



RAPPORT DE CONCLUSIONS

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

CPVP-LPRPDE-039525/CAI QC-1023158/OIPC BC P20- 81997/OIPC AB-015017

Enquête conjointe du Commissaire à la protection de la vie privée du Canada (CPVP), de la Commission d'accès à l'information du Québec (CAI), du Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (CIPVP de la C.-B.) et du Commissariat à l'information et à la protection de la vie privée de l'Alberta (CIPVP de l'Alb.) sur la conformité de Clearview AI, Inc. à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP du Québec), à la *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI du Québec), à la *Personal Information Protection Act* de la Colombie-Britannique (PIPA de la C.-B.) et à la *Personal Information Protection Act* de l'Alberta (PIPA de l'Alb.)

Table des matières

Aperçu	3
Contexte	6
Enjeux	7
Méthodologie	7
Représentations de Clearview et notre enquête	8
Aperçu de la mise en œuvre de la reconnaissance faciale par Clearview	8
Pratiques de confidentialité de Clearview en matière de consentement	9
Objectifs de Clearview	9
Comparaison avec d'autres organismes	10
Analyse	11
Contestation de la juridiction par Clearview	11
Enjeu 1 : Clearview a-t-elle obtenu le consentement requis?	15
Enjeu 2 : Clearview a-t-elle recueilli, utilisé ou communiqué des renseignements personnels à des fins acceptables?	22
Autres préoccupations concernant les fins acceptables	27
Exactitude	27
Collecte en violation des dispositions contractuelles.....	29
Risque de préjudices causés par une atteinte à la vie privée	29
Enjeu 3 : Clearview a-t-elle satisfait à ses obligations concernant la biométrie au Québec?	30
Recommandations	31
Réponse de Clearview à nos conclusions	31
Conclusions	32

Aperçu

Le Commissariat à la protection de la vie privée du Canada (le CPVP), la Commission d'accès à l'information du Québec (la CAI), le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (le CIPVP de la C.-B.) et le Commissariat à l'information et à la protection de la vie privée de l'Alberta (le CIPVP de l'Alberta), désignés collectivement comme étant « les commissariats », ont ouvert une enquête conjointe¹ visant à déterminer si la collecte, l'utilisation et la communication de renseignements personnels par Clearview AI, Inc. (« Clearview ») au moyen de son dispositif de reconnaissance faciale étaient conformes aux lois fédérale et provinciales sur la protection des renseignements personnels applicables au secteur privé.

Plus précisément, les commissariats ont cherché à déterminer si Clearview :

- i. a obtenu le consentement requis pour la collecte, l'utilisation et la communication de renseignements personnels;
- ii. a recueilli, utilisé et communiqué les renseignements personnels à des fins acceptables².

En outre, la CAI a cherché à déterminer si Clearview avait :

- iii. déclaré la création d'une banque de mesures et de caractéristiques biométriques.

Le dispositif de reconnaissance faciale de Clearview comporte quatre grandes étapes successives. Clearview :

- i. « **prélève** » les images comportant des visages et les données connexes à partir de sources en ligne accessibles au public (y compris les médias sociaux), et stocke ces données dans sa base de données;
- ii. **crée des identifiants biométriques** sous forme de représentations numériques pour chaque image;
- iii. **permet aux utilisateurs de télécharger une image**, qui est ensuite évaluée par rapport à ces identifiants biométriques et mise en correspondance avec les images de sa base de données;
- iv. **fournit une liste de résultats**, contenant toutes les images et métadonnées correspondantes. Si un utilisateur clique sur l'un de ces résultats, il est redirigé vers la page source de l'image.

¹ Tout au long du présent rapport, les termes « nous » et « notre » sont fréquemment utilisés. Lorsqu'ils sont utilisés dans un autre contexte que celui d'un document cité, ces termes renvoient collectivement au CPVP, à la CAI, au CIPVP de la C.-B. et au CIPVP de l'Alb.

² Dans le présent rapport, l'expression « fins acceptables » englobe les « fins raisonnables » au sens de la PIPA de l'Alb. et de la PIPA de la C.-B., et l'« intérêt légitime » au sens de la LPRPSP du Québec.

Grâce à ce processus, Clearview a constitué une base de données de plus de trois milliards d'images de visages et d'identificateurs biométriques correspondants, y compris ceux d'un grand nombre d'individus au Canada, incluant des enfants.

Clearview a affirmé que le dispositif est destiné à être utilisé par les organismes chargés de l'application de la loi³ pour répondre à des besoins légitimes d'application de la loi et d'enquête. Diverses organisations, y compris des entités du secteur privé, ont eu recours à ce service en y accédant au moyen d'un essai gratuit.

Les données biométriques sont considérées comme sensibles, dans la plupart des cas, et les données de reconnaissance faciale sont particulièrement sensibles. En outre, les personnes qui ont publié leurs images en ligne, ou dont les images ont été publiées par un ou plusieurs tiers, ne pouvaient raisonnablement s'attendre à ce que Clearview les recueille, utilise et communique à des fins d'identification. Par conséquent, il est généralement nécessaire d'obtenir un consentement explicite. Au Québec, une telle utilisation de renseignements biométriques requiert un consentement exprès.

Clearview n'a pas cherché à obtenir le consentement des personnes au sujet desquelles elle a recueilli ces renseignements. Clearview indique que les renseignements personnels étaient « accessibles au public » et donc exemptés des exigences de consentement. Les renseignements recueillis sur des sites Web publics, par exemple les profils de médias sociaux et les profils professionnels, puis utilisés à des fins non connexes ne relèvent pas de l'exception prévue par la LPRPDE, la PIPA de l'Alberta et la PIPA de la Colombie-Britannique concernant les renseignements « auxquels le public a accès ». Ces renseignements ne sont pas non plus considérés comme ayant « un caractère public en vertu de la loi », ce qui les soustrairait à la LPRPSP du Québec, et aucune exception de cette nature existe pour les autres renseignements biométriques selon la LCCJTI. Nous avons donc conclu que Clearview n'était pas exemptée de l'obligation d'obtenir un consentement.

En outre, nous avons déterminé que Clearview a recueilli, utilisé et communiqué des renseignements personnels d'individus au Canada à des fins inappropriées qui ne peuvent pas être justifiées par l'obtention d'un consentement. Nous avons conclu que la collecte massive d'images et la création de dispositifs de reconnaissance faciale biométriques par Clearview, dans le but avoué de fournir un service au personnel des organismes chargés de l'application de la loi, et leur utilisation par d'autres personnes au moyen des comptes d'essai, représentent l'identification et la surveillance de masse de personnes par une entité privée dans le cadre d'une activité commerciale. Nous avons conclu que l'utilisation des renseignements par Clearview était à des fins inappropriées lorsque celle-ci : i) n'avait aucun lien avec les motifs pour lesquels ces images avaient été initialement publiées; ii) était souvent au détriment de la personne dont les images avaient été recueillies; iii) pouvait porter un préjudice important à ces personnes, dont la

³ Bien que Clearview ait indiqué que le service était initialement destiné aux entreprises spécialisées dans le maintien de l'ordre et de la sécurité, au moment de la rédaction du présent rapport, selon les conditions de service de Clearview, seuls les organismes gouvernementaux peuvent créer un compte.

grande majorité n'a jamais été et ne sera jamais impliquée dans un crime. De surcroît, Clearview a recueilli les images d'une manière déraisonnable, à travers la collecte de masse, non sélective, de sites Web accessibles au public.

Au cours de notre enquête, nous avons également relevé d'autres sujets de préoccupation sur lesquels nous ne nous sommes finalement pas prononcés, mais que nous avons jugé opportun de soulever dans notre rapport. Il s'agit notamment du fait que l'efficacité et la précision des technologies de reconnaissance faciale en général et la fiabilité des résultats des tests de Clearview en particulier, ont fait l'objet de contestations et de doutes crédibles.

Nous avons informé Clearview de nos conclusions et de nos recommandations préliminaires afin qu'elle se conforme à la législation applicable à la protection des renseignements personnels dans le secteur privé tant au niveau fédéral que provincial. Nous avons recommandé que Clearview : i) cesse d'offrir son dispositif de reconnaissance faciale aux clients au Canada; ii) mette fin à la collecte, à l'utilisation et à la communication d'images et de matrices faciales biométriques recueillies auprès d'individus au Canada; iii) supprime les images et les matrices faciales biométriques recueillies auprès d'individus au Canada qu'elle a en sa possession.

Clearview a formellement rejeté nos conclusions.

Clearview a déclaré que ses activités n'ont pas porté préjudice aux personnes. Selon nous, la position de Clearview ne tient pas compte de : i) la multitude de cas où des correspondances fausses ou mal appliquées pourraient nuire à la réputation des personnes; ii) plus fondamentalement, l'atteinte au droit à la vie privée des personnes et le préjudice général infligé à tous les membres de la société, qui se trouvent sous la surveillance de masse continue de Clearview en raison du ratissage aveugle et du traitement qu'elle fait de leurs images faciales.

En ce qui concerne les mesures correctives, Clearview a indiqué s'être retirée du marché canadien au cours de notre enquête et s'est dite « prête à envisager » de rester en dehors du marché canadien pendant deux années supplémentaires, en attendant que les commissariats fournissent des lignes directrices en la matière. Clearview a indiqué que nos commissariats devraient suspendre leur enquête et s'abstenir de publier un rapport final. « Pendant une telle suspension, [elle] serait disposée à prendre des mesures, au meilleur de ses capacités et sans préjudice, pour tenter de limiter la collecte et la communication des images qu'elle peut reconnaître comme étant canadiennes [...] » [nous soulignons]. Clearview ne s'est pas engagée à suivre nos recommandations. Les commissariats considèrent qu'il n'est pas approprié de suspendre l'enquête et souhaitent publier ce rapport. Nous avons donc considéré que l'affaire était **fondée** et nous réitérons nos recommandations de notre rapport préliminaire.

En outre, la CAI a déterminé que, contrairement aux exigences de la LCCJTI, Clearview n'avait pas informé la CAI qu'elle avait créé une base de données de caractéristiques biométriques, ni obtenu le consentement exprès des individus à ce que la vérification ou la confirmation de leur identité soit fait à l'aide d'un procédé de reconnaissance faciale.

Contexte

1. Le présent rapport d'enquête concerne la conformité de Clearview AI, Inc. (Clearview) à la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada (LPRPDE), à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP du Québec) et à la *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI) du Québec, ainsi qu'à la *Personal Information Protection Act* de la Colombie-Britannique (PIPA de la C.-B.) et à la *Personal Information Protection Act* de l'Alberta (PIPA de l'Alb.), collectivement appelées les « Lois ».
2. Clearview est une entreprise technologique dont le siège social se trouve aux États-Unis; elle a développé et livré son logiciel de reconnaissance faciale⁴ et sa solution de base de données combinée (l'application) à des clients dans le monde entier. L'application de Clearview permet aux clients de télécharger une image numérique du visage d'une personne et d'effectuer une recherche à partir de celle-ci. L'algorithme est ensuite appliqué à l'image numérique et le résultat est comparé à la base de données de Clearview afin de trouver et d'afficher les correspondances probables et les sources d'information qui y sont associées.
3. En janvier et en février 2020, les médias⁵ ont signalé que Clearview enrichissait sa base de données de reconnaissance faciale en recueillant des images numériques sur divers sites Web publics incluant, sans toutefois s'y limiter, Facebook, YouTube, Instagram, Twitter et Venmo, en contravention apparente des conditions d'utilisation établies par ces organisations et sans le consentement des individus. Par ailleurs, ces images numériques étaient ensuite stockées indéfiniment dans la base de données de Clearview pour l'approvisionnement et servir de résultats pour les recherches de reconnaissance faciale.
4. En février 2020, de nombreux⁶ médias ont confirmé qu'un certain nombre d'organismes d'application de la loi et d'organismes privés au Canada⁷ avaient eu recours aux services de Clearview pour identifier des individus.

