Vol. 33, n° 2

Revue des décisions marquantes de l'année 2020 en matière de vie privée et de protection des renseignements personnels

François Joli-Cœur et Simon Du Perron*

* Respectivement avocat et stagiaire chez Borden Ladner Gervais.

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

RÉSUMÉ

Cet article analyse certaines décisions marquantes en matière de vie privée et de protection des renseignements personnels rendues au cours de l'année 2020 ou à la fin de l'année 2019. Fruit d'une année hors du commun, cette revue jurisprudentielle s'avère variée tant du point de vue des thèmes abordés (biométrie, pratiques commerciales trompeuses, sécurité de l'information, actions collectives, réputation en ligne) que de celui des autorités impliquées dans les décisions (Cour supérieure, Commission d'accès à l'information, Commissaire à la protection de la vie privée du Canada, Bureau de la concurrence).

ABSTRACT

This article analyzes some of the landmark privacy and data protection decisions that were issued in 2020 or in late 2019. Being the product of an unprecedented year, this case law review proves to be diverse both in terms of issues (biometrics, deceptive marketing practices, information security, class actions, online reputation) and authorities involved (Superior Court, Commission d'accès à l'information, Office of the Privacy Commissioner of Canada, Competition Bureau).

INTRODUCTION

L'année 2020 est une année hors-norme à bien des égards. En effet, la pandémie de COVID-19 a chamboulé nos vies quotidiennes et a poussé plusieurs organisations, les petites comme les plus grandes, à faire preuve d'adaptabilité. Les contrecoups de la pandémie se sont également fait sentir au chapitre de l'activité judiciaire, qui a été considérablement ralentie pendant plusieurs mois[1]. Ainsi, le volume de décisions rendues par des tribunaux en matière de droit de la vie privée cette année est assez mince.

L'année 2020 n'en demeure pas moins une année marquante au point de vue de la protection des renseignements personnels avec l'introduction de réformes majeures de la législation tant au Québec[2] qu'au fédéral[3]. Bien que les deux projets de loi soient toujours à l'étude au moment d'écrire ces lignes, il est clair que les organisations, publiques comme privées, vont devoir réviser leurs pratiques en matière de protection des renseignements personnels afin de s'assurer qu'elles sont conformes aux nouveaux standards en la matière.

Étant donné le bassin réduit de décisions judiciaires rendues en 2020, nous avons fait le choix d'élargir la portée du présent article en considérant les décisions et rapports d'enquêtes de commissaires à la vie privée. Nous nous sommes également permis de regarder du côté de l'année 2019 afin de faire ressortir certaines décisions marquantes. Ainsi, le présent article débutera par l'analyse de deux affaires qui mettent en cause la collecte et l'utilisation de renseignements biométriques (*Les 3 Piliers* et *Cadillac Fairview*). Nous nous

1. Louis-Samuel PERRON et Mayssa FERAH, « L'arrêt partiel des activités judiciaires décrété », *La Presse*, 13 mars 2020, en ligne : <https://www.lapresse.ca/covid-19/2020-03-13/l-arret-partiel-des-activites-judiciaires-decrete>.
2. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi nº 64 (Adoption du principe – 20 octobre 2020), 1re sess., 42e légis. (Qc).
3. *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, projet de loi C-11 (Dépôt et première lecture – 17 novembre 2020), 2e sess., 43e légis. (Can.).

pencherons ensuite sur l'interaction entre la protection des renseignements personnels et le droit de la concurrence (*Facebook*) avant d'aborder la question des menaces internes en matière de sécurité de l'information (*Desjardins*) ainsi que les actions collectives à la suite d'un incident de confidentialité (*Equifax*). Nous conclurons cet article en abordant l'enjeu de la réputation en ligne des professionnels de la santé (*RateMDs*).

1 LES RENSEIGNEMENTS BIOMÉTRIQUES : LES AFFAIRES *LES 3 PILIERS* ET *CADILLAC FAