Vol. 36, nº 1 & 2

Décisions marquantes de l'année 2023 en matière de vie privée et de protection des renseignements personnels

Julie Uzan-Naulin, Soleïca Monnier, Iara Griffith et Alexander J. Shapiro*

RÉSUMÉ / ABSTRACT 167

INTRODUCTION 169

1. ATTEINTES À LA VIE PRIVÉE ET DOMMAGES-INTÉRÊTS : LES AFFAIRES *CHAREST* ET *GOOGLE* 170

1.1 La vie privée et les dommages-intérêts font-ils bon ménage ? 170

1.2 L'affaire *Charest* 172

1.2.1 Contexte 172

1.2.2 Décision 174

1.2.3 Observations 174

a) L'UPAC n'a pas protégé adéquatement les renseignements personnels 174

* Les auteurs sont avocats au bureau de Montréal de Fasken. Les opinions exprimées dans cet article sont celles des auteurs et peuvent ou non être partagées par Fasken ou ses clients.

La recherche jurisprudentielle est à jour en date du 29 avril 2024.

[Note : cet article a été soumis à une évaluation à double anonymat.]

b) Un régime de dommages-intérêts sous stéroïdes 176

1.3 L'affaire *Google* 177

1.3.1 Contexte 177

1.3.2 Décision 179

1.3.3 Observations 180

2. UTILISATION DE LA GÉNÉALOGIE GÉNÉTIQUE COMMERCIALE À DES FINS D'EXPULSION : L'AFFAIRE *ASFC* 183

2.1 Contexte 183

2.2 Décision 184

2.2.1 Le lien direct entre la mesure de renvoi et la collecte 184

2.2.2 Là où le bât blesse : la validité du consentement 185

2.2.3 Attention aux recours à des services commerciaux de tiers 186

2.3 Observations 187

2.3.1 Absence de test de nécessité dans la LPRP 187

2.3.2 L'*autorisation* est-elle un consentement ? 189

2.3.3 Une ÉFVP est-elle requise ? 191

3. COMMUNICATION DE RENSEIGNEMENTS PERSONNELS SANS CONSENTEMENT : LES AFFAIRES *CAMBRIDGE ANALYTICA* ET *HOME DEPOT* 191

3.1 L'affaire *Cambridge Analytica* 192

3.1.1 Contexte 192

a) L'enquête conjointe des commissaires 192

b) La décision de la Cour fédérale 193

i. La nature du recours 194

ii. L'obligation d'obtenir un consentement valable 195

iii. L'obligation de protéger les renseignements personnels 196

3.1.2 Observations 198

a) L'importance de la preuve 198

b) La possession (ou détention) juridique et le principe de responsabilité 198

3.2 L'affaire *Home Depot* 202

3.2.1 Contexte 202

a) L'obligation d'obtenir un consentement 203

b) La forme du consentement 203

3.2.2 Observations 204

4. DEMANDE D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS ET RISQUES IDENTIFICATOIRES : L'AFFAIRE *SHIAB* 207

4.1 Contexte 207

4.1.1 La demande d'accès en cause 207

4.1.2 La précédente demande d'accès 210

4.1.3 Décision 210

4.2 Observations 212

4.2.1 La notion de risques identificatoires 212

4.2.2 La distinction entre l'anonymisation et la dépersonnalisation 213

4.2.3 La décision *Shiab* au regard du *Règlement sur l'anonymisation* 215

CONCLUSION 216

RÉSUMÉ

Cet article examine et commente les décisions marquantes de l'an 2023 rendues par la Cour supérieure, la Cour fédérale et d'autres instances administratives quant au respect de la vie privée et la protection des renseignements personnels. Ces décisions touchent à la diffusion de contenus diffamatoires en ligne, à l'utilisation et la communication de renseignements personnels à des fins d'expulsion, de prospection commerciale et de profilage politique, ainsi qu'à l'analyse de risques identificatoires.

MOTS-CLÉS

Droit à la vie privée – Droit à la réputation – Responsabilité civile – Responsabilité des intermédiaires – Dommages-intérêts punitifs – LCCJTI – Loi 25 – Généalogie génétique commerciale – Consentement – Nécessité – Communication de renseignements personnels – Portée de l'obligation de protection – Renseignements personnels sensibles – Attentes raisonnables – Anonymisation – Dépersonnalisation – Risques identificatoires

ABSTRACT

In this article, the authors examine and comment on the landmark decisions of 2023 issued by the Superior Court, the Federal Court and other administrative bodies regarding privacy and the protection of personal information. These decisions touch on the dissemination of defamatory content online, the use and communication of personal information for expulsion purposes, commercial prospecting and political profiling, as well as identification risk analysis.

KEY WORDS

Right to privacy – Right to reputation – Civil liability – Liability of intermediaries – Punitive damages – ALFIT – Law 25 – Commercial genetic genealogy – Consent – Necessity – Disclosure of personal information – Scope of security obligations – Sensitive personal information – Reasonable expectations – Anonymization – Deidentification – Identifying risks

INTRODUCTION

À l'intersection des droits individuels et du progrès technologique, la protection de la vie privée préoccupe les citoyens branchés que nous sommes. À la fois sujet complexe et domaine effervescent, elle soulève de nombreux enjeux juridiques, éthiques et économiques.

À même la vague qui déferle depuis l'Europe[1], le Québec est la première province canadienne à lancer une réforme de ses lois sur la vie privée. Il va sans dire, 2023 est une année charnière. En effet, elle marque l'entrée en vigueur des principaux changements introduits par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ci-après « Loi 25 »)[2]. Celle-ci apporte des changements importants à la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « Loi sur le privé »)[3] et à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « Loi sur l'accès »)[4]. Du côté du gouvernement fédéral, on attend toujours la mise à jour de la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « LPRPDE »)[5], ressuscitée via le projet de loi C-27[6], qui prévoit notamment la création d'un tribunal sur la protection des renseignements personnels et des données et une nouvelle loi pour encadrer l'utilisation de l'intelligence artificielle.

Dans ce contexte, les tribunaux et les commissariats à la protection de la vie privée ont rendu d'importantes décisions. Même

---

1. Avec le *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »).
2. L.Q. 2021, c. 25 (ci-après « Loi 25 »).
3. RLRQ, c. P-39.1 (ci-après « Loi sur le privé »).
4. RLRQ, c. A-2.1 (ci-après « Loi sur l'accès »).
5. L.C. 2000, c. 5 (ci-après « LPRPDE »).
6. *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, projet de loi nº C-27 (1re lecture – 16 juin 2022), 1re sess., 44e légis. (Can.); voir aussi *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois,* projet de loi nº C-26 (1re lecture – 14 juin 2022), 1re sess., 44e légis. (Can.).

avant l'entrée en vigueur de nouveaux mécanismes prévus à la Loi 25, la Cour supérieure a accordé des dommages-intérêts compensatoires et punitifs importants pour des atteintes à la vie privée et à la réputation entourant la diffusion de contenu diffamatoire. La Cour fédérale s'est penchée sur la portée des exigences de consentement et de protection prévues à la LPRPDE, tandis que le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») a enquêté sur des pratiques mettant en cause l'absence de consentement éclairé, d'une part, dans le cadre de la communication de renseignements personnels à des fins de prospection commerciale et, d'autre part, pour l'utilisation d'outils de généalogie génétique commerciale par des institutions fédérales. Enfin, au Québec, la Commission d'accès à l'information (ci-après « CAI ») a abordé les risques identificatoires susceptibles de compromettre la confidentialité de renseignements visés par une demande d'accès. Cet article examine ces décisions et offre des pistes de réflexion quant à leur pertinence pour le domaine du droit à la vie privée au Canada.

1. ATTEINTES À LA VIE PRIVÉE ET DOMMAGES-INTÉRÊTS : LES AFFAIRES *CHAREST* ET *GOOGLE*

1.1 La vie privée et les dommages-intérêts font-ils bon ménage ?

En droit civil, une personne peut engager sa responsabilité lorsqu'elle commet une (i) faute, (ii) causant un préjudice, et lorsqu'il existe un (iii) lien de causalité entre la faute et le préjudice[7]. Ce principe est consacré dans le *Code civil du Québec* (ci-après « C.c.Q. ») en matière extracontractuelle[8].

Une victime peut aussi demander qu'on lui accorde des dommages-intérêts dans le but de punir le comportement malveillant et répréhensible d'un tiers[9], soit des dommages-intérêts « punitifs » ou « exemplaires », à condition qu'une loi ne le prévoie expressément[10].

---

7. Jean-Louis BAUDOUIN et Yvon RENAUD, *Code civil du Québec annoté*, Montréal, Wilson & Lafleur, 2023, art. 1457, en ligne : <https://edoctrine.caij.qc.ca/wilson-et-lafleur-ccq-annote/ccqa-2023/ccqa-2023-presentation>.
8. RLRQ, c. C-1991 (ci-après « C.c.Q. »), art. 1457.
9. *Fillion* c. *Chiasson*, 2007 QCCA 570, nº 53.
10. C.c.Q., préc., note 8, art. 1621 ; le régime le plus populaire est celui de l'article 49 de la *Charte des droits et libertés de la personne*, RLRQ, c. C-12 (ci-après « Charte »), qui prévoit la possibilité de demander l'octroi de dommages-intérêts punitifs en cas d'atteinte illicite et intentionnelle.

La violation d'un droit protégé par la *Charte des droits et libertés de la personne* (ci-après « Charte »), y compris le droit à la vie privée[11], constitue souvent une faute[12]. Cependant, la preuve d'un préjudice indemnisable demeure compliquée, car beaucoup banalisent les atteintes à la vie privée – bourreaux comme victimes[13]. Ce constat justifie d'ailleurs la popularité croissante des régimes de sanctions administratives pécuniaires (ci-après « SAP ») et des régimes pénaux, par exemple, au Québec via la Loi 25, et en Europe avec le RGPD. En effet, ces régimes n'exigent pas de faire la preuve d'un préjudice ; le comportement fautif de l'organisation ou de l'un de ses préposés suffit pour engager sa responsabilité.

Les lois des secteurs public[14] et privé[15] complètent le régime de droit commun quant aux dommages-intérêts punitifs. En effet, elles permettent l'octroi de tels dommages-intérêts pour toute atteinte illicite au droit à la vie privée, une hypothèse déjà prévue par la Charte[16], mais aussi lorsque l'atteinte résulte d'une faute lourde[17] :

> Lorsqu'une atteinte illicite à un droit conféré par la présente loi ou par les articles 35 à 40 du Code civil cause un préjudice et que cette atteinte est intentionnelle ou résulte d'une faute lourde, le tribunal accorde des dommages-intérêts punitifs d'au moins 1 000 $.[18] (Nos soulignements)

---

11. Charte, préc., note 10, art. 5 ; C.c.Q., préc., note 8, art. 3, 35-37.
12. *Imperial Tobacco Canada ltée* c. *Conseil québécois sur le tabac et la santé*, 2019 QCCA 358 ; *Béliveau St-Jacques* c. *Fédération des employées et employés de services publics inc.*, [1996] 2 R.C.S. 345 ; *Droit de la famille – 22187*, 2022 QCCS 377.
13. « Les compagnies doivent comprendre qu'elles ne devraient pas banaliser l'utilisation des renseignements personnels. […] Ces exemples nous rappellent le travail qu'il reste à faire pour favoriser une culture où la protection de la vie privée est le paramètre par défaut et où les Canadiennes et les Canadiens ont le réflexe de toujours demander pourquoi leurs renseignements personnels sont demandés », dans CPVP, « Le droit à la vie privée : un droit fondamental à l'ère numérique » (10 mars 2023), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2023/sp-d_20230224/> (consulté le 23 mars 2024).
14. Loi sur l'accès, préc., note 4, art. 167.
15. Loi sur le privé, préc., note 3, art. 93.1.
16. Sébastien BEAUREGARD et Lukasz GRANOSIK, « Les renseignements personnels et la responsabilité civile : à quel prix ? », dans Service de la formation permanente, Barreau du Québec, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels – les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, Montréal, Éditions Yvon Blais, 2012, p. 52-53, en ligne : <https://edoctrine.caij.qc.ca/developpements-recents/358/368100902>.
17. C.c.Q., préc., note 8, art. 1474 al. 1 : « […] la faute lourde est celle qui dénote une insouciance, une imprudence ou une négligence grossières. »
18. Loi sur le privé, préc., note 3, art. 93.1, qui reprend essentiellement le libellé de l'art. 167 de la Loi sur l'accès.

Des dommages-intérêts additionnels peuvent donc être octroyés selon ces dispositions, en plus du régime prévu à la Charte, lequel exige une atteinte illicite et intentionnelle. Le législateur a cru pertinent de fixer un montant minimal de 1 000 $, soulignant l'objectif dissuasif du régime[19]. Au contraire des SAP que la CAI peut imposer dans le secteur privé, seuls les tribunaux de droit commun ont compétence pour accorder des dommages-intérêts compensatoires ou punitifs.

Les recours pour atteinte à la réputation, similaires au recours pour atteinte à la vie privée[20], sont les rares à justifier des dommages-intérêts en jurisprudence. En 2023, deux décisions importantes méritent une attention particulière.

1.2 L'affaire *Charest*

Dans la décision *Charest*[21], la Cour supérieure impose des dommages-intérêts punitifs de 350 000 $ en application de la Loi sur l'accès, rejetant la réclamation en dommages punitifs basée sur une violation de la Charte. Elle impose également des dommages-intérêts compensatoires de 35 000 $.

