Commentaire du Rapport de conclusions d'enquête conjoint sur Clearview

11 février 2021

Le 3 février 2021, 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 »; ensemble, les « commissariats ») publiaient un Rapport de conclusions d'enquête conjoint (le « rapport ») présentant les résultats de leur enquête visant à établir si la collecte, l'utilisation et la communication de renseignements personnels par Clearview AI, Inc. (« Clearview ») au moyen de son dispositif de reconnaissance faciale respecte les lois fédérales et provinciales sur la protection des renseignements personnels applicables au secteur privé (les « lois sur la protection des renseignements personnels »).

Dans ce rapport d'envergure, les commissariats qualifient les activités de Clearview de surveillance de masse et d'atteinte au droit à la vie privée du public[1] et traitent de questions comme la portée de l'exception à l'obligation d'obtenir le consentement pour les renseignements accessibles au public, le caractère acceptable des fins justifiant les collectes de Clearview et les obligations relatives aux données biométriques.

Contexte

Clearview, une entreprise de technologie des États-Unis, a créé un système logiciel de reconnaissance faciale utilisant une base de données qui met des images obtenues de diverses sources en ligne en correspondance avec (i) des données de reconnaissance faciale tirées de ces images et (ii) des hyperliens vers ces sources. Ce système permet de télécharger l'image numérique d'un visage et d'effectuer une recherche à partir de celle-ci. L'algorithme de reconnaissance faciale est ensuite appliqué à l'image, le résultat est comparé à la base de données de Clearview et les correspondances probables sont affichées avec l'information de source s'y rapportant[2].

En janvier et en février 2020, les médias rapportaient que Clearview remplissait sa base de données de reconnaissance faciale d'images numériques provenant de divers sites Web publics – principalement de médias sociaux[3] – et que nombre d'organismes privés et d'application de la loi avaient fait appel aux services de Clearview pour identifier des personnes[4].

Les commissariats ont lancé une enquête conjointe sur Clearview en février 2020.

Conclusions

Sans surprise, la substantifique moelle des conclusions cadre avec la jurisprudence et les orientations des commissariats.

Ces derniers ont confirmé que les activités de Clearview tombaient sous le coup des lois sur la protection des renseignements personnels fédérales et provinciales[5] et que les données tirées de profils de médias sociaux publics ne sont pas visées par l'exception à l'obligation d'obtenir le consentement que prévoient ces lois pour les renseignements « auxquels le public a accès » ou ayant « un caractère public en vertu de la loi[6] ». Dans leur étude de la définition de « renseignements auxquels le public a accès », les commissariats n'ont pas tardé à invoquer une conclusion antérieure du Commissariat à la protection de la vie privée du Canada selon laquelle les renseignements publiés sur les médias sociaux se trouvent sous l'égide de la *Loi sur la* protection des renseignements personnels et les documents électroniques (la « LPRPDE »)[7]. Ils ont conclu que Clearview aurait dû obtenir le consentement des personnes visées.

Toujours conformément aux constatations antérieures[8], le rapport fait état du caractère particulièrement sensible des données biométriques faciales et de l'obligation corrélative de Clearview, à laquelle elle a manqué, d'obtenir le consentement explicite et positif de toute personne au Canada dont elle a recueilli l'image[9].

Les commissariats ont de plus conclu qu'une personne raisonnable ne jugerait pas que les fins du système de Clearview sont acceptables, raisonnables ou légitimes dans les circonstances[10]. Ainsi, même si les consentements requis avaient été obtenus, expressément ou non, ceux-ci n'auraient pas été valables.

Le rapport comporte également des remarques générales sur les fins acceptables ainsi que sur la propension connue des systèmes semblables à celui de Clearview à générer de faux positifs[11], la possibilité que Clearview ait contrevenu aux conditions d'utilisation des diverses plateformes de médias sociaux où elle a recueilli des renseignements personnels[12] et le risque de préjudice que présente la création d'une mégabase centralisée de données biométriques faciales[13].

Enfin, le rapport indique que le système de Clearview tombe sous le coup des lois québécoises subordonnant la collecte de renseignements biométriques à l'obtention d'un consentement exprès. Au surplus, du fait qu'elle a exploité au Québec une base de données de son cru renfermant des mesures ou des caractéristiques biométriques, Clearview avait par ailleurs l'obligation d'en déclarer l'existence à la CAI[14].