⁴ La [reconnaissance faciale](#) désigne en général une catégorie de logiciels biométriques qui cartographie mathématiquement les traits du visage d'un individu et stocke les données sous forme de code numérique appelé empreinte faciale (*faceprint*).

⁵ K. Hill, « [The secretive company that might end privacy as we know it](#) », *The New York Times*, 18 janvier 2020; K. Fan, « [Clearview AI responds to cease-and-desist letters by claiming first amendment right to publicly available data](#) », *Harvard Journal of Law and Technology*, 25 février 2020.

⁶ « [Toronto Police admit using secretive facial recognition technology Clearview AI](#) », *CBC*, 13 février 2020; W. Gillis et K. Allen, « [Peel and Halton police reveal they too used controversial facial recognition tool](#) », *The Star*, 14 février 2020.

⁷ K. Allen *et al.*, « [Facial recognition app Clearview AI has been used far more widely in Canada than previously known](#) », *The Star*, 27 février 2020.

5. En février 2020, convaincus qu'il y avait des motifs raisonnables d'enquêter sur ces questions, le Commissariat à la protection de la vie privée du Canada (le CPVP), la Commission d'accès à l'information du Québec (la CAI), le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (le CIPVP de la C.-B.) et le Commissariat à l'information et à la protection de la vie privée de l'Alberta (le CIPVP de l'Alberta), collectivement appelés « les commissariats », ont ouvert des enquêtes en vertu du paragraphe 11(2) de la LPRPDE, de l'article 81 de la LPRPSP du Québec, de l'alinéa 36(1)a) de la PIPA de la C.-B. et de l'alinéa 36(1)a) de la PIPA de l'Alb., respectivement. Les commissariats ont décidé de mener une enquête conjointe afin de maximiser l'expertise et leurs ressources, tout en évitant un dédoublement de leurs efforts et de ceux de Clearview.

Enjeux

6. La présente enquête concerne les questions suivantes :
 - i. Clearview devait-elle, selon les Lois obtenir le consentement requis pour la collecte, l'utilisation et la communication de renseignements personnels et, le cas échéant, l'a-t-elle fait?
 - ii. Clearview a-t-elle recueilli, utilisé et communiqué des renseignements personnels à des fins qui sont raisonnables ou qu'une personne raisonnable estimerait acceptables dans les circonstances et en raison d'un intérêt légitime?⁸
7. La question suivante, propre au Québec, a également été examinée :
 - i. Clearview a-t-elle informé la CAI du Québec de la création d'une banque de mesures et de caractéristiques biométriques?
8. Au cours de l'enquête, plus particulièrement à la suite de la lettre d'intention à laquelle nous faisons référence au paragraphe 11, Clearview a également affirmé que les commissariats n'étaient pas compétents pour s'intéresser aux activités de Clearview en question. Nous abordons cet enjeu dans notre analyse, avant d'aborder les enjeux identifiés ci-haut.

Méthodologie

9. En plus d'un important travail de recherche de renseignements à partir de sources ouvertes, l'équipe d'enquêteurs (l'équipe) a analysé les représentations transmises par Clearview et les documents en lien avec ses activités. L'équipe a également examiné les représentations formulées par un certain nombre de tierces parties désignées comme utilisateurs possibles du service de Clearview.

⁸ Dans le présent rapport, l'expression « fins acceptables » englobe les « fins raisonnables » au sens de la PIPA de l'Alb. et de la PIPA de la C.-B., et l'« intérêt légitime » au sens de la LPRPSP.

10. Entre février et novembre 2020, Clearview a fourni plusieurs séries de représentations écrites aux commissariats. Par ailleurs, nous avons offert à Clearview plusieurs occasions de nous rencontrer pour poser des questions et fournir d'autres éléments probants. Nous avons organisé deux rencontres de ce genre en juin 2020.
11. À l'issue de la phase de collecte des preuves de l'enquête conjointe, nous avons adressé une « lettre d'intention » à Clearview le 29 octobre 2020, dans laquelle nous avons exposé et expliqué les raisons de nos conclusions préliminaires, formulé plusieurs recommandations ou ordonnances envisagées et invité Clearview à nous répondre. Nous avons ensuite rencontré Clearview le 17 novembre pour clarifier notre point de vue, donner l'occasion de poser des questions et discuter des solutions possibles pour remédier à la situation. Le 20 novembre, Clearview a fourni une réponse écrite dans laquelle elle exprimait son désaccord avec nos conclusions préliminaires et les ordonnances et recommandations envisagées, et remettait en question la compétence des commissariats. Dans cette lettre, Clearview a présenté un éventail de nouveaux arguments et a fourni de nouvelles informations que les commissariats ont examinées et évaluées avant de produire le présent rapport de conclusions.

Représentations de Clearview et notre enquête

12. Cette section porte sur les représentations initiales fournies par Clearview jusqu'à l'émission de notre lettre d'intention. D'autres représentations fournies par Clearview dans sa réponse à notre lettre d'intention sont incluses dans notre analyse de chaque enjeu.

Aperçu de la mise en œuvre de la reconnaissance faciale par Clearview

13. Dans ses représentations, Clearview a expliqué que sa technologie de reconnaissance faciale repose sur cinq composantes principales : i) « Image Crawler » (indexeur d'images); ii) « Image Store » (catalogue d'images); iii) « Metadata Store » (catalogue de métadonnées); iv) « Neural Network » (réseau neuronal); et v) « Vector Database » (base de données vectorielle). L'indexeur d'images est essentiellement un outil automatisé qui fouille dans les pages Web « publiques » et recueille les images qu'il considère comme contenant des visages, ainsi que les métadonnées connexes comme le titre, le lien vers la source et la description; ce processus est couramment appelé « ratissage ». Les images et les métadonnées obtenues au moyen de ce ratissage sont stockées indéfiniment sur les serveurs de Clearview, dans les catalogues d'images et de métadonnées, respectivement. Le réseau neuronal est à la base de l'algorithme qui analyse les images numériques de visages pour en faire des représentations numériques appelées « vecteurs ». Les vecteurs de Clearview comprennent 512 points de données représentant les diverses lignes uniques qui composent un visage. Clearview stocke ensuite l'ensemble de ces vecteurs dans sa base de données vectorielle, où ils sont associés aux images stockées sur son serveur. Un vecteur est associé à chaque image de la base de données afin de permettre l'identification et la mise en correspondance.

14. Lorsqu'un utilisateur de l'application souhaite identifier une personne, il doit télécharger une image de la personne visée dans l'application et lancer une recherche. Le réseau neuronal analyse ensuite l'image et produit un vecteur. Ce vecteur est ensuite comparé à tous les vecteurs stockés dans la base de données de Clearview et l'application extrait les images correspondantes de la base de données vectorielle et les fournit à l'utilisateur, accompagnées des métadonnées connexes, sous forme de résultats de recherche. Clearview a affirmé que les images téléchargées par les utilisateurs sont stockées séparément des images obtenues au moyen du ratissage et qu'elles ne figurent pas dans les résultats de recherche.
15. Clearview a fait savoir que ses résultats de recherche se présentent sous forme de liste d'images miniatures semblant correspondre à la personne; ces images sont accompagnées du nom de l'image, d'une description et d'un lien vers la source. Pour obtenir davantage de renseignements, l'utilisateur doit ensuite cliquer sur le lien menant à la source afin d'accéder à la page Web où l'image a été recueillie initialement. Clearview a déclaré qu'elle [traduction] « ne possède ni ne conserve aucune information liée aux noms, aux adresses, à la nationalité, à la date de naissance [ou] à l'emplacement » en lien avec les images de sa base de données.

Pratiques de confidentialité de Clearview en matière de consentement

16. Au départ, Clearview a indiqué qu'elle ne cherche pas à obtenir le consentement des personnes au sujet desquelles elle recueille des renseignements. Clearview a plutôt fait valoir que les images qu'elle recueille sont, selon elle, du domaine public et qu'il n'est par conséquent pas requis que les personnes sachent que l'on recueille leur information ni qu'elles y consentent.
17. À l'appui de sa position, Clearview a affirmé qu'elle ne recueillait des images que sur des pages Web accessibles au public et qu'elle ne recueillait aucune image protégée par des paramètres de confidentialité, comme celles associées à certains comptes de médias sociaux, et ne récupérait pas non plus d'images sur des pages où des fichiers robots (« robots.txt ») étaient activés⁹. Clearview a confirmé que son indexeur d'images est configuré pour respecter les consignes incluses dans le fichier robots.txt.

Objectifs de Clearview

18. Dans ses premières représentations, Clearview avait indiqué aux commissariats que son application était réservée à l'usage exclusif des forces de l'ordre. Les conditions d'utilisation de Clearview indiquaient d'ailleurs clairement que : [traduction] « [I]es utilisateurs peuvent recourir au service pour répondre à des besoins légitimes d'application de la loi et d'enquête » et que [traduction] « il est interdit aux utilisateurs de recourir au service pour toute autre raison que pour répondre à des besoins d'application

⁹ Un fichier robots.txt peut être configuré par les administrateurs d'une page Web afin d'indiquer aux robots Web (collecteurs) les pages ou le contenu auquel ils peuvent accéder ou non. Nous notons que le respect des consignes indiquées dans un fichier robots.txt est facultatif et que les robots collecteurs peuvent ne pas en tenir compte.

de la loi et d'enquête ». En réponse à notre lettre d'intention, Clearview a fait savoir que les termes de ses conditions d'utilisation permettaient aux sociétés de sécurité d'accéder à ses services auparavant.

