AU-DELÀ DES FRONTIÈRES : UNE COUR DE LA COLOMBIE-BRITANNIQUE REND UNE DÉCISION PHARE SUR L'APPLICATION JURIDICTIONNELLE DE LA *PERSONAL INFORMATION PROTECTION ACT*

Publié le 13 janvier, 2025

Catégories: Perspectives, Publications

Dans une décision très attendue qui pourrait avoir des répercussions dans d'autres juridictions, la Cour suprême de la Colombie-Britannique a donné des indications claires sur l'application aux organisations étrangères de la *Personal Information Protection Act*, SBC 2003, ch. 63 (« **PIPA de la C.-B.** »).

Dans l'arrêt *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, la Cour a confirmé l'ordonnance du bureau du commissaire à l'information et à la protection de la vie privée (Office of the Information and Privacy Commissioner) (« **OIPC** ») à l'encontre de Clearview AI Inc. (« **Clearview** »), une société de reconnaissance faciale basée aux États-Unis, en lien avec des infractions à la PIPA de la C.-B. que cette société a commises[1].

La décision de la Cour a établi que la PIPA de la C.-B. s'applique aux organisations situées à l'extérieur de la Colombie-Britannique (« **C.-B.** ») qui ont un [traduction] « lien réel et substantiel » avec cette province. Bien que cette conclusion semble soutenir une analyse contextuelle semblable au critère appliqué lors de l'examen de l'application de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (« **LPRPDE** ») du gouvernement fédéral à des organisations situées en à l'extérieur du Canada, la Cour de la C.-B. a exprimé qu'un lien suffisant peut être établi aux fins de la PIPA de la C.-B. simplement en recueillant des données de personnes en C.-B. au moyen de l'Internet[2].

Contexte général

Clearview exploite un système de reconnaissance faciale qui extrait des images accessibles au public dans les médias sociaux et d'autres plateformes en ligne, et les convertit ensuite en identifiants biométriques. Clearview vend des logiciels aux services de police et aux entités du secteur privé. Ces logiciels leur permettent de mettre en correspondance des visages et des images contenues dans la base de données biométriques interrogeable de Clearview. Au moment où les activités de Clearview ont été portées à l'attention des autorités de protection

de la vie privée du Canada, la société avait recueilli plus de trois milliards d'images faciales, y compris celles de personnes en C.-B., sans leur consentement. Selon le site Web de Clearview, sa base de données contient plus de 50 milliards d'images faciales recueillies sur Internet (en moyenne six par personne sur la planète)[3].

En 2020, le Commissariat à la protection de la vie privée du Canada (**CPVP**), l'OIPC et les commissaires à la protection de la vie privée de l'Alberta et du Québec ont enquêté sur Clearview pour violations des lois canadiennes sur la protection de la vie privée. Cette enquête a donné lieu à un rapport d'enquête conjointe (le « **Rapport d'enquête conjointe** »). Ce rapport a indiqué que Clearview avait enfreint les lois canadiennes sur la protection des renseignements personnels dans le secteur privé et a formulé des recommandations précises pour que Clearview respecte ces lois[4].

La même année, Clearview a volontairement cessé d'offrir ses services aux utilisateurs canadiens. Cependant, la société a laissé entendre que c'était une mesure temporaire et qu'elle continuait à recueillir et à stocker des images de Canadiens[5].

L'ordonnance de l'OIPC

En 2021, l'OIPC a rendu une ordonnance qui imposait à Clearview de se conformer aux recommandations du Rapport d'enquête conjointe. Les autorités de protection de la vie privée de l'Alberta et du Québec ont rendu des ordonnances semblables dans leur propre province. Plus précisément, l'ordonnance de l'OIPC exigeait de Clearview qu'elle[6] :

1. cesse d'offrir ses services de reconnaissance faciale en C.-B.;
2. mette tout en œuvre pour cesser de recueillir, d'utiliser ou de communiquer des images et des données de reconnaissance faciale de personnes en C.-B. sans leur consentement;
3. mette tout en œuvre pour supprimer les portraits et les données de reconnaissance faciale précédemment recueillies auprès de personnes en C.-B. sans leur consentement.

Clearview a contesté l'ordonnance de l'OIPC en faisant valoir qu'elle n'était pas soumise à la PIPA de la C.-B. parce qu'elle n'exerçait pas d'activités commerciales dans cette province. Clearview a notamment mis l'accent sur le fait qu'elle n'a pas d'employés, de bureaux ou de serveurs en Colombie-Britannique.

À titre subsidiaire, Clearview a fait valoir que l'ordonnance devrait être annulée pour les raisons suivantes : i) les renseignements personnels recueillis à partir de sources en ligne étaient [traduction] « accessibles au public » en vertu de la PIPA de la C.-B. et des règlements connexes et, par conséquent, Clearview n'avait pas besoin de consentement pour les recueillir; ii) contrairement aux conclusions du Rapport d'enquête conjointe, une personne raisonnable considérerait que l'objectif de Clearview pour la collecte, l'utilisation et la communication des renseignements personnels était approprié eu égard aux circonstances; et iii) l'ordonnance de l'OIPC

n'était pas nécessaire et n'avait pas force exécutoire[7].