Commentaire

Consentement

Comme nous l'avons mentionné, les commissariats ont établi que les renseignements publiés sur un profil public de médias sociaux ne sont pas visés par les exceptions

applicables aux renseignements « accessibles au public » ou « ayant un caractère public en vertu de la loi » prévues dans les lois sur la protection des renseignements personnels. Clearview aurait donc dû obtenir le consentement des personnes concernées.

Or, comme la société avait d'emblée déclaré ne pas l'avoir fait en invoquant ces exceptions, l'analyse des commissariats aurait pu en rester là : la question était tranchée. Néanmoins, une part considérable du rapport est consacrée à l'analyse du caractère acceptable des fins de Clearview.

Cela s'explique sans doute par la volonté des commissariats que ce nouveau précédent résiste au projet de loi C-11, dont l'adoption entraînerait le remplacement de la LPRPDE par une nouvelle loi sur la protection des renseignements personnels, ainsi qu'à d'éventuels changements législatifs au palier provincial.

Par exemple, le projet de loi se calque sur la LPRPDE pour ce qui est des exceptions à l'obligation d'obtenir le consentement applicables aux renseignements accessibles au public[15], tout en laissant le soin des détails à la réglementation. Or, d'aucuns s'inquiètent[16] des pressions qui s'exercent pour inclure à la définition de renseignements accessibles au public les renseignements personnels qu'une personne publie sciemment sur un site Web public[17]. Si le projet de loi C-11 devient loi, un règlement sera préparé pour son application; si ce règlement élargit la définition susmentionnée, l'analyse présentée dans le rapport pourrait s'en trouver affaiblie, voire anéantie.

Qui plus est, même si la définition d'information accessible au public prévue dans un tel règlement excluait les renseignements trouvés sur les médias sociaux et d'autres sites Web publics, il se pourrait bien qu'une autre disposition du projet de loi C-11 soit interprétée comme permettant les activités auxquelles se livre Clearview, comme le moissonnage de renseignements personnels sur ces sites. L'alinéa 18(2)e) du projet de loi C-11 permet la collecte et l'utilisation de renseignements personnels, à l'insu de la personne concernée ou sans son consentement, en vue d'une activité d'affaires « dans le cadre [de laquelle] il est pratiquement impossible pour l'organisation d'obtenir le consentement de l'individu, en raison de l'absence de lien direct avec celui-ci[18]. »

Toutefois, comme le projet de loi le fait par ailleurs sien, le critère de la LPRPDE relatif aux fins acceptables pourra toujours s'appliquer, même en cas d'exception à l'obligation d'obtenir le consentement[19]. C'est pourquoi il nous semble probable que les commissariats aient abordé la question de l'acceptabilité des fins par prudence, de peur que le projet de loi ou d'éventuelles réformes législatives provinciales en matière de protection des renseignements personnels viennent faire échec à leur raisonnement sur le consentement et les exceptions à son égard.

Les organisations intéressées devraient donc garder à l'esprit que les organismes canadiens de réglementation de la protection des renseignements personnels veilleront sans doute, dans leurs futures enquêtes et analyses, à ce que leurs conclusions résistent à l'adoption du projet de loi C-11.

Fins acceptables

Dans la section du rapport qui traite des fins acceptables, les commissariats concluent que « la surveillance de masse continue de Clearview[,] en raison du ratissage aveugle et du traitement qu'elle fait [des] images faciales [de personnes] » porte « atteinte [à leur] droit à la vie privée[20]. »

Si cette déclaration peut sembler quelque peu exagérée, il ne fait aucun doute que le système créé par Clearview *promeut* la surveillance et est susceptible d'accroître les capacités de surveillance de ses clients. Selon les ressources dont ils disposent, leur utilisation du système pourrait effectivement être considérée comme de la surveillance de masse.

Pour étayer la conclusion voulant que les activités de Clearview constituent de la surveillance de masse, le rapport les dépeint comme suit : le moissonnage à grande échelle d'images de personnes, dont d'enfants, la création de dispositifs de reconnaissance faciale à partir de ces images et la compilation d'hyperliens menant à leurs sources respectives, le tout à des fins lucratives étrangères à celles de la publication de ces images, ainsi que potentiellement nuisibles – voire gravement préjudiciables – aux personnes qui y figurent[21]. Les commissariats ont conclu que ces fins, prises dans leur ensemble, ne sont pas ce qu'une personne raisonnable qualifierait d'acceptable, raisonnable ou légitime dans les circonstances[22].