19. Clearview a soutenu que sa technologie présentait [traduction] « des avantages considérables et concrets en matière de sécurité publique en améliorant sensiblement la capacité des forces de l'ordre à identifier les suspects, les victimes et les témoins, et à enquêter sur ces personnes ». Clearview a fait état de multiples succès dans des dossiers allant [traduction] « du meurtre, du vol à main armée et de l'exploitation sexuelle des enfants au terrorisme, au grand trafic de stupéfiants et aux fraudes de plusieurs millions de dollars ».
20. Lorsqu'on l'a questionnée sur le préjudice que sa technologie pourrait éventuellement porter aux Canadiens, Clearview a déclaré qu'un tel préjudice était tout à fait hypothétique. Clearview a affirmé que tout [traduction] « préjudice qu'une personne subirait à la suite d'une recherche de son image dans la base de données de Clearview est comparable au préjudice subi par cette personne lorsque quelqu'un recherche son nom sur Google ». Clearview a ajouté qu'absolument aucun utilisateur ne pouvait parcourir sa base de données au complet puisque les résultats n'étaient fournis que pour les correspondances, atténuant ainsi les risques éventuels.
21. Elle a déclaré que même en cas de compromission et de diffusion de sa base de données, les images qu'elle contient sont déjà toutes accessibles en ligne et ne constituent donc pas des renseignements sensibles; quant aux vecteurs utilisés pour la mise en correspondance biométrique, ils sont hachés¹⁰ et ne peuvent donc servir en dehors de l'application Clearview.
22. Même si Clearview permettait au départ à divers organismes publics et privés de créer des comptes, nous constatons qu'en réaction à notre enquête, Clearview a déclaré avoir suspendu l'accès pour tous les utilisateurs au Canada, sauf pour la GRC, en mars 2020. À la suite d'autres échanges avec les commissariats en cours d'enquête, Clearview a abandonné volontairement le marché canadien en juillet 2020.

Comparaison avec d'autres organismes

23. Clearview a affirmé que son application est essentiellement un moteur de recherches d'images et a demandé aux commissariats pourquoi elle était « traitée différemment des autres moteurs de recherche ».
24. Cette enquête porte sur les pratiques de Clearview et non sur celles des moteurs de recherche cités par Clearview. Les commissariats lancent et mènent des enquêtes sur les organismes sur la base des faits propres à chaque cas. À ce titre, nous n'émettons pas d'avis sur les obligations de tout autre organisme dans le présent rapport.

¹⁰ Le hachage est une technique cryptographique qui consiste à utiliser une fonction à sens unique pour transformer des données en un code unique. Le hachage protège contre la rétroingénierie (ou d'autres moyens de récupérer les données d'origine), que celle-ci soit le fait de l'organisme qui recueille et détient l'information ou de tiers.

Analyse

Contestation de la juridiction par Clearview

25. Aux derniers stades de notre enquête, après avoir reçu la lettre d'intention des commissariats demandant une réponse aux conclusions préliminaires dans cette affaire, Clearview a fait valoir qu'aucun des commissariats n'avait compétence sur ses activités, affirmant que [traduction] « Clearview n'exerce aucune activité au Canada » et que [traduction] « Clearview est d'avis dans les circonstances qu'aucune des lois invoquées ne s'applique et qu'aucun facteur connexe ne crée un lien réel et substantiel avec le Canada ». Clearview a fait valoir que la LRPDE ne s'applique pas [traduction] « parce qu'il n'y a pas de lien réel et substantiel avec le Canada ».
26. Plus précisément, Clearview a fait valoir que les circonstances en l'espèce étaient telles qu'il n'existait aucun lien réel et substantiel avec le Canada et que :
 - i. le contenu mentionné dans la plateforme de Clearview n'était pas [traduction] « uniquement canadien » et qu'il a du contenu provenant de [traduction] « plusieurs autres pays dans le monde »;
 - ii. les services de Clearview n'étaient [traduction] « pas directement et uniquement destinés aux Canadiens » et [traduction] « peu de Canadiens auraient utilisé ses services ». Clearview a affirmé que [traduction] « au-delà des utilisateurs ayant fait un essai, la seule allégation est qu'une entité canadienne, la GRC, aurait utilisé les services de Clearview »; et
 - iii. [traduction] « il semble n'y avoir aucune preuve que les services de Clearview concernent principalement les Canadiens ».
27. Clearview a ajouté qu'elle n'est soumise à aucune loi provinciale sur la protection de la vie privée, puisque selon elle :
 - i. elle n'a pas recueilli, utilisé ou communiqué de renseignements personnels [traduction] « dans les provinces de l'Alberta, du Québec ou de la Colombie-Britannique, mais plutôt aux États-Unis »;
 - ii. il n'y avait [traduction] « aucune preuve ou allégation » que Clearview menait ses activités dans ces provinces;
 - iii. la collecte, l'utilisation ou la communication devaient avoir lieu entièrement dans chaque province pour que ces lois soient applicables, et il n'y a [traduction] « aucune preuve ou allégation » que cela ait eu lieu.

Compétence du CPVP

28. Le CPVP note que la LPRPDE s'applique aux organismes situés à l'extérieur du Canada lorsqu'il existe des « liens réels et substantiels » avec le Canada¹¹. À notre avis, les circonstances de cette affaire démontrent clairement qu'il existe des liens réels et substantiels avec le Canada. Pour parvenir à cette conclusion, nous avons examiné les facteurs de rattachement pertinents qui découlent de la jurisprudence, notamment les facteurs énoncés dans la décision *A.T. c. Globe24h* : 1) l'emplacement du public cible du site Web, 2) la source du contenu du site Web, 3) l'emplacement de l'opérateur du site Web et 4) l'emplacement du serveur hôte¹².
29. En ce qui concerne l'emplacement du public cible de Clearview :
- i. Clearview affirme que son activité au Canada était limitée, mais cela ne cadre pas avec le fait qu'elle a activement commercialisé ses services auprès d'organismes canadiens en participant à des conférences du secteur, en produisant du matériel promotionnel, en recueillant des témoignages de professionnels canadiens de l'application de la loi, ainsi qu'en proposant des présentations et des essais ciblant des agences précises. En outre, Clearview a déclaré publiquement, dans des déclarations aux médias¹³ et dans son propre matériel promotionnel¹⁴, que le Canada faisait partie de son marché principal.
 - ii. Le fait qu'une seule agence soit devenue un client payant est, à notre avis, sans importance. Clearview menait bel et bien des activités de nature commerciale, en offrant des périodes d'essai dans le but explicite d'inciter à l'achat de comptes. Les représentations de Clearview ont confirmé que 48 comptes (d'essai ou autres) ont été créés pour des organismes chargés de l'application de la loi à l'échelle du Canada, et que des milliers de recherches ont été effectuées par le biais de ces comptes. En particulier, nous notons que divers organismes provinciaux chargés de l'application de la loi ont utilisé des comptes d'essai de l'application pendant plusieurs mois produisant pour chacun des comptes des dizaines et des centaines, voire des milliers de recherches dans un cas. De plus, en présentant simplement la GRC comme [traduction] « seule entité canadienne », Clearview ne tient pas compte du fait que la GRC est l'organisme national chargé de l'application de la loi du Canada, opérant dans tout le pays et détenant des mandats de police nationaux, fédéraux, provinciaux et municipaux.

¹¹ *Lawson c. Accusearch Inc.*, 2007 CF 125, para. 38 à 51; *A.T. c. Globe24h.com*, 2017 CF 114 (CanLII), [2017] 4 RCF 310, para.graphes 50 à 64, citant l'arrêt *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 RCS 427, aux paragraphes 54 à 63.

¹² *A.T. c. Globe24h.com*, 2017 CF 114 (CanLII), [2017] 4 RCF 310.

¹³ R. Mac *et al.*, « [Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA](#) », *Buzzfeed News*, 27 février 2020.

¹⁴ [Site Web archivé Clearview.ai](#).

30. En ce qui concerne la source du contenu de Clearview :

- i. Il n'est pas nécessaire que le contenu de Clearview provienne exclusivement de sources canadiennes pour qu'il y ait des liens réels et substantiels avec le Canada.
- ii. Tel qu'il est indiqué dans la décision *Lawson c. Accusearch Inc.*, il n'est pas nécessaire de désigner des sources de contenu canadiennes précises pour établir que nous avons compétence.
- iii. L'affirmation de Clearview selon laquelle elle recueille des images sans tenir compte de la géographie ou de la source n'exclut pas que nous ayons compétence lorsqu'une partie importante de son contenu provient du Canada. Bien qu'on ne connaisse pas le nombre exact d'images provenant de personnes vivant au Canada puisque Clearview ne conserve pas la source nationale, la nature aveugle du ratissage effectué par Clearview assure de manière quasi certaine que des millions d'images de personnes vivant au Canada¹⁵ ont été recueillies et utilisées pour établir des vecteurs d'images biométriques à inclure dans sa base de données, notamment pour les commercialiser auprès d'organismes canadiens chargés de l'application de la loi.

31. Enfin, en ce qui concerne l'emplacement des activités du site Web de Clearview et du serveur hôte :

- i. Nous notons que Clearview mène ses activités exclusivement par le biais d'un site Web ou d'une application. Tel qu'il est indiqué au paragraphe 54 de la décision *A.T. c. Globe24h.com*, une présence physique au Canada n'est pas nécessaire pour établir un lien réel et substantiel lorsqu'il s'agit de sites Web sous le régime de la LPRPDE, car les télécommunications se font [traduction] « à la fois ici et à l'autre endroit ».
- ii. Les activités de Clearview nécessitent la transmission et la réception de renseignements personnels entre le Canada et les États-Unis, tant lors de la collecte d'information que de leur communication par le biais de ses logiciels.
- iii. Selon la Cour suprême du Canada¹⁶ : « Le lieu de réception peut constituer un facteur de rattachement tout aussi "important" que le lieu d'origine (sans compter l'emplacement physique du serveur hôte, qui peut se trouver dans un pays tiers). »

¹⁵ Facebook a récemment publié des données montrant qu'il y a 23 millions de comptes canadiens actifs sur Facebook et 8,5 millions de comptes sur Instagram (un service axé sur l'image). Les Canadiens ont partagé 1 429 milliards de photos et 79 millions de vidéos sur Instagram et partagent en moyenne 2 millions de photos par jour. Shankar, B. « [Facebook has 23 million monthly users in Canada](#) », *MobileSyrup*, 21 juin 2017 [en anglais].

¹⁶ *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 RCS 427, par. 59.

Compétence provinciale

32. Nous rejetons en outre l'affirmation de Clearview selon laquelle elle n'est pas assujettie à la PIPA de l'Alb., à la PIPA de la C.-B. ou à la LPRPSP du Québec (les lois provinciales), respectivement, et nous estimons que les activités de Clearview relèvent de la compétence du CPVP et des provinces¹⁷.
33. La législation provinciale sur la protection de la vie privée s'applique à tout organisme du secteur privé qui recueille, utilise et communique des renseignements sur des personnes dans la province concernée. Le ratissage aveugle auquel a procédé Clearview a sans nul doute permis de recueillir les renseignements personnels de personnes vivant au Québec, en Alberta et en Colombie-Britannique, dont les résidents représentent ensemble près de la moitié de la population canadienne. En outre, les organismes chargés de l'application de la loi situés dans les provinces et soumis à la supervision provinciale ont été ciblés et ont utilisé des comptes d'essai du logiciel Clearview avec lesquels ils ont fourni, et Clearview a recueilli, des informations personnelles sous la forme de photographies d'individus¹⁸.
34. Clearview est une entreprise commerciale qui a recueilli, utilisé et communiqué des renseignements personnels sur des personnes vivant au Québec, en Alberta et en Colombie-Britannique dans le but de vendre un produit aux organismes chargés de l'application de la loi dans ces provinces. Ce n'est pas parce qu'une entreprise n'est pas située au Québec, en Alberta ou en Colombie-Britannique qu'elle peut se soustraire aux obligations découlant de la LPRPSP du Québec, de la PIPA de l'Alb. et de la PIPA de la C.-B. En effet, à partir du moment où une entreprise collecte les renseignements personnels dans une de ces provinces ou y exerce des activités, la législation provinciale s'applique¹⁹.
35. Compte tenu de ce qui précède, les commissariats n'acceptent pas l'affirmation de Clearview selon laquelle les lois provinciales ne s'appliquent pas et sont d'avis que :
 - i. les législations provinciales précitées s'appliquent, tel qu'il a été indiqué précédemment;

¹⁷ [Bell Mobilité](#), CAI 1005977-S, décision de D. Poitras, 5 février 2020.