1.2.1 Contexte

Cette affaire s'inscrit dans la foulée des fuites de renseignements liées à des enquêtes policières sur la collusion au sein de l'industrie de la construction.

Le demandeur est premier ministre de 2003 à 2012, à titre de chef du Parti libéral du Québec (ci-après « PLQ »). Sous sa gouverne, le PLQ lance la Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction, aussi appelée la commission Charbonneau.

L'Unité permanente anticorruption (ci-après « UPAC »), créée en parallèle, mène des enquêtes en lien avec les révélations faites durant la commission Charbonneau.

---

19. *Lacroix* c. *Bilodeau*, [1998] C.A.I. 471 (C.Q.), p. 28-29.
20. Ces droits sont d'ailleurs énoncés ensemble dans le C.c.Q., préc., note 8, art. 35, lequel prévoit : « Toute personne a droit au respect de sa réputation et de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise. »
21. *Charest* c. *Québec (PG)*, 2023 QCCS 1050 (ci-après « *Charest* »).

Le 24 avril 2017, *Le Journal de Montréal* publie des documents confidentiels de l'UPAC concernant l'enquête Mâchurer, censée faire la lumière sur le financement sectoriel du PLQ. Ces documents révèlent notamment ce qui suit :

- le demandeur a fait l'objet d'une surveillance policière jusqu'en janvier 2016 ;
- l'UPAC envisageait d'intercepter ses communications privées avec Marc Bibeau, le responsable du financement pour le PLQ ;
- l'UPAC connaissait les entrées et sorties du pays des deux hommes ;
- le demandeur a voyagé avec Marc Bibeau à New York ;
- l'enquête visait la corruption et l'abus de confiance, des infractions criminelles ;
- la photo du demandeur apparaissait sur un organigramme intitulé « Financement politique illégal : le projet MÂCHURER » ;
- ont aussi été divulgués la date de naissance du demandeur, ses adresses, son numéro de permis de conduire, son numéro de téléphone, son état civil, ses antécédents civils et criminels, ainsi que l'immatriculation, la marque, l'année et la couleur de son véhicule[22].

Le journal décrit le demandeur comme un sujet d'intérêt, mais les renseignements divulgués ne cernent pas son rôle dans cette décision. À la fin 2019, Les Éditions du Journal de Montréal publient un livre qui reprend, notamment, les informations diffusées en 2017.

L'UPAC lance une enquête administrative quant à la divulgation des renseignements, mais aucune accusation n'en ressort. On y apprend que les normes de la Sûreté du Québec en matière de protection des renseignements personnels – notamment pour retrouver toute personne ayant consulté, copié ou transmis des documents confidentiels – n'étaient pas suivies[23], si bien que l'identité de l'auteur de la fuite demeure inconnue. En effet, le serveur ne conservait aucune journalisation des opérations effectuées par les utilisateurs en lien avec la consultation et le transfert de fichiers vers un autre support[24].

22. *Id.*, par. 7.
23. *Id.*, par. 11.
24. *Id.*, par. 12.

Cette fuite figure parmi les 54 relevées au sein de l'UPAC, dont on soupçonne la haute direction d'être l'auteure.

Le demandeur n'a fait l'objet d'aucune accusation en lien avec l'enquête Mâchurer[25].

1.2.2 Décision

Comme tout organisme public assujetti à la Loi sur l'accès, l'UPAC doit protéger les renseignements personnels qu'elle détient[26]. Cette obligation importe d'autant plus que l'UPAC bénéficie de privilèges aux fins de la collecte de renseignements.

Or, les renseignements transmis aux journalistes contiennent des renseignements personnels sur le demandeur et aucune exception dans la Loi sur l'accès ne permettait à l'UPAC de les divulguer aux médias.

Une atteinte est considérée comme illicite lorsqu'elle résulte d'un comportement fautif[27]. Ici, la divulgation constituait une atteinte illicite aux droits du demandeur, alors que, de manière prépondérante, la preuve démontre qu'un membre de l'UPAC était à l'origine de la fuite[28], même s'il n'est pas possible de l'identifier.

M. Charest a droit à 35 000 $ en dommages-intérêts compensatoires et 350 000 $ en dommages-intérêts punitifs[29].

1.2.3 Observations

a) L'UPAC n'a pas protégé adéquatement les renseignements personnels

Assez rapidement, le tribunal conclut à une contravention à l'obligation de protéger les renseignements personnels de M. Charest par l'UPAC[30]. Sur le plan technologique, la gestion des documents de l'UPAC ne respecte pas les normes de la Sûreté du Québec, car elle ne

25. *Id.*, par. 6, 20.
26. Loi sur l'accès, préc., note 4, art. 52.2.
27. *Charest*, préc., note 21, par. 29.
28. *Id.*, par. 31.
29. La poursuite pour abus de procédure à l'encontre du Procureur général du Québec a été rejetée, voir *Charest* c. *Québec (PG)*, 2024 QCCS 1066, par. 2.
30. Loi sur l'accès, préc., note 4, art. 52.2.

permet pas d'identifier les personnes qui manipulent les documents[31] ni ne tient compte de la nature sensible des renseignements personnels qui ont fait l'objet des fuites et de l'importante expectative de vie privée qu'ils sous-tendent[32].

La Loi sur l'accès interdit par ailleurs à l'UPAC d'utiliser et de divulguer des renseignements personnels sans le consentement de M. Charest[33], sauf en cas d'exceptions inapplicables en l'espèce[34]. La Cour fait référence à l'affaire *Denis* c. *Côté*[35], où la Cour suprême avait conclu qu'au moins un employé de l'État avait participé aux fuites d'informations secrètes. Ce groupe d'individus aurait poursuivi des fins personnelles incompatibles avec celles de l'État et, pour cette raison, leurs actes ne pouvaient engager la responsabilité de l'État.

À aucun moment le tribunal ne cite l'obligation générale des organismes publics de prendre des mesures de sécurité raisonnables pour protéger les renseignements personnels recueillis, utilisés, communiqués, conservés ou détruits sous leur responsabilité[36]. Selon cette obligation, un organisme public doit prendre des mesures raisonnables, compte tenu, notamment, de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support[37]. À notre avis, en omettant de mettre en place des mesures de journalisation appropriées, l'UPAC aurait enfreint cette obligation.

Autre constat, cette fois moins étonnant considérant le caractère méconnu de cette loi : la Cour omet d'aborder l'obligation de documenter toute modification à un document technologique prévue à la *Loi concernant le cadre juridique des technologies de l'information* (ci-après « LCCJTI »)[38]. Celle-ci aurait également justifié l'obligation

31. *Charest*, préc., note 21, par. 11-12.
32. *Id.*, par. 39-41.
33. Loi sur l'accès, préc., note 4, art. 59, 59.1 et 65.1.
34. *Charest*, préc., note 21, par. 27 et 64.
35. *Denis* c. *Côté*, 2019 CSC 44.
36. Loi sur l'accès, préc., note 4, art. 63.1.
37. *Id*.
38. RLRQ, c. C-1.1 (ci-après « LCCJTI »), art. 21 : « Lorsqu'une modification est apportée à un document technologique durant la période où il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct. »

de mettre en place une journalisation (des modifications) à l'égard des documents en cause.

Malgré ces probables oublis, la Cour conclut que l'UPAC doit indemniser M. Charest pour son comportement fautif. La décision demeure l'une des rares à sanctionner un organisme public pour un manquement à l'obligation de protection des renseignements personnels[39], sans compter l'octroi de dommages-intérêts punitifs, d'ordinaire exceptionnels.

b) Un régime de dommages-intérêts sous stéroïdes

De l'avis de la Cour, même si M. Charest n'a pas démontré que le gouvernement agissait comme l'auteur d'une violation intentionnelle de son droit à la vie privée[40], l'article 167 de la Loi sur l'accès permet d'imposer le paiement de dommages-intérêts à l'UPAC. En effet, cet article ne requérait pas d'identifier l'auteur de l'atteinte au droit à la protection des renseignements personnels[41], car l'obligation de protection vise l'organisme public, et non les membres de cet organisme ou du gouvernement dans son ensemble[42].

Cette décision crée un précédent d'intérêt, puisqu'elle établit un régime de réparation du dommage dont la preuve semble plus facile à administrer que celle des régimes de droit commun, y compris pour l'obtention de dommages punitifs.

Dans sa décision, la Cour souligne à plusieurs reprises le caractère politique indéniable de la divulgation illégale des renseignements personnels de M. Charest. La Cour s'interroge : « Quoi de plus grave dans un État de droit qu'un policier hors la loi ? »[43] Elle conclut :

> un montant significatif doit être accordé pour rappeler à tous les organismes publics, que ce soit l'UPAC, l'Agence du revenu du Québec, le Directeur de l'état civil ou autres, de leur obligation de protéger les renseignements personnels qu'ils détiennent, même s'ils pensent tirer davantage d'une

39. Une recherche sur CanLII avec les articles 52.2 et 63.1 ne produit que deux résultats au 25 mars 2024.
40. *Charest*, préc., note 21, par. 57.
41. *Id.*, par. 58.
42. *Id.*, par. 59.
43. *Id.*, par. 72.

divulgation anonyme et illégale des informations privées d'une personnalité publique.[44]

La décision donne le ton aux organismes publics, quelques mois après l'entrée en vigueur de la plupart des obligations et des sanctions introduites par la Loi 25.

1.3 L'affaire *Google*

Les droits à la vie privée et à la réputation sont corollaires. Comme l'affaire *Charest*, l'affaire *Google*[45] met en cause la diffusion de contenu préjudiciable au sujet d'une personne, mais sur la base d'une atteinte à la réputation. La décision traite de demandes de désindexation successives d'un lien menant à un contenu diffamatoire. Ces demandes s'apparentent à l'exercice du droit à la désindexation désormais en vigueur dans la Loi sur le privé[46].

Cette décision est aussi d'intérêt en ce qu'elle concerne l'application des dispositions traitant de la responsabilité des intermédiaires techniques selon la LCCJTI[47].

En effet, au Canada, cette affaire est l'une des rares à conclure à la responsabilité d'un intermédiaire pour du contenu de tiers hébergé sur sa plateforme[48]. De plus, le quantum des dommages est à nouveau surprenant, témoignant de l'importance grandissante du contrôle de la circulation de l'information, y compris des renseignements personnels à caractère diffamatoire.

1.3.1 Contexte

Le demandeur est un homme d'affaires à succès. Un matin de 2007, il se réveille accusé d'un crime particulièrement odieux qu'il n'a pas commis : maltraitance d'enfants et pédophilie[49]. Le message propageant ces propos apparaît sur un site regroupant des avis de consommateurs souhaitant signaler des situations d'abus ou de

44. *Id.*, par. 84.
45. *A.B.* c. *Google*, 2023 QCCS 1167 (ci-après « *Google* »).
46. Loi sur le privé, préc., note 3, art. 28.1.
47. LCCJTI, préc., note 38, art. 22, 27, 36, 37.
48. Au titre des recours qui n'ont pas abouti, voir *Lehouillier-Dumas* c. *Facebook inc.*, 2021 QCCS 2074 ; *Prud'homme* c. *Rawdon (Municipalité de)*, 2010 QCCA 584.
49. *Google*, préc., note 45, par. 1.

fraudes. Il est également répertorié sur le moteur de recherche du défendeur.

Le demandeur découvre le message diffamatoire en cherchant son propre nom, ne s'expliquant pas pourquoi ses affaires se détériorent[50].

Après la mise en ligne du contenu diffamatoire, la vie du demandeur bascule. Il souffre autant dans sa vie personnelle que professionnelle, et n'arrive plus à joindre les deux bouts, forcé de déménager à plusieurs reprises[51].

Dès 2007, le demandeur se lance dans une série d'échanges avec Google pour faire retirer le contenu diffamatoire[52]. Malgré les efforts du demandeur, Google refuse de supprimer l'hyperlien vers le contenu en question. D'abord, l'entreprise justifie sa décision par le fait qu'elle n'est pas responsable du contenu hébergé par les pages qu'elle indexe selon le droit américain[53]. Entre-temps, le demandeur déménage au Québec.

En 2009, le lien vers le contenu diffamatoire réapparaît et le demandeur s'adresse à nouveau à Google pour le faire désindexer, une demande finalement acceptée[54]. Entre 2009 et 2015, le demandeur fait plusieurs demandes similaires auprès de Google, ces demandes étant traitées de manière individualisée par Google (*on a URL by URL basis*)[55]. Sauf qu'en 2015, alors que le demandeur vit au Québec, l'entreprise change d'avis et refuse de donner suite aux demandes de désindexation. Elle justifie sa position par une interprétation nouvelle du droit issue d'un jugement de la Cour suprême du Canada de 2011 : l'affaire *Crookes*[56]. Malgré les demandes de l'homme d'affaires, le lien reste accessible sur le moteur de recherche, y compris lors du procès[57].

---

50. *Id.*, par. 45.
51. *Id.*, par. 74.
52. *Id.*, par. 66 et s.
53. *Id.*, par. 69 ; et ce, en vertu du *Communications Decency Act*, 47 USC (1996), § 230(c)(1).
54. *Google*, préc., note 45, par. 81-83.
55. *Id.*, par. 95.
56. *Crookes* c. *Newton*, 2011 CSC 47. Cet arrêt énonce qu'en matière de diffamation, la simple diffusion d'hyperliens ne constitue pas une répétition de l'information diffamatoire. Sans répétition, il n'y a pas diffusion et donc pas de diffamation.
57. *Google*, préc., note 45, par. 125-127.

