée est essentielle à la dignité, à l'autonomie, à l'épanouissement personnel, et 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.

Le processus visant à fixer des limites appropriées à l'utilisation de la technologie de RF demeure inachevé. Contrairement à d'autres formes de données biométriques recueillies par les organismes d'application de la loi, la RF n'est pas assujettie à un ensemble de règles claires et complètes.

Son utilisation est réglementée par une mosaïque de lois et de décisions judiciaires qui, pour la plupart, ne tiennent pas compte des risques propres à la technologie. Cette situation crée une incertitude quant aux utilisations acceptables de la reconnaissance faciale et quant aux conditions d'utilisation.

La nature des risques liés à la technologie de RF nous enjoints à réfléchir collectivement aux limites de ce que constitue une utilisation acceptable de la technologie. Ces limites dépendent en partie des attentes que nous établissons maintenant pour la protection de la vie privée à l'avenir, face à l'augmentation constante des capacités technologiques permettant de s'immiscer dans la vie privée des Canadiens, et susceptibles de bouleverser leurs attentes raisonnables en la matière.

Nous comptons nous pencher sur ces questions importantes en collaboration avec les services de police, le Parlement et divers intervenants.

Ce n'est que par le respect de la loi et des valeurs qui nous sont chères que nous serons en mesure de profiter en toute sécurité des avantages que recèlent les nouvelles technologies, tout en préservant les droits et libertés dont nous sommes si fiers à titre de Canadiens.

2. Rapport de conclusions : Enquête sur le recours par la GRC à la technologie de reconnaissance faciale de Clearview AI pour la collecte de renseignements personnels

Plainte déposée en vertu de la *Loi sur la protection des renseignements personnels*

Aperçu

1. Clearview AI (Clearview) est une société établie aux États-Unis. Cette dernière a créé une importante base de données d'images faciales qu'elle tient à jour (cette base de données contient aussi les hyperliens menant à l'endroit où ces images ont été trouvées sur Internet). Les titulaires de compte Clearview peuvent effectuer des recherches dans cette base de données pour établir une correspondance entre deux images faciales au moyen de la technologie de reconnaissance faciale (TRF). La GRC a confirmé qu'elle a acheté deux licences afin d'utiliser les services de Clearview en octobre 2019 et que ses membres avaient également eu recours aux services de Clearview depuis lors, par l'entremise d'un certain nombre de comptes d'essai gratuit. Le Commissariat à la protection de la vie privée du Canada (le Commissariat) a reçu une plainte au titre de la *Loi sur la protection des renseignements personnels* (la *Loi*) exprimant des préoccupations au sujet de l'utilisation des services de Clearview par la GRC.

2. Dans une affaire connexe, le 21 février 2020, le Commissariat a lancé une enquête conjointe avec les autorités provinciales responsables de la protection de la vie privée du Québec, de l'Alberta et de la Colombie-Britannique sur la collecte d'images faciales par Clearview dans sa base de données et les communications subséquentes aux clients. Dans le cadre de cette enquête, nous avons constaté que les pratiques de collecte de renseignements personnels de Clearview contrevenaient à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), ainsi qu'aux lois provinciales sur la protection des renseignements personnels du Québec, de l'Alberta et de la Colombie-Britannique[1].

3. L'article 4 de la *Loi* prévoit que « [l]es seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ». À notre avis, les programmes et les activités d'une institution doivent se limiter aux activités légales de l'institution et qui respectent le principe de la primauté du droit.

4. À la suite de notre examen de la preuve et de nos analyses juridiques, nous concluons que, puisque les pratiques de collecte de renseignements personnels de Clearview n'étaient pas conformes à ses obligations juridiques, la collecte subséquente de ces

[1] 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 Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissaire à l'information et à la protection de la vie privée de l'Alberta.

renseignements par la GRC ne fait pas partie de ses activités et programmes légitimes et constitue donc une contravention à l'article 4 de la *Loi*.

5. Les dossiers de Clearview démontrent que la GRC a effectué des centaines de recherches au moyen de la TRF de Clearview par l'entremise d'au moins 19 comptes dans tout le pays. Compte tenu de l'ampleur considérable de ces collectes de renseignements personnels qui contreviennent à la *Loi* ainsi que dans le but d'étayer nos recommandations quant aux mesures correctives appropriées, nous avons examiné la pertinence des contrôles en place à la GRC pour nous assurer qu'elle se conforme à l'article 4 de la *Loi* lorsqu'elle recueille des renseignements personnels par de nouvelles méthodes et à partir de nouvelles sources.

6. Nous avons constaté que la GRC n'a pas évalué correctement les risques potentiels de manquement à la *Loi* que l'utilisation de l'énorme base de données de Clearview et de la technologie de reconnaissance faciale présentait manifestement. De plus, l'organisation n'a pas de système en place pour assurer le suivi, analyser, examiner et contrôler cette nouvelle méthode de collecte de renseignements personnels. Nous avons donc recommandé que, d'ici 12 mois, la GRC mette en place des mesures systémiques et donne une formation pertinente pour comprendre, assurer le suivi, analyser, examiner et contrôler cette nouvelle façon de recueillir des renseignements personnels, afin de veiller à ce que la collecte soit limitée comme l'exige la *Loi*. Ces recommandations ne se limitent pas à la présente affaire; elle s'applique aussi à toute nouvelle technologie entraînant la collecte ou l'utilisation de renseignements personnels.

7. Bien que la GRC n'ait pas souscrit à nos conclusions, selon lesquelles nous estimons qu'elle avait contrevenu à la *Loi*, elle a néanmoins accepté de mettre en œuvre nos recommandations. Par conséquent, nous concluons que la plainte est **fondée et conditionnellement résolue**. La mise en œuvre de nos recommandations exigera de la GRC de travailler de manière concertée à l'échelle de l'organisation. La GRC a déjà pris certaines mesures correctives préliminaires, comme la création du Programme national d'intégration des technologies. Il reste toutefois beaucoup de travail à accomplir pour changer la culture à l'interne concernant la prise de décision – il faudra compter sur des procédures, des outils et de la formation qui soient bien intégrés. Nous encourageons vivement la GRC à consacrer les ressources nécessaires à cet égard et à désigner des « champions » parmi les cadres supérieurs pour réussir la mise en œuvre des recommandations.

Contexte

8. La GRC est le service de police national du Canada et un organisme partenaire de Sécurité publique Canada. Elle offre tous les services de police à l'échelle fédérale au Canada et des services de police sous contrat aux trois territoires, à huit des dix provinces (à l'exception de l'Ontario et du Québec), à plus de 150 municipalités, à plus de 600 collectivités autochtones et à trois aéroports internationaux. La GRC a pour mission de faire respecter la loi, de prévenir la criminalité et de protéger la vie. Pour s'acquitter de son mandat, elle doit mener des enquêtes, ce qui entraîne la collecte de

renseignements et l'identification des victimes, des contrevenants ou des scènes de crime[2].

9. Le plaignant, Monsieur Charlie Angus, le député de la circonscription Timmins-Baie James, a exprimé diverses préoccupations au sujet de l'utilisation de la technologie de Clearview par la GRC, laquelle n'avait pas, au moment où la plainte a été déposée à la fin de janvier 2020, confirmé qu'elle l'avait utilisée. Plus précisément, le plaignant a écrit ce qui suit[3] :

> [Traduction]
> Au Canada, d'importantes manifestations dirigées par des Autochtones ont eu lieu pour s'opposer aux mégaprojets d'exploitation des ressources naturelles, et les participants aux manifestations sociales partagent une histoire pleine de méfiance avec la GRC. Une technologie comme celle de Clearview AI pourrait-elle être utilisée pour identifier les manifestants et créer des profils de dissidence civique? Compte tenu de la puissance de ces technologies, il nous faut être vigilants. À l'heure actuelle, les organismes Canadiens d'application de la loi et Clearview AI demeurent très discrets quant à l'ampleur de leur collaboration. Il est impératif que nous comprenions mieux la manière dont cette technologie peut être utilisée sur les Canadiens, et à quelles fins.
>
> Toute utilisation de cette technologie doit faire l'objet d'une surveillance judiciaire transparente. Or, cette technologie est mise à l'essai et mise en œuvre dans un vide législatif et juridique. À cette fin, je vous demande de mener une enquête afin d'établir si la GRC ou d'autres corps policiers ont recours à des services tels que ceux offerts par Clearview AI. Je vous demande de formuler des recommandations sur l'admissibilité, les limites et la portée de l'utilisation de la reconnaissance faciale par des organismes d'application de la loi.

10. À la suite de la réception de la plainte et à la lumière des reportages des médias sur l'utilisation des services de Clearview par les services de police, nous avons d'abord demandé à la GRC, le 29 janvier 2020, si elle utilisait la TRF de Clearview. À ce moment-là, la GRC a informé à tort le Commissariat qu'elle n'avait pas utilisé cette technologie[4]. La GRC s'est aussi engagée à effectuer des évaluations des facteurs relatifs à la vie privée (EFVP) avant de recourir à la technologie de reconnaissance faciale. Cependant, après qu'on eut signalé le vol de la liste des clients de Clearview en février 2020, liste dont faisait partie la GRC, celle-ci a alors révélé publiquement, et au Commissariat, qu'elle avait en fait utilisé des renseignements personnels recueillis de Clearview dans le cadre d'enquêtes. En réponse à la recommandation du Commissariat de cesser d'utiliser la TRF de Clearview au cours de l'enquête, la GRC a en outre exprimé son intention de continuer à utiliser la TRF de Clearview à son Centre national contre l'exploitation d'enfants (CNCEE) et dans d'autres situations d'urgence[5].

