HALTE À LA SURVEILLANCE MASSIVE – LES COMMISSAIRES CANADIENS À LA PROTECTION DE LA VIE PRIVÉE CONCLUENT QUE LE DISPOSITIF DE RECONNAISSANCE FACIALE DE CLEARVIEW AI ENFREINT LES LOIS CANADIENNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Publié le 22 février, 2021

Catégories: Perspectives, Publications

Le 2 février 2021, le Commissaire à la protection de la vie privée du Canada (le « **CPVPC** ») et les commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique, de l'Alberta et du Québec (désignés collectivement les « **commissaires** ») ont publié leur rapport conjoint (le « **rapport** »), selon lequel une entreprise de technologie américaine, Clearview AI (« **Clearview** ») a enfreint les lois fédérale et provinciales sur la protection des renseignements personnels en recueillant des photos publiques diffusées en ligne de Canadiens à leur insu et sans leur consentement[1]. Clearview recueille ces images pour alimenter sa base de données de reconnaissance faciale, destinée à être utilisée par les organismes chargés de l'application de la loi, mais aussi par diverses autres organisations, y compris des entités du secteur privé.

Le rapport traite des graves préoccupations des commissaires à l'égard des activités de Clearview, qu'ils ont décrites comme « l'identification et la surveillance de masse » de Canadiens, y compris des mineurs[2]. Le rapport a clarifié la position des commissaires sur plusieurs questions clés, notamment l'application des lois canadiennes sur la protection des renseignements personnels aux entités étrangères, la nature des renseignements biométriques et le consentement requis pour l'utilisation de l'information publiée en ligne, notamment dans les médias sociaux. Le rapport établit une ligne de conduite raisonnablement claire pour les entreprises en ce qui concerne le consentement qui pourrait être requis, compte tenu de la possibilité que la technologie de reconnaissance faciale ou des technologies semblables soient utilisées dans le cadre d'activités commerciales, entre autres par des entreprises étrangères n'ayant pas de présence physique au Canada.

Contexte

Clearview a créé un logiciel de reconnaissance faciale qui permet aux utilisateurs de télécharger une image du visage d'une personne et de chercher des correspondances semblables dans la base de données de Clearview

à l'aide d'un algorithme de reconnaissance faciale. Clearview obtient les images contenues dans sa base de données par le « ratissage » de sites Web publics, dont Facebook, YouTube, Instagram et Twitter, et le stockage des photographies des personnes. Les données de Clearview ne contiennent aucune image protégée par des paramètres de confidentialité (par exemple, les comptes Instagram qui sont définis comme étant privés). Au total, Clearview a « 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 »[3]. Clearview affirme que ses services sont conçus pour répondre aux besoins d'application de la loi et d'enquête de ses clients, dont la GRC.

En février 2020, les commissaires ont lancé une enquête sur Clearview à la suite d'une importante controverse médiatique au sujet de la collecte et de l'utilisation alléguées de renseignements personnels par l'entreprise sans le consentement des personnes concernées[4]. En réaction à l'enquête, Clearview a cessé d'offrir ses services de reconnaissance faciale au Canada le 6 juillet 2020[5]. Le rapport expose les conclusions de l'enquête des commissaires.

Le rapport

Les commissaires ont conclu que Clearview avait enfreint les lois suivantes sur la protection des renseignements personnels (désignées collectivement, les « **lois** ») :

a. la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada (la « **LPRPDE**»);
b. la *Loi sur la protection des renseignements personnels dans le secteur privé* et la *Loi concernant le cadre juridique des technologies de l'information* du Québec (les « **lois du Québec**»);
c. la *Personal Information Protection Act* de la Colombie-Britannique (la « **PIPA de la C.-B.** »);
d. la *Personal Information Protection Act* de l'Alberta (la « **PIPA de l'Alb.**»).

Pour en arriver à cette conclusion, les commissaires ont examiné trois questions centrales :

a. Les lois fédérale et provinciales canadiennes sur la protection des renseignements personnels s'appliquaient-elles à Clearview?
b. Clearview a-t-elle obtenu les consentements nécessaires?
c. Les fins pour lesquelles Clearview a utilisé l'information étaient-elles appropriées, raisonnables ou légitimes dans les circonstances?