1.3.2 Décision

Google plaide que le droit québécois, notamment la LCCJTI, doit être interprété de manière cohérente à l'Accord Canada-États-Unis-Mexique (ci-après « CUSMA »)[58], qui prévoit une immunité absolue pour les intermédiaires à l'égard de l'ensemble du contenu hébergé ou indexé sur leur plateforme[59].

Or, pour la Cour, les dispositions du CUSMA et de la LCCJTI sont compatibles : la LCCJTI précise une exception au principe général de non-responsabilité des intermédiaires, dès lors que ces derniers connaissent l'existence d'un contenu illicite et n'agissent pas promptement pour le retirer[60].

De plus, la Cour juge que les principes de l'arrêt *Crookes* ne s'appliquent pas aux faits en l'espèce. En effet, la responsabilité des créateurs de contenu et celle des intermédiaires ne sont pas régies par les mêmes principes en droit québécois. La LCCJTI s'applique aux intermédiaires pour déterminer leur responsabilité civile[61], alors que les principes de responsabilité civile extracontractuelle prévus au C.c.Q.[62] s'appliquent aux créateurs de contenu qui diffusent du contenu diffamatoire. Au contraire, les principes de la common law s'appliquaient dans l'affaire *Crookes*.

En l'espèce, contrairement à l'article 22 LCCJTI, l'entreprise donne accès à un texte illicite, le message diffamatoire, alors que le demandeur l'a informé de son caractère illicite. Elle commet ainsi une faute[63]. Selon la Cour, un intermédiaire raisonnable dont l'activité consiste à fournir des résultats de recherche en réponse à des mots clés, ainsi que des liens vers des sites, ne diffuse pas sciemment de fausses informations[64]. Pour elle, la position de la défenderesse se résume essentiellement à affirmer qu'elle rend le lien disponible parce qu'elle le peut et parce que la Cour suprême dans l'affaire *Crookes* lui a dit qu'elle pouvait le faire. Selon la Cour, la défenderesse s'est

58. 30 novembre 2018 (en vigueur au 1er juillet 2020), ratifié par la *Loi de mise en œuvre de l'Accord Canada–États-Unis–Mexique*, LC 2020, c. 1, art. 19.17.2.
59. *Google*, préc., note 45, par. 161-179.
60. LCCJTI, préc., note 38, art. 22 ; *Google*, préc., note 45, par. 179.
61. *Google*, préc., note 45, par. 236.
62. C.c.Q., préc., note 8, art. 1457 ; voir aussi l'arrêt de principe *Prud'homme* c. *Prud'homme*, 2002 CSC 85.
63. *Google*, préc., note 45, par. 251.
64. *Id.*, par. 252.

fondée sur une mauvaise interprétation de l'arrêt, elle n'a donc aucun moyen de défense[65].

La Cour souligne que ses conclusions ne visent en aucun cas à ouvrir une boîte de Pandore quant à la responsabilité de Google[66]. Le message est clair : la responsabilité des intermédiaires ne peut être retenue pour du contenu de tiers que si un degré de certitude (*level of certainty*) est atteint quant à l'existence d'une activité illicite[67] et que l'intermédiaire en a connaissance.

Après l'étude de cas similaires et en considérant les faits en l'espèce[68], la Cour détermine que le demandeur a droit à 500 000 $ en dommages-intérêts compensatoires pour le préjudice moral subi[69]. Elle n'octroie aucun dommages punitifs, faute de preuve d'intention de contrevenir à la loi de la part de la défenderesse[70]. De plus, la Cour ordonne à la défenderesse de s'assurer que les résultats de recherche n'indexeront plus le contenu diffamatoire, pour toutes recherches réalisées par des utilisateurs dans la province de Québec[71].

Le demandeur a porté la décision en appel[72].

1.3.3 Observations

Un critère se dégage de la jurisprudence pour déterminer la responsabilité des intermédiaires quant au contenu de tiers hébergé sur leur plateforme : l'atteinte d'un certain degré ou « seuil » de certitude (*level of certainty*) à l'égard du caractère illicite du contenu, seuil qui semble plutôt élevé.

Dans l'affaire *Lehouillier-Dumas*[73] de 2021, la Cour supérieure avait retenu un critère similaire, menant cependant à un résultat différent. Dans la foulée du mouvement #metoo, une liste de noms d'agresseurs sexuels allégués avait fait surface sur la page d'un réseau social. L'une des personnes ainsi listées avait demandé à la Cour supérieure d'autoriser une action collective contre la plateforme pour

65. *Id.*, par. 551.
66. *Id.*, par. 260.
67. *Id.*, par. 261-270.
68. *Id.*, par. 544 et s.
69. *Id.*, par. 637.
70. *Id.*, par. 562.
71. *Id.*, par. 638. Pour le raisonnement complet, voir par. 565-593.
72. *A.B.* c. *Google*, 2023 QCCA 630, par. 2-3.
73. *Lehouillier-Dumas* c. *Facebook inc.*, préc., note 48, par. 87 et s.

atteinte à sa réputation. Selon la Cour, la responsabilité du réseau social ne pouvait être retenue en l'absence de preuve du caractère illicite de la publication. En effet :

> personne n'était en mesure de trancher la question à savoir si le contenu reproché était licite ou non. […] [L]es allégations factuelles sur l'information transmise à Facebook dans le cadre de la dénonciation ne suffisent pas pour créer une obligation de retirer le contenu en cause.[74]

Ainsi, puisqu'au moment des faits, la publication n'était que « potentiellement » illicite, le demandeur n'a pu atteindre le *degré de certitude* nécessaire[75]. Selon la Cour, une simple plainte assortie d'allégations factuelles ne peut suffire à atteindre le « seuil de connaissance » nécessaire quant au caractère illicite d'un contenu hébergé par une plateforme[76]. Inversement, les intermédiaires comme Facebook et Google n'ont aucune obligation de surveiller activement le contenu circulant sur leur plateforme[77] ni de faire enquête à la suite de la réception d'une plainte – ils ne disposent d'ailleurs d'aucun tel pouvoir[78]. La Cour supérieure refuse donc d'autoriser le recours du demandeur[79]. Au contraire, dans l'affaire *Google*, le caractère diffamatoire – et donc, illicite – du message en cause ne laissait planer aucun doute.

Ce degré élevé de certitude quant à la connaissance du caractère illicite explique sans doute la rareté des recours fructueux selon le régime de responsabilité de la LCCJTI.

Les décisions *Google* et *Lehouillier-Dumas* rappellent qu'il revient au demandeur de démontrer le caractère illicite des propos circulant sur les plateformes. Le résultat de tels recours demeure intimement lié aux faits de l'espèce et à la preuve[80]. Dans une affaire

---

74. *Id.*, par. 86 *in fine*.
75. *Id.*, par. 96, voir aussi par. 86.
76. Au sujet du seuil de connaissance du caractère illicite, voir *id.*, par. 69-79, citant Pierre TRUDEL, « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information », dans Service de la formation permanente, Barreau du Québec, *Développements récents en droit de l'Internet*, Montréal, Éditions Yvon Blais, 2001, p. 13-14.
77. LCCJTI, préc., note 38, art. 27.
78. *Lehouillier-Dumas* c. *Facebook inc.*, préc., note 48, par. 96 et s.
79. *Id.*, par. 174.
80. Dans *Prud'homme* c. *Rawdon (Municipalité de)*, préc., note 48, la responsabilité d'auteur de contenu diffamatoire sur un forum de discussion municipal n'avait pu être retenue, faute de preuve.

de 2010, un contrat entre la plateforme Canoe et son modérateur de contenu prévoyait que l'intermédiaire devait modérer et surveiller les messages échangés sur le blogue d'un journaliste. Ainsi, lorsque les échanges ont dérapé, la plateforme a été tenue responsable de réparer le préjudice causé par les propos diffamatoires échangés[81].

Les intermédiaires ne sont pas à l'abri de recours en responsabilité civile pour un contenu qu'ils auraient eux-mêmes publié ou créé[82]. En effet, le régime d'exonération de responsabilité des intermédiaires ne vise que le contenu de tiers publié sur leur plateforme.

Inédite, l'affaire *Google* s'inscrit dans une tendance générale au Québec et ailleurs[83] à restreindre l'immunité relative dont bénéficient les intermédiaires. Selon certains, l'évolution du paysage numérique et des rapports de pouvoir entre les grandes plateformes et les autres justifierait l'imposition d'obligations supplémentaires aux intermédiaires numériques pour la surveillance du contenu qu'ils hébergent[84].

Trois actions collectives ont récemment été autorisées au Québec sur ces questions[85]. Les jugements sur le fond permettront de préciser, confirmer ou renverser la tendance dessinée par l'affaire *Google*, laquelle restreint timidement l'immunité des intermédiaires, dès lors qu'un seuil de certitude existe quant au caractère illicite d'un contenu hébergé, et qu'il en a connaissance.

---

81. *Corriveau* c. *Canoe inc.*, 2010 QCCS 3396. Dans cette affaire, Canoe était contractuellement tenue de surveiller le blogue selon un règlement interne. Canoe a été reconnue responsable du dommage causé par les propos diffamatoires.
82. *Renaud* c. *Google*, 2019 QCCQ 7021.
83. *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE*, 19 octobre 2022, Legislative Body: EP, CONSIL, plus communément appelé le *Digital Services Act* (DSA).
84. Vincent GAUTRAIS, Pierre TRUDEL et Nicolas VERMEYS, *LCCJTI+ : perspectives de mise à jour de la Loi concernant le cadre juridique des technologies de l'information (RLRQ c. C-1.1) 2001-2023*, Centre de recherche en droit public, 2023, p. 83 et s., voir propositions 10 à 12. Cette étude a été réalisée à la suite d'un mandat confié aux auteurs par le ministère de la Justice du Québec en mars 2023.
85. *Homsy* c. *Google*, 2022 QCCS 722, demande d'autorisation accordée en appel dans *Homsy* c. *Google*, 2023 QCCA 1220 ; *Beaulieu* c. *Facebook inc.*, 2022 QCCA 1736 ; *Option consommateurs* c. *Google*, 2022 QCCS 2308.

2. UTILISATION DE LA GÉNÉALOGIE GÉNÉTIQUE COMMERCIALE À DES FINS D'EXPULSION : L'AFFAIRE *ASFC*

Une enquête du CPVP concernant la *Loi sur la protection des renseignements personnels* (ci-après « LPRP »)[86], applicable aux institutions fédérales, a retenu notre attention.

2.1 Contexte

Un ancien réfugié détenu par l'Agence des services frontaliers du Canada (ci-après « ASFC ») est menacé d'expulsion du pays. L'ASFC tente de déterminer sa nationalité afin de l'expulser vers le pays approprié[87]. Pour procéder, elle a recours à un service commercial de généalogie génétique, FamilyTreeDNA, qui permet de comparer le profil génétique du détenu à celui d'autres utilisateurs[88].

L'ASFC demande au plaignant d'autoriser le prélèvement d'un échantillon génétique. Elle utilise un formulaire l'informant des éléments suivants :

- que l'ASFC prélèverait un frottis buccal ;
- soumettrait l'échantillon à FamilyTreeDNA aux fins d'analyse ;
- recueillerait des renseignements auprès de FamilyTreeDNA ;
- communiquerait avec les personnes avec qui une correspondance génétique est établie afin d'obtenir des renseignements à propos de sa nationalité.

Il accepte[89]. Cela dit, au moment de fournir le formulaire de consentement, l'ASFC ne lui présente ni la politique de confidentialité ni les conditions d'utilisation de FamilyTreeDNA[90].

---

86. L.R.C. 1985, c. P-21 (ci-après « LPRP »).
87. CPVP, « L'utilisation de la généalogie génétique commerciale par l'Agence des services frontaliers du Canada dans une affaire d'expulsion contrevient à la Loi sur la protection des renseignements personnels » (19 septembre 2023), par. 1, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-institutions-federales/2022-23/pa_20230424_asfc-adn/> (consulté le 28 janvier 2024).
88. *Id.*, par. 9.
89. *Id.*, par. 12.
90. *Id.*, par. 36.

L'ASFC procède à la création d'un compte FamilyTreeDNA au moyen de l'échantillon recueilli. Elle compare alors le profil génétique à ceux de parents potentiels dans la base de données de FamilyTreeDNA. L'ASFC contacte un nombre limité de personnes, mais ne parvient pas établir la nationalité du détenu en utilisant ce service[91].

Au terme de ce processus, le détenu dépose une plainte auprès du CPVP, alléguant que la collecte de ses renseignements génétiques est réalisée en contravention de la loi. Il conteste la nécessité de la collecte et la validité de son consentement[92].

2.2 Décision

Dans son analyse, le CPVP interprète la LPRP. Cette loi exige que la collecte de renseignements personnels ait un lien direct avec les programmes ou les activités de l'institution fédérale visée[93] et que celle-ci obtienne l'autorisation de la personne concernée pour la collecte indirecte de ses renseignements personnels[94].

2.2.1 Le lien direct entre la mesure de renvoi et la collecte

Une institution fédérale ne peut recueillir que les renseignements personnels qui ont un lien direct avec ses programmes ou ses activités[95]. Pour déterminer si ces conditions d'application ont été respectées, le CPVP procède en deux étapes :

- définir la portée de l'activité ou du programme[96] ;
- établir un lien direct entre la collecte et l'activité ou le programme[97].