¹⁸ A. Smith, « [After officers tested Clearview AI, Calgary police improving tracking system for new technologies](#) », *Calgary Herald*, 11 mars 2020 [en anglais]; B. Carney, « [Despite Denials, RCMP Used Facial Recognition Program for 18 Years](#) », *The Tyee*, 10 mars 2020 [en anglais]; « [Une application utilisée par la police peut identifier les gens à partir d'une seule photo](#) », *Radio-Canada*, 20 janvier 2020; T. Péloquin, « [Reconnaissance faciale: le SPVM refuse de dire s'il utilise un logiciel controversé](#) », *La Presse*, 18 février 2020; J. Bronskill, « [RCMP facing proposed class action over use of Clearview AI's facial-recognition technology](#) », *The Globe and Mail*, 13 juillet 2020 [en anglais]; documents soumis par Clearview.

¹⁹ *Firquet c. Acti-Com*, 2018 QCCAI 245 (CanLII); *Serres Floraplus inc. c. Norséco inc.*, 2008 QCCS 1455 (CanLII); D. Douville, « [La Loi sur la protection des renseignements personnels dans le secteur privé : quand s'applique-t-elle aux entreprises situées à l'extérieur du Québec?](#) », *Bulletin Fasken*, 16 mai 2019; Micheal Geist, « [Is there a there there? Toward greater certainty for internet jurisdiction](#) », *Berkeley Technology Law Journal*, vol. 16, n° 3 (2001), p. 1345 [en anglais].

- ii. les lois provinciales n'empêchent pas la réalisation de l'objectif de la LPRPDE, ni n'entraînent de conflit opérationnel ou de conflit d'intention;
- iii. Chaque loi provinciale a été jugée essentiellement similaire à la LPRPDE²⁰.

Enjeu 1 : Clearview a-t-elle obtenu le consentement requis?

- 36. À notre avis, Clearview n'a pas obtenu le consentement requis pour la collecte, l'utilisation et la communication de renseignements personnels par l'intermédiaire de l'application. Pour en arriver à cette conclusion, nous notons que Clearview n'a fait aucune tentative pour obtenir le consentement des personnes, étant donné son interprétation erronée de la législation canadienne sur la protection des renseignements personnels, qui détermine la notion de renseignements « auxquels le public a accès » ou ayant « un caractère public en vertu de la loi ».
- 37. Les Lois stipulent que le consentement de la personne est requis pour la collecte, l'utilisation ou la communication de renseignements personnels à moins qu'une exception ne s'applique²¹. Le type de consentement requis variera en fonction des circonstances et du type de renseignement concerné.
- 38. Les *Lignes directrices pour l'obtention d'un consentement valable*²² (les « Lignes directrices ») publiées conjointement par le CPVP, le CIPVP de l'Alb. et le CIPVP de la C.-B. prévoient qu'« en règle générale, les organisations doivent obtenir un consentement *explicite* de l'intéressé dans les cas suivants : i) les renseignements recueillis, utilisés ou communiqués sont sensibles; ii) la collecte, l'utilisation ou la communication de l'information ne répond pas aux attentes raisonnables de l'intéressé; iii) la collecte, l'utilisation ou la communication de l'information crée un risque résiduel important de préjudice grave. »
- 39. Au-delà de la collecte d'images par Clearview, nous notons également que sa création d'informations biométriques sous forme de vecteurs constituait une collecte et une utilisation distinctes et supplémentaires d'informations personnelles, tel que l'ont conclu le CPVP, le CIPVP de l'Alb. et le CIPVP de la C.-B. dans l'affaire de la Corporation Cadillac Fairview limitée²³.

²⁰ [Décret d'exclusion visant des organisations de la province de Québec](#) (DORS/2003-374), [Décret d'exclusion visant des organisations de la province d'Alberta](#) (DORS/2004/219) et [Décret d'exclusion visant des organisations de la province de la Colombie-Britannique](#) (DORS 2004/220).

²¹ Paragraphe 5(1) et articles 6.1 et 7 de la [LPRPDE](#), principe 4.3 de l'annexe 1, article 7 de la [PIPA de l'Alb.](#), articles 6 à 8 de la [PIPA de la C.-B.](#), articles 6 et 12 à 14 de la [LPRPSP du Québec](#), et article 44 de la [LCCJTI](#).

²² [Lignes directrices pour l'obtention d'un consentement valable](#), CPVP, 2018.

²³ [Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, le commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique](#), CPVP, CIPVP de l'Alb. et CIPVP de la C.-B., paragraphe 68.

40. En ce qui concerne les caractéristiques et mesures biométriques, la LCCJTI du Québec exige clairement le consentement exprès de la personne concernée. Un consentement est exprès lorsqu'il est explicite et sans équivoque : pour le donner, la personne concernée pose un geste manifestant clairement son accord²⁴. Pour pouvoir poser un tel geste, la personne doit être informée des tenants et des aboutissants de son consentement²⁵. Son consentement doit, en effet, être libre, éclairé, spécifique et limité dans le temps²⁶.
41. À notre avis, les renseignements biométriques sont sensibles dans presque toutes les circonstances. Ils sont intrinsèquement liés à la personne, et dans la plupart des cas de manière permanente. Ils sont distinctifs, peu susceptibles de varier dans le temps, difficiles à modifier et en grande partie uniques à la personne. Cela dit, dans la catégorie des renseignements biométriques, il existe des degrés de sensibilité. Nous estimons que les renseignements biométriques faciaux sont particulièrement sensibles puisque la possession d'un modèle de reconnaissance faciale peut permettre d'identifier une personne par comparaison avec un vaste éventail d'images facilement disponibles sur Internet, comme le montre l'affaire en question, ou par surveillance clandestine.
42. Pour ces raisons, nous estimons que faute d'exception applicable, Clearview aurait dû obtenir un consentement explicite (positif) avant de recueillir les images de toute personne au Canada.
43. Dans ses représentations, Clearview a reconnu qu'elle ne cherchait pas à obtenir le consentement des personnes au sujet desquelles elle a recueilli, utilisé ou communiqué ces renseignements. Clearview a fait valoir que ces renseignements étaient des renseignements « accessibles au public » (« publicly available ») et qu'il n'existait pas d'attente raisonnable en matière de respect de la vie privée.
44. Les commissariats soulignent que la LPRPDE, la PIPA de la C.-B. et la PIPA de l'Alb. prévoient des exceptions à l'obligation d'obtenir le consentement lorsque les renseignements personnels en question sont des renseignements auxquels le public a accès au sens de l'alinéa 7(1)d) de la LPRPDE, des alinéas 12(1)e), 15(1)e) et 18(1)e) de la PIPA de la C.-B., et des alinéas 14e), 17e) et 20j) de la PIPA de l'Alb. La définition de renseignements « auxquels le public a accès » est établie par les règlements d'application de chaque loi²⁷ et se distingue d'une interprétation commune de la notion de renseignements « accessibles au public » (« publicly accessible »).

²⁴ [Biométrie : principes à respecter et obligations légales des organisations - Guide d'accompagnement pour les organismes publics et les entreprises](#), CAI, juillet 2020.

²⁵ [LPRPSP du Québec](#), article 8.

²⁶ [LPRPSP du Québec](#), article 14.

²⁷ Article 1 du règlement du [Règlement précisant les renseignements auxquels le public a accès](#); article 6 du [Règlement d'application de la PIPA de la C.-B.](#), Prescribed source of public information, et article 7 du [Règlement d'application de la PIPA de l'Alb.](#), Publicly available information.

45. Les renseignements provenant de sources telles que les médias sociaux ou les profils professionnels, recueillis sur des sites Web publics puis utilisés à des fins non connexes, ne relèvent pas de l'exception prévue par la LPRPDE concernant les renseignements « auxquels le public a accès »²⁸. De même, les règlements d'application respectifs de la PIPA de l'Alb. et de la PIPA de la C.-B.²⁹ désignent des sources de renseignements publics qui comprennent des annuaires, des registres et des publications. Les sites Web de médias sociaux et les moteurs de recherche ne sont pas répertoriés comme des sources désignées de renseignements accessibles au public en application de ces deux lois. Ainsi, la collecte de renseignements auprès de ces sources ne serait autorisée qu'avec le consentement des intéressés et uniquement si les fins sont celles qu'une personne raisonnable jugerait appropriées³⁰.
46. La LPRPSP du Québec et la LCCJTI n'établissent pas de distinction et ne tiennent pas compte de la notion de « renseignements auxquels le public a accès ». Par contre, la LPRPSP du Québec ne s'applique pas aux renseignements qui ont un « caractère public en vertu de la loi ». Or, aucune loi au Québec ne confère un caractère public aux renseignements personnels du seul fait qu'ils sont diffusés sur les réseaux sociaux ou le Web. De plus, la CAI du Québec a déjà statué que même si un renseignement personnel est diffusé sur un site public, cela ne veut pas dire que ce renseignement peut être utilisé à d'autres fins sans le consentement de la personne concernée³¹. La publication d'images sur un site Web ne signifie pas forcément que son auteur consent à ce qu'elles soient utilisées par un tiers.
47. Par conséquent, les commissariats ne considèrent pas les renseignements personnels recueillis, utilisés ou communiqués par Clearview comme étant des renseignements « auxquels le public a accès », comme le prévoient les Lois, ou des renseignements qui ont un « caractère public en vertu de la loi »; ainsi, l'exception ne s'applique pas.
48. Étant donné qu'aucune tentative n'a été faite pour obtenir le consentement des personnes concernées et qu'aucune exception à l'obligation d'obtenir le consentement n'est jugée applicable, nous estimons que Clearview a enfreint l'article 6.1 et le principe 4.3 de l'annexe 1 de la LPRPDE, l'article 7 de la PIPA de l'Alb., les articles 6 à 8 de la PIPA de la C.-B., les articles 6 et 12 à 14 de la LPRPSP du Québec et l'article 44 de la LCCJTI.

²⁸ [La réutilisation de profils d'utilisateurs Facebook canadiens effectuées par une entreprise contrevient à la loi en matière de protection de la vie privée](#), CPVP, paras 112-113.

²⁹ Article 6 du [Règlement d'application de la PIPA de la C.-B.](#), Prescribed source of public information, et article 7 du [Règlement d'application de la PIPA de l'Alb.](#), Publicly available information.