---

[2] Vous trouverez ici un complément d'information sur la GRC.
[3] La lettre de plainte du plaignant a été affichée dans son intégralité sur le site Web professionnel de celui-ci. (Site Web en anglais seulement) (Consulté pour la dernière fois le 17 mai 2021).
[4] Voir le paragraphe 51 pour obtenir des précisions à cet égard.
[5] Voir le paragraphe 68 pour obtenir des précisions à cet égard.

11. De plus, malgré l'engagement susmentionné qu'elle a pris envers le Commissariat selon lequel elle devait réaliser des EFVP avant d'avoir recours à la TRF, en juin 2020, soit huit mois après avoir commencé à recueillir des renseignements personnels auprès de Clearview, la GRC n'avait rempli que la liste de vérification de l'EFVP – un outil du Secrétariat du Conseil du Trésor (SCT) utilisé pour décider si une EFVP est requise selon les directives du SCT[6].

12. La GRC avait commencé à utiliser la TRF de Clearview en octobre 2019. En réponse à notre enquête conjointe connexe sur les pratiques de Clearview, la société a annoncé, le 3 juillet 2020, qu'elle avait cessé ses activités commerciales liées à son outil de reconnaissance faciale et qu'elle avait mis fin à ses contrats au Canada, y compris à ceux avec la GRC.

13. Lorsqu'elle a utilisé des comptes payants et d'essai, la GRC a téléversé des images de personnes dans la base de données de Clearview, laquelle a ensuite affiché un certain nombre d'images correspondantes à l'aide de la TRF. À chaque image correspondante, Clearview fournissait un hyperlien vers la page Web d'où provenait l'image.

14. Selon la GRC, des comptes Clearview ont été créés dans cinq divisions de la GRC : Direction générale, Colombie-Britannique, Alberta, Manitoba et Nouveau-Brunswick (deux licences payées pour le CNCEE et 17 licences d'essai gratuites).

15. La GRC a d'abord indiqué qu'elle utilisait principalement la TRF de Clearview pour identifier, localiser et secourir les enfants qui ont été ou qui sont victimes d'abus sexuels en ligne, et qu'elle savait « que quelques unités au sein de la GRC mettent à l'essai, dans une capacité limitée, Clearview AI afin d'en déterminer l'utilité et de faciliter les enquêtes criminelles »[7].

16. En réponse à notre question sur le nombre de « demandes » de recherches qu'elle avait effectuées au moyen de la technologie de Clearview, la GRC nous a indiqué, en mai 2020, que le nombre total d'utilisations s'élevait à 78. Elle a déclaré que 19 visaient à identifier des victimes (recherches effectuées par le CNCEE), 14 visaient à tenter de localiser un suspect identifié qui échappait à la police, et 45 étaient à des fins d'essais à l'aide d'images de membres de la GRC, de personnes consentantes ou d'objets inanimés. Elle a nuancé ces chiffres en précisant qu'à moins que l'application n'ait été utilisée dans le cadre d'une enquête, les « demandes » ne faisaient l'objet d'aucun suivi – toutes ses réponses nécessitant des estimations se fondaient sur l'information fournie « au meilleur de leurs connaissances » par les personnes qui ont utilisé l'application.

17. Nous avons plus tard pu établir, après recoupement avec les données de Clearview, que 521 recherches ont été effectuées à partir de comptes de la GRC. De ce nombre, 33 recherches ont été faites à partir de comptes portant la mention *« Royal Canadian Mounted Police (Victim ID) »* (Gendarmerie royale du Canada (identification des victimes)), et 488 à partir de comptes portant la mention *« Royal Canadian Mounted*

[6] Selon la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor.
[7] Communiqué de presse diffusé par la GRC le 27 février 2020 concernant l'utilisation de la technologie de reconnaissance faciale

Police » (Gendarmerie royale du Canada). Quand nous avons demandé à la GRC d'expliquer pourquoi il y avait un si grand écart entre les données qu'elle nous avait fournies et celles de Clearview, elle nous a indiqué que certaines des « utilisations » dont elle avait initialement fait rapport au Commissariat comprenaient en fait de multiples recherches effectuées relativement à une même personne. Elle a expliqué que, par exemple, les spécialistes de l'identification des victimes pouvaient utiliser plusieurs images d'un même enfant à des âges différents ou plusieurs images prises sous différentes conditions d'éclairage, différents angles ou différentes mises au point de l'image. Elle a ajouté qu'avant le 6 juillet, date à laquelle elle a cessé d'avoir accès aux services de Clearview, elle *était* en mesure de faire le suivi de chaque recherche dans la base de données de Clearview, mais que par la suite, elle ne pouvait plus le faire[8]. Toutefois, soulignons que l'information que la GRC a fournie initialement au Commissariat (voir le paragraphe 16) a été transmise à ce dernier avant le 6 juillet 2020 alors qu'elle avait encore pleinement accès à la base de données de Clearview, et que les recherches supplémentaires en question n'avaient pas été prises en compte dans l'information fournie à ce moment-là.

18. Selon nous, bien qu'il soit possible que les 521 recherches consignées par Clearview puissent être liées aux 78 « utilisations » dont la GRC nous a rendu compte, cela ne peut être comptabilisé dans le nombre de recherches effectuées. Par conséquent, si nous nous appuyons sur les chiffres auxquels nous avons accès (tirés des dossiers de Clearview), nous remarquons qu'environ 6 % des recherches semblent être liées à l'identification des victimes effectuée par le CNCEE, et que pour environ 85 % des recherches, la GRC n'est pas en mesure d'en rendre compte. Dans ce contexte, les motifs pour lesquels le personnel de la GRC a effectué ces recherches demeurent inconnus.

Analyse

19. Les images en question constituent des « renseignements personnels » au sens de l'article 3 de la Loi, puisque les images faciales sont des renseignements relatifs à un « individu identifiable ». En fait, les images faciales sont considérées comme des renseignements biométriques très sensibles, car elles constituent une caractéristique unique et permanente de notre corps, elles ne varient pas de manière significative au fil du temps et elles représentent le noyau de notre identité. D'autres renseignements personnels sont également recueillis par association avec les hyperliens intégrés aux images.

20. La méthode d'utilisation de la TRF de Clearview commence par le téléversement d'une image de la GRC à Clearview. L'image est analysée par le logiciel de Clearview pour cartographier mathématiquement les caractéristiques faciales. Le résultat est ensuite utilisé pour rechercher des visages similaires dans la base de données de Clearview, puisque c'est la décomposition analytique des caractéristiques faciales qui permet de

[8] La GRC a également laissé entendre que le nombre de recherches effectuées par le CNCEE pouvait être sous-évalué – citant le fait que le nombre de recherches effectuées par le CNCEE était « nettement supérieur ».

« reconnaître » les visages. Clearview affiche les correspondances probables, sous forme d'images, à la GRC. Il s'agit d'une collecte de renseignements par la GRC auprès de Clearview. Chaque image contient un hyperlien qui pointe vers l'adresse Internet d'où elle a été extraite. Cela permet à la GRC de recueillir des renseignements contextuels supplémentaires sur l'Internet si ceux-ci sont toujours accessibles. Selon l'adresse Web, l'hyperlien lui-même peut contenir des renseignements personnels dans certains cas.

Enjeu : La collecte de Clearview n'était pas directement liée à un programme ou à une activité

21. L'article 4 de la *Loi* exige que les institutions fédérales restreignent la collecte des renseignements personnels à ceux qui ont un lien direct avec leurs programmes ou leurs activités. Pour établir si une collecte répond à ce critère, il faut d'abord définir clairement la portée ou la nature des « programmes » ou « activités » visés.

22. À notre avis, la portée ou la nature d'un programme ou d'une activité visé à l'article 4 de la *Loi* se limite aux activités légales de l'institution et exclut ce qui est contraire au principe de la primauté du droit. Au terme de l'analyse qui suit, notre enquête a permis de révéler que la collecte de renseignements personnels auprès de Clearview ne faisait pas partie, au sens de l'article 4, d'un programme ou d'une activité légitime de la GRC.

23. En tant qu'organisme d'application de la loi exerçant des fonctions policières, la GRC dispose de vastes pouvoirs pour recueillir des renseignements personnels, souvent à l'insu de la personne concernée ou sans le consentement de celle-ci. Ces fonctions policières vont de l'enquête sur la grande criminalité au maintien de la paix. La GRC a indiqué qu'elle [traduction] « a le pouvoir, sous le régime de la common law et du droit législatif (article 18 de la *Loi sur la Gendarmerie royale du Canada*[9] et alinéa 14(1)*a*) du *Règlement de la Gendarmerie royale du Canada*[10]), de recueillir, d'utiliser et de communiquer des renseignements pertinents qui peuvent servir à une enquête criminelle, ainsi qu'à préserver la paix et à protéger la vie ». Elle estime que cela comprend la collecte de renseignements personnels auprès de Clearview dans le cadre d'une enquête criminelle.