Pour la première étape, le CPVP conclut qu'une mesure de renvoi[98] constitue un programme ou activité au sens de la LPRP, en

91. *Id.*, par. 13.
92. *Id.*, par. 2.
93. LPRP, préc., note 86, art. 4.
94. *Id.*, art. 5(1).
95. *Id.*, art. 4.
96. CPVP, préc., note 87, par. 20.
97. *Id.*, par. 21.
98. CPVP, préc., note 87, voir la note 2 de la décision : « Une personne peut être visée par une mesure de renvoi conformément au paragraphe 44(2) de la *Loi sur l'immigration et la protection des réfugiés* (LIPR). Les mesures de renvoi sont émises lorsqu'une personne est jugée interdite de territoire au Canada. »

ce qu'elle découle du mandat que confère la *Loi sur l'immigration et la protection des réfugiés* à l'ASFC[99].

Quant à la deuxième étape, le CPVP détermine qu'il existe un lien direct entre l'exécution de la mesure de renvoi et la collecte de renseignements personnels.

Le CPVP déplore que le test prévu à la LPRP n'englobe pas les critères de proportionnalité et de nécessité développés par la jurisprudence en matière de protection de la vie privée au Canada[100]. Ainsi, il se cantonne à appliquer le test prévu par la LPRP[101], qui se limite à déterminer s'il existe un lien direct entre la collecte et la mesure de renvoi[102].

2.2.2 Là où le bât blesse : la validité du consentement

La LPRP exige qu'une institution fédérale obtienne, sauf exception, l'« autorisation » de la personne concernée afin de recueillir indirectement ses renseignements personnels pour les utiliser à des fins administratives[103]. Dans ce contexte, le CPVP se demande si le plaignant a validement autorisé l'ASFC à recueillir des renseignements sur sa parenté génétique auprès de FamilyTreeDNA. Pour trancher, le CPVP s'inspire d'une affaire pénale mettant en cause la validité du consentement à la collecte des renseignements biométriques par des policiers[104]. La Cour d'appel de l'Ontario dans l'affaire *R.* v. *Wills* exige d'établir, selon la prépondérance des probabilités, que la personne concernée :

(i) a donné son consentement exprès ou tacite ;

(ii) avait la capacité de le faire ;

(iii) l'a fait de manière volontaire, conformément à l'interprétation présentée dans la décision *Goldman*[105], et ne découlait pas de

---

99. *Id.*, par. 21.
100. Voir la décision de principe *Laval (Ville)* c. *X.*, 2003 CanLII 44085 (QC C.Q.) ; CPVP, préc., note 87, par. 23.
101. *Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN)* c. *Canada (PG)*, 2019 CAF 212 (ci-après « *SACC CAF* »).
102. CPVP, préc., note 87, par. 23.
103. LPRP, préc., note 86, art. 5(1).
104. CPVP, préc., note 87, par. 27 ; *R.* v. *Wills*, 1992 CanLII 2780 (ON C.A.) (ci-après « *Wills* »).
105. *Goldman* c. *R.*, [1979] 1 R.C.S. 976.

mesures d'oppression, de coercition ou d'autre action externe de la part des agents, lesquels l'auraient privé d'exercer un libre choix ;

(iv) était consciente de la nature de l'action des agents à laquelle on lui demandait de consentir ;

(v) était au courant de son droit de refuser de permettre aux agents de faire ce qu'ils demandaient ;

(vi) connaissait les conséquences que son consentement était susceptible d'entraîner[106].

En adaptant ce test aux faits en l'espèce, le CPVP conclut que le plaignant n'a pas autorisé la collecte de ses renseignements personnels de façon éclairée[107]. En effet, l'autorisation ne satisfaisait pas aux exigences de la partie (iv) du test mentionné ci-dessus, car l'ASFC n'a pas fourni au plaignant les conditions d'utilisation et la politique de confidentialité de FamilyTreeDNA, qui contenaient l'information requise pour la collecte et l'utilisation de ses renseignements personnels par FamilyTreeDNA[108]. Elle ne satisfait pas non plus aux parties (v) et (vi) du test, parce que l'ASFC n'a pas informé le plaignant des dispositions de renonciation disponibles et du fait qu'il pouvait prendre le contrôle du compte FamilyTreeDNA créé par l'ASFC pour faire cesser la collecte indirecte continue par cette dernière[109].

2.2.3 Attention aux recours à des services commerciaux de tiers

Le CPVP remarque que le recours par une institution fédérale aux services commerciaux de tiers est délicat[110]. Lorsqu'elle ne peut empêcher le tiers d'utiliser ou de communiquer les renseignements personnels à des fins secondaires[111], l'institution devrait simplement

106. CPVP, préc., note 87, par. 27 ; *Wills*, préc., note 104.
107. CPVP, préc., note 87, par. 42.
108. *Id.*, par. 36.
109. *Id.*, par. 40.
110. *Id.*, par. 85, le CPVP fait également référence à l'enquête sur Clearview AI à la note 30.
111. Nous assimilons les fins secondaires à celles qui ne sont pas essentielles à la fourniture d'un produit ou d'un service et qui peuvent être refusées sans impact sur ledit produit ou le service, voir CPVP, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA et COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE

éviter de recourir à ses services. Dans les autres cas, il importe d'envisager la mise en place de clauses contractuelles spéciales, ainsi qu'une surveillance et une gestion minutieuses[112]. De l'avis du CPVP, l'implantation de telles mesures aurait pu réduire la gravité des répercussions des infractions. En effet, elle aurait permis d'éviter la collecte, la conservation et la communication continues des renseignements personnels du plaignant et des autres utilisateurs de FamilyTreeDNA au moyen du compte que l'ASFC a gardé ouvert pendant plusieurs années[113].

2.3 Observations

2.3.1 Absence de test de nécessité dans la LPRP

La conclusion du CPVP selon laquelle la LPRP n'englobe pas les critères de proportionnalité et de nécessité, « comme l'ont confirmé les tribunaux »[114], semble découler de l'affaire SACC[115]. Dans cette affaire de 2019, la Cour d'appel fédérale[116] confirme la décision d'instance inférieure selon laquelle le législateur n'avait pas l'intention de créer un critère de nécessité aux fins de la LPRP, le libellé de l'article 4 étant « sans équivoque »[117]. Selon la Cour, l'expression « lien direct » n'est pas synonyme de « nécessaire ». Conclure autrement consisterait à se substituer au législateur[118]. L'expression sous-tend un lien direct, immédiat et sans intermédiaire entre les renseignements recueillis et les activités ou les programmes du gouvernement[119]. En l'absence d'une intention claire de créer un critère de nécessité, la Cour d'appel fédérale affirme que la norme prévue à la LPRP est moins stricte que celle applicable dans les autres lois fédérales et provinciales[120].

LA COLOMBIE-BRITANNIQUE, « Lignes directrices pour l'obtention d'un consentement valable » (24 mai 2018), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/> (consulté le 23 mars 2024) « 3. Donner clairement aux individus la possibilité de choisir "oui" ou "non". »

112. CPVP, préc., note 87, par. 86.
113. *Id.*, par. 86 *in fine*.
114. *Id.*, par. 23.
115. *Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN)* c. *Canada (PG)*, 2016 CF 1289 (ci-après « *SACC CF* »).
116. *SACC CAF*, préc., note 101.
117. *Id.*, par. 40.
118. *Id.*, par. 41.
119. *Id.*, par. 38.
120. Voir *id.*, par. 42 : « Contrairement au Commissaire à la vie privée, je suis d'avis que "l'absence spécifique" du mot "nécessaire" à l'article 4 de la LPRP lui est fatale. »

Or, les tribunaux emploient couramment le *test de nécessité* pour appliquer les lois fédérales et provinciales sur la protection des renseignements personnels[121]. Le test permet de déterminer si une collecte de renseignements personnels est permise dans les circonstances. Il est hérité de la jurisprudence constitutionnelle développée dans l'affaire *Oakes*[122] et consiste à déterminer si la collecte répond à un objectif important, légitime, urgent et réel, et qu'elle est proportionnée à l'importance de l'objectif[123]. L'application de tests différents pour évaluer la licéité d'une collecte de renseignements personnels sous-tend une protection inégale des renseignements personnels, selon qu'une personne interagit avec une institution assujettie à la LPRP ou une organisation soumise à la LPRPDE ou aux lois provinciales.

Comme le souligne le CPVP depuis déjà plusieurs années[124], le législateur fédéral aurait intérêt à envisager une mise à jour de la LPRP dans le cadre de la réforme de la deuxième partie de la LPRPDE que propose le projet de loi C-27[125].

Le gouvernement fédéral a d'ailleurs lancé une consultation publique sur la modernisation de la LPRP en 2020 – la loi n'ayant

---

121. Pensons à la Loi sur le privé, préc., note 3, art. 5 ; Loi sur l'accès, préc., note 4, art. 64 ; *Loi sur l'accès à l'information et la protection de la vie privée*, LRO 1990, c. F-31, art. 38(2) ; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165, art. 26(c) ; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c. 5, art. 24(1)c) ; *Access to Information and Protection of Privacy Act*, 2015, SNL 2015, c. A-1.2, art. 61(c).
122. *R.* c. *Oakes*, [1986] 1 R.C.S. 103.
123. *Laval (Ville)* c. *X.*, préc., note 100.
124. CPVP, « Protéger et promouvoir le droit à la vie privée dans un monde numérique – Rapport annuel au Parlement 2022-2023 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques » (19 septembre 2023), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202223/ar_202223/> (consulté le 12 avril 2024) ; CPVP, « Consultation publique sur la modernisation de la Loi sur la protection des renseignements personnels – Mémoire du Commissariat à la protection de la vie privée du Canada au ministre de la Justice et procureur général du Canada » (24 mars 2021), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/memoires-presentes-dans-le-cadre-de-consultations/sub_jus_pa_2103/> (consulté le 12 avril 2024) ; CPVP, « Réforme de la Loi sur la protection des renseignements personnels à une époque de changements et de transparence » (23 mars 2016), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2016/parl_sub_160322/#toc1_2a> (consulté le 12 avril 2024).
125. *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, préc., note 6, qui apporte des changements substantiels à la législation fédérale relative à la protection des renseignements personnels.

presque pas été modifiée depuis son adoption il y a 40 ans[126]. Le gouvernement ne semblait pas enthousiaste à l'idée d'ajouter un test de nécessité à LPRP : un seuil exprès de nécessité pourrait « nuire indûment à la capacité des organismes publics fédéraux de s'acquitter efficacement de leur mandat », et « la norme générale de "nécessité raisonnable" pourrait […] empêcher le gouvernement d'accomplir son travail dans l'intérêt public »[127].

Il préconisait plutôt une approche plus souple et créative pour lui permettre, par exemple, de recueillir des données dans le cadre de systèmes d'intelligence artificielle, sans pour autant savoir à quelles fins elles seraient utilisées au moment de la collecte[128]. Au contraire, lors des consultations publiques, les intervenants ont majoritairement revendiqué l'introduction du critère de nécessité[129]. Reste à voir comment (et si) le législateur fédéral se positionnera dans une éventuelle modernisation de la LPRP.

*2.3.2 L'***autorisation** ***est-elle un consentement ?***

Dans l'affaire ASFC, le CPVP reprend les critères du test de *Wills* pour déterminer les critères sous-jacents à *l'autorisation* contenue à l'article 5 de la LPRP[130] :

> 5(1) Une institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels destinés à des fins administratives le concernant, sauf autorisation contraire de l'individu ou autres cas d'autorisation prévus au paragraphe 8(2). (Nos soulignements)

126. MINISTÈRE DE LA JUSTICE DU CANADA, « Respect, responsabilité, adaptabilité : consultation publique concernant la modernisation de la Loi sur la protection des renseignements personnels » (16 novembre 2020), en ligne : <https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/dd-dp/rar-raa.html> (consulté le 12 avril 2024).
127. *Id.*, « 6. Mettre à jour les règles relatives à la collecte, à l'utilisation, à la communication et à la conservation des renseignements personnels ».
128. *Id.*, « 2.2 Un cadre renforcé pour la collecte de renseignements personnels ».
129. MINISTÈRE DE LA JUSTICE DU CANADA, *Moderniser la Loi sur la protection des renseignements personnel – Rapport sur ce que nous avons entendu : consultation publique en ligne de Justice Canada sur la modernisation de la Loi sur la protection des renseignements personnels*, 2020, p. 12-13, « Mettre à jour les circonstances dans lesquelles des renseignements personnels peuvent être recueillis ».
130. CPVP, préc., note 87, par. 28.

Il justifie ce recours par deux motifs : (1) le critère de *Wills* offre, selon lui, une méthode d'analyse contextuelle utile des divers volets du « consentement » en ce qui concerne le point de vue de la personne, ainsi que des mesures et des objectifs de l'institution fédérale ; (2) les circonstances des deux affaires sont similaires[131].

Or, dans l'affaire *Postes Canada*[132] de mai 2023 – à peine un mois après l'affaire ASFC, tout en soulignant l'absence de définition de l'autorisation dans la LPRP, le CPVP fait un rapprochement avec la notion de consentement dans les lois sur la protection des renseignements personnels[133] et mentionne qu'à son avis, l'autorisation implique de :

(i) connaître la pratique ou s'y attendre raisonnablement ;

(ii) avoir pris une mesure dont on peut déduire raisonnablement qu'il autorise la pratique, que ce soit de manière expresse, comme par le biais d'une autorisation signée, ou, à tout le moins, de manière implicite au moyen de son comportement.

À notre sens, une définition unique et harmonisée de l'autorisation améliorerait la prévisibilité de l'application de la LPRP pour les institutions fédérales assujetties, alors que la possibilité de recueillir des renseignements personnels en dépend.