Les conclusions de la Cour

Le critère de la compétence extraterritoriale

Dans le Rapport d'enquête conjointe, les organismes de réglementation ont adopté la position selon laquelle les lois provinciales sur la protection de la vie privée, y compris la PIPA de la C.-B., s'appliquent à toute organisation du secteur privé qui recueille, utilise et communique des renseignements sur des personnes dans la province concernée[8]. Leur conclusion selon laquelle le lieu où se trouvent les personnes concernées est déterminant indique que les lois provinciales sur la protection de la vie privée ont une portée plus large que la loi fédérale sur la protection de la vie privée, puisque le CPVP et les tribunaux reconnaissent depuis longtemps que la LPRPDE ne s'applique que si l'organisation a un [traduction] « lien réel et substantiel » avec le Canada[9].

Toutefois, il ne semble pas que l'OIPC ait fait valoir cette compétence étendue auprès de la Cour dans le cadre du contrôle judiciaire. Les parties ont plutôt convenu que le critère du [traduction] « lien réel et substantiel » est le critère approprié pour déterminer si la loi de réglementation provinciale est constitutionnellement applicable aux parties hors province[10]. Cette approche reflète en fait celle utilisée par le CPVP et la Cour fédérale au moment de déterminer si la LPRPDE s'applique[11]. Par conséquent, il est maintenant clair que l'application des lois fédérales et de la C.-B. sur la protection de la vie privée exige une analyse contextuelle du lien de l'organisation avec les territoires de compétences pertinents.

Application du critère à Clearview

La Cour était d'accord avec l'OIPC que Clearview est soumis à la PIPA de la Colombie-Britannique. La décision présente une longue analyse dans laquelle elle note que Clearview[12] :

- a fourni ses services à des entités en C.-B., y compris aux forces de l'ordre de la C.-B.;
- a exercé des activités commerciales et de marketing en C.-B.;
- a recueilli, utilisé et communiqué des renseignements concernant des personnes en Colombie-Britannique.

La prise en compte de tous ces facteurs est conforme à l'approche adoptée par les tribunaux et le CPVP lors de l'évaluation de l'application de la LPRPDE à des organisations situées à l'étranger. Cependant, la Cour de la C.-B. ne s'est pas arrêtée à cette analyse. Dans une remarque incidente, la Cour a indiqué que, même si Clearview ne commercialisait pas ou ne fournissait pas ses services en C.-B., l'acte de collecte, d'utilisation et de communication de renseignements personnels de personnes en C.-B., recueillis sur Internet, créerait à lui seul un lien suffisant avec la C.-B. pour que la PIPA de la C.-B. s'applique[13].

La Cour a également tranché que les principes d'ordre et d'équité justifiaient l'application de la PIPA de la C.-B. à Clearview, étant donné que :

1. les questions liées à la protection de la vie privée dépassent de plus en plus les frontières et (à l'instar de la réglementation des valeurs mobilières) l'autorité réglementaire multiterritoriale [traduction] « […] favorise une protection ininterrompue de la réglementation et l'imposition de mesures correctives d'intérêt public dans l'ensemble des territoires touchés par un stratagème illégal unique[14] »;
2. l'application de la PIPA de la C.-B. à Clearview n'a rien d'injuste puisque la société a choisi d'entrer sur le marché de la C.-B., de faire de la publicité pour son produit auprès des organismes d'application de la loi de la C.-B. et d'extraire des données d'Internet qui comprennent des renseignements personnels sur des habitants de cette province[15].

Enfin, il convient de noter que, dans cette affaire, la Cour a jugé que la PIPA de la C.-B. ne s'appliquait pas uniquement aux renseignements personnels concernant les résidents de la Colombie-Britannique. Elle régit également la conduite des organisations qui recueillent des renseignements personnels sur des personnes ayant un lien direct avec la C.-B., qu'il soit temporaire ou permanent. Par conséquent, l'OIPC a été habilité à rendre des ordonnances concernant des renseignements personnels sur des personnes en C.-B., que ces personnes résident dans la province ou la visitent temporairement[16].

Autres points saillants

1. **Renseignements auxquels le public a accès :** la Cour a rejeté l'argument de Clearview selon lequel elle n'avait pas besoin de consentement pour recueillir, utiliser et communiquer les renseignements personnels extraits de sites Web publics, puisque ces renseignements étaient un renseignement [traduction] « auquel le public a accès ». Bien que la PIPA de la C.-B. prévoie certaines exemptions aux exigences de la loi en matière de consentement en ce qui concerne les renseignements auxquels le public a accès à partir d'une source prévue par règlement, la Cour a convenu avec l'OIPC que ces exemptions devaient être interprétées de manière restrictive. En particulier, bien que le consentement ne soit pas nécessaire pour recueillir, utiliser et communiquer des « publications » accessibles au public (comme les journaux, les livres et les magazines), cette exemption **ne s'applique pas** à tout le contenu affiché sur des blogues publics, des médias sociaux publics et d'autres sites Web[17]. Encore une fois, cette conclusion est semblable à l'approche adoptée par le CPVP et les tribunaux lorsqu'ils interprètent l'exemption relative au renseignement « auquel le public a accès » prévue par la LPRPDE[18].
2. **Objectif raisonnable :** la Cour a confirmé la décision de l'OIPC selon laquelle Clearview n'avait pas de [traduction] « but raisonnable » pour recueillir, utiliser et communiquer des renseignements personnels. En particulier, la Cour a souligné les risques de dommages importants pour les personnes, y compris le

potentiel de résultats inexacts de la reconnaissance faciale et d'atteintes à la protection de données[19].