[9] *Loi sur la Gendarmerie royale du Canada (L.R.C. (1985), ch. R-10)*
[10] *Règlement de la Gendarmerie royale du Canada (2014) (DORS/2014-281)*

24. En ce qui concerne la position de la GRC selon laquelle la collecte de renseignements personnels auprès de Clearview est conforme à ses pouvoirs sous le régime de la common law, la GRC a expliqué ce qui suit :

> [Traduction]
> Selon la common law, les pouvoirs policiers sont reconnus comme découlant de la nature et de l'étendue des fonctions policières, notamment « le maintien de la paix, la prévention du crime et la protection de la vie et des biens »[11].

25. L'article 18 de la *Loi sur la Gendarmerie royale du Canada* et l'alinéa 14(1)a) du *Règlement de la Gendarmerie royale du Canada* sont ainsi libellés :

> ***Loi sur la Gendarmerie royale du Canada – Fonctions***
> 18. Sous réserve des ordres du commissaire, les membres qui ont qualité d'agent de la paix sont tenus :
>
> a) de remplir toutes les fonctions des agents de la paix en ce qui concerne le maintien de la paix, la prévention du crime et des infractions aux lois fédérales et à celles en vigueur dans la province où ils peuvent être employés, ainsi que l'arrestation des criminels, des contrevenants et des autres personnes pouvant être légalement mises sous garde […]
>
> ***Règlement de la Gendarmerie royale du Canada – Fonctions***
> 14. (1) En plus de remplir les fonctions prévues par la Loi, les membres qui sont agents de la paix sont tenus :
>
> a) de faire respecter les lois fédérales et leurs règlements et de prêter aux ministères fédéraux l'aide qu'ordonne le ministre […]

26. Il ne fait aucun doute que, de façon générale, les enquêtes sur les crimes relèvent des pouvoirs de la GRC au titre de la common law et des dispositions prévues à l'article 18 de la *Loi sur la Gendarmerie royale du Canada* et à l'alinéa 14(1)a) du *Règlement de la Gendarmerie royale du Canada* et que normalement, elles constituent un « programme ou une activité » de la GRC. Toutefois, même dans le cadre d'enquêtes, il y a des limites juridiques aux pouvoirs de la GRC. Elle ne peut mener des activités illégales ou

[11] Voici quelques exemples précis de jurisprudence citée par la GRC :

- *R c. Waterfield*, [1963] 3 All ER 659
- *R c. Stenning, 1970 CanLII 12 (CSC)*, [1970] RCS 631, par le juge Martland, p. 636-637 – première application de R. c. Waterfield au Canada
- *Brown c. Regional Municipality of Durham Police Service Board,* 1998 CanLII 7198 (ON CA), par le juge Doherty
- *Dedman c. La Reine,* 1985 CanLII 41 (CSC), [1985] 2 RCS 2, par le juge Le Dain
- *Waterfield,* précité ([traduction] « l'agent de police agissait-il dans l'exercice de ses fonctions et la conduite en question constituait-elle un usage justifiable des pouvoirs policiers liés à ces fonctions?)

Il convient de noter que la GRC n'a pas fourni d'autres détails pour étayer la manière dont ces affaires appuient sa position selon laquelle la collecte et l'utilisation de renseignements provenant de Clearview étaient conformes aux pouvoirs que lui confère la common law.

contraires au principe de la primauté du droit. Pour être visés à l'article 4 de la *Loi sur la protection des renseignements personnels*, un « programme » ou une « activité » doit donc être mené de façon conforme à la loi et conforme au principe de la primauté du droit.

27. En l'espèce, nous sommes d'avis que l'article 4 de la *Loi* ne peut être interprété comme permettant la collecte de renseignements personnels auprès d'un agent tiers qui a recueilli, utilisé ou communiqué les renseignements en contravention d'une loi à laquelle ce tiers est assujetti[12]. Il s'ensuit nécessairement que la collecte de renseignements personnels par la GRC au moyen de contrats avec une entreprise privée, laquelle a elle-même recueilli les renseignements personnels de façon illégale, constituerait une violation de l'article 4 de la *Loi.* Conclure autrement reviendrait à permettre aux institutions fédérales de réaliser leur mandat tout en récompensant les organisations dont les pratiques de collecte de renseignements personnels sont illégales et notamment non conformes aux lois canadiennes sur la protection des renseignements personnels.

28. La GRC n'a pris aucune mesure concrète pour vérifier la légalité de la collecte des renseignements. Au regard de toute contrainte juridique pertinente imposée à ses programmes ou à ses activités liés aux collectes de Clearview, et de sa conformité aux lois sur la protection des renseignements personnels, les déclarations écrites de la GRC indiquent qu'elle [traduction] « s'est fiée aux affirmations de Clearview AI selon lesquelles les images de la société provenaient toutes de renseignements accessibles au public ».

29. Toutefois, selon la LPRPDE et les lois provinciales sur la protection des renseignements personnels, les organisations du secteur privé doivent obtenir le consentement des particuliers pour la collecte de leurs renseignements personnels, à moins que certaines conditions précises ne soient respectées (dont celles qui sont énoncées dans les lois et les règlements qui définissent les renseignements « auxquels le public a accès »). Nous n'avons trouvé aucune preuve selon laquelle Clearview a obtenu un tel consentement, et ce, malgré le fait que sa collecte de renseignements s'est faite à partir de sources qui ne constituent pas des renseignements « auxquels le public a accès » au sens du Règlement fédéral ou des lois provinciales applicables au Québec, en Colombie-Britannique et en Alberta[13]. Dans le cadre de notre enquête conjointe sur Clearview, la société a confirmé qu'elle ne demandait pas le consentement des personnes concernées pour la collecte de leurs images, comme en témoigne nos conclusions selon lesquelles Clearview a enfreint la LPRPDE et les lois provinciales sur la protection des renseignements personnels au Québec, en Alberta et en Colombie-Britannique.

30. Nous sommes préoccupés du fait que la GRC veuille abdiquer sa responsabilité de respecter le droit à la vie privée des Canadiens en se contentant d'accepter les affirmations générales d'une entreprise privée sans aucune tentative de validation. En réponse à une version préliminaire du présent rapport de conclusions d'enquête, la GRC a fait valoir que l'article 4 de la *Loi* n'impose pas expressément le devoir de confirmer de

[12] Par souci de clarté, ceci ne s'applique pas aux dénonciateurs.

[13] Voir les paragraphes 44 à 46 de l'enquête conjointe sur Clearview AI pour obtenir des précisions sur la notion de renseignements accessibles au public.

manière définitive l'autorité en matière de collecte pour une tierce partie non gouvernementale. Elle a donc affirmé qu'elle était habilitée à recueillir des renseignements auprès de Clearview en vertu de l'article 4 de la *Loi.* Elle a également ajouté que d'exiger de la GRC qu'elle s'assure qu'un tiers se conforme aux lois lui imposerait une obligation déraisonnable, puisqu'elle ne dispose pas d'une expertise juridique dans le domaine de la LPRPDE ni en ce qui a trait à l'étendue des obligations juridiques d'un tiers. Elle a par ailleurs reconnu que lorsqu'il y a « apparence d'illégalité », cela peut avoir une incidence sur sa capacité de recueillir des renseignements personnels, mais a soutenu que ce n'était pas le cas dans la présente affaire.

31. Nous sommes déçus que la GRC, en tant qu'acteur étatique doté de pouvoirs de coercition, choisisse de se fier à des entités commerciales pour remplir son mandat envers les Canadiens sans accepter la responsabilité de sélectionner des partenaires qui se conforment aux lois. En clair, la GRC a l'obligation de s'informer de la légalité des pratiques de collecte des renseignements personnels des partenaires auprès desquels elle recueille ce genre de renseignements.

32. Compte tenu de ce qui précède, nous sommes d'avis que la collecte par la GRC de renseignements personnels recueillis illégalement par Clearview ne faisait pas partie d'un programme ou d'une activité légitime de la GRC et contrevenait donc à l'article 4 de la *Loi*.

Enjeu : La GRC doit prendre des mesures correctives appropriées afin d'élaborer des contrôles visant à empêcher des contraventions de ce genre à l'avenir

33. Comme il a été mentionné précédemment (au paragraphe 10), la GRC n'a pas procédé à une évaluation de la conformité à l'article 4 de la *Loi* avant de commencer à recueillir des renseignements sur les Canadiens par l'entremise de Clearview. En outre, elle a autorisé la création et l'utilisation par les membres de la GRC de 16 comptes pour lesquels elle n'a pas été en mesure de fournir une justification raisonnable de leur raison d'être ou de leur utilisation (voir le paragraphe 18).