Or, la LPRP semble distinguer le *consentement* de l'*autorisation*[134], au point de vue strictement textuel[135]. En pratique, les deux termes paraissent interchangeables. Dans un souci d'uniformité avec

131. *Id*.
132. CPVP, « Enquête sur la collecte et l'utilisation par la Société canadienne des postes de renseignements personnels à des fins de marketing non conformes à la Loi » (19 septembre 2023), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-institutions-federales/2022-23/pa_20230512_scp/#fn21-rf> (consulté le 7 avril 2024).
133. *Id.*, par. 44 : « De façon semblable à notre analyse ci-dessus de ce qui constitue une « autorisation, les lignes directrices conjointes délivrées par le CPVP et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique pour l'obtention d'un consentement valable précisent que dans les cas où un individu ne s'attendrait raisonnablement pas à ce que ses renseignements personnels soient recueillis, utilisés ou communiqués d'une façon particulière, un consentement exprès est généralement exigé. »
134. À titre illustratif, l'article 5 traite d'une *autorisation*, tandis que l'article 8 évoque un *consentement*.
135. Un tel argument rappellerait la position de la Cour d'appel fédérale dans *SACC CAF*, préc., note 101.

les autres lois sur la protection des renseignements personnels, le terme *consentement* pourrait être préféré.

2.3.3 Une ÉFVP est-elle requise ?

Enfin, le CPVP observe que l'ASFC n'a pas effectué d'évaluation des facteurs relatifs à la vie privée (ci-après « ÉFVP ») avant d'avoir recours à la généalogie génétique, qui sous-tend pourtant une utilisation de renseignements personnels biométriques sensibles.

Bien qu'une ÉFVP ne soit pas une exigence stricte de la LPRP[136], une directive du Secrétariat du Conseil du Trésor du Canada l'exige[137]. Un récent scandale a révélé qu'un bassin d'institutions fédérales utilisant des logiciels intrusifs ne procédait pas à des ÉFVP selon la directive[138]. Cette décision relate donc une problématique réelle de la LPRP, qui devrait être modifiée afin de prévoir une obligation de réaliser une ÉFVP[139].

3. COMMUNICATION DE RENSEIGNEMENTS PERSONNELS SANS CONSENTEMENT : LES AFFAIRES *CAMBRIDGE ANALYTICA* ET *HOME DEPOT*

De manière générale, les lois sur la protection des renseignements personnels s'articulent autour des mêmes principes, notamment, celui de la responsabilité[140] et de la limitation de l'utilisation et de la communication[141]. En effet, elles définissent la portée de la

136. Le CPVP le réclame dans son dernier rapport, préc., note 124 (« Examen par le Commissariat des évaluations des facteurs relatifs à la vie privée »).
137. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Directive sur l'évaluation des facteurs relatifs à la vie privée » (29 mars 2010), en ligne : <https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18308> (consulté le 10 avril 2024).
138. Brigitte BUREAU, « Des outils potentiellement intrusifs utilisés par au moins 13 ministères fédéraux », *ICI.Radio-Canada – Zone Politique* (29 novembre 2023), en ligne : <https://ici.radio-canada.ca/info/long-format/2030420/logiciels-espionnage-vie-privee-gouvernement-federal> (consulté le 12 avril 2024).
139. Le CPVP a publié un nouveau formulaire de présentation des ÉFVP, voir « Pour les institutions fédérales » (20 mars 2024), en ligne : <https://www.priv.gc.ca/fr/pour-les-institutions-federales/> (consulté le 12 avril 2024).
140. LPRPDE, préc., note 5, ann. 1, art. 4.1.3 ; Loi sur le privé, préc., note 3, art. 3.1, 1 ; *Personal Information Protection Act*, SA 2003, c. P-6.5 (ci-après « PIPA de l'AB »), art. 5(1) et 5(2) ; *Personal Information Protection Act*, SBC 2003, c. 63 (ci-après « PIPA de C.-B. »), art. 4(2).
141. LPRPDE, préc., note 5, ann. 1, art. 4.5 ; Loi sur le privé, préc., note 3, art. 12, 13 ; PIPA de l'AB, préc., note 140, art. 16, 19 ; PIPA de C.-B., préc., note 140, art. 14, 17.

responsabilité d'une organisation quant aux renseignements qu'elle détient (ou contrôle) et encadrent les situations qui lui permettent de communiquer des renseignements personnels à un tiers, avec ou sans consentement. Les décisions discutées ci-dessous traitent des exigences liées à la communication de renseignements personnels.

3.1 L'affaire *Cambridge Analytica*

3.1.1 Contexte

En 2018, des rapports révèlent que Cambridge Analytica, une société de consultation, a illégalement obtenu les renseignements personnels de millions d'utilisateurs de Facebook à des fins de profilage politique. En effet, au moyen d'une application tierce intégrée à la plateforme de Facebook (« *this is your digital life* », ci-après « TYDL »), Cambridge Analytica a utilisé ces renseignements pour développer des modèles psychographiques et influencer les opinions politiques lors des élections, notamment l'élection présidentielle américaine de 2016.

Pour accéder aux renseignements des utilisateurs, l'entreprise a prétendu vouloir s'en servir pour mener de la « recherche universitaire »[142]. L'affaire donne lieu à des enquêtes gouvernementales, à des audiences parlementaires et à des changements importants dans les pratiques du géant des réseaux sociaux en matière de protection des renseignements personnels.

a) L'enquête conjointe des commissaires

À la suite d'une plainte reçue en mars 2018, le CPVP et le Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique publient conjointement les conclusions de leur rapport d'enquête sur la conformité de Facebook à la LPRPDE, en 2019[143]. Au terme de cette enquête, les commissaires reprochent notamment à Facebook de ne pas avoir obtenu de consentement valable de ses utilisateurs ni de leurs amis à l'égard de la com-

142. CPVP, *Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc.*, (25 avril 2019), Conclusions en vertu de la LPRPDE nº 2019-002 (ci-après « *Enquête Facebook* »), par. 24, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-002/> (consulté le 23 mars 2024).

143. *Id*.

munication de leurs renseignements personnels. Ils concluent aussi que les mesures de sécurité prises par Facebook étaient insuffisantes.

Dans un rapport préliminaire, les commissaires ont soumis plusieurs recommandations à Facebook, appuyées d'une entente de conformité, notamment pour permettre à l'entreprise de se conformer à la LPRPDE et à la PIPA de C.-B.[144] de la Colombie-Britannique et assurer la mise en œuvre efficace de ses engagements[145]. Essentiellement, les commissaires ont recommandé à Facebook de :

1. mettre en œuvre des mesures pour obtenir un consentement valable des utilisateurs-installateurs et de leurs amis, indiquant la nature, les objectifs et les conséquences des communications[146];

2. mettre en place un mécanisme facilement accessible et paramétrable permettant aux utilisateurs de savoir quelles applications ont accès à leurs renseignements personnels[147];

3. examiner toutes les applications intégrées et fournir des avis détaillés aux utilisateurs leur permettant de désactiver les communications continues avec certaines ou toutes les applications[148];

4. accepter d'être surveillée par un tiers désigné par les commissaires quant à sa conformité aux recommandations pendant cinq ans[149];

5. permettre aux commissaires de mener des audits sur les politiques et les pratiques de confidentialité de Facebook pendant cinq ans[150].

Facebook a contesté les conclusions des commissaires et a proposé des engagements qui ne les ont pas satisfaits[151].

b) La décision de la Cour fédérale

Muni de son rapport, le CPVP dépose en avril 2020 une demande auprès de la Cour fédérale pour obtenir des mesures correctives qui obligeraient Facebook (devenue Meta) à modifier ses activités[152].

144. PIPA de C.-B., préc., note 140.
145. *Id.*, par. 186, 189.
146. *Id.*, par. 190.
147. *Id.*, par. 194.
148. *Id*.
149. *Id.*, par. 197.
150. *Id.*, par. 199.
151. *Id.*, par. 188, 192.
152. La demande est présentée en vertu de la LPRPDE, préc., note 5, art. 15a).

Quelque 272 Canadiens ont installé l'application TYDL, et ces installations auraient permis la communication de données concernant plus de 600 000 Canadiens[153]. Les parties conviennent que Cambridge Analytica a enfreint plusieurs dispositions des politiques de Facebook : notamment, elle a utilisé les renseignements à des fins autres, elle a vendu les renseignements et les a communiqués à des tiers. Enfin, l'application exigeait des autorisations dont elle n'avait pas besoin pour fonctionner[154].

i. La nature du recours

Le recours initié par le commissaire donne lieu à une audience *de novo*[155]. Ce processus sous-tend une nouvelle audience pour en examiner le bien-fondé, et non une révision du rapport de conclusions du commissaire. En ce sens, le demandeur doit prouver qu'il y a eu manquement à la LPRPDE[156]. S'il peut déposer son rapport d'enquête en preuve, celui-ci ne fait l'objet d'aucune retenue judiciaire[157].

La jurisprudence reconnaît à la LPRPDE un statut quasi constitutionnel, car la faculté d'une personne d'exercer un droit de regard sur ses renseignements personnels est intimement liée à son autonomie, à sa dignité et à son droit à la vie privée[158]. Ce statut doit éclairer l'interprétation de la LPRPDE. De plus, la LPRPDE vise à mettre en équilibre deux intérêts concurrents : le droit à la vie privée et le besoin commercial d'accéder aux renseignements personnels[159]. La Cour doit user « de souplesse, de sens commun et de pragmatisme » pour l'interpréter[160].

---

153. *Canada (CPVP)* c. *Facebook*, 2023 CF 533, par. 37. Cette décision a depuis été infirmée par la Cour d'appel fédérale : *Privacy Commissioner of Canada* v. *Facebook, inc.*, 2024, CAF 140 (en anglais seulement). Notre analyse se limite à la décision de la Cour fédérale.
154. *Canada (CPVP)* c. *Facebook*, 2023 CF 533, par. 40.
155. *Id.*, par. 49.
156. *Kniss* c. *Canada (CPVP)*, 2013 CF 31, par. 28.
157. *Englander* c. *Telus Communications Inc.*, 2004 CAF 387 (ci-après « *Englander* »), par. 47-48 .
158. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 51 ; *Alberta (Information and Privacy Commissioner)* c. *Travailleurs et travailleuses unis de l'alimentation et du commerce*, 2013 CSC 62, par. 19 ; *Nammo* c. *TransUnion of Canada Inc.*, 2010 CF 1284, par. 74 ; *Bertucci* c. *Banque Royale du Canada*, 2016 CF 332, par. 34.
159. *Englander*, préc., note 157, par. 38, 46 ; *Lavigne* c. *Canada (Commissariat aux langues officielles)*, 2002 CSC 53, par. 25.
160. *Englander*, préc., note 157, par. 46.

ii. L'obligation d'obtenir un consentement valable

À son annexe 1, la LPRPDE énonce les principes d'obtention d'un consentement valable[161], lesquels sont incorporés aux dispositions essentielles de la loi par renvoi[162]. Selon ces principes, une organisation doit déployer des efforts raisonnables pour informer la personne des fins auxquelles les renseignements sont utilisés et obtenir son consentement[163]. Cette information doit être fournie de manière à ce que la personne puisse la « comprendre raisonnablement ». La « forme du consentement […] peut varier selon les circonstances et la nature des renseignements »[164].

Dans cette affaire, la Cour devait déterminer si Facebook a déployé des efforts raisonnables pour s'assurer que ses utilisateurs et leurs amis avaient été informés des fins auxquelles les renseignements les concernant seraient utilisés par les applications tierces[165].

Selon le commissaire, Facebook n'a pas obtenu le consentement valable de ses utilisateurs avant de communiquer les renseignements les concernant à l'application de Cambridge Analytica. Il soutient que Facebook s'est fiée aux développeurs de l'application pour obtenir le consentement et que ce consentement n'est pas valable au sens de la LPRPDE[166]. En gros, les mesures de protection de la vie privée de Facebook sont, selon le CPVP, obscures et ambiguës, soit trop compliquées, soit trop simplistes[167].

Selon Facebook, Cambridge Analytica est responsable de la communication de renseignements personnels contrairement aux politiques de confidentialité de Facebook, et non le réseau social[168].

Pour soupeser ces deux postures, la Cour constate un manque de preuve, outre les captures de pages Web pertinentes tirées de l'affidavit déposé en faveur de Facebook[169]. Le CPVP n'a, par exemple, soumis aucune expertise précisant ce que Facebook aurait pu faire

---

161. LPRPDE, préc., note 5, ann. 1, art. 4.3 ; *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 56.
162. LPRPDE, préc., note 5, art. 5(1).
163. LPRPDE, préc., note 5, ann. 1, principe 4.3.2 ; *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 57.
164. LPRPDE, préc., note 5, ann. 1, principe 4.3.4 ; *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 58.
165. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 62.
166. *Id.*, par. 63.
167. *Id.*, par. 66.
168. *Id.*, par. 69.
169. *Id.*, par. 70.

différemment[170] ni aucune preuve subjective rédigée par des utilisateurs de Facebook indiquant leurs attentes en matière de protection des renseignements personnels ou leur compréhension des enjeux liés à la protection de ces renseignements personnels lorsqu'ils utilisent Facebook.

Même si ces éléments de preuve n'étaient pas strictement nécessaires, ils auraient pu éclairer la Cour quant au « caractère raisonnable du consentement valable dans un domaine où la norme de raisonnabilité et les attentes des utilisateurs dépendent autant du contexte et sont en constante évolution »[171].