3. **Validité de l'ordonnance :** la Cour a rejeté les arguments de Clearview selon lesquels l'ordonnance de l'OIPC était inutile, trop large ou inapplicable. La Cour a conclu que l'ordonnance était nécessaire et conforme aux objectifs de la PIPA de la C.-B., à savoir la protection des renseignements personnels et des droits individuels. En se fondant sur des déclarations faites par Clearview dans une procédure judiciaire distincte en Illinois, elle a également estimé que Clearview était en mesure de [traduction] « mettre tout en œuvre » pour cesser de recueillir les renseignements personnels de la CB et pour supprimer les données qui proviennent de la C.-B. qu'elle a précédemment recueillies[20].

Importance de la décision

Cette décision renforce la jurisprudence existante qui indique clairement que les lois sur la protection de la vie privée en vigueur au Canada peuvent s'appliquer à des organisations situées à l'extérieur du pays ou de la province concernés. Bien que cette décision ne soit pas contraignante pour les tribunaux ou les autorités de réglementation des autres provinces, elle s'appuie sur la jurisprudence de la Cour suprême du Canada qui serait également applicable dans d'autres provinces et territoires. Par conséquent, il est fort possible qu'une analyse semblable soit effectuée pour évaluer l'application de la *Personal Information Protection Act* de l'Alberta et de la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec.

Les organisations du Canada et du monde entier devraient envisager l'application du critère du [traduction] « lien réel et substantiel » et évaluer si leurs activités sont soumises aux lois fédérales et provinciales sur la protection de la vie privée et si elles s'y conforment. Notamment, les organisations situées à l'étranger doivent tenir compte du contexte réglementaire et juridique plus large qui s'applique à la reconnaissance faciale et aux technologies de récupération de données, y compris les définitions étroites de renseignement personnel « auquel le public a accès » dans les lois canadiennes pertinentes. Ne pas en tenir compte peut entraîner des coûts importants et avoir des répercussions sur les activités d'une société, comme l'a montré la Cour dans cette affaire lorsqu'elle a confirmé les ordonnances de l'OIPC interdisant effectivement à Clearview d'offrir ses services en C.-B. et obligeant la société à suivre une procédure potentiellement coûteuse pour établir une barrière virtuelle pour sa collecte de données et purger les données de la Colombie-Britannique.

L'équipe expérimentée de McMillan en matière de protection des données et de la vie privée peut aider les organisations à effectuer une analyse juridictionnelle approfondie et aider les entreprises à comprendre leurs obligations prévues par les lois canadiennes sur la protection de la vie privée.

--

Bulletins connexes :

- *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*
- *Clearview AI sommée de suivre les recommandations d'organismes de réglementation provinciaux sur la protection de la vie privée*
- *Protection de la vie privée : plusieurs pays publient une déclaration commune sur l'extraction de données*

[1] *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311 (en anglais) [***Clearview v. OIPC***].
[2] *Clearview v. OIPC*, par. 90.
[3] Clearview AI, « Overview », Clearview AI (date inconnue), en ligne (en anglais).
[4] Commissariat à la protection de la vie privée du Canada, *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* (février 2021), par. 111 et 118 [**Rapport d'enquête conjointe**].
[5] *Clearview v. OIPC*, par. 2.
[6] OIPC, *Order P21-08* (14 décembre 2021).
[7] *Clearview v. OIPC*, par. 4.
[8] Rapport d'enquête conjointe, par. 33.
[9] Rapport d'enquête conjointe, par. 28.
[10] *Clearview v. OIPC*, par. 70-75.
[11] *T. c. Globe24h.com*, 2017 CF 114; *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, par. 54-63 et les autres documents qui y sont cités.
[12] *Clearview v. OIPC*, par. 76 et 81.
[13] *Clearview v. OIPC*, par. 90-102.
[14] *Clearview v. OIPC*, par. 105, citant *Sharp c. Autorité des marchés financiers*, 2023 CSC 29, par. 134.
[15] *Clearview v. OIPC*, par. 107.
[16] *Clearview v. OIPC*, par. 289-291.
[17] *Clearview v. OIPC*, par. 164.
[18] Voir, par exemple, le Rapport d'enquête conjointe, par. 45; *T. c. Globe24h.com*, 2017 CF 114, par. 77.
[19] *Clearview v. OIPC*, par. 257.
[20] *Clearview v. OIPC*, par. 267, 270-273, 279 et 292.

Par Lyndsay Wasser, Kristen Pennington, Robbie Grant, Gary Preteau (stagiaire en droit)

Mise en garde