34. À notre connaissance, la GRC ne recueille plus de renseignements personnels auprès de Clearview depuis que la société a cessé d'offrir ses services au Canada en juillet 2020. Toutefois, compte tenu de la nature étendue de la collecte par la GRC de renseignements personnels auprès de Clearview avant cette date, laquelle collecte comprenait des utilisations dont la GRC ne pouvait rendre compte, nous avons examiné le caractère adéquat des contrôles que l'organisation avait ou a mise en place afin de se conformer à l'article 4 de la *Loi*. La présente analyse étaye nos recommandations de mesures correctives dans cette affaire.

35. Pour les raisons décrites en détail ci-dessous, nous craignons que, en l'absence de changements systémiques et d'une meilleure formation, d'éventuelles contraventions semblables à la *Loi* continuent de se produire à l'avenir en raison de la technologie de

reconnaissance faciale et d'autres technologies ou stratégies entraînant la collecte de renseignements personnels.

36. Nous nous attendions[14] à ce qu'un programme institutionnel permettant de recueilllir des renseignements personnels susceptibles de présenter un risque élevé pour la vie privée des gens dispose de structures solides, appuyées par une expertise appropriée, pour garantir la conformité à l'article 4 de la *Loi* en ce qui concerne les renseignements qui sont recueillis; particulièrement lorsqu'il est question de procéder à une nouvelle collecte de renseignements personnels[15]. Une nouvelle collecte comprend : i) la collecte de nouveaux types de renseignements personnels; ii) la collecte de renseignements personnels à de nouvelles fins; iii) la collecte de renseignements personnels par de nouveaux moyens (p. ex. en utilisant la biométrie ou d'autres nouvelles technologies); iv) la collecte de renseignements personnels provenant de nouvelles sources[16].

37. Nos attentes sont appuyées par la *Politique sur la protection de la vie privée* du SCT et la *Directive sur l'évaluation des facteurs relatifs à la vie privée* auxquelles la GRC est également assujettie. La *Directive* précise ce qui suit :

    - « Une EFVP est la composante de la gestion du risque qui vise à assurer la conformité avec les obligations de la LPRP et d'évaluer les incidences que peuvent avoir des programmes ou activités, nouveaux ou ayant subi des modifications importantes comportant des renseignements personnels, sur la vie privée. » La définition de l'expression « modification importante » englobe « tout changement ou amendement aux pratiques relatives à la vie privée liées [sic] à des activités qui font usages [sic] de moyens automatisés ou technologiques pour identifier, créer, analyser, comparer, extraire, recueillir, apparier ou définir des renseignements personnels ».

    - Les institutions doivent établir un processus d'élaboration et d'approbation pour les EFVP qui, entre autres « est proportionné au niveau de risque d'entrave à la vie privée lié aux programmes ou aux activités de l'institution fédérale ». Ce processus doit « s'assurer que les évaluations des facteurs relatifs à la vie privée sont complétées par les agents principaux ou les cadres responsables pour les programmes ou les activités, nouveaux ou ayant subi des modifications importantes, au sein de l'institution ».

    - Pour tous les renseignements personnels recueillis en vue d'être utilisés dans le cadre de décisions administratives concernant une personne [comme les décisions

[14] Consulter Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée, plus précisément la section intitulée « Responsabilité ».
[15] Comme la plainte contre la GRC porte sur la collecte de renseignements personnels, le présent rapport traite précisément de cette question. Les mêmes principes s'appliqueraient à toute nouvelle utilisation ou communication de renseignements personnels.
[16] Ces quatre cas pourraient avoir une incidence sur la question de savoir si une collecte, qui peut sembler conforme à première vue, est réellement en conformité avec l'article 4 de la *Loi.*

relatives à l'application de la loi], les EFVP doivent également être effectuées, entre autres, lorsque la sous-traitance d'activités au secteur privé entraîne des modifications importantes au programme ou aux activités.

- Les EFVP de base doivent être fournies au Commissariat à la protection de la vie privée du Canada et, selon la Politique sur la protection de la vie privée du SCT, les responsables des institutions fédérales sont tenus d' « aviser le commissaire à la protection de la vie privée de toute initiative prévue (loi, règlement, politique, programme) pouvant avoir rapport avec la Loi sur la protection des renseignements personnels ou l'une de ses dispositions, ou pouvant avoir une incidence sur la vie privée des Canadiens et Canadiennes. Cet avis doit être transmis **suffisamment tôt** pour permettre au commissaire d'examiner les enjeux et d'en discuter. » [caractères gras ajoutés]

38. Toutes les institutions sont tenues, par la Politique du SCT, de mener des EFVP pour les programmes ou les activités nouveaux ou ayant subi des modifications importantes touchant des renseignements personnels[17]. Toutes les institutions devraient également veiller à ce que leurs décideurs comprennent leurs obligations visant à prévenir les contraventions à la *Loi* et y donnent suite. Nous savons cependant que les programmes institutionnels ne présentent pas tous le même niveau de risque. Lorsque le risque qu'une collecte de renseignements personnels porte atteinte à la vie privée est plus élevé, nous nous attendons à ce que les mesures connexes visant à assurer une évaluation adéquate de ces risques soient plus rigoureuses[18]. Par conséquent, nous nous attendons au moins à ce qu'une institution ayant des programmes de collecte de renseignements personnels qui pourraient présenter un risque élevé pour la vie privée des gens mette en place tous les éléments suivants :

    A) Connaissance des obligations : Programmes de formation pour veiller à ce que toutes les personnes habilitées à prendre des décisions concernant la collecte de renseignements personnels comprennent les limites de la collecte au titre de l'article 4 de la *Loi*.

    B) Connaissance des nouvelles méthodes de collecte : Systèmes et procédures permettant d'effectuer le suivi des collectes actuelles et éventuelles de renseignements personnels.

    C) Processus permettant de déceler les éventuels problèmes de conformité : Procédures, notamment des points de contrôle dans les processus permettant d'être informé d'une nouvelle collecte, pour avertir les décideurs qu'une évaluation visant à assurer la conformité à l'article 4 de la *Loi* peut être justifiée.

[17] Pour plus de renseignements sur les attentes du Commissariat à l'égard des institutions dans le cadre des EFVP, veuillez consulter : Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée.

[18] Ceci correspond aux attentes du SCT, décrites au paragraphe 38 ci-dessus, selon lesquelles les institutions doivent établir un processus d'élaboration et d'approbation pour les EFVP qui, entre autres « est proportionné au niveau de risque d'entrave à la vie privée lié aux programmes ou aux activités de l'institution […] ».

D) **Processus permettant de réaliser des évaluations en temps voulu lorsque cela est justifié :** Systèmes, procédures et formation sur les rôles et les responsabilités pour garantir que, si une évaluation complète de la conformité est justifiée, cette évaluation sera effectuée en temps opportun, avant le début de la collecte.

E) **Contrôles efficaces de la collecte :** Des contrôles efficaces, y compris une surveillance dynamique, pour limiter la collecte de renseignements personnels par le personnel d'une institution à ce qu'il a jugé admissible au titre de la *Loi.*

A) Connaissance des obligations

39. La connaissance par les décideurs des limites pertinentes à la collecte de renseignements personnels, propres à une activité ou à un programme précis, est essentielle au respect de la *Loi.* Elle devrait être renforcée par des programmes de formation et un accès à l'expertise, notamment les services juridiques et les experts en matière de protection de la vie privée, de manière à ce que toutes les personnes habilitées à prendre des décisions concernant la collecte de renseignements personnels comprennent bien les limites de la collecte au titre de l'article 4 de la *Loi.*

40. La GRC a défendu les actes de ses décideurs (ceux qui ont recueilli des renseignements personnels auprès de Clearview). Plus précisément, elle a déclaré, en réponse à nos questions sur les raisons pour lesquelle elle considérait que les collectes étaient légales, qu'elle [traduction] « s'est fiée aux affirmations de Clearview AI selon lesquelles les images de la société provenaient toutes de renseignements accessibles au public. Il était raisonnable de se fier aux affirmations de Clearview. Rien n'obligeait la GRC à mener une enquête approfondie sur la constitution de la base de donnée de la société[19]. »

41. Comme nous l'avons indiqué ci-dessus (au paragraphe 32), le Commissariat a conclu que Clearview a recueilli des renseignements personnels de façon illégale et que, par conséquent, la collecte de ces renseignements par la GRC auprès de Clearview constitue une contravention à la *Loi sur la protection des renseignements personnels*[20]. Toutefois, ce n'est pas le seul problème potentiel de conformité à la *Loi* que la GRC avait l'obligation d'examiner.

42. Selon la *Charte canadienne des droits et libertés*[21](la *Charte*), la collecte de renseignements personnels par les organismes d'application de la loi constitue une

[19] Notons par ailleurs que les institutions doivent se conformer à l'article 4 de la *Loi* même lorsqu'elles recueillent des renseignements accessibles au public. Bien que la *Loi* précise que ses articles 7 et 8 ne s'appliquent pas aux renseignements accessibles au public, une telle exception ne s'applique pas aux autres dispositions de la *Loi,* y compris l'article 4.

[20] 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 Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissaire à l'information et à la protection de la vie privée de l'Alberta.