Par ailleurs, la Cour note que le CPVP n'a pas invoqué les larges pouvoirs que lui confère la LPRPDE pour contraindre Facebook à produire des éléments de preuve[172]. Le CPVP avait le fardeau d'établir le manquement à la LPRPDE sur la foi de la preuve, et non à partir d'hypothèses et de déductions.

La Cour refuse de donner suite aux inférences que le commissaire l'invite à tirer, « dont la plupart sont dénuées de fondement en droit ou au vu du dossier »[173].

Elle conclut que le commissaire n'a pas démontré que Facebook a enfreint la LPRPDE pour avoir omis d'obtenir des consentements valables[174].

iii. L'obligation de protéger les renseignements personnels

Dans sa demande, le CPVP alléguait aussi que Facebook avait enfreint l'obligation de protéger les renseignements personnels au moyen de mesures de sécurité correspondant à leur degré de sensibilité[175]. Ces mesures doivent protéger les renseignements personnels à l'égard de la perte, du vol, et la consultation, la communication, la copie, l'utilisation ou la modification non autorisées[176].

---

170. *Id*.
171. *Id*.
172. LPRPDE, préc., note 5, art. 12.1.
173. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 76.
174. *Id.*, par. 78.
175. LPRPDE, préc., note 5, ann. 1, art. 4.7.1 ; *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 80.
176. LPRPDE, préc., note 5, ann. 1, art. 4.7 ; *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 79.

La Cour note qu'une atteinte à la protection des renseignements personnels ne signifie pas que les mesures de sécurité d'une organisation sont inadéquates selon la LPRPDE ; de même, l'absence d'une telle atteinte ne signifie pas que les mesures de sécurité d'une organisation sont adéquates[177].

D'après Facebook, ses obligations de sécurité cessent une fois les renseignements communiqués à un tiers avec le consentement de l'utilisateur[178]. Selon le CPVP, Facebook conserve le contrôle des renseignements personnels communiqués aux applications tierces parce qu'elle a le droit contractuel de demander les renseignements aux applications[179].

La Cour accueille les arguments de Facebook et conclut que les obligations de sécurité de cette dernière prennent fin une fois les renseignements communiqués à un tiers, s'appuyant sur les propos de la Cour d'appel fédérale dans *Englander*, selon laquelle les mesures de sécurité imposées aux organisations sont liées à la façon de « gérer » les renseignements personnels « en leur possession »[180].

Selon la Cour, le contexte donné par d'autres dispositions de la LPRPDE limite clairement la portée des obligations de sécurité. Elle cite l'exemple du principe de responsabilité selon lequel une « organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement »[181] (nos soulignements). La loi n'étend pas cette responsabilité aux renseignements communiqués *en toutes circonstances*, précise la Cour[182]. Par ailleurs, les exemples de mesures de sécurité matérielles, administratives et techniques citées dans la loi[183] ne visent pas la protection des renseignements sur lesquels une organisation n'exerce aucun contrôle[184].

Enfin, la Cour souligne que, même si les obligations de préservation de la confidentialité s'appliquaient à Facebook après la communication de renseignements à des applications tierces, le CPVP n'a pas présenté assez de preuve pour déterminer si les ententes

177. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 81.
178. *Id*.
179. *Id.*, par. 84.
180. *Id.*, par. 85 ; *Englander*, préc., note 157, par. 41.
181. LPRPDE, préc., note 5, ann. 1, art. 4.1.3.
182. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 86.
183. LPRPDE, préc., note 5, ann. 1, art. 4.7.3.
184. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 88.

contractuelles et les politiques de mise en application des règles de Facebook constituaient des mesures de protection adéquates[185].

En somme, la Cour rejette la demande et conclut que le CPVP n'est pas parvenu à démontrer que Facebook avait enfreint la LPRPDE.

3.1.2 Observations

a) L'importance de la preuve

Cette affaire met en lumière l'importance d'étayer sa preuve, peu importe l'expertise ou la qualification du demandeur. Lors d'une audience *de novo*, la Cour ne peut conclure à une violation de la loi en l'absence de preuve concrète (pour reprendre la Cour, « *in an evidentiary vacuum* »). C'est au CPVP qu'incombe le fardeau de preuve. Même s'il a conclu que Facebook a enfreint la LPRPDE dans son rapport d'enquête, il devait présenter des éléments de preuve convaincants pour établir une violation devant la Cour. Dans sa décision, la Cour offre plusieurs exemples des éléments que le CPVP aurait pu présenter pour étoffer son dossier, ainsi que des mécanismes (*duces tecum*) dont il aurait pu se prévaloir pour contraindre l'autre partie à produire des documents :

- Preuve d'expert ;
- Preuve quant aux attentes de confidentialité des utilisateurs ;
- Preuve sur l'incompréhensibilité des enjeux en cause par les utilisateurs.

Alors que l'affaire *Lamoureux*[186] offrait l'exemple d'une réponse organisationnelle adéquate pour la gestion d'un incident de confidentialité, l'affaire *Cambridge Analytica* donne un exemple de ce à quoi les tribunaux s'attendent pour démontrer une violation de la LPRPDE, dont l'interprétation se veut souple et pragmatique.

b) La possession (ou détention) juridique et le principe de responsabilité

Cette décision invite également à réfléchir à la portée du principe de responsabilité des organisations. Contrairement au RGPD,

185. *Id.*, par. 90.
186. *Lamoureux* c. *Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2021 QCCS 1093.

qui a introduit les concepts de « responsable du traitement » et de « sous-traitant »[187] pour distinguer l'entité qui détermine les finalités du traitement et celle qui l'exécute *au nom* et *pour le compte* de l'autre, les lois canadiennes encadrent la responsabilité autour des concepts généraux de « possession », « garde » et « détention » des renseignements personnels :

LPRPDE	**PIPA de l'AB**	**PIPA de C.-B.**	**Loi sur le privé**
Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, **y compris les renseignements confiés à une tierce partie aux fins de traitement**. [ann. 1, principe 4.1.3]	An organization is responsible for personal information that **is in its custody or under its control**. For the purposes of this Act, **where an organization engages the services of a person, whether as an agent, by contract or otherwise**, the organization is, **with respect to those services, responsible** for that person's compliance with this Act. [art. 5(1) et (2)]	An organization is responsible for personal information **under its control, including personal information that is not in the custody** of the organization. [art. 4(2)]	Toute personne qui exploite une entreprise est **responsable de la protection des renseignements personnels qu'elle détient**. La présente loi […] s'applique [aux renseignements personnels], **que leur conservation soit assurée par l'entreprise ou par un tiers**. [art. 3.1 et 1]

187. Et aussi de co-responsables ou responsables indépendants.

Par conséquent, chaque loi canadienne assimile la responsabilité des prestataires de services et des mandataires à celle de l'organisation qui « détient » ou a la « possession » des renseignements personnels (du client). Dans la décision, la Cour souligne que la LPRPDE n'étend pas la responsabilité de Facebook aux renseignements communiqués *en toutes circonstances* : elle ne vise que ceux « confiés à une tierce partie aux fins de traitement » (nos soulignements)[188]. Ainsi, cette responsabilité semble se limiter à la situation où l'organisation qui reçoit des renseignements personnels agit comme prestataire de services pour le compte de l'autre.

En l'espèce, selon la Cour, les obligations de protection d'une organisation en vertu de la LPRPDE prennent fin une fois qu'un utilisateur autorise cette organisation à communiquer ses renseignements à une application tierce, car la loi encadre la gestion des renseignements personnels « en la possession » de l'organisation[189]. Or, alors que la « possession » détermine l'attribution des obligations, la Cour n'analyse par la notion de possession (ou détention) « juridique » ou « physique » des renseignements ni ne se penche sur la qualification juridique des parties (y compris du point de vue des tiers comme des utilisateurs). Elle ne traite pas non plus des dispositions contractuelles qui lient Facebook et les applications tierces[190].

En droit européen, si aucune partie n'agit pour le compte de l'autre, on considérerait probablement que Facebook est « responsable indépendant » vis-à-vis des applications tierces qui bénéficieraient du même statut. Cela signifie que les entités auraient une responsabilité indépendante dans le traitement des renseignements personnels. Mais même si les obligations en matière de sécurité devaient s'appliquer à Facebook après la communication des renseignements à des tiers, la Cour estime la preuve trop mince pour conclure à quoi que ce soit[191].

Dans le cadre d'une entente de règlement basée sur les mêmes faits, en 2019, Facebook a accepté de payer une amende de 5 milliards de dollars (US), soit 7 % de ses revenus à l'époque, et s'est engagée à

188. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 86.
189. *Id.*, par. 82, 85, citant *Englander*, préc., note 157, par. 41.
190. Voir, avec les adaptations nécessaires, la réflexion de Raymond DORAY, *Accès à l'information : Loi annotée, jurisprudence, analyse et commentaires*, 1, Montréal, Yvon Blais, 2020, p. I/1-4, cité dans *Gyulai* c. *Montréal (Ville de)*, 2009 QCCQ 1809, confirmé dans *Montréal (Ville de)* c. *Cour du Québec*, 2009 QCCS 2895.
191. *Canada (CPVP)* c. *Facebook*, préc., note 153, par. 90.

entreprendre une vaste réforme de ses pratiques en protection de la vie privée[192]. Selon le FTC :

> Facebook doit exercer une plus grande surveillance à l'égard des applications tierces, notamment en mettant fin aux activités des développeurs d'applications qui ne certifient pas qu'ils respectent les politiques de la plateforme Facebook ou qui ne justifient pas leur besoin d'avoir accès aux données particulières sur les utilisateurs.[193] (Notre traduction)

En somme, la question de la responsabilité de plusieurs parties impliquées dans un même traitement de renseignements personnels demeure vague en droit canadien, alors qu'elle est essentielle à la saine application des lois sur la protection des renseignements personnels. Les seules décisions qui en interprètent les balises relèvent de l'accès à l'information, où la transparence des organisations prime. Dans un monde numérique, les experts reconnaissent le besoin de transposer ces principes, avec les adaptations nécessaires, à la protection des renseignements personnels[194].

Avec la mondialisation, la complexification des rapports entre les différentes parties prenantes de l'industrie et l'opacité des traitements de renseignements personnels sur la toile, l'identification de critères pour qualifier la responsabilité d'acteurs numériques dans la gestion des renseignements personnels d'internautes se fait attendre.

---

192. « FTC Agreement Brings Rigorous New Standards for Protecting Your Privacy », *Meta* (24 juillet 2019), en ligne : <https://about.fb.com/news/2019/07/ftc-agreement/> (consulté le 12 avril 2024) ; « Final FTC Agreement Represents a New Level of Accountability for Privacy », *Meta* (24 avril 2020), en ligne : <https://about.fb.com/news/2020/04/final-ftc-agreement/> (consulté le 12 avril 2024).
193. FEDERAL TRADE COMMISSIONER, « FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook », *Federal Trade Commission* (24 juillet 2019), en ligne : <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> (consulté le 29 mars 2024).
194. « La jurisprudence relative à la détention résulte de décisions relatives à des demandes d'accès à des documents. Ces décisions ont été rendues dans un contexte où il n'y avait pas lieu d'apporter les nuances reflétant la complexité des environnements en réseaux. Dans ces situations, la Commission d'accès à l'information (CAI) a appliqué une conception large de la notion de détention », dans Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 142.

3.2 L'affaire *Home Depot*

3.2.1 Contexte

En supprimant son compte Facebook, une personne a réalisé que le réseau social tenait un registre de la plupart de ses achats en magasin effectués chez Home Depot, dans une section désignée, alors qu'elle n'avait jamais autorisé Home Depot à communiquer ces renseignements. Insatisfaite de la réponse du détaillant, qui a d'abord nié avoir transmis les renseignements, elle a formulé une plainte auprès du CPVP[195]. Elle a fait valoir que Home Depot avait enfreint la LPRPDE[196] en communiquant ses renseignements personnels sans l'en avoir informée et sans obtenir son consentement.

Depuis 2018, Home Depot se sert d'un outil commercial appelé « Conversions hors ligne »[197]. Il permet aux entreprises d'évaluer la mesure dans laquelle les publicités sur un réseau social entraînent des résultats réels, comme les achats en magasin[198]. Plus précisément, les entreprises peuvent transmettre à Meta, agissant en qualité de fournisseur de services, des données sur les transactions en magasin, dont l'adresse courriel de clients ayant demandé un reçu électronique, afin de mesurer l'efficacité d'une campagne publicitaire sur les plateformes de ce prestataire, de même que ses répercussions sur les ventes en magasin[199]. L'outil permet aussi de créer des auditoires semblables dans le but de diffuser des publicités auprès de personnes ayant un profil semblable aux clients hors ligne[200]. Si les clients en magasin acceptent le reçu électronique, le système leur demande de fournir une adresse courriel, sans mentionner quelque communication un tiers[201].

Home Depot fait ensuite parvenir la version hachée de l'adresse courriel du client et les détails sur l'achat hors ligne à Meta, qui fait concorder les coordonnées à celles du compte Facebook du client et compare les renseignements sur les achats hors ligne aux publicités sur Facebook à l'intention du client afin de mesurer l'efficacité de ces dernières. Si la version hachée du courriel n'est pas déjà associée à un compte Facebook, Meta ne peut pas établir un lien entre le courriel

195. CPVP, *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, (26 janvier 2023), Conclusions en vertu de la LPRPDE nº 2023-001, par. 1 (ci-après « *Home Depot* »).
196. LPRPDE, préc., note 5.
197. *Home Depot*, préc., note 195, par. 3.
198. *Id*.
199. *Id.*, par. 4.
200. *Id.*, par. 3.
201. *Id.*, par. 6.

et une personne[202]. Meta présente finalement des rapports globaux à Home Depot, y compris les ventes en magasin qui peuvent être attribuables à une campagne publicitaire précise[203].

a) L'obligation d'obtenir un consentement

En transmettant les données sur les transactions en magasin à un tiers, Home Depot communique des renseignements personnels au sens de la LPRPDE, précise le CPVP[204].