³⁰ [Always, sometimes, or never? Personal information & tenant screening](#), OIPC BC, 2018.

³¹ [Confédération des syndicats nationaux](#), CAI 1009621-S et 1009629-S, décision de C. Chassigneux, 12 novembre 2019. Voir également, LPRPSP, section 13.

Réponse de Clearview concernant le consentement

49. Dans sa réponse, Clearview a déclaré ce qui suit :

[traduction] « *Concernant l'obligation d'obtenir un consentement découlant des lois fédérales et provinciales, et supposant, sans renoncer à l'invalidité des lois invoquées ci-dessus, que de telles lois s'appliquent, Clearview soutient que l'exception relative aux publications auxquelles le public a accès s'applique. Les renseignements recueillis par Clearview ne sont rien de plus que des renseignements auxquels le public a accès.* »

50. Clearview a fait valoir que sa collecte de renseignements relevait de l'exception prévue par le règlement en ce qui concerne « *les renseignements personnels qui figurent dans une publication, y compris les magazines, livres et journaux, sous forme imprimée ou électronique, qui est accessible au public, si l'intéressé a fourni les renseignements*³² ». En ce qui concerne la législation du Québec, qui ne contient pas de telles exceptions, Clearview a affirmé qu'il faut forcément considérer que l'exception est implicite. Elle a fait valoir qu'autrement, [traduction] « *la législation n'est pas valide parce qu'elle viole les garanties de liberté d'expression des chartes québécoise et canadienne* ».

51. Clearview a en outre fait valoir que la définition réglementaire des renseignements auxquels le public a accès [traduction] « *n'est pas distincte de la compréhension commune des mots* » et que si le Parlement [traduction] « *a bien défini certaines catégories d'éléments pouvant être inclus dans ce qui est déclaré comme étant public, il n'a pas restreint la définition en ce qui concerne la publication* ». Elle a déclaré ce qui suit :

[traduction] « *Dans la soumission de Clearview, la définition [d'une publication] pourrait difficilement être plus large. C'est pourquoi des renseignements personnels figurant dans des blogues publics, des médias sociaux publics ou tout autre site Web public font partie de l'exception concernant les renseignements "auxquels le public a accès" puisqu'ils font partie de la définition d'une publication. Par conséquent, la collecte de tels renseignements ne nécessite pas de consentement.* »

52. À l'appui de sa position, Clearview a renvoyé à l'arrêt *Lukács c. Canada*³³ de la Cour d'appel fédérale, affirmant que « [c]ette décision laisse manifestement entendre que ces termes ne sont pas précis et qu'ils englobent toute publication "mise à la disponibilité de l'ensemble des citoyens ou à laquelle ils ont accès". »

53. Clearview a ajouté que l'attente en matière de protection des renseignements dans l'opinion publique [traduction] « *est ou devrait être réduite* » et qu'il faudrait privilégier une interprétation large des renseignements accessibles au public. Voici ce qu'elle a déclaré :

³² Alinéa 1e) du [Règlement précisant les renseignements auxquels le public a accès](#); article 6 du [Règlement d'application de la PIPA de la C.-B.](#), Prescribed source of public information, et article 7 du [Règlement d'application de la PIPA de l'Alb.](#), Publicly available information.

³³ [Lukács c. Canada](#) (Transport, Infrastructure et Collectivités), 2015 CAF 140 (CanLII), para. 69.

[traduction] « *Même si la loi et ses exceptions sont ambiguës et nécessitent une interprétation, elles doivent être interprétées conformément à la Charte canadienne. Restreindre la libre circulation des renseignements accessibles au public contrevient à la protection constitutionnelle de la liberté d'expression. Par conséquent, les exceptions à ce principe doivent être interprétées de manière étroite et une interprétation large des renseignements auxquels le public a accès doit être priorisée pour ne pas limiter indûment la liberté d'expression.* »

54. Enfin, Clearview a fait valoir le point suivant :

[traduction] « *Étant donné ces circonstances, [...] les effets positifs liés à la protection des renseignements personnels ne l'emportent pas sur les effets négatifs sur la liberté d'expression de Clearview. Il n'y a pas de préoccupation urgente et substantielle qui justifie une entrave à la liberté d'expression étant donné l'absence d'attentes raisonnables relatives à la confidentialité des images que des personnes ont versées elles-mêmes au domaine public ou permis qu'elles le soient.* »

55. Sur la base de ces arguments, Clearview a affirmé qu'elle n'avait enfreint aucune des Lois, car tous les renseignements recueillis et utilisés étaient exemptés en tant que renseignements accessibles au public.
56. Comme nous le notons au paragraphe 36, Clearview n'a fait aucune tentative pour obtenir le consentement des personnes. Au lieu de cela, Clearview s'appuie entièrement sur son argument selon lequel les renseignements personnels recueillis, utilisés et communiqués étaient accessibles au public et donc exemptés des exigences de consentement. Lors de l'examen des représentations de Clearview, les commissariats ont conclu que cet argument est erroné et que l'exemption ne s'applique pas dans les circonstances de cette affaire.
57. Tel qu'il est indiqué dans la LPRPDE et confirmé dans la décision *Turner c. Telus Communications Inc.*³⁴, les renseignements ne seront considérés comme « accessibles au public » que s'il s'agit de renseignements réglementaires **et** que le public y a accès.
58. Clearview a en outre fait valoir qu'il convenait d'adopter une interprétation [traduction] « en langage clair » des règlements et qu'il fallait par conséquent appliquer une définition large du terme « publication » pour déterminer si l'exemption s'appliquait. Clearview a également ajouté que cette interprétation large serait conforme à la *Charte canadienne des droits et libertés*, c'est-à-dire qu'elle respecterait la liberté d'expression.
59. Nous concluons que ce n'est pas le cas, sur la base des faits, du droit ou de la jurisprudence disponible, tel qu'il est indiqué ci-dessous.

³⁴ [Turner v. Telus Communications Inc.](#), 2005 CF 1601, para. 50 et 54.

60. Nous sommes d'avis que l'arrêt *Lukács c. Canada* ne s'applique pas à la présente affaire puisque celle-ci concerne l'application de la *Loi sur la protection des renseignements personnels*, qui est distincte de la LPRPDE. Plus précisément, nous notons qu'à la différence de la *Loi sur la protection des renseignements personnels*, la signification de « renseignements auxquels le public a accès » et de ce qui est considéré comme une « publication » est précisément défini dans la LPRPDE, la PIPA de l'Alb.³⁵ et la PIPA de la C.-B.³⁶ par règlement (les « règlements »). Les règlements l'emportent donc.
61. Lorsque nous interprétons les règlements, nous constatons que comme les Lois sont considérées par les tribunaux comme des textes quasi constitutionnels³⁷, les droits conférés par les Lois devraient être interprétés de manière large, ciblée et libérale, et les restrictions visant ces droits devraient être interprétées de manière étroite³⁸.
62. Les règlements créent une exception à un principe fondamental de la protection de la vie privée — l'obligation de recueillir, d'utiliser et de communiquer des renseignements personnels avec le consentement de l'intéressé — et doivent donc être interprétés de manière restrictive. Dans cette optique, nous n'acceptons pas les arguments de Clearview en faveur d'une interprétation plus large du « langage clair ».
63. Par exemple, les médias sociaux, à partir desquels Clearview a obtenu une partie importante des images de sa base de données, ne sont pas désignés comme une « publication » dans le texte du règlement de la LPRPDE. Le CPVP est d'avis que les pages Web de médias sociaux diffèrent considérablement des sources désignées dans le règlement de la LPRPDE. Comme le CPVP l'a déjà constaté dans l'affaire *Profile Technologies*³⁹, il existe un certain nombre de différences essentielles entre les sources d'information en ligne telles que les médias sociaux, et les exemples de « publications » figurant au point 1e) :
- i. Les pages Web des médias sociaux contiennent un contenu dynamique, les nouveaux renseignements étant ajoutés, modifiés ou supprimés en temps réel.

³⁵ Article 7 du [Règlement d'application de la PIPA de l'Alb.](#)

³⁶ Article 6 du [Règlement d'application de la PIPA de la C.-B.](#)

³⁷ Par exemple dans : [Nammo c. Transunion of Canada Inc.](#), 2010 CF 1284, para. 74 et 75; [Bertucci c. Banque Royale du Canada](#), 2016 CF 332, para. 34; [Alberta \(Information and Privacy Commissioner\) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401](#), 2013 CSC 62, para. 19 et 22; [Cash Converters Canada Inc. v. Oshawa \(City\)](#), 2007 ONCA 502 (CanLII), para. 29, citant [Lavigne c. Canada \(Commissariat aux langues officielles\)](#), 2002 CSC 53 (CanLII), [2002] 2 RCS 773 et [Daqq c. Canada \(Ministre des Finances\)](#), 1997 CanLII 358 (CSC), [1997] 2 RCS 403.

³⁸ [Québec \(Commission des droits de la personne et des droits de la jeunesse\) c. Montréal \(Ville\); Québec \(Commission des droits de la personne et des droits de la jeunesse\) c. Boisbriand \(Ville\)](#), 2000 CSC 27, para. 28-30.

[Nouveau-Brunswick \(Commission des droits de la personne\) c. Potash Corporation of Saskatchewan Inc.](#), [2008] 2 RCS 604, 2008 CSC 45 (CanLII), para. 19, 65-67.

³⁹ Voir généralement : [La réutilisation de profils d'utilisateurs Facebook canadiens effectuées par une entreprise contrevient à la loi en matière de protection de la vie privée](#), CPVP, para. 87-96.

- ii. Les personnes exercent un niveau de contrôle direct, ce qui est un élément fondamental de la protection de la vie privée, sur leurs comptes de médias sociaux et sur l'accessibilité aux contenus connexes au fil du temps (par exemple, au moyen de paramètres de confidentialité).
64. En outre, le CIPVP de la C.-B. estime que les sites de médias sociaux ne sont pas des sources désignées d'information « accessibles au public » et que toute collecte auprès de ces sources ne serait autorisée qu'avec le consentement de l'intéressé et uniquement à des fins qu'une personne raisonnable jugerait appropriées.
65. En définitive, les affirmations de Clearview selon lesquelles le terme « publication » inclut nécessairement [traduction] « les blogues publics, les médias sociaux publics ou tout autre site Web public », si on les amène à leur conclusion logique, infèrent que **tout** le contenu accessible au public sur Internet serait une publication sous une forme ou une autre, ce qui créerait une exemption extrêmement large qui saperait le contrôle que les utilisateurs pourraient autrement avoir sur leurs renseignements à la source. À cet égard, il a été noté que le contrôle est une composante fondamentale de la protection de la vie privée⁴⁰.
66. Même si ces pages Web devaient être considérées comme des « publications » au sens des règlements — ce que nous rejetons — l'alinéa 1e) du règlement de la LPRPDE et l'alinéa 7e) du règlement de la PIPA de l'Alb. précisent que l'exception s'applique uniquement « si l'intéressé a fourni les renseignements », ou quand [traduction] « il est raisonnable de supposer que la personne sur laquelle portent les renseignements a fourni ces renseignements », respectivement. Comme Clearview réalise une collecte massive d'images, au moyen d'outils automatisés, il est inévitable que dans de nombreux cas, les images aient été téléchargées par une tierce partie.
67. La CAI considère que, pour les motifs suivants, on ne peut retenir l'argument de Clearview voulant que la LPRPSP inclut implicitement une exclusion pour les renseignements personnels « accessibles publiquement » (publicly available information), faute de quoi elle brimerait la liberté d'expression :
- i. Le texte de la loi indique clairement que seuls les renseignements ayant un caractère public « en vertu de la loi » sont exclus, ce qui n'inclut pas des renseignements autrement accessibles au public en l'absence d'une loi confirmant leur caractère public;
 - ii. À titre de loi quasi constitutionnelle et prépondérante sur les autres lois au Québec, dont l'objectif est de préciser l'exercice de droits conférés par le *Code civil du Québec*, notamment le droit au respect de la vie privée, toute exception doit être interprétée restrictivement;

⁴⁰ [Alberta \(Information and Privacy Commissioner\) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401](#), [2013] 3 R.C.S. 733, au para. 19, où l'on renvoie à la disposition de déclaration d'objet de la PIPA de l'Alberta, qui est similaire aux dispositions de déclaration d'objet de la LPRPDE et de la PIPA de la C.-B.