Cette analyse pose cependant problème. Hormis la création de dispositifs de reconnaissance faciale, les moteurs de recherche mènent l'ensemble des activités ci-dessus énumérées, à des fins commerciales qui pourraient avoir des conséquences négatives.

À ce propos, il convient de noter qu'en réponse à la préoccupation de Clearview voulant que ses activités fussent traitées différemment de celles d'autres moteurs de recherche d'images[23], les commissariats ont affirmé dans le rapport que, leur enquête portant exclusivement sur les pratiques de Clearview, ils « [n'ont pas émis] d'avis sur les obligations de tout autre organisme[24]. » Ils avaient manifestement compris que qualifier la plateforme de Clearview de moteur de recherche les aurait obligés à traiter du sujet épineux de l'exploration, du moissonnage, du référencement et des autres opérations du genre qu'effectuent les moteurs de recherche[25].

Par conséquent, si le rapport conclut au caractère inacceptable des fins de Clearview sur la foi des multiples facteurs susmentionnée, son insistance répétée sur les données biométriques générées par cette dernière, de même que le fait que les commissariats aient expressément réservé leur avis quant à des organisations qu'elle considère comme lui étant analogues, permettent raisonnablement de conclure que la préoccupation essentielle en l'occurrence a trait à la création de dispositifs de reconnaissance faciale à partir des images recueillies. Cette hypothèse cadre avec de récentes constatations démontrant que les commissariats voient les technologies de biométrie faciale d'un œil particulièrement mauvais, même lorsqu'elles ne servent pas à l'identification personnelle[26].

Si notre conclusion s'avère exacte, cela signifierait que l'analyse sur les fins acceptables présentée dans le rapport ne s'applique pas nécessairement aux moteurs de recherche à l'aide d'images qui n'utilisent pas la biométrie faciale, ainsi que d'autres systèmes et services de collecte de données à grande échelle.

Évidemment, les autres activités susmentionnées pourraient créer d'autres embûches en matière de droit de la protection des renseignements personnels. Quand bien même celles-ci seraient surmontées, il y a lieu de garder à l'esprit qu'ajouter la biométrie faciale à un système ou un service pourrait en « contaminer » les fins.

Biométrie

La conclusion du rapport selon laquelle Clearview aurait dû obtenir le consentement exprès des personnes visées par sa collecte de données biométriques en vertu de l'article 44 de la Loi concernant le cadre juridique des technologies de l'information du Québec indique que ce dernier doit recevoir une interprétation large. Cela n'a rien de surprenant.

Il pourrait être plaidé éloquemment que les systèmes comme celui de Clearview n'appartiennent pas à la catégorie classique des systèmes d'identification, en ce que Clearview elle-même ne veille en rien à l'exactitude des données d'identification qu'elle emmagasine (contrairement aux bases de données d'empreintes digitales utilisées par les forces de l'ordre, par exemple). Ainsi, il se peut que la source rattachée à une donnée ne contienne aucun renseignement identificatoire parce que le profil en question a été créé sous un pseudonyme, parce que l'image a été moissonnée sur un profil tiers, ou pour une autre raison.

Force est cependant d'admettre que l'approche globale de Clearview cadre avec la description que fait la CAI québécoise des systèmes d'identification dans ses orientations, c'est-à-dire des systèmes conçus pour trouver « une identité dans une banque de données, parmi plusieurs autres identités. » Les caractéristiques et mesures biométriques d'une personne inconnue sont comparées avec celles de la base de données afin de répondre à une question : « Qui est-ce?[27] » C'est évidemment pour répondre à cette question que les clients de Clearview s'inscrivent à son service.

Par conséquent, le caractère peu fiable du système de Clearview et le fait que celle-ci tienne intentionnellement au minimum le contrôle de la qualité de ses sources ne suffisent pas à empêcher que ce système soit qualifié de système d'identification.