1. ***Les commissaires avaient-ils compétence sur Clearview?***

Clearview a soutenu que les lois ne s'appliquaient pas à elle, parce qu'elle n'avait pas de lien réel et substantiel avec le Canada. Clearview s'est appuyée sur le fait qu'elle était située aux États-Unis, que les services n'étaient

pas destinés aux Canadiens et que le contenu de la plateforme provenait de partout dans le monde. Sur le plan provincial, Clearview a fait valoir qu'elle ne faisait pas affaire avec l'Alberta, la Colombie-Britannique ou le Québec et qu'elle n'avait pas recueilli, utilisé ou communiqué de renseignements personnels dans ces provinces.

Les commissaires ont conclu que les lois s'appliquaient à Clearview pour plusieurs raisons. Clearview a activement commercialisé ses services auprès d'organismes canadiens et a déclaré publiquement, dans des déclarations aux médias, « que le Canada faisait partie de son marché principal »[6]. De plus, 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. Les commissaires ont plutôt constaté qu'il y avait des liens réels et substantiels parce qu'une partie importante des données de Clearview provenait de particuliers canadiens. Bien que le nombre exact d'images provenant de personnes vivant au Canada ne soit pas connu, l'ampleur du ratissage effectué par Clearview assure de manière quasi certaine que des millions d'images de personnes vivant au Canada ont été recueillies et utilisées pour établir des renseignements biométriques.

Les commissaires ont également conclu que les activités de Clearview relevaient de la compétence des lois provinciales sur la protection des renseignements personnels, puisque celles-ci s'appliquent à « tout organisme du secteur privé qui recueille, utilise et communique des renseignements sur des personnes dans la province concernée »[7]. Les commissaires ont constaté que 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. Le fait que Clearview n'avait pas de présence physique dans l'une ou l'autre de ces provinces n'était pas pertinent.

2. ***Clearview a-t-elle obtenu le consentement requis?***

Les commissaires ont constaté que les données recueillies par Clearview 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 », y compris des mineurs[8]. Par conséquent, Clearview devait obtenir le consentement exprès pour la collecte des images et la création de renseignements biométriques à partir de ces images. Les commissaires ont précisé que les renseignements biométriques sont de nature sensible dans presque toutes les circonstances parce qu'ils sont distinctifs, peu susceptibles de varier dans le temps et uniques à la personne, ce qui les lie à la personne de manière permanente.

Clearview a admis qu'elle n'avait pris aucune mesure pour obtenir le consentement exprès des personnes dont elle a obtenu les images, mais a soutenu qu'elle était exemptée de ces exigences parce que les renseignements étaient accessibles au public.

Les commissaires ont rejeté l'argument de Clearview et conclu que le consentement exprès était nécessaire

dans les circonstances. 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 »[9]. De plus, bien que la PIPA de la C.-B. et la PIPA de l'Alb. exemptent certaines sources d'information publique de l'obligation d'obtenir le consentement, ces lois n'accordent aucune exemption pour les médias sociaux et les sites de réseautage. De fait, les commissaires ont conclu que les médias sociaux diffèrent considérablement des autres publications désignées, comme les journaux ou les magazines, en partie en raison de la nature dynamique et changeante du contenu des médias sociaux et du contrôle direct que les personnes exercent sur leurs comptes de médias sociaux et leurs paramètres de confidentialité. De même, les commissaires ont déterminé que les renseignements personnels ne se voient pas accorder « un caractère public en vertu de la loi » du seul fait qu'ils sont « diffusés sur les réseaux sociaux ou le Web » et que ce contenu n'est pas non plus exempté de l'application des lois du Québec[10].
Par conséquent, toute collecte de renseignements dans les médias sociaux ou les sites de réseautage nécessitait un consentement exprès et devait s'effectuer à des fins raisonnablement appropriées.