Aux termes de la LPRPDE, une personne doit être **informée de toute** collecte, utilisation ou **communication de renseignements personnels** qui la concernent **et y consentir**, à moins qu'il ne soit pas approprié de le faire[205]. Selon le CPVP, Home Depot a omis d'obtenir un consentement valide pour la communication de renseignements. En effet, l'organisation ne pouvait se fonder sur sa politique de confidentialité ou celle de Meta pour obtenir un consentement.

Bien qu'un contrat autorisait Meta à se servir de ces renseignements pour le compte de Home Depot et à ses propres fins commerciales, l'utilisation des renseignements va bien au-delà des fins commerciales de Home Depot et des fins comprises par le client. Ces utilisations englobent l'optimisation de l'efficacité des modèles de présentation de publicités ou la personnalisation des fonctionnalités et du contenu figurant sur les plateformes de Meta[206].

b) La forme du consentement

Le CPVP est d'avis que l'entreprise aurait dû obtenir un consentement exprès auprès de sa clientèle.

Pour déterminer quelle forme le consentement doit revêtir, une organisation doit évaluer la sensibilité des renseignements personnels et les attentes raisonnables de la personne concernée[207], suivant la LPRPDE. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de

202. *Id.*, par. 7.
203. *Id.*, par. 8.
204. *Id.*, par. 10.
205. LPRPDE, préc., note 5, ann. 1, principe 4.3 ; *Home Depot*, préc., note 195, par. 9.
206. *Home Depot*, préc., note 195, par. 16.
207. LPRPDE, préc., note 5, ann. 1, principes 4.3.4 et 4.3.5.

facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé[208].

Les Lignes directrices pour l'obtention d'un consentement valable[209] prévoient que les organisations doivent généralement obtenir un consentement exprès lorsque la collecte, l'utilisation ou la communication :

✓ met en cause des renseignements personnels sensibles

✓ ne répond pas aux attentes raisonnables de l'intéressé

✓ crée un risque résiduel important de préjudice grave

Dans le cas qui nous intéresse, le CPVP estime que la plupart des clients ignoreraient complètement cette pratique et ne s'y attendraient raisonnablement pas. Même si leurs renseignements n'étaient pas forcément sensibles, les clients de Home Depot ne s'attendent raisonnablement pas à ce que leur adresse électronique et les détails de leur achat hors ligne soient transmis à Meta lorsqu'ils acceptent un reçu sous forme électronique, estime le CPVP.

En effet, lorsqu'un client fournit son adresse courriel pour recevoir un reçu électronique, on ne saurait conclure qu'il autorise le détaillant à utiliser les renseignements à des fins secondaires[210] ni à les transmettre à une importante plateforme de publicité en ligne, afin qu'ils soient utilisés aux fins de cette dernière, y compris à des fins de publicités ciblées, qui ne se rattachent pas au détaillant lui-même[211].

3.2.2 Observations

La décision *Home Depot* met en lumière l'importance qu'accorde le CPVP aux attentes raisonnables des personnes concernées quant à l'utilisation de leurs renseignements personnels pour déterminer la forme du consentement.

Dans son annexe sur la forme du consentement, au sujet des attentes raisonnables, la LPRPDE précise que le consentement ne doit pas être obtenu par un « subterfuge ». Elle utilise l'exemple d'une

208. *Home Depot*, préc., note 195, par. 19.
209. CPVP, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA ET COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, préc., note 111.
210. Voir *Wills*, préc., note 104.
211. *Home Depot*, préc., note 195, par. 30.

personne qui fournit ses renseignements personnels à un professionnel de la santé qui ne s'attendrait pas à ce que ses renseignements personnels soient communiqués sans consentement à une entreprise qui vend des soins de santé.

L'importance accordée aux attentes raisonnables semble varier selon le régime juridique applicable. Il convient de faire un rapprochement entre les facteurs à pondérer pour déterminer la forme du consentement et les *Lignes directrices de la CAI sur les critères de validité du consentement*[212] en droit québécois. Dans ses lignes directrices, la CAI introduit les concepts de finalités primaires, c'est-à-dire celles liées à la fourniture d'un produit ou d'un service qu'une personne a demandés, et secondaires, c'est-à-dire celles qui ne sont pas nécessaires à la fourniture d'un produit ou d'un service.

Le CPVP fait une distinction similaire dans ses *Lignes directrices pour l'obtention d'un consentement valable* :

> Les organisations devraient établir une distinction entre les fins qui sont essentielles à la prestation d'un service et celles qui ne le sont pas et expliquer toutes les options offertes. […] Pour que la collecte, l'utilisation ou la communication constitue une condition de service valide, elle doit être essentielle à la fourniture de ce produit ou ce service, c'est-à-dire qu'elle est nécessaire pour réaliser les fins légitimes précisées explicitement. […] Autrement, pour toute autre collecte, utilisation ou communication, les individus doivent avoir un choix (sauf si une exception à l'exigence générale relative à l'obtention du consentement s'applique).[213] (Nos soulignements)

Au fédéral, la question de la sensibilité des renseignements, des attentes raisonnables d'une personne et du risque résiduel de préjudice se pose d'emblée pour déterminer quelle forme de consentement demander. La réponse positive à une de ces questions commande l'obtention d'un consentement **exprès**. La ligne est fine : dans des décisions antérieures, le CPVP a conclu que l'utilisation de la géolocalisation précise afin de diffuser de la publicité ciblée sur des

---

212. CAI, « Lignes directrices sur les critères de validité du consentement », en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_LD_Criteres_validite_consentement.pdf> (consulté le 23 mars 2024), glossaire (p. 1).
213. CPVP, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA ET COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, préc., note 111.

affichages devait faire l'objet d'un consentement exprès[214], mais que l'utilisation de l'emplacement approximatif offerte par l'adresse IP pour présenter des publicités pertinentes pouvait faire l'objet d'un consentement implicite[215].

Au Québec, c'est après avoir déterminé si l'utilisation projetée vise des fins primaires (essentielles au service) ou secondaires (facultatives) que ces questions se posent[216]. Autrement dit, pour utiliser des renseignements personnels, même sensibles, à des fins primaires, une organisation peut s'appuyer sur un consentement tacite sans autre examen.

Or, avec la popularité grandissante des technologies publicitaires alimentées par les données, tant sous le régime fédéral que provincial, l'utilisation des renseignements personnels à des fins de prospection commerciale n'est pas considérée comme essentielle à la fourniture d'un produit ou d'un service.

Malgré les différents cadres d'analyse, la forme de consentement se heurte au même point : de manière générale, les fins de marketing et de prospection commerciale outrepassent les attentes raisonnables d'une personne. Dans une autre affaire[217], le CPVP conclut que l'institution fédérale ne pouvait utiliser les renseignements personnels qu'elle recueille sur les enveloppes et les colis livrés pour créer des listes d'adresse de marketing postal qu'elle loue au secteur privé sans « autorisation ». Le CPVP reprend alors la notion d'attente raisonnable qu'une personne doit avoir pour autoriser une pratique[218].

En principe, le seul mécanisme de retrait du consentement (*opt-out*) ne suffit pas[219]. Comme l'utilisation de renseignements personnels

214. CPVP, *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*, Conclusions en vertu de la LPRPDE nº 2020-004.
215. CPVP, *Enquête sur les pratiques de traitement des renseignements personnels de Ganz Inc.*, Rapport de conclusions en vertu de la LPRPDE nº 2014-011.
216. CAI, préc., note 212, par. B.6 *a contrario*, glossaire (p. 1).
217. CPVP, préc., note 132.
218. Voir par exemple *id.* ; CPVP, *Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons*, (1er juin 2022), Conclusions en vertu de la LPRPDE nº 2022-001 (ci-après « *Tim Hortons* »), où il était question de renseignements sensibles.
219. CPVP, « Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne » (17 décembre 2015), en ligne : <https://www.priv.

à des fins de marketing constitue une finalité secondaire, la personne concernée doit avoir l'occasion d'accepter ou de refuser au moment où ses renseignements sont recueillis. Cela limite beaucoup la portée de l'utilisation de ce type d'outils, dont la valeur repose essentiellement sur la possibilité de recueillir une pléthore de données.

Au Québec, si la CAI emboîte le pas, cette interprétation risque de se répercuter sur les technologies de ciblage et l'industrie du *Ad Tech*. D'autant plus que les nouvelles technologies venues remplacer les témoins tiers (*third-party cookies*), les *Data Clean Rooms*, reposent sur l'appariement d'adresses courriel hachées – ou plus rarement d'autres identifiants hachés – entre des partenaires pour créer des profils d'utilisateurs détaillés à des fins de publicité ciblée. Il sera intéressant de suivre les développements au Québec, compte tenu des impacts sur cette industrie évaluée à plusieurs milliards de dollars.

4. DEMANDE D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS ET RISQUES IDENTIFICATOIRES : L'AFFAIRE *SHIAB*

Dans l'affaire *Shiab*[220], la CAI considère que des informations qui révèlent des attributs se rattachant à une personne physique dans le cadre de son emploi (connues sous l'expression anglaise *work product*), et ceux se rattachant à des patients, constituent des renseignements personnels. Les renseignements en cause concernent la facturation de services médicaux rendus par des professionnels de la santé à des patients.

4.1 Contexte

4.1.1 La demande d'accès en cause

Dans cette décision, le demandeur s'est adressé à la Régie de l'assurance maladie du Québec (ci-après « RAMQ ») afin d'obtenir une copie numérisée des bases de données de tous les actes médicaux facturés par les professionnels de la santé à la RAMQ, pour la période s'échelonnant de 2011 jusqu'aux plus récentes données disponibles à

gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/gl_ba_1112/> (consulté le 7 avril 2024).

220. *Shiab* c. *Régie de l'assurance maladie du Québec (RAMQ)*, 2023 QCCAI 30 (ci-après « *Shiab* »).

la date de la demande d'accès, à savoir le 27 mai 2022. Sa demande d'accès, très précise, est formulée comme suit :

> Copie numérisée des bases de données de tous les actes médicaux facturés par les professionnels de la santé à la Régie de l'assurance maladie du Québec de 2011 aux plus récentes données disponibles ;
>
> Les données doivent inclure, au minimum, les informations suivantes tirées des fichiers « Services médicaux » et « Services médicaux – sans bénéficiaire » de vos bases de données :
>
> - Numéro de facture banalisé
> - Numéro banalisé de l'individu
> - Classe du professionnel
> - Numéro banalisé du professionnel
> - Spécialité du professionnel
> - Code d'entente de facturation
> - Code de groupe d'actes
> - Code d'acte
> - Rôle dans l'exécution de l'acte
> - Date du service
> - Type de l'établissement
> - Numéro banalisé du lieu de prestation de soins
> - Code de localité banalisé du lieu de prestation de soins
> - Région du lieu de dispensation
> - Montant facturé
> - Classe du professionnel référent
> - Numéro banalisé du professionnel référent
> - Spécialité du professionnel référent

> Les données doivent inclure, au minimum, les informations suivantes tirées des fichiers « Professionnel » de vos bases de données :
>
> - Classe du professionnel
> - Numéro banalisé du professionnel
> - Sexe du professionnel
>
> Les données doivent inclure, au minimum, les informations suivantes tirées des fichiers « Services médicaux – Diagnostics » de vos bases de données :
>
> - Numéro de facture banalisé
> - Numéro banalisé de l'individu
> - Code de diagnostic
> - Numéro séquentiel du système de diagnostic

La RAMQ refuse de faire droit à sa demande pour les motifs suivants :

- la liste de renseignements concerne des professionnels de la santé et tout renseignement obtenu aux fins de la rémunération de ces professionnels sont confidentiels en vertu de la *Loi sur l'assurance maladie* (ci-après « LAM »)[221] ;
- ce type de demande s'apparente davantage à une demande de renseignements à des fins d'études, de recherche ou de production de statistiques, et requiert le concours de la CAI ;
- la LAM prévoit que la RAMQ peut uniquement révéler, aux fins de statistiques, des renseignements obtenus pour l'exécution de la LAM, pourvu qu'il ne soit pas possible de les relier à une personne particulière[222]. En l'espèce, la RAMQ considère que le seul fait de remplacer les identifiants par un numéro balisé ne suffit pas pour assurer l'anonymisation des renseignements ;

221. RLRQ c. A-29 (ci-après « LAM »), art. 63 al. 1.
222. *Id.*, art. 67 al. 1.

- les renseignements qui portent sur une personne physique et permettent de l'identifier doivent être protégés en vertu de la Loi sur l'accès[223].

4.1.2 La précédente demande d'accès

La RAMQ soulève également le caractère répétitif des demandes. L'organisme a refusé une demande d'accès antérieure similaire[224], se fondant notamment sur un rapport émis par la Direction de l'intelligence d'affaires et de l'analytique (DIAA) selon lequel les risques identificatoires sont susceptibles de compromettre la confidentialité des données.

Considérant la similarité de la demande actuelle[225] avec la demande d'accès antérieure, et tenant compte des conclusions du rapport portant sur l'analyse des risques identificatoires, l'organisme réitère son refus[226].