Points à retenir

- Les organisations intéressées seraient avisées de noter que les organismes canadiens de réglementation en matière de protection des renseignements personnels veilleront sans doute, dans leurs futures enquêtes et analyses, à ce que leurs conclusions résistent à l'adoption du projet de loi C-11 et aux réformes législatives provinciales qui suivront vraisemblablement dans son sillage.
- L'incorporation de biométrie faciale à un projet ou à une initiative comportant la collecte et l'utilisation de renseignements personnels augmente le risque que ce projet ou cette initiative fasse l'objet d'une conclusion négative d'un organisme canadien de réglementation de la protection des renseignements personnels, au motif que les fins en sont inacceptables.
- Même les systèmes permettant ou facilitant l'identification de personnes qui sont peu fiables ou dont la qualité des sources est délibérément gardée au minimum peuvent être qualifiés de systèmes d'identification.

Conclusion

Comme nous l'avons mentionné, les grandes conclusions du rapport ne sont pas surprenantes. Qui plus est, le gouvernement fédéral et les gouvernements provinciaux auraient fort intérêt à tenir compte des activités analogues à celles de Clearview AI dans le cadre de leur réforme envisagée du cadre de la protection des renseignements applicable au secteur privé canadien. Étant donné la plus grande latitude qui pourrait être accordée à l'issue de ces réformes pour soutenir l'innovation bénéfique et, le cas échéant, la probabilité que des organismes en tirent parti, nous pouvons nous attendre à voir d'autres conclusions où les commissariats utiliseront le critère des fins acceptables pour restreindre certaines activités.

Énième fruit d'une tendance au sein des commissariats, le rapport reflète aussi le désir de ces derniers de présenter un front essentiellement uni pour ce qui est de leurs positions sur divers enjeux cruciaux. Ce phénomène est encourageant en ce qu'il jette les bases d'une harmonisation des directives dont pourraient particulièrement bénéficier les organisations au rayonnement national. Advenant que des provinces autres que l'Alberta, la Colombie-Britannique et le Québec décident ultérieurement d'encadrer eux-mêmes leurs propres secteurs privés, ces rapports conjoints deviendront en outre essentiels pour naviguer les méandres du droit canadien de la protection des renseignements personnels.

[1] Rapport, paragr. 72; voir également le communiqué du CPVP intitulé « Les pratiques illégales de Clearview AI représentent une surveillance de masse des Canadiens, selon les commissaires » du 3 février 2021.

[2] Rapport, paragr. 2.

[3] Hill, K. « The secretive company that might end privacy as we know it », *The New York Times*, 18 janvier 2020; Fan, K., « 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.

[4] « Toronto Police admit using secretive facial recognition technology Clearview AI », *CBC*, 13 février 2020; Gillis, W. et Allen, K., « Peel and Halton police reveal they too used controversial facial recognition tool », *The Toronto Star*, 14 février 2020; Allen, K. et al., « Facial recognition app Clearview AI has been used far more widely in Canada than previously known », *The Toronto Star*, 27 février 2020.

[5] Rapport, paragr. 35.

[6] Rapport, paragr. 43 à 48.

[7] Rapport de conclusions d'enquête en vertu de la LPRPDE no 2018-002 du CPVP, juin 2018.

[8] « Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la 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'Alberta et *CIPVP de la C.-B.*, paragr. 68.

[9] Rapport, paragr. 42.

[10] Rapport, paragr. 72.

[11] Rapport, paragr. 94 et 95, en référence à « 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.

[12] Rapport, paragr. 100.

[13] Rapport, paragr. 101.

[14] Rapport, paragr. 105.

[15] Projet de loi C-11, art. 51.

[16] Voir p. ex. Scassa, T., « How Might Bill C-11 Affect the Outcome of a Clearview AI-type Complaint? », 4 février 2021.

[17] Voir le « Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique »,février 2018, 42e législature, 1re session, p. 26 à 28.

[18] Projet de loi C-11, al. 18 (2)e).

[19] Projet de loi C-11, art. 12.

[20] Rapport, paragr. 89.

[21] Rapport, paragr. 76.

[22] Rapport, paragr. 73.

[23] Rapport, paragr. 23.

[24] Rapport, paragr. 24.

[25] Il est intéressant de noter qu'*A.T. c. Globe24h.com*, l'un des grands précédents dont l'analyse porte sur le référencement, n'a été cité qu'en vue d'établir si le cas de Clearview avait un lien réel et substantiel avec le Canada.

[26] Voir l'« Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la 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'Alberta et *CIPVP de la C.-B*.

[27] Voir « Biométrie :principes à respecter et obligations légales des organisations », *CAI*, juillet 2020.

Par

Max Jarvie

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels

---

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749