3. ***Clearview a-t-elle agi à des fins acceptables, raisonnables ou légitimes?***

Les commissaires ont rejeté l'argument de Clearview selon lequel ses fins étaient acceptables du fait que les renseignements recueillis servaient à l'application de la loi et à la sécurité nationale. Les commissaires ont plutôt conclu que le « véritable objectif » de Clearview en recueillant ces renseignements s'apparentait plus à une opération commerciale à but lucratif qu'à l'application de la loi[11]. Cet objectif commercial n'était pas acceptable, raisonnable ou légitime s'il visait « l'identification et la surveillance de masse de personnes » au moyen de la technologie de Clearview[12]. La surveillance et les renseignements biométriques de Clearview sont souvent utilisés au détriment de la personne à cause des risques de poursuite, d'embarras ou d'enquête auxquels elle s'expose. Il s'ensuit un risque de préjudice grave aux individus dont les images sont recueillies, y compris les préjudices associés à une erreur d'identification ou à d'éventuelles atteintes à la sécurité des données. L'objectif commercial de Clearview ne pouvait justifier la collecte massive de renseignements de nature très délicate vraisemblablement préjudiciables pour les personnes surveillées.

Autres préoccupations

Les commissaires ont également soulevé d'autres préoccupations qu'ils ont jugées importantes, mais sur lesquelles ils ne se sont pas prononcés.

Ils ont exprimé des préoccupations importantes au sujet de l'exactitude de la technologie de reconnaissance faciale, en particulier quant au risque d'erreur d'identification. Les commissaires ont fait référence à des études démontrant que ces technologies entraînent souvent des erreurs d'identification chez les personnes de couleur, en particulier les femmes. Dans certains cas, le taux de faux positifs était de 10 à 100 fois plus élevé que

chez les personnes de race blanche. Ces personnes sont ainsi exposées à un risque important de traitement discriminatoire, particulièrement dans le contexte de l'application de la loi, où les faux positifs peuvent faire l'objet de sanctions criminelles injustifiées.

De plus, les commissaires ont noté que Clearview avait 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 renseignements. Les commissaires ne se sont pas prononcés sur le fait que ces violations contractuelles se soient produites ou non, mais ils ont conclu que de telles violations constituaient un facteur pertinent pour examiner le caractère inapproprié de la conduite de Clearview.

Les commissaires ont également constaté que le volume important de renseignements de nature très délicate conservés par Clearview en faisait une cible probable pour les atteintes à la sécurité des données; de fait, Clearview a fait l'objet, durant la seule année 2020, de deux fuites à l'endroit de sa liste de clients, de son code source et de la vidéo de son projet pilote.

Recommandations

Les commissaires ont recommandé à Clearview de :

a. cesser d'offrir ses services de reconnaissance faciale à des clients au Canada;
b. 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;
c. supprimer les images et les matrices faciales biométriques recueillies auprès d'individus au Canada.

Bien que Clearview ait volontairement quitté le marché canadien en juillet 2020, l'entreprise a refusé d'accepter les conclusions et les recommandations du rapport des commissaires. Si Clearview continue de rejeter les recommandations des commissaires, ceux-ci ont indiqué qu'ils intenteront d'autres poursuites judiciaires pour amener l'entreprise à s'y conformer.

Quelles seront les répercussions du rapport?

Les commissaires ont adopté une position ferme à l'égard de l'utilisation du contenu en ligne, y compris le contenu des médias sociaux, par des entreprises tierces à des fins commerciales. Ils ont conclu qu'une entreprise n'a pas le droit d'utiliser ce contenu comme bon lui semble simplement parce qu'elle a trouvé ce contenu en ligne. La nature dynamique, en temps réel et axée sur l'utilisateur des médias sociaux les rend fondamentalement différents des autres formes de communication accessibles au public et exemptes de consentement. Une entreprise commerciale ne peut utiliser les médias sociaux qu'avec le consentement exprès de la personne visée par le contenu et seulement dans un but raisonnable et approprié. Par conséquent, toute entreprise qui cherche à exploiter un commerce en ligne et qui désire utiliser du contenu

généralement accessible en ligne par l'entremise de sites de médias sociaux ou autrement et pouvant être classé comme des renseignements personnels devra prendre des mesures claires pour obtenir le consentement exprès de l'utilisateur avant de s'approprier le contenu à ses propres fins. Compte tenu de la décision des commissaires et de leurs motifs exprimés dans le rapport, toute autre entreprise aura de la difficulté à affirmer qu'elle a le droit de recueillir des renseignements de cette nature.