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

fouille, une perquisition ou une saisie lorsqu'une personne a une attente raisonnable en matière de respect de la vie privée à l'égard des renseignements en question. La Cour suprême du Canada a aussi conclu que les personnes peuvent avoir une attente raisonnable en matière de respect de la vie privée, même dans les lieux publics[22]. Les tribunaux peuvent tenir compte du caractère intrusif d'une technologie lorsqu'ils déterminent si une personne avait une attente raisonnable en matière de respect de la vie privée[23], et ils ont reconnu l'importance de la protection des renseignements personnels et de l'anonymat des activités sur Internet[24]. Bien que nous ne tirions aucune conclusion quant à la conformité à la *Charte* de l'utilisation par la GRC de la technologie de Clearview, à notre avis, il aurait dû être clair pour la GRC que la collecte à partir d'une base de données privée et la collecte de renseignements au moyen de la technologie de reconnaissance faciale justifiaient une évaluation de sa part quant à la conformité à la *Charte* et aux principes de la common law.

43. Il doit exister une assise juridique pour que les insitutions fédérales puissent recueillir des renseignements personnels. La GRC a fait valoir que sa collecte de renseignements personnels auprès de Clearview était autorisée au titre de la *Loi sur la Gendarmerie royale du Canada* et de la common law. Qui plus est, la common law établit clairement des limites aux pouvoirs de collecte de la GRC en tant que corps policier. Entre autres contraintes, des limites ont été établies par les tribunaux dans l'affaire *R. c. Waterfield*[25] et confirmées par la Cour suprême du Canada dans l'affaire *R. c. Stenning*[26] et plus récemment dans l'affaire *Fleming c. Ontario*[27]. Plus précisément, pour déterminer si la conduite policière (comme une fouille) est autorisée au titre de la common law, il faut tenir compte des deux facteurs suivants :

    i. établir si la conduite en question s'inscrit dans le cadre général d'un devoir policier statutaire ou en common law;
    ii. établir si la conduite en question constitue un exercice justifiable des pouvoirs policiers afférents à ce devoir.

44. La seconde étape du test consiste à déterminer si la conduite constitue un exercice justifiable des pouvoirs policiers afférents à ce devoir. Il faut considérer trois facteurs pour répondre à cette question : 1) l'importance que présente l'accomplissement de ce devoir pour l'intérêt public; 2) la nécessité de l'atteinte à la liberté individuelle pour l'accomplissement de ce devoir et 3) l'ampleur de l'atteinte à la liberté et à la vie privée d'une personne[28].

---

[22] Par exemple, *R. c. Spencer,* 2014 CSC 43*, R. c. Jarvis*, 2019 CSC 10 (concernant l'attente raisonnable en matière de respect de la vie privée pour les besoins du paragraphe 162(1) du *Code criminel*).

[23] Par exemple, *R. c. Jarvis*, 2019 CSC 10 (concernant l'attente raisonnable en matière de respect de la vie privée aux fins de l'art. 162[1] du *Code criminel*), *R. c. Wise, 1992*.

[24] Par exemple, dans *R. c. Spencer* 2014 CSC 43 : « Un certain degré d'anonymat est propre à beaucoup d'activités menées sur Internet et l'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives. »

[25] *R. c. Waterfield*, précité.

[26] *R. c. Stenning*, précité.

[27] *Fleming c. Ontario*, 2019 CSC 45.

[28] *Knowlton c. R.*, 1973 CanLII 148 (CSC), [1974] RCS 443. Page 446; voir également *Fleming, supra*, par. 75.

45. En ce qui concerne le premier élément du test, comme il a été mentionné précédemment (au paragraphe 18), la GRC n'a pas rendu compte de 85 % des recherches qu'elle a effectuées au moyen de ses comptes Clearview. Par conséquent, il semble qu'elle ne soit pas en mesure de démontrer que l'évaluation du premier facteur de l'arrêt *Waterfield* ait été effectuée. La GRC a souligné qu'avant sa directive sur l'usage de la technologie de Clearview diffusée après le début de l'enquête du Commissariat, l'usage de la technologie de Clearview en dehors du cadre d'une enquête n'aurait pas fait l'objet d'un suivi, car il n'y avait pas d'exigence établie à cet égard. Cela constitue un manquement important de responsabilité de la part de la GRC.

46. En ce qui concerne le second élément du test, nous remarquons que l'utilisation de la technologie de reconnaissance faciale, et le pouvoir de celle-ci de perturber l'anonymat dans les lieux publics, peut constituer une atteinte particulièrement importante à la liberté et à la vie privée. De plus, le recours par la GRC à un service comme celui de Clearview, fondé sur l'extraction systématique et le traitement de milliards d'images de personnes innocentes de tout crime, constitue une intrusion majeure et substantielle par l'État dans la vie privée des Canadiens.

47. Avant de recourir à un tel service, un corps policier devrait à tout le moins se demander si cela est nécessaire à l'enquête qu'il mène, et si l'intérêt public particulier qui est recherché est proportionnel à l'intrusion subie[29].

48. Dans ce contexte, le fait que plusieurs décideurs à la GRC n'aient pas jugé nécessaire de se pencher sur les limites à imposer à l'utilisation d'une telle technologie au titre de la common law donne à penser qu'ils ne comprennent pas vraiment les obligations pertinentes de la GRC en matière de protection de la vie privée.

Recommandations :

i. Nous avons recommandé, et la GRC a accepté notre recommandation, d'engager un dialogue avec le Commissariat et d'autres organismes de réglementation de la protection de la vie privée sur les questions entourant l'utilisation de la technologie de reconnaissance faciale.

ii. Nous avons également recommandé, et la GRC a accepté notre recommandation, de mettre sur pied un programme de formation au plus tard 12 mois après la réception du présent rapport afin de s'assurer que tous les décideurs sont formés sur les limites de la collecte de renseignements personnels au titre de la *Loi,* notamment :

    a) Lors de la passation de contrats pour des services de collecte de renseignements personnels, ne pas recourir à des fournisseurs de services qui recueillent des renseignements personnels en enfreignant les lois canadiennes.

[29] *R. c. Waterfield*, précité; voir également *Fleming,* précité.

b) Acquérir une compréhension approfondie et nuancée des limites associées à la collecte des données personnelles, en particulier lorsque de nouvelles technologies portant atteinte à la vie privée sont utilisées, notamment les outils de surveillance de masse.

49. Comme il a été mentionné ci-dessus (au paragraphe 30), la GRC n'est pas d'accord avec notre conclusion selon laquelle elle a l'obligation de s'informer de la légalité des pratiques de collecte des renseignements personnels des partenaires auprès desquels elle recueille ce genre de renseignements. Nous notons que la GRC, malgré son désaccord avec notre conclusion, reconnaît que ses pratiques actuelles présentent des lacunes. Pour cette raison, la GRC a accepté de mettre en oeuvre les recommandations ci-dessus, notamment de mener une évaluation complète de la conformité des tiers aux lois canadiennes en matière de protection des renseignements personnels, auxquelles ces tiers sont assujettis.

B) Connaissance des nouvelles méthodes de collecte

50. La connaissance des nouvelles techniques de collecte de renseignements personnels, lesquelles sont utilisées (ou envisagées ou mises à l'essai), est un élément essentiel pour mettre en pratique une compréhension théorique des obligations prévues à l'article 4 de la *Loi*. Cette connaissance est nécessaire parce qu'elle permet de limiter adéquatement la collecte et d'offrir une garantie de fiabilité aux partenaires externes, tout en préservant la confiance du public.

51. Les faits relatifs à cette affaire démontrent clairement les importantes lacunes des mécanismes mis en place par la GRC pour se sensibiliser aux nouvelles pratiques de collecte de renseignements personnels qu'elle entreprend. Comme il a été mentionné précédemment (au paragraphe 10), la GRC a informé à tort le Commissariat, le 29 janvier 2020, qu'elle n'avait pas utilisé la technologie de Clearview dans le cadre d'une enquête, malgré le fait qu'elle avait acheté des licences auprès de Clearview en octobre 2019 et qu'elle avait depuis largement utilisé les services de Clearview. Pour expliquer cette déclaration erronée, la GRC précise qu'aucun de ses experts internes des Services d'enquêtes techniques, qui ont été consultés par les membres de l'Unité de l'accès à l'information et de la protection des renseignements personnels de la GRC, n'était au courant de l'utilisation de cette technologie, alors même que la technologie de Clearview était largement utilisée dans cinq divisions différentes de la GRC.

52. Ce n'est qu'après avoir appris que la liste des clients de Clearview, dont elle fait partie, a été déclarée volée en février 2020, que la GRC a corrigé la déclaration erronée faite au Commissariat.

53. De plus, comme nous l'avons déjà mentionné, la GRC n'a fourni une justification raisonnable que pour environ 15 % des recherches d'un ensemble de plus

500 recherches au total, selon les dossiers de Clearview. Le but des autres recherches demeure inconnu[30].

54. La GRC n'avait pas encore établi un mécanisme, que ce soit à l'échelle locale ou nationale, pour assurer le suivi de l'examen ou de l'utilisation réelle des nouvelles technologies d'enquête ou d'autres nouvelles méthodes de collecte de renseignements personnels.

Recommandation :

i. Nous avons recommandé, et la GRC a accepté notre recommandation, de mettre en place des mécanismes et des procédures au plus tard 12 mois après la réception du présent rapport pour s'assurer que toute nouvelle méthode de collecte de renseignements personnels dans l'ensemble de la GRC fait l'objet d'un suivi interne fiable, de manière à ce que la GRC puisse prendre des décisions éclairées à cet égard.