- iii. Il n'existe donc pas d'exclusion implicite à la LPRPSP pour les renseignements accessibles publiquement dont la loi ne reconnaît pas le caractère public;
- iv. Puisque Clearview n'a pas avisé le procureur général comme requis par l'article 76 du *Code de procédure civile*, la Commission ne peut examiner les prétentions soulevées par Clearview selon lesquelles la LPRPSP serait inopérante. En effet, un tel examen ne peut avoir lieu sans que le procureur général du Québec ait été avisé et ait eu l'occasion de faire valoir son point de vue, et ce, sous peine de nullité.
- v. Au surplus, il ne suffit pas d'invoquer une atteinte à la liberté d'expression. Clearview n'a pas expliqué ni démontré en quoi ses activités constituent l'expression d'un message à transmettre en lien avec la recherche de la vérité, la participation au sein de la société ou l'enrichissement et l'épanouissement personnels⁴¹.

Enjeu 2 : Clearview a-t-elle recueilli, utilisé ou communiqué des renseignements personnels à des fins acceptables?

- 68. À notre avis, pour les raisons exposées ci-dessous, l'objectif de la collecte, de l'utilisation ou de la communication de renseignements personnels par Clearview n'était ni approprié ni légitime.
- 69. Conformément au *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*⁴² du CPVP, celui-ci considère les facteurs⁴³ définis par les tribunaux pour déterminer si un organisme a recueilli, utilisé ou communiqué des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Ces facteurs doivent être appliqués en tenant compte du contexte, c'est-à-dire avec souplesse et variabilité en fonction des circonstances⁴⁴. En appliquant le paragraphe 5(3), les tribunaux ont déterminé que le CPVP doit se livrer à une [traduction] « pondération des droits » entre le droit à la vie privée de la personne et les besoins commerciaux de

⁴¹ *Irwin Toy Ltd. c. Québec (Procureur général)*, 1989 CanLII 87 (CSC), [1989] 1 RCS 927, pp. 976-977; *Institut généalogique Drouin inc. c. Commission d'accès à l'information du Québec*, 2017 QCCQ 7573 (CanLII).

⁴² *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*, CPVP, 2018.

⁴³ Le caractère sensible des renseignements personnels en question; le besoin ou les intérêts commerciaux légitimes des fins visées par l'organisme; l'efficacité de la collecte, de l'utilisation et de la communication pour répondre au besoin de l'organisme; l'existence de moyens portant moins atteinte à la vie privée qui permettent d'atteindre les mêmes fins pour un coût et des avantages comparables; la proportionnalité de l'atteinte à la vie privée par rapport aux avantages.

⁴⁴ *Eastmond c. Canadien Pacifique Ltée*, 2004 CF 852, para. 131.

l'organisme concerné⁴⁵. Cette pondération des droits doit se faire « du point de vue d'une personne raisonnable »⁴⁶. Des facteurs similaires sont également pris en compte par le CIPVP de la C.-B. pour déterminer si les fins sont raisonnables⁴⁷.

70. L'article 2 de la PIPA de l'Alberta stipule que pour déterminer si une chose ou une question est raisonnable ou déraisonnable, la norme à appliquer est « ce qu'une personne raisonnable jugerait approprié dans les circonstances ». Les ordonnances rendues par le CIPVP de l'Alb. ont aussi identifié plusieurs questions destinées à déterminer si la collecte des renseignements personnels dans un cas donné a été effectuée pour un objectif raisonnable⁴⁸, entre autres si elle a été effectuée de manière raisonnable.
71. Enfin, dans l'analyse de l'intérêt sérieux et légitime de Clearview à constituer un dossier sur autrui en vertu de l'article 4 de la LPRPSP du Québec, la CAI considère la légalité de l'objectif poursuivi et sa conformité au droit, à la justice et à l'équité⁴⁹.
72. Nous constatons que la collecte d'images et la création de dispositifs de reconnaissance faciale biométriques par Clearview, dans le but avoué de fournir un service au personnel des organismes d'application de la loi, et leur utilisation par d'autres personnes au moyen des comptes d'essai, représentent l'identification et la surveillance de masse de personnes par une entité privée dans le cadre d'une activité commerciale.
73. À notre avis, pour les raisons exposées ci-dessous, une personne raisonnable ne considérerait pas cette fin comme acceptable, raisonnable ou légitime dans les circonstances, au sens du paragraphe 5(3) de la LPRPDE, des articles 11, 14 et 17 de la PIPA de la C.-B.⁵⁰, des articles 11, 16 et 19 de la PIPA de l'Alb. et de l'article 4 de la LPRPSP du Québec.
74. Comme nous l'avons indiqué précédemment, les commissariats estiment que l'information en question (la reconnaissance faciale obtenue à partir d'images numériques) est de nature sensible. Les renseignements biométriques sont distinctifs, peu susceptibles de varier dans le temps, difficiles à modifier et en grande partie propres à la personne. Les données biométriques faciales sont de nature particulièrement sensible, car elles constituent l'essence de l'identité d'une personne et permettent d'identifier et de surveiller les personnes.

⁴⁵ [Turner v. Telus Communications Inc.](#), 2005 CF 1601, confirmée dans 2007 CAF 21.

⁴⁶ *Ibid.* [[Turner v. Telus Communications Inc.](#), 2005 CF 1601, confirmée dans 2007 CAF 21].

⁴⁷ Voir par exemple : [Ordonnance P12-01](#) (2012 BCIPC No. 25), [Ordonnance P13-02](#) (2013 BCIPC No. 24) et [Ordonnance 20-04](#) (2020 BCIPCD No. 24) de l'OIPC de la C.-B.

⁴⁸ [Ordonnance P2006-011](#) — Le CIPVP de l'Alb. a formulé plusieurs questions destinées à déterminer si la collecte des renseignements personnels est motivée par une fin raisonnable : 1) Y a-t-il un enjeu légitime à résoudre grâce à la collecte de renseignements personnels? 2) La collecte des renseignements personnels a-t-elle de bonnes chances de permettre de résoudre efficacement l'enjeu légitime en question? 3) Les renseignements personnels sont-ils recueillis de manière raisonnable?

⁴⁹ [Institut généalogique Drouin Inc.](#), CAI 091570, décision de D. Poitras, 6 février 2015.

⁵⁰ [Cruz Ventures Ltd. \(Wild Coyote Club\) \(Re\)](#), 2009 CanLII 38705 (BC IPC), para. 135-136.

75. Nous notons également que les renseignements contextuels supplémentaires fournis par les liens sources (c'est-à-dire les médias sociaux et les sites Web) peuvent comprendre des renseignements personnels importants présentant différents degrés de sensibilité. De plus, Clearview effectue entre autres la collecte de masse, non sélective, de renseignements personnels de mineurs, qui seraient considérés comme sensibles.
76. À notre avis, dans les circonstances, Clearview ne peut justifier aucune fin acceptable en ce qui a trait aux aspects suivants :
- i. le prélèvement massif et systématique des images de millions d'individus partout au Canada, y compris des enfants, parmi plus de 3 milliards d'images qui ont été prélevées dans le monde entier;
 - ii. l'élaboration d'un dispositif biométrique de reconnaissance faciale reposant sur ces images et la conservation de ces renseignements même après que l'image d'origine ou le lien ait été retiré d'Internet; ou
 - iii. l'utilisation et la communication ultérieures de ces renseignements à ses propres fins commerciales;
- lorsque ces fins :
- iv. sont sans rapport avec les fins pour lesquelles les images ont été publiées à l'origine (p. ex. médias sociaux ou réseautage professionnel);
 - v. sont souvent au détriment de la personne (enquête, poursuites éventuelles, embarras, etc.);
 - vi. présentent un risque de préjudice grave aux individus dont les images sont recueillies par Clearview (y compris les préjudices associés à une erreur d'identification ou à d'éventuelles atteintes à la sécurité des données), alors que la grande majorité des individus en question n'ont jamais été impliqués dans un crime et ne le seront jamais pas plus qu'ils seront désignés pour contribuer à la résolution d'un crime grave.
77. En outre, comme il est expliqué ci-dessus, nous estimons que Clearview n'a pas recueilli de manière légale les renseignements personnels biométriques sensibles. Elle recueille ces renseignements afin d'enrichir sa base de données pour la reconnaissance faciale sans obtenir le consentement explicite et exprès des personnes concernées, comme l'exigent les Lois, ou sans aucune forme d'avis ou de consentement.
78. Elle n'a pas recueilli ces renseignements directement auprès des intéressés. De plus, Clearview n'entretenait aucune relation avec les tiers administrant les sites Web où elle en a fait la collecte, lesquels pourraient, hypothétiquement, avoir obtenu un consentement pour les fins visées par l'entreprise. En fait, selon les allégations crédibles formulées par plusieurs de ces tiers, Clearview n'était pas autorisée à recueillir les renseignements sur leurs sites Web. Clearview a atteint ses fins par le biais d'une collecte de renseignements qui contrevient fondamentalement aux lois canadiennes sur

la protection des renseignements personnels. Par conséquent, ces fins ne peuvent être considérées comme acceptables.

79. Par conséquent, nous estimons que Clearview a enfreint le paragraphe 5(3) de la LPRPDE, l'article 4 de la LPRPSP du Québec, les articles 11, 14 et 17 de la PIPA de la C.-B., et les articles 11, 16 et 19 de la PIPA de l'Alb.

Réponse de Clearview concernant les fins acceptables

80. Clearview n'était pas d'accord avec notre qualification préliminaire de ses fins et a déclaré que sa collecte de renseignements visait à [traduction] « permettre aux organismes d'application de la loi d'obtenir des renseignements rapidement et avec exactitude dans le cadre d'une enquête en cours » et qu'une personne raisonnable considérerait cette fin comme [traduction] « appropriée, raisonnable et légitime dans les circonstances ». Clearview a réitéré son point de vue selon lequel ces renseignements étaient accessibles au public et donc non sensibles.