Le rapport clarifie également la position des commissaires par rapport aux données biométriques et aux logiciels de reconnaissance faciale. Ces types de technologies peuvent faire des choses étonnantes, mais elles risquent aussi de contrevenir facilement aux lois sur la protection des renseignements personnels en raison de la nature potentiellement intrusive de leur fonctionnalité. Par conséquent, les commissaires se sont appuyés sur la décision du CPVPC et des commissaires de l'Alberta et de la Colombie-Britannique dans l'affaire Cadillac Fairview, selon laquelle Cadillac Fairview devait obtenir le consentement exprès de ses clients pour recueillir, utiliser et communiquer leurs renseignements biométriques obtenus au moyen d'un logiciel de reconnaissance faciale[13]. Les commissaires ont clairement exprimé leur position selon laquelle les renseignements biométriques sont de nature très délicate et qu'en conséquence, toute entité cherchant à recueillir, à utiliser ou à traiter autrement ces renseignements doit examiner sérieusement les mesures à prendre pour obtenir le consentement exprès des personnes touchées avant de les recueillir. Le défi consiste bien entendu à déterminer comment une entreprise est capable d'obtenir, par des moyens pratiques et réalisables, le consentement de milliers, voire de millions de personnes qu'elle n'est légitimement pas en mesure de contacter, avant de recueillir les renseignements à leur sujet. Les commissaires se sont prononcés très clairement à ce sujet, de sorte que toute entreprise souhaitant utiliser cette technologie à grande échelle devra évaluer les mesures à sa disposition pour se conformer à la décision des commissaires dans l'affaire Clearview.

Enfin, les entreprises étrangères doivent reconnaître que le simple fait de ne pas avoir d'emplacement ou de présence physique au Canada pour leurs activités ne les met pas à l'abri des lois canadiennes sur la protection des renseignements personnels. La LPRPDE s'applique aux organisations de l'extérieur du Canada qui ont un « lien réel et substantiel » avec le Canada, et le CPVPC tiendra compte de plusieurs facteurs pour déterminer si ce critère est respecté[14]. La PIPA de l'Alb., la PIPA de la C.-B. et les lois du Québec s'appliquent aux organisations qui recueillent des renseignements personnels sur les personnes vivant dans ces provinces. Par conséquent, les entreprises étrangères devront examiner attentivement si les activités qu'elles se proposent de mener, en ligne ou autrement, peuvent être assujetties aux lois.

Toute entreprise, canadienne ou étrangère, qui envisage de faire affaire au Canada dans un domaine comme la reconnaissance faciale et dont les activités risquent de porter atteinte aux droits des Canadiens en matière de protection des renseignements personnels serait bien avisée d'examiner soigneusement et stratégiquement la

meilleure façon de mener ces activités au Canada, que ce soit par l'obtention du consentement des personnes concernées ou autrement, et de reconnaître qu'elle sera probablement visée par les lois canadiennes sur la protection des renseignements personnels telles qu'elles sont actuellement établies.

[1] *Rapport de conclusions d'enquête en vertu de la LPRPDE n° 2021-001* (2020) (Commissaire à la protection de la vie privée du Canada) [le « **rapport** »].
[2] *Ibid* à « Aperçu ».
[3] *Ibid.*
[4] Commissariat à la protection de la vie privée du Canada, Annonce, « Des commissaires lancent une enquête conjointe sur Clearview AI dans un contexte de préoccupations croissantes quant à l'utilisation de la technologie de reconnaissance faciale » (21 février 2020).
[5] Commissariat à la protection de la vie privée du Canada, Communiqué, « Clearview AI cesse d'offrir sa technologie de reconnaissance faciale au Canada » (6 juillet 2020).
[6] Rapport, *supra* note 1, paragraphe 29 i.
[7] *Ibid*, au paragraphe 33.
[8] *Ibid*, au paragraphe 74.
[9] *Ibid*, au paragraphe 45.
[10] *Ibid*, au paragraphe 46.
[11] *Ibid*, au paragraphe 88.
[12] *Ibid*, au paragraphe 76.

[13] *Rapport de conclusions d'enquête en vertu de la LPRPDE n° 2020-004* (2020) (Commissaire à la protection de la vie privée du Canada).
[14] Rapport, *supra* note 1, au paragraphe 28.

par Robert Piasentin, Grace Shaw et Julianna Ivanyi (étudiante en droit)

Mise en garde