55. Relativement à l'engagement ci-dessus, la GRC a mis sur pied en mars 2021, comme mesure préliminaire, le « Programme national d'intégration des technologies ». Ce programme vise à créer un cadre pour la mise en œuvre d'un système centralisé qui permettra à la GRC de recenser et d'examiner les nouvelles techniques d'enquête qui ont recours à la collecte de nouveaux types de renseignements aux fins d'enquête, et d'en assurer le suivi.

C) Processus permettant de déceler les éventuels problèmes de conformité

56. Il est crucial de cerner les collectes de renseignements personnels réelles ou éventuelles qui justifient une évaluation de la conformité à la *Loi avant* qu'elles ne soient entreprises. Nous nous attendons à ce que ces vérifications soient proportionnelles aux risques pour la vie privée des personnes, compte tenu du volume, de la sensibilité et de la complexité des activités de collecte de renseignements personnels. Nous nous attendons également à ce que les vérifications soient intégrées aux processus appropriés, selon les activités de l'institution. Ainsi, les décideurs habilités à prendre des décisions relatives à de nouvelles méthodes de collecte de renseignements personnels susceptibles de présenter des risques élevés peuvent démontrer la façon dont ils ont respecté la *Loi*.

57. En plus d'être intégrées aux processus d'élaboration et d'approbation de nouveaux programmes, nous nous attendons à ce que de telles vérifications soient intégrées à d'autres processus où de nouveaux types de renseignements personnels, de nouveaux objectifs de collecte, de nouvelles façons de recueillir des renseignements ou de nouvelles sources de renseignements personnels pourraient se présenter. En voici quelques exemples à titre d'illustration :

- les processus de conclusion d'ententes d'échange de renseignements;
- les processus d'approvisionnement;

[30] Nous soulignons que la GRC ne pouvait plus procéder à l'audit des registres d'accès conservés dans ses comptes Clearview après que Clearview ait suspendu ses comptes le 6 juillet 2020.

- les processus régissant les projets pilotes et la mise à l'essai de services;
- les processus d'approbation des nouvelles technologies.

58. L'un des meilleurs exemples pour illustrer les lacunes de la GRC est le fait que l'organisation a indiqué qu'elle ne fait référence au besoin de réaliser des EFVP que dans les manuels de GI ou de TI. Les EFVP (ou les autres mesures pour évaluer la conformité à la *Loi*) sont nécessaires en dehors des processus de GI ou de TI. Toute direction ou tout échelon de la GRC susceptible de procéder à une nouvelle collecte de renseignements personnels doit avoir établi des procédures pour entreprendre une évaluation de la conformité à la *Loi* lorsque cela est justifié.

59. La GRC a indiqué que ses membres sont habilités à utiliser leur pouvoir discrétionnaire pour mettre à l'essai de nouvelles techniques de collecte de renseignements personnels à condition d'obtenir les approbations appropriées à l'échelle locale. La décision de mener ou non une EFVP revient aux superviseurs. Dans cette affaire, la GRC a créé un total de 19 comptes payants et d'essai pour recueillir des renseignements personnels auprès d'une nouvelle source importante du secteur privé, y compris deux contrats payés, sans que cela ne donne lieu à une évaluation de conformité à l'article 4 de la *Loi.* De plus, la collecte de renseignements personnels par la GRC au moyen d'une nouvelle technologie portant atteinte à la vie privée (reconnaissance faciale), qui constitue manifestement une modification susbstantielle à la façon de recueillir des renseignements personnels, laquelle pourrait avoir une incidence sur la conformité, n'a pas donné lieu à une évaluation de la conformié à la *Loi* avant son utilisation.

60. D'après les observations de la GRC, ce n'est que le 6 février 2020, soit plus de quatre mois après avoir conclu un contrat avec Clearview, qu'elle a commencé à envisager d'effectuer une évaluation de la conformité à la *Loi* pour la collecte de renseignements auprès de Clearview. Les dossiers de la GRC indiquent en outre que l'organisation n'a commencé à remplir une liste de vérification de l'EFVP (outil utilisé par le SCT pour déterminer si une EFVP est justifiée[31]) qu'en mars 2020. Cette étape préliminaire visant à cerner les problèmes n'a été achevée qu'en juin 2020. Comme en témoigne cette affaire, l'adoption d'une approche ponctuelle, peu supervisée et a posteriori augmentera la probabilité d'atteinte à la vie privée et entraînera des préjudices qui auraient pu être évités.

61. Le Commissariat est d'avis qu'avec un processus d'examen adéquat, la contravention en question aurait pu être évitée. En effet, cela aurait été possible si la GRC avait cerné rapidement les problèmes de conformité éventuels liés à l'utilisation de la technologie de Clearview AI, afin d'entreprendre une évaluation appropriée de la conformité à la *Loi*, éclairée par une consultation adéquate d'experts en la matière. Si la GRC avait avisé le Commissariat, comme elle était tenue de le faire selon la *Politique sur la protection de la vie privée* du SCT (voir paragraphe 37), une discussion préliminaire au sujet des répercussions sur la vie privée aurait pu avoir lieu. Il est très préoccupant que la GRC n'ait pas jugé nécessaire de procéder à une évaluation de la conformité (sous la forme d'une EFVP ou autre) avant de recueillir des renseignements personnels au moyen de l'un des 19 comptes qu'elle a créés.

[31] Selon la Directive sur l'évaluation des facteurs relatifs à la vie privée du SCT.

Recommandation :

i. Nous avons recommandé, et la GRC a accepté notre recommendation, de mettre en place, et ce, au plus tard 12 mois après la reception du présent rapport, un système de contrôles permettant de recenser toute nouvelle collecte présentant des risques potentiellement élevés, afin d'avertir les décideurs qu'une évaluation de la conformité pourrait être nécessaire. Les décideurs peuvent ensuite démontrer qu'ils ont tenu compte de la conformité aux exigences énoncées à l'article 4 de la *Loi* avant de commencer à recueillir des renseignements personnels et entreprendre des évaluations complètes au besoin.

D) Processus permettant de réaliser des évaluations en temps voulu lorsque cela est justifié

62. Lorsqu'un problème de conformité éventuel est recensé à la suite des contrôles ci-dessus (c.-à-d. lorsque la conformité à la *Loi* peut être en cause), les évaluations de la conformité à la *Loi* devraient être entreprises et terminées avant le début de la collecte. Cette façon de procéder permet de réduire le risque de collecte illégale et d'éviter les préjudices connexes aux personnes qui pourraient autrement être visées par une telle collecte de leurs renseignements personnels. Ces évaluations devraient être éclairées par une expertise pertinente en matière de protection de la vie privée et de droit et, lorsque cela est justifié, par le Commissariat.

63. Même si, comme nous l'avons décrit ci-dessus, les processus internes de la GRC n'ont pas permis en l'espèce de recenser de manière proactive les préoccupations potentielles en matière de protection de la vie privée, il aurait néanmoins dû être évident pour la GRC qu'une évaluation complète des collectes effectuées auprès de Clearview était justifiée après que la question eut été soulevée dans les médias en janvier 2020. En effet, la GRC s'est expressément engagée auprès du Commissariat en janvier (lorsqu'elle a affirmé qu'elle n'utilisait pas Clearview) à effectuer une EFVP avant de déployer activement une telle technologie.

64. En dépit de cette nécessité évidente et de cette déclaration au Commissariat, la GRC n'a fourni aucune preuve permettant de conclure qu'elle avait entrepris une véritable évaluation de la conformité à la *Loi* (au-delà de la liste de contrôle pour l'identification des problèmes mentionnée ci-dessus), avant que Clearview AI cesse d'offrir ses services de reconnaissance faciale du Canada en juillet 2020.

65. La GRC a indiqué qu'elle n'avait pas de matériel de formation pour le personnel chargé de mener des EFVP, malgré la quantité importante de renseignements personnels sensibles qu'elle recueille en tant qu'organisme d'application de la loi.

66. Il est encore plus préoccupant qu'aucun des décideurs de la GRC n'ait effectué une telle évaluation avant le début de la collecte. Cela, malgré les déclarations antérieures de la GRC au Commissariat selon lesquelles elle était consciente des répercussions possibles des services de Clearview sur la protection de la vie privée et s'engageait à

effectuer une EFVP avant de recourir à ce service. Nous sommes d'avis qu'il s'agit d'un manquement grave de la part de la GRC de s'assurer qu'elle respecte ses obligations prévues par la *Loi*.