81. Clearview a affirmé ce qui suit :

[traduction] « [L]a différence entre les fins pour lesquelles les images ont été publiées à l'origine et celles pour lesquelles Clearview a utilisé, recueilli ou communiqué ces images n'est pas pertinente. Si les fins justifiant les actions de Clearview sont appropriées et légitimes, il est raisonnable de croire que Clearview a respecté l'article de la loi même si de telles images ne sont pas utilisées, recueillies ou communiquées pour les mêmes raisons qu'elles ont été affichées initialement. »

82. Clearview a également affirmé qu'on ne pouvait pas la tenir responsable de préjudices subis par des personnes à la suite de l'utilisation de ses services :

[traduction] « Des poursuites menées par les organismes d'application de la loi qui ont utilisé les services de Clearview ne constituent en aucun cas une conséquence directe et unique des services offerts. Clearview ne peut pas être tenue responsable d'offrir des services à une entité qui commet ensuite des erreurs par rapport à l'évaluation d'une personne visée par une enquête. De nombreux facteurs sont pris en compte par les organismes d'application de la loi lorsqu'ils font leur travail. Clearview offre des correspondances potentielles, tout comme des témoins font une identification potentielle dans le contexte d'une parade d'identification ou du témoignage d'un témoin oculaire. Il revient aux responsables de l'application de la loi de déterminer l'utilisation appropriée de ces renseignements dans le cadre de leurs enquêtes. »

83. Clearview a affirmé qu'il était incorrect de qualifier ses objectifs comme préjudiciables pour les personnes :

[traduction] « Les objectifs que poursuit Clearview ne sont pas au détriment des personnes, mais plutôt à l'avantage de la collectivité et de l'intérêt public en aidant les organismes d'application de la loi responsables de la sécurité publique dans le cadre de leurs enquêtes. On peut dire que le fait de limiter un tel service nuirait à l'intérêt

public. Clearview facilite les recherches en fournissant une plateforme qui contient tous les renseignements nécessaires, soit des renseignements qui sont déjà accessibles, mais qui se trouvent sur plusieurs sites Web tiers. »

84. Clearview a en outre soutenu que le seul préjudice potentiel pour la plupart des personnes serait qu'un lien vers une photo pourrait être envoyé à un organisme chargé de l'application de la loi, ce qui, à son avis, ne pourrait pas être qualifié de significatif. Elle a estimé que ce préjudice potentiel n'était pas disproportionné par rapport aux [traduction] « avantages et aux objectifs auxquels [Clearview] contribue ».
85. Pour conclure, Clearview a renvoyé à la disposition de déclaration d'objet de la LPRPDE, en faisant la déclaration suivante :

[traduction] « [L]orsqu'il faut déterminer si les fins sont appropriées, on doit évaluer l'équilibre entre le droit à la vie privée d'une personne et le besoin des organisations de recueillir, d'utiliser et de communiquer des renseignements personnels. »

Elle a ajouté ceci :

[traduction] « Étant donné les avantages potentiels importants que peuvent procurer les services de Clearview aux organismes d'application de la loi et à la sécurité nationale, ainsi que l'improbabilité qu'un préjudice grave soit causé, en particulier considérant que les renseignements conservés sont déjà accessibles au public et qu'ils sont distribués aux organismes d'application de la loi aux fins légitimes d'enquête uniquement, les motifs de Clearview sont entièrement appropriés. »

86. Nous ne sommes pas convaincus par les arguments de Clearview, qui renvoient à la même jurisprudence que celle sur laquelle nous nous sommes appuyés. Nous restons d'avis, à la lumière de notre analyse exposée ci-dessus aux paragraphes 73 à 78, que Clearview recueille des renseignements personnels biométriques sensibles, à des fins qu'une personne raisonnable ne jugerait pas appropriées dans les circonstances.
87. Alors que les organismes chargés de l'application de la loi s'appuient, pour mener leurs activités, sur le large pouvoir de collecte que l'on trouve dans les lois sur la protection des renseignements personnels dans le secteur public, ces actions sont limitées par la *Charte* et Clearview ne bénéficie pas d'un tel pouvoir de collecte en tant qu'organisme privé.
88. Bien que certains des renseignements recueillis aient pu en fin de compte servir à l'application de la loi, le véritable objectif de Clearview en recueillant ces renseignements s'apparente plus à une opération commerciale à but lucratif qu'à l'application de la loi⁵¹.

⁵¹ [Cash Converters Canada Inc. v. Oshawa \(City\)](#), 2007 ONCA 502 (CanLII), para. 38.

89. Enfin, nous notons que Clearview met l'accent sur le fait que ses activités n'ont pas porté préjudice aux personnes. En adoptant cette position, Clearview ne reconnaît pas : i) la multitude de cas où des correspondances fausses ou mal appliquées pourraient nuire à la réputation des personnes, et ii) plus fondamentalement, l'atteinte au droit à la vie privée des personnes et le préjudice général infligé à tous les membres de la société, qui se trouvent sous la surveillance de masse continue de Clearview en raison du ratissage aveugle et du traitement qu'elle fait de leurs images faciales.

Autres préoccupations concernant les fins acceptables

90. Nous relevons un certain nombre de questions supplémentaires. Nous ne nous prononcerons pas précisément sur celles-ci, mais elles continuent de nous préoccuper fortement dans le contexte des pratiques de reconnaissance faciale de Clearview.

Exactitude

91. Bien que les commissariats n'aient pas effectué d'évaluation technique de l'exactitude de la technologie de reconnaissance faciale de Clearview, nous avons un certain nombre de préoccupations liées à la technologie de reconnaissance faciale en général.
92. Les commissariats reconnaissent que les technologies de reconnaissance faciale peuvent être utilisées pour rendre de nombreux services à la société et aux personnes, et qu'il en existe un certain nombre d'utilisations légitimes dans les entreprises et les administrations. Par exemple, la reconnaissance faciale peut aider les entreprises à vérifier l'identité d'une personne, ou les organismes d'application de la loi à enquêter sur des crimes graves et complexes. Toutefois, si la technologie de reconnaissance faciale, et celle de Clearview en particulier, peut être efficace dans certaines circonstances, nous relevons d'importantes préoccupations concernant l'efficacité et l'exactitude des technologies de reconnaissance faciale, notamment en ce qui concerne certaines tranches de la population.
93. Malgré le perfectionnement de la technologie de reconnaissance faciale grâce à l'augmentation de la capacité informatique, l'amélioration des algorithmes sous-jacents et la disponibilité d'énormes volumes de données, cette technologie n'est pas parfaite et peut entraîner des erreurs d'identification. Ces erreurs peuvent être dues, entre autres, à la qualité des photos et des vidéos et au rendement des algorithmes utilisés pour comparer les caractéristiques des visages. Plus précisément, les commissariats notent des problèmes d'exactitude allégués émanant de diverses études et enquêtes sur les algorithmes de reconnaissance faciale utilisés dans un certain nombre de solutions technologiques.
94. Les problèmes d'exactitude de la technologie de reconnaissance faciale peuvent prendre deux formes générales : i) le défaut d'identification d'une personne dont le visage est enregistré dans la base de données de référence, ce qu'on appelle un « faux négatif »; ou ii) la mise en correspondance de visages qui appartiennent en fait à deux personnes différentes, ce qu'on appelle un « faux positif ». Alors que le premier problème concerne principalement les utilisateurs de la technologie de reconnaissance

faciale, le second présente des risques importants de préjudice pour les personnes, en particulier lorsque la reconnaissance faciale est utilisée dans le cadre de l'application de la loi⁵².

95. En particulier, nous faisons référence aux rapports selon lesquels la technologie de reconnaissance faciale a révélé des occurrences beaucoup plus élevées de faux positifs ou d'identifications erronées lors de l'évaluation du visage des personnes de couleur, et en particulier celui des femmes de couleur, ce qui pourrait entraîner un traitement discriminatoire pour ces personnes⁵³. Par exemple, des recherches menées par le National Institute of Standards and Technology ont montré que le taux de faux positifs chez les Asiatiques et les Noirs était souvent de 10 à 100 fois plus élevé que chez les Blancs⁵⁴. De telles erreurs d'identification peuvent faire en sorte que des personnes soient privées de certaines chances, ou qu'elles soient visées par des enquêtes et détenues sur la base de renseignements incorrects. Ces préjudices seraient généralement considérés comme importants⁵⁵.
96. Nous notons que Clearview a mandaté un groupe d'experts indépendants pour effectuer un essai d'exactitude de sa technologie, lequel était, selon elle, fondé sur la méthodologie d'un essai antérieur effectué par l'American Civil Liberties Union (ACLU). Une copie des résultats de cet essai a été fournie dans les représentations de Clearview, faisant état d'un taux d'exactitude de sa technologie de 100 %. Au cours de notre enquête, nous avons constaté que des préoccupations importantes au sujet de la méthodologie d'essai et des conclusions avaient été soulevées par divers chercheurs, y compris au sein même de l'équipe de l'ACLU, qui a qualifié l'étude de « trompeuse » et a déposé une plainte auprès de Clearview⁵⁶.
97. Dans ses représentations, Clearview a fait valoir que l'ACLU et d'autres critiques n'avaient pas réussi à démontrer en quoi les résultats de l'essai étaient trompeurs. Elle a répété que lors de l'essai, l'application de Clearview faisait correspondre correctement toutes les images recherchées, sans aucune inexactitude. Le CPVP ne se prononcera pas sur le bien-fondé de ces plaintes, mais nous notons qu'il est difficile de se prononcer sur l'exactitude en raison des préoccupations récurrentes quant à l'opacité de la technologie de Clearview, qui est exclusive et à laquelle la majorité des chercheurs n'ont pas accès.

⁵² J. Angwin *et al.*, « [Machine Bias](#) », *ProPublica*, 23 mai 2016.

⁵³ Voir « [NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software](#) », *National Institute of Standards and Technology* (NIST), décembre 2019; « [Black and Asian faces misidentified more often by facial recognition software](#) », *CBC News*, décembre 2019, et « [Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use](#) », *Washington Post*, décembre 2019.

⁵⁴ « [Face Recognition Vendor Test, Part 3: Demographic Effects](#) », *National Institute of Standards and Technology* (NIST), décembre 2019.

⁵⁵ [Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5\(3\)](#), CPVP, 2018.

⁵⁶ C. Haskins *et al.*, « [The ACLU Slammed A Facial Recognition Company That Scrapes Photos From Instagram And Facebook](#) », *Buzzfeed News*, février 2020.

Collecte en violation des dispositions contractuelles

98. Nous notons que Clearview a reçu des lettres de la part de Google, Facebook, Twitter, YouTube et LinkedIn concernant la violation des conditions de service dans le cadre de sa pratique de collecte de renseignements⁵⁷.
99. Clearview a indiqué avoir répondu à ces lettres en faisant valoir son droit, au titre du premier amendement de la Constitution américaine, de prélever les renseignements « publics ». Clearview a également affirmé que les clauses contractuelles n'ont aucune incidence sur notre enquête ou sur la pertinence de ses objectifs.
100. Bien que nous ne nous prononcions pas sur le fait qu'une ou plusieurs violations contractuelles se soient produites ou non, dans la mesure où Clearview a prélevé des renseignements personnels en violation des clauses contractuelles des plateformes, cela constituerait, à notre avis, un facteur supplémentaire pertinent pour examiner le caractère inapproprié des objectifs de Clearview, dans les circonstances.