C'est dans ce contexte que la CAI est saisie d'une demande de révision et doit notamment se prononcer quant à la qualification des renseignements demandés à titre de renseignements personnels.

4.1.3 Décision

La CAI considère que les renseignements en cause constituent des renseignements personnels n'ayant pas le caractère de renseignements publics. De ce fait, ils ne peuvent être communiqués sans le consentement des personnes concernées. Ces renseignements concernent aussi bien les médecins que les patients.

Tout d'abord, elle considère que les renseignements en lien avec la facturation de services médicaux par les professionnels de santé révèlent de façon indirecte la façon de travailler et la charge de travail des professionnels dès lors qu'il s'agit de renseignements qui font connaître quelque chose à propos d'une personne physique. De plus, ils sont susceptibles de la distinguer par rapport à quelqu'un d'autre. Ainsi, ces renseignements révèlent indirectement la charge

---

223. Loi sur l'accès, préc., note 4, art. 53, 54 et 59.
224. Ainsi que d'une demande de révision à la CAI. À la suite d'une médiation, le demandeur s'est désisté de sa demande de révision en août 2019.
225. Bien que la nouvelle demande vise plus de renseignements, notamment le sexe du professionnel.
226. *Shiab*, préc., note 220, par. 15.

de travail et les moments de présences dans les établissements de l'organisme. En effet, les renseignements concernent des actes médicaux facturés par des médecins, en fonction d'un code propre à l'acte. Ce code permet de cerner ce que le médecin a fait comme acte médical. De plus, même s'il n'est pas identifié directement, le médecin l'est via son numéro d'inscription au Tableau, qui lui est propre. Compte tenu de ces éléments, le code de l'acte, le numéro et la date de prescription permettent de déterminer ainsi que les jours de travail des professionnels au sein des établissements de l'organisme.

Il convient de rappeler que la CAI avait déjà qualifié de renseignements personnels le nombre d'accouchements accomplis par un médecin durant une période donnée[227].

Ensuite, la CAI s'attarde aux renseignements personnels des patients. Elle considère que ces renseignements révèlent des informations sur les patients puisque relatifs aux services médicaux reçus par chacun des usagers assurés par le régime de soins.

Une fois le caractère personnel du renseignement identifié, la CAI a dû évaluer si les renseignements concernant les médecins et ceux concernant les patients sont des renseignements de nature publique. Ce n'est pas le cas en l'espèce. En effet, pour les renseignements concernant les médecins, elle se fonde sur sa précédente décision[228] dans laquelle elle considère que des éléments qui révèlent de façon indirecte la charge de travail d'un médecin accoucheur ainsi que les moments de ses présences dans les établissements de l'organisme sont des renseignements personnels qui n'ont pas un caractère public.

Quant aux renseignements personnels concernant les patients, il importe de souligner la confidentialité du dossier de tout usager. La CAI rappelle :

> le fait que le professionnel de la santé ou que l'établissement soit autorisé à communiquer un renseignement médical confidentiel à la RAMQ pour les fins de l'administration du régime de santé publique […] n'a pas pour effet de dépouiller ce renseignement médical de sa confidentialité initiale.[229]

---

227. *A.L.* c. *CHU de Québec*, 2015 QCCAI 309, par. 62-63.
228. *Shiab*, préc., note 220, par. 39 ; *A.L.* c. *CHU de Québec*, préc., note 227, par. 62-63.
229. *Shiab*, préc., note 220, par. 47.

En d'autres termes, au sens de la Loi sur l'accès et de la LAM, les renseignements visés par la demande sont des renseignements personnels ne pouvant être communiqués sans le consentement des personnes concernées, qu'ils concernent les professionnels de la santé ou les patients[230].

4.2 Observations

Dans cette affaire, la CAI se fonde sur la notion de risques identificatoires pour déterminer s'il est possible de réidentifier la personne concernée, ce qui est le cas en l'espèce. Autrement dit, il est question de renseignements dépersonnalisés au sens de la Loi 25.

4.2.1 La notion de risques identificatoires

Pour déterminer si les renseignements en cause sont des renseignements personnels, la CAI s'attache à déterminer si les risques identificatoires, c'est-à-dire la possibilité qu'une personne soit identifiée, sont réels et bien présents en cas de communication au demandeur. Pour ce faire, la CAI se fonde sur le rapport émis par la DIAA dans des circonstances similaires.

En l'espèce, la demande vise des microdonnées de la RAMQ, c'est-à-dire des renseignements détaillés concernant des professionnels et des usagers (les patients). Dans une telle situation, les chercheurs désirant utiliser de tels renseignements s'adressent habituellement à la DIAA après avoir reçu l'aval de la CAI[231]. Dans la présente décision, au moment de la demande d'accès, le demandeur n'a pas obtenu cette autorisation et la demande d'accès ne contient aucun consentement des personnes concernées par les renseignements visés.

En l'espèce, les renseignements visés par la demande d'accès sont des renseignements personnels confidentiels. Même si des identifiants sont banalisés, le risque d'identification demeure trop important, et ce, en raison des éléments suivants :

- Dans les documents visés par la demande d'accès, on trouve notamment le numéro d'assurance maladie ainsi que le nom de la personne assurée ainsi que, notamment, le nom du professionnel de la santé, son adresse professionnelle, le montant payé par la RAMQ, etc.

230. LAM, préc., note 221.
231. En application de la Loi sur l'accès, préc., note 4, art. 125.

- Pour extraire de telles données sans pouvoir identifier la personne concernée, il faut respecter un certain nombre de normes, notamment ne produire aucune statistique sur la base du diagnostic et appliquer des techniques de masquage des données.
- En outre, certains regroupements doivent être appliqués comme celui de la spécialité du professionnel, la suppression du code d'entente de facturation, le masquage du code de diagnostic, etc.
- Malgré cela, il y a toujours un risque de réidentification.

C'est pour cela que la CAI conclut que les risques d'identification des personnes sont « présents et réels » et donc que la RAMQ doit, à juste titre, refuser de communiquer les renseignements demandés. Essentiellement, et à la lumière de la Loi 25, les renseignements ne sont que dépersonnalisés et, en aucun cas, anonymisés.

4.2.2 La distinction entre l'anonymisation et la dépersonnalisation

La Loi sur l'accès dispose que :

> Pour l'application de la présente loi, un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée.[232]

Les renseignements dépersonnalisés se distinguent des renseignements anonymisés. En effet, un renseignement est anonymisé « lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne »[233]. Par ailleurs, l'anonymisation doit suivre les meilleures pratiques généralement reconnues et les critères et modalités déterminés par règlement[234].

Si une personne concernée peut toujours être identifiée indirectement, par mise en correspondance avec d'autres informations, par

232. *Id.*, art. 65.1 al. 5.
233. *Id.*, art. 73 al. 2 ; Loi sur le privé, préc., note 3, art. 23 al. 2.
234. Loi sur l'accès, préc., note 4, art. 73 al. 3 ; Loi sur le privé, préc., note 3, art. 23 al. 3.

inférence ou autrement, le renseignement n'est que dépersonnalisé[235]. Ainsi, il existe un risque identificatoire « présent et réel »[236].

La dépersonnalisation a une nature réversible, contrairement à l'anonymisation qui, par définition, est irréversible. Pour les organisations, cette distinction revêt une importance capitale : l'anonymisation permettrait de libérer la donnée sortante des restrictions légales applicables aux renseignements personnels, contrairement à la dépersonnalisation. Ici, parce que les renseignements sont simplement dépersonnalisés, ils ne peuvent être communiqués.

Si dans l'affaire qui nous intéresse, la CAI ne mentionne pas les notions d'anonymisation ou de dépersonnalisation, il ne s'agit pas de la première décision de la CAI sur le sujet. La CAI a, avant même l'entrée en vigueur des dispositions pertinentes, considéré que des renseignements dont on avait retiré plus de 80 identifiants aux fins de développer un algorithme prédictif constituaient des renseignements dépersonnalisés plutôt qu'anonymisés[237].

Cette distinction entre anonymisation et dépersonnalisation rappelle celle applicable dans l'Union européenne. En vertu du RGPD, la pseudonymisation correspond au :

> traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.[238]

Comme la dépersonnalisation québécoise, la pseudonymisation permet donc de traiter des données sans identifier directement les personnes concernées et s'apparente davantage à une mesure de sécurité[239] et ne permet pas de se soustraire à l'application de la loi.

---

235. Loi sur l'accès, préc., note 4, art. 65.1 al. 5 ; Loi sur le privé, préc., note 3, art. 12 al. 4(1).
236. *Shiab*, préc., note 220, par. 84.
237. *Enquête concernant le Centre de services scolaire du Val-des-Cerfs (anciennement Commission scolaire du Val-des-Cerfs)*, 2022 QCCAI 1020040, par. 14.
238. RGPD, préc., note 1, art. 4 al. 5.
239. Voir notamment *id.*, considérant 28.

La CAI aurait peut-être raisonné différemment en considérant le *Règlement sur l'anonymisation des renseignements personnels* édicté le 15 mai 2024[240].

4.2.3 La décision Shiab *au regard du* Règlement sur l'anonymisation

En vertu du projet de règlement, le jeu de données composé d'identifiants indirects et quasi-identifiants devra faire l'objet d'une analyse préliminaire du risque de réidentification en tenant compte des critères cumulatifs, issus de l'interprétation européenne, suivants :

- **L'individualisation** : *Le fait de ne pas être en mesure d'isoler ou de distinguer une personne dans un ensemble de données.* Par exemple, un jeu de données présentant l'adresse résidentielle et la date de naissance des personnes concernées permet de manière évidente de retracer individuellement leur identité. Dans la décision qui nous intéresse, le risque d'individualisation est important, notamment eu égard au système de code utilisé.

- **La corrélation** : *Le fait de ne pas être en mesure de relier entre eux des ensembles de données qui concernent une même personne.* Par exemple, deux jeux de données présentant des attributs rattachés à un matricule ou un numéro unique d'identification peuvent être combinés grâce à cet identifiant unique.

- **L'inférence** : *Le fait d'être (ou ne pas être) en mesure de déduire des renseignements personnels à partir d'autres renseignements disponibles.* Par exemple, une base de données présentant, pour chaque individu, son emploi et sa ville de résidence, permettrait de retracer facilement l'identité de la personne concernée pour chaque cas où il n'y a qu'une seule personne occupant cet emploi dans la ville donnée.

Enfin, lors de cette phase préliminaire, il importe aussi d'analyser le risque que d'autres renseignements disponibles[241], notamment

240. *Règlement sur l'anonymisation des renseignements personnels*, (2024) 156 *G.O.* II, 2847, D. 783-2024.

241. L'interprétation de la « disponibilité » des autres renseignements devrait s'analyser du point de vue du destinataire des données résultantes, et donc des autres données auxquelles cette personne a accès, si on se fie aux récentes décisions en la matière dans l'UE. Voir *Affaire T-557/20 (Conseil de résolution unique* c. *Contrôleur européen de la protection des données)*, 2023, en ligne : <https://

dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne physique[242].

Ce quatrième facteur nous apparaît comme complexe à analyser, compte tenu de la montée grandissante des bases de données massives publiques[243]. En effet, comment prouver que, sur toutes les bases existantes dans le monde, aucune ne permet de faire d'inférence à l'égard d'un individu ? La posture européenne selon laquelle la disponibilité devrait s'analyser du point de vue du destinataire et non du point de vue des bases de données disponibles devrait servir d'inspiration. À tout le moins, ce quatrième facteur mériterait d'être précisé.

CONCLUSION

Les décisions commentées confirment le changement de posture amorcé par la réforme des lois sur la protection des renseignements personnels au Canada. Si la validité du consentement reste au cœur de certains dossiers, nous évoquons les limites qu'impose l'obsolescence de certaines lois comme la LPRP, qui a fêté ses 40 ans en 2023. Nous rappelons la difficile conciliation des intérêts commerciaux et des droits individuels.

Ainsi, dans le cas d'une force policière usant de certains privilèges, on souligne la nécessité d'appliquer avec rigueur un protocole respectueux de la confidentialité, et ce, dans toutes les étapes d'une enquête. Pour un réseau social en ligne, cependant, le manque de preuve du CPVP évite un véritable débat de fond. En général, une preuve dûment étayée contribuera à trancher dans un sens ou dans l'autre.

En ce qui concerne les demandes d'accès à des fins de recherche, les organisations devront veiller à ne pas communiquer de renseignements simplement dépersonnalisés, car ceux-ci demeurent des renseignements personnels dont l'accès est restreint.

---

curia.europa.eu/juris/document/document.jsf?text=&docid=272910&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=5021256> (consulté le 2 avril 2024).

242. *Id*.

243. Jacob JOLIJ, Els MAECKELBERGHE, Rosalie KOOLHOVEN et Monicque LORIST, *Privacy and anonymity in public sharing of high-dimensional datasets: legal and ethical restrictions (document en prépublication)*, 14 septembre 2017, doi: 10.31234/osf.io/pmvg4.

Ces décisions interviennent dans un contexte turbulent sur le plan législatif. Partout au monde, les législateurs ont intérêt à se concerter pour mettre en place des régimes juridiques compatibles à l'ère numérique. Rappelons que l'approche fondée sur les principes et la neutralité technologique favorisent une évolution plus souple de la loi pour suivre le progrès.

L'entrée en vigueur des modifications découlant de la Loi 25 et la réforme législative fédérale ont marqué 2023, mais il faudra s'armer de patience avant d'en constater les effets directs en jurisprudence.