Recommandations :

i. Nous avons recommandé, et la GRC a accepté notre recommendation, de mettre sur pied un programme de formation à l'intention de tous les décideurs (c.-à-d. toute personne habilitée à prendre des décisions visant à recueillir de nouveaux renseignements personnels) sur leurs rôles et responsabilités en la matière, pour cerner et évaluer le besoin de collecte de renseigments et pour éviter que des renseignements soient recueillis en contravention de la *Loi*, au plus tard 12 mois après la réception du présent rapport.

ii. Nous avons également recommandé, et la GRC a accepté notre recommendation, qu'au plus tard 12 mois après la réception du présent rapport, la GRC démontre qu'elle a affecté les ressources nécessaires et mis en place les processus pour s'assurer que des évaluations de la conformité à la *Loi* sont menées lorsque nécessaire et de façon cohérente par toutes les divisions de la GRC. Ces ressources et ces processus devraient permettre de s'assurer que les évaluations sont effectuées en temps opportun, en s'appuyant sur une expertise pertinente en la matière, en fonction des problèmes relevés, *avant* que des renseignements personnels ne soient recueillis à des fins d'application de la loi.

67. Comme mesure préliminaire pour donner suite à ces engagements, la GRC a mis sur pied en mars 2021, comme il est indiqué ci-dessus, le « Programme national d'intégration des technologies ».

E) Contrôles efficaces de la collecte

68. Lorsque la GRC a créé pour la première fois des comptes payants pour recourir aux services de Clearview en octobre 2019, elle ne disposait pas de politiques précises limitant les fins auxquelles ces renseignements pouvaient être recueillis, malgré les répercussions évidentes sur la vie privée décrites ci-dessus. Après les préoccupations exprimées par le public et l'annonce de notre enquête, la GRC a émis une directive interne à l'intention de ses membres, le 5 mars 2020, imposant des limites à la collecte par l'entremise de Clearview. Plus précisément, cette directive contenait de l'information et des instructions à l'intention des membres de la GRC, dont les éléments suivants :

> [Traduction]
> Étant donné la vitesse avec laquelle la technologie évolue, la GRC continue d'étudier l'utilisation plus large des technologies émergentes afin de déterminer comment elles pourraient potentiellement être utiles aux opérations policières. Bien que l'utilisation des nouvelles technologies puisse améliorer notre capacité à mener des enquêtes de manière plus efficace et efficiente, nous devons trouver un équilibre avec le droit des personnes à la vie privée.

> […]
>
> […] La GRC et d'autres organismes d'application de la loi s'efforcent en permanence de recenser, de tester et éventuellement d'acquérir des technologies nouvelles et innovantes pour faire avancer les enquêtes criminelles relevant de leur compétence. Pour encadrer la découverte, la mise à l'essai réussie et l'adoption d'une nouvelle technologie, il faut établir des politiques opérationnelles qui permettent d'assurer la gouvernance et la responsabilité à l'égard de l'utilisation de la technologie en question et de l'acquisition, de l'utilisation et du stockage des données en cause. Ces politiques doivent tenir compte de la *Charte,* de la *Loi sur la protection des renseignements personnels* et d'autres lois, règlements et politiques pertinents.
>
> Notre examen de l'utilisation permanente de cette technologie, et particulièrement de celle de Clearview AI, se poursuit. Dans l'intervalle, compte tenu des sensibilités entourant la technologie de reconnaissance faciale, nous ne l'utiliserons que dans des circonstances très limitées et bien précises.
>
> Dorénavant, les divisions doivent examiner attentivement le recours aux technologies de reconnaissance faciale, y compris celle de Clearview AI, et n'y recourir que dans des situations d'urgence pour identifier les victimes dans le cadre d'enquêtes sur l'exploitation sexuelle des enfants ou dans des situations où une menace à la vie ou des lésions corporelles graves peuvent être imminentes. Les divisions doivent s'assurer que les officiers responsables des enquêtes criminelles (OREC) approuvent toute demande d'utilisation de la technologie de reconnaissance faciale. Pour ce qui est de la direction générale, toute utilisation doit être approuvée par le directeur général du programme ayant présenté la demande. Il vous est également demandé d'informer [le commissaire adjoint des opérations techniques des services de police spécialisés] de toute utilisation de la technologie de reconnaissance faciale. Cela permettra d'assurer une surveillance nationale et de garantir que l'organisation est informée en permanence de l'utilisation limitée de cette technologie.

69. Au cours de notre enquête, la GRC a également centralisé la gestion des comptes Clearview et créé une fonction d'audit pour surveiller l'utilisation de Clearview par les membres de la GRC.

70. Nous apprécions ces éléments favorables qui témoignent du fait que la GRC a compris, après que des préoccupations aient été exprimées par des intervenants externes, que les situations dans lesquelles elle pourrait légalement recueillir des renseignements sur Internet au moyen de la technologie de reconnaissance faciale pourraient être limitées par la common law (et, par conséquent, par l'article 4 de la *Loi*).

71. Toutefois (comme il en est fait mention au paragraphe 18 ci-dessus), seules 6 % des recherches effectuées par la GRC au moyen de la technologie de Clearview semblaient être liées à l'identification des victimes, et la GRC n'a pu rendre compte que d'approximativement 9 % des recherches supplémentaires répertoriées. Elle est

incapable de rendre compte de la grande majorité (85 %) des recherches qu'elle a effectuées selon les dossiers de Clearview. Nous ne pouvons affirmer avec certitude que les recherches étaient limitées aux fins susmentionnées, ni même qu'elles étaient effectuées pour des motifs professionnels. L'absence de documents attestant de motifs professionnels indique le contraire.

72. De plus, la GRC n'a pas précisé si les membres de son organisation qui ont recueilli des renseignements après avoir créé des comptes d'essai de Clearview ont enfreint des politiques ou des procédures internes lorsqu'ils l'ont fait. Ce manque de contrôle relativement à une nouvelle collecte importante de renseignements personnels est très préoccupant. Nous savons que pour fonctionner de manière efficace, la GRC demande à son personnel d'innover et de prendre des initiatives, mais il est aussi important que des mesures soient mises en place pour s'assurer que ces innovations ne contreviennent pas à la loi.

Recommandations :

i. Nous avons recommandé, et la GRC a accepté notre recommendation, de mettre en place des contrôles clairs qui entreront en vigueur au plus tard 12 mois après la réception du présent rapport. Ces contrôles devront comprendre ce qui suit : i) des politiques visant à préciser les personnes habilitées à prendre la décision d'entreprendre de nouvelles collectes de renseignements personnels ainsi que les mesures que doivent prendre le personnel pour décider si la collecte envisagée est permise, ii) des mécanismes de surveillance des collectes non autorisées, y compris de celles effectuées à des fins inappropriées.

ii. Nous avons également recommandé, et la GRC a accepté notre recommendation, d'établir, au plus tard 12 mois après la réception du présent rapport, une méthode et une chaîne de responsabilité claires afin que les membres de l'organisation puissent suggérer de nouvelles techniques de collecte aux décideurs ayant reçu la formation appropriée.

Autres

73. Étant donné que la collecte de renseignements personnels auprès de Clearview par la GRC n'était pas conforme à l'article 4 de la *Loi* et que la GRC ne recueille plus de renseignements auprès de Clearview, nous n'avons pas examiné en détail les procédures accessoires de la GRC relatives à leur utilisation.

74. Toutefois, dans le but de guider les pratiques futures de la GRC, nous présentons certaines observations relatives à d'autres articles de la *Loi* qui pourraient s'appliquer à toute activité comparables menées par la GRC à l'avenir.

Protection contre l'utilisation ou la communication involontaire

75. L'article 8 de la *Loi* prévoit qu'une institution ne peut communiquer des renseignements personnels qu'aux fins auxquelles ils ont été recueillis ou pour les usages qui sont compatbles avec ces fins. Cette disposition s'appliquerait, par exemple, aux images recueillies par la GRC et téléchargées dans l'application Clearview à des fins de reconnaissance faciale.

76. Pour que les institutions s'assurent de respecter ces limites, y compris lorsqu'elles passent des contrats de services (comme c'était le cas dans la présente affaire), la *Directive sur les pratiques relatives à la protection de la vie privée* du SCT prévoit que, lorsque des renseignements personnels sont communiqués à une institution du secteur privé, les marchés conclus avec les entités du secteur privé doivent définir les dispositions et les mesures visant à régler les problèmes de protection de la vie privée. Il s'agit notamment de dispositions visant à limiter le traitement, l'utilisation ou la communication inappropriés par l'entité sous contrat et à garantir une protection adéquate des renseignements personnels contre les communications involontaires à des tiers. De plus, les dispositions relatives à la protection doivent garantir le respect des normes de sécurité gouvernementales.

77. De telles mesures sont manifestement importantes. Notons à cet égard que Clearview a fait l'objet d'une atteinte à la protection des données en février 2020, bien que nous n'ayons aucune indication que cette atteinte ait eu une incidence sur les images téléchargées dans l'application Clearview par la GRC.

78. Selon ses observations, la GRC a pris certaines mesures pour protéger les renseignements personnels communiqués à Clearview contre toute utilisation ou communication inappropriée subséquente :

    - Pour le petit sous-ensemble de recherches effectuées auprès de Clearview dont elle a pu rendre compte, la GRC avait mis en place des procédures exigeant que les photos soient recadrées pour ne garder que le visage recherché avant de les téléverser dans l'application Clearview, afin d'éviter de télécharger des informations non pertinentes et de limiter le risque de communication.
    - Elle a indiqué que Clearview lui a confirmé que les transmissions de données sont cryptées et que les images téléversées ne sont pas ajoutées à la base de données de Clearview.
    - Elle a demandé à Clearview de réduire à 45 jours la période de conservation des images téléversées et de ne conserver par la suite qu'une vignette à faible résolution pendant 6 mois.