Risque de préjudices causés par une atteinte à la vie privée

101. La grande quantité de renseignements biométriques sensibles détenus par Clearview en ferait, à notre avis, une cible de grande valeur pour les acteurs malveillants. Clearview a fait valoir que [traduction] « le risque de préjudices causés par une atteinte à la vie privée n'est pas un facteur approprié au moment d'évaluer les objectifs des actions de Clearview, car cela irait bien au-delà de la portée de la loi, qui vise à établir des règles reconnaissant le droit à la vie privée des personnes »; elle a affirmé que ce risque est présent dans [traduction] « presque toutes les sphères de la société ». Elle a également soutenu que même si ces risques étaient pris en compte, il n'y avait aucun risque de préjudice important ni aucune probabilité que les renseignements soient volés. Nous ne nous prononcerons pas sur les mesures de protection de Clearview, qui sont exclues de la présente enquête, mais nous notons que l'entreprise a annoncé publiquement qu'elle avait fait l'objet d'une atteinte à deux reprises l'an dernier. Une première fois en février 2020, lorsque sa liste de clients a été diffusée⁵⁸, et une autre fois en avril de la même année, lorsque son code source et la vidéo du projet pilote ont été recueillis et ont fait l'objet de fuites partielles⁵⁹. À notre avis, la collecte et l'utilisation ultérieure par Clearview de milliards d'images et de matrices faciales liées à des données sources représentent un risque important pour des dizaines de millions d'individus au Canada si elles sont compromises.

⁵⁷ C. Wood, « [Facebook has sent a cease-and-desist letter to facial recognition startup Clearview AI for scraping billions of photos](#) », *Business Insider*, 6 février 2020.

⁵⁸ « [Clearview AI: Face-collecting company database hacked](#) », *BBC*, 27 février 2020.

⁵⁹ Z. Whittaker, « [Security lapse revealed Clearview AI source code](#) », *TechCrunch*, 16 avril 2020.

Enjeu 3 : Clearview a-t-elle satisfait à ses obligations concernant la biométrie au Québec?

102. Lorsqu'une entreprise constitue un système biométrique au Québec, elle doit respecter les règles énoncées dans la LPRPSP du Québec et dans la LCCJTI. En effet, elle doit notamment :
- i. obtenir le consentement exprès de la personne concernée pour cette fin conformément à l'article 44 de la LCCJTI;
 - ii. déclarer la création ou l'existence du système biométrique à la CAI conformément à l'article 45 de la LCCJTI.
103. Il ressort de l'enquête que Clearview n'a pas obtenu le consentement exprès des personnes concernées, puisqu'elle a reconnu qu'aucune tentative de recherche de consentement n'avait eu lieu. De plus, l'entreprise n'a pas déclaré son système biométrique à la CAI du Québec.

Réponse de Clearview concernant la loi sur la biométrie du Québec

104. Clearview prétend ne pas avoir constitué de système biométrique au Québec, ses activités se déroulant aux États-Unis. Soulignant le fait qu'une loi provinciale ne peut avoir une portée extraterritoriale en l'absence d'une volonté expresse ou implicite du législateur, Clearview conclut que la LCCJTI ne peut s'appliquer à elle, car cela conférerait à la Loi une portée extraterritoriale qu'aucune disposition ne lui confère, explicitement ou implicitement.
105. La CAI ne partage pas l'opinion de Clearview en ce qui concerne la LCCJTI. En effet, Clearview ne nie pas le fait d'avoir constitué un système biométrique. La CAI est donc d'avis que, même si le système est à l'extérieur du Québec, Clearview a néanmoins recueilli des images dans le cadre de l'exploitation d'une entreprise au Québec et doit donc obtenir le consentement exprès des personnes avant de pouvoir vérifier ou confirmer l'identité de ces personnes.
106. Le caractère véritable des dispositions en cause de la LCCJTI est le respect de la vie privée des personnes concernées et la protection de leurs renseignements personnels. La volonté que cette obligation impérative soit imposée à tous se traduit par l'utilisation du terme « nul ». Les effets extraterritoriaux ne sont qu'accessoirs.
107. En fait, Clearview, en offrant ses services à l'intérieur des limites de la province et en y recueillant et en y utilisant des renseignements personnels, exploite une entreprise au Québec. Par conséquent, Clearview est assujettie à la législation applicable dans la juridiction dans laquelle elle exerce ses activités, soit la province de Québec⁶⁰. L'emplacement physique de Clearview et le lieu de ses activités principales ne sont donc que des accessoires qui ne lui permettent pas de s'exclure de l'application de la LCCJTI.

⁶⁰ [*Procureur général \(Québec\) c. Kelloqg's Co. of Canada et autre*](#), [1978] 2 R.C.S. 211.

108. En effet, Clearview doit obtenir le consentement exprès des personnes avant de pouvoir vérifier ou confirmer l'identité de ces personnes (art. 44 de la LCCJTI) tel que spécifié au paragraphe 40. La sensibilité des renseignements recueillis, utilisés ou communiqués et l'impact que peut avoir l'utilisation de ces renseignements sur la vie privée des personnes concernées requièrent effectivement que celles-ci soient informées et expriment leur consentement. Le recours à un système biométrique ne peut se faire à l'insu des personnes concernées⁶¹.
109. Clearview devait aussi déclarer sa banque de mesures et de caractéristiques biométriques à la Commission selon l'article 45 de la LCCJTI.
110. Par conséquent, la CAI estime que Clearview n'a pas respecté les articles 44 et 45 de la LCCJTI.

Recommandations

111. Dans notre lettre d'intention, nous avons fait part à Clearview que nous pourrions ordonner ou recommander de :
- i. cesser d'offrir à des clients au Canada les services de reconnaissance faciale qui ont fait l'objet de la présente enquête;
 - ii. mettre fin à la collecte, à l'utilisation et à la communication d'images et de matrices faciales biométriques auprès d'individus au Canada;
 - iii. supprimer les images et les matrices faciales biométriques recueillies auprès d'individus au Canada qu'elle a en sa possession.
112. En ce qui concerne la première recommandation, nous avons demandé à Clearview de confirmer qu'elle ne reprendrait pas son offre de fournir les services de reconnaissances faciale au Canada à l'avenir. Nous avons également demandé les engagements de Clearview pour expliquer comment et quand il mettrait en œuvre les deuxièmes et troisièmes recommandations.

Réponse de Clearview à nos conclusions

113. Tel qu'il est indiqué dans le présent rapport, Clearview a formellement rejeté nos conclusions.
114. Malgré cela, notant qu'à la suite d'autres échanges avec les commissariats, elle s'était volontairement retirée du marché canadien plus tôt dans l'enquête, Clearview a indiqué qu'elle était [traduction] « prête à envisager le maintien de ce statut pendant deux années supplémentaires, afin de permettre aux différents commissaires de fournir des

⁶¹ [Les 3 Piliers Inc.](#), CAI 1018507-S, décision de C. Chassigneux, 14 février 2020.

lignes directrices détaillées et significatives sur la manière dont l'intelligence artificielle pourrait être traitée en droit canadien ».

115. Clearview a indiqué que, comme elle ne menait pas [traduction] « actuellement ses activités » au Canada, les commissariats devraient suspendre leur enquête et s'abstenir de publier un rapport ou de prendre une décision définitive sur cette question.
116. Clearview a indiqué que [traduction] « pendant une telle suspension, [elle] serait disposée à prendre des mesures, au meilleur de ses capacités et sans préjudice, pour tenter de limiter la collecte et la communication des images qu'elle peut reconnaître comme étant canadiennes [...] ».
117. Au moment de la rédaction du présent rapport, Clearview ne s'était pas engagée à suivre nos recommandations ou ordonnances envisagées; les commissariats ont donc jugé opportun de publier le présent rapport.

Conclusions

118. En conclusion, nous constatons que Clearview a recueilli, utilisé et communiqué des renseignements personnels en développant et en fournissant son application de reconnaissance faciale, sans obtenir le consentement requis. Nous concluons donc que Clearview a enfreint le principe 4.3 de l'annexe 1, ainsi que l'article 6.1 de la LPRPDE; le paragraphe 7(1) de la PIPA de l'Alb.; les articles 6 à 8 de la PIPA de la C.-B., ainsi que les articles 6 et 12 à 14 de la LPRPSP du Québec.
119. Nous estimons également que la collecte, l'utilisation et la communication de renseignements personnels par Clearview par le biais de son application de reconnaissance faciale ont eu lieu à des fins qu'une personne raisonnable jugerait inappropriées. Par conséquent, nous concluons que Clearview a enfreint le paragraphe 5(3) de la LPRPDE, les articles 11, 16 et 19 de la PIPA de l'Alb., les articles 11, 14 et 17 de la PIPA de la C.-B. et l'article 4 de la LPRPSP du Québec.
120. De plus, la CAI conclut que Clearview ne respecte pas les articles 44 et 45 de la LCCJTI en utilisant des renseignements biométriques aux fins d'identification sans le consentement exprès des personnes concernées et en n'ayant pas déclaré à la CAI la banque de mesures et caractéristiques biométriques qu'elle détient.
121. Pour toutes les raisons ci-dessus, et malgré l'opposition de Clearview, nous estimons que l'affaire est **fondée** et nous recommandons à Clearview de :
 - i. cesser d'offrir à des clients au Canada les services de reconnaissance faciale qui ont fait l'objet de la présente enquête;
 - ii. mettre fin à la collecte, à l'utilisation et à la communication d'images et de matrices faciales biométriques recueillies auprès d'individus au Canada;

- iii. supprimer les images et les matrices faciales biométriques recueillies auprès d'individus au Canada qu'elle a en sa possession.
122. Nous notons d'une part, la demande de Clearview auprès de nos commissariats de suspendre nos enquêtes et d'autre part, son offre de prendre des mesures pour limiter la collecte et la communication d'images de Canadiens. Toutefois nous ne sommes pas d'avis que la suspension de notre enquête serait appropriée. Au contraire, nous estimons qu'il est important de conclure nos enquêtes conjointes et, dans ce cas particulier, de publier nos constatations, nos conclusions, nos recommandations ou nos ordonnances dans l'intérêt public. Entre autres considérations, cela garantira que d'autres organisations bénéficieront de nos conclusions alors qu'elles envisagent des initiatives susceptibles de partager certaines similitudes avec les pratiques de Clearview.
123. Si Clearview maintient son refus d'accepter les conclusions et les recommandations de quatre autorités canadiennes indépendantes chargées de faire respecter la protection des renseignements personnels, nous entreprendrons les autres actions qui s'offrent à nous en vertu de nos Lois respectives pour obliger Clearview à respecter les lois fédérale et provinciales sur la protection des renseignements personnels applicables au secteur privé.