79. Toutefois, la GRC n'a pas démontré qu'elle avait inclus une partie ou la totalité des éléments susmentionnés dans ses contrats (contrat de licence) avec Clearview. La GRC a fait valoir que ses licences (que ce soit pour les comptes payants ou les comptes d'essai) n'étaient assujetties qu'aux conditions d'utilisation et à la politique de confidentialité de Clearview.

Exactitude

80. Le paragraphe 6(2) de la *Loi* précise qu'« une institution fédérale est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels qu'elle utilise à des fins administratives soient à jour, exacts et complets. »

81. La GRC a fait valoir que, en ce qui concerne l'exactitude des résultats obtenus au moyen de la technologie de Clearview et utilisés par la GRC, elle a ordonné à ses membres, par l'entremise des consignes de sécurité du CNCEE, de traiter tous les renseignements comme des pistes, et non comme des correspondances d'identité confirmées. La décision de prendre ou non d'autres mesures était fondée sur l'évaluation des membres.

82. En ce qui a trait à l'utilisation de la technologie de reconnaissance faciale en général, nous croyons qu'il est important de souligner qu'il existe des préoccupations quant à l'exactitude et au biais algorithmique des technologies de reconnaissance faciale. Cela comprend la possibilité que les résultats d'identification soient de « faux positifs », lesquels pourraient avoir une incidence sur les décisions prises par les organismes d'application de la loi relativement à certaines personnes, comme la possibilité de se renseigner davantage au sujet de celles-ci. De telles actions peuvent à leur tour avoir une incidence importante sur la vie privée des personnes.

83. Par exemple, il existe une abondante littérature scientifique décrivant en détail l'inexactitude des données anthropométriques[32] aux fins de détermination de la race ou de l'ascendance dans le domaine de l'anthropologie judiciaire sur le plan de l'analyse du squelette, en particulier du crâne et du visage, et l'utilisation de tissus mous externes utilisés pour l'identification judiciaire du portrait approximatif (reconstitution faciale) semble encore moins précise. Selon Ubelaker et coll., [traduction] « les techniques de reconstitution faciale s'améliorent grâce à de meilleurs renseignements concernant le lien entre les tissus durs et les tissus mous du visage et à une technologie informatique plus sophistiquée. Malgré ces progrès, la reconstitution faciale ne représente pas une méthode d'identification scientifique[33]. » Nous croyons qu'il est important de le savoir parce que la technologie de reconnaissance faciale est fondée sur des données anthropométriques qui mènent à certaines hypothèses au sujet des traits faciaux qu'ont en commun divers groupes ethniques et raciaux.

84. Une étude récente menée par le National Institute of Standards and Technology des États-Unis (NIST) dans le cadre de sa série « Face Recognition Vendor Test[34] » s'est intéressée aux différences démographiques dans les algorithmes contemporains de

[32] Les « données anthropométriques » désignent les mesures de la taille et de la forme de diverses parties du corps humain.
[33] DH Ubelaker, A Shamlou, A Kunkle (2019) « Contributions of forensic anthropology to positive scientific identification: a critical review. » *Forensic Sciences Research* 4(1) : 45-50. (En anglais seulement) (Consulté pour la dernière fois le 23 octobre 2020).
[34] Face Recognition Vendor Test (En anglais seulement) (Consulté pour la dernière fois le 23 octobre 2020).

reconnaissance faciale (NISTIR 8280)[35]. En résumé, l'étude du NIST a permis de tirer les conclusions suivantes :

i. En ce qui concerne la correspondance entre deux individus, l'équipe a constaté des taux plus élevés de faux positifs pour les personnes d'origine asiatique et afro-américaine que pour les personnes de race blanche.

ii. Parmi les algorithmes mis au point aux États-Unis, il y avait des taux élevés comparables de faux positifs dans la correspondance entre deux personnes pour les personnes d'origine asiatique, afro-américaine et autochtone.

iii. Cependant, une exception notable a été remarquée pour certains algorithmes développés dans les pays asiatiques.

iv. Pour les correspondances de type un individu à plusieurs autres individus, l'équipe a constaté des taux plus élevés de faux positifs pour les Afro-Américaines.

v. Cependant, ce ne sont pas tous les algorithmes qui donnent ce taux élevé de faux positifs dans l'ensemble des données démographiques des correspondances de type un individu à plusieurs individus[36].

85. Dans le but de se conformer à l'article 6 de la *Loi,* dans la mesure où la GRC envisage l'utilisation future de technologies de reconnaissance faciale précises, il sera important que l'organisation évalue soigneusement les mesures qui pourraient s'avérer nécessaires pour répondre aux préoccupations liées à l'exactitude, en particulier au risque de faux positifs. Nous nous réjouissons à l'idée de pouvoir poursuivre le dialogue sur cette question avec la GRC dans le cadre de discussions prévues avec le Commissariat et d'autres organismes de réglementation de la protection de la vie privée, en vue d'élaborer un document d'orientation sur l'utilisation de la technologie de reconnaissance faciale par les organismes d'application de la loi.

Conclusion

86. Nous concluons que la collecte de renseignements personnels par la GRC auprès de Clearview contrevenait à l'article 4 de la *Loi.* Cette conclusion est fondée sur le fait que la collecte de renseignements personnels sur les Canadiens par Clearview contrevenait aux lois canadiennes en matière de protection des renseignements personnels. Il s'ensuit donc que la GRC a contrevenu à la *Loi* lorsqu'elle a par la suite recueilli ces renseignements personnels illégalement obtenus par Clearview.

[35] Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. (En anglais seulement) (Consulté pour la dernière fois le 20 mai 2020).
[36] NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software; voir également les articles Facial-Recognition Software Might Have a Racial Bias Problem et Facial Recognition Is Accurate, if You're a White Guy [En anglais seulement] (Consultés pour la dernière fois le 20 mai 2021).

87. La GRC a commis des manquements graves et systémiques à l'obligation de se conformer à la Loi avant de recueillir des renseignements auprès de Clearview et, de façon plus générale, avant toute nouvelle collecte de renseignements personnels. Il s'agit notamment d'omissions généralisées pour ce qui est de savoir ce qu'elle recueillait, de contrôler la méthode de collecte, de cerner les problèmes éventuels de conformité, ainsi que d'évaluer et de prévenir les contraventions à la *Loi.*

88. Avant que le Commissariat ne formule les recommandations ci-dessus, en réponse aux questions que nous avons soulevées, la GRC avait déjà commencé à explorer des façons d'améliorer son examen des pratiques en matière de collecte afin de se conformer à ses obligations légales, et en mars 2021, elle a lancé le « Programme national d'intégration des technologies ». De plus, la GRC s'est engagée à mettre en oeuvre les recommandations formulées par le Commissariat dans le présent rapport.

89. Nous demeurons préoccupés par le fait que la GRC n'a pas souscrit à nos conclusions, selon lesquelles nous estimons qu'elle avait contrevenu à la *Loi*, et qu'elle affirme ne pas être tenue de s'assurer que les agents tiers auprès desquels elle recueille des renseignements personnels ont agi conformément aux lois en ce qui concerne la collecte et l'utilisation de ces renseignements. Cela dit, nous accueillons favorablement les mesures préliminaires que la GRC a déjà prises, comme il est indiqué ci-dessus, ainsi que son engagement à mettre en œuvre toutes nos recommandations. Le Commissariat conclut donc que la plainte est **fondée et conditionnellement résolue.**

90. La mise en œuvre de nos recommandations exigera de la GRC de travailler de manière concertée à l'échelle de l'organisation. Il reste beaucoup de travail à accomplir pour changer la culture à l'interne concernant la prise de décision – il faudra compter sur des procédures, des outils et de la formation qui soient bien intégrés. Nous encourageons vivement la GRC à consacrer les ressources nécessaires à cet égard et à désigner des « champions » parmi les cadres supérieurs pour réussir la mise en œuvre des recommandations. En mettant pleinement en œuvre nos recommandations, la GRC sera en mesure d'explorer plus efficacement les nouvelles technologies et d'utiliser ces dernières de façon plus responsable pour réaliser son important mandat.

3. 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

Table des matières

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].

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 :

[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.

- 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

[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.

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 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

[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.
[4] *Code criminel, L.R.C. (1985), ch. C-46,* art. 487.01.

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

---

[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.
[9] *Fleming c. Ontario*, *ibid*, paragraphe 46.

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 collecte de renseignements personnels à des fins d'« application de la loi »[13]. Les services de police

---

[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.
[13] Par exemple, voir la *Freedom of Information and Protection of Privacy Act* de l'Alberta, alinéa 33 *b)*.

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 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

[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.
[19] *R. c. Spencer,* 2014, 2 CSC 212.

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 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

[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.

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].

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

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

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 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 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 :

---

[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.

- 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 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

[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).
[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.

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 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

[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).

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).

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.

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 :

[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.

- 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 :

    - Déterminer les périodes de conservation applicables aux renseignements personnels dès leur collecte.

---

[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.

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

[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.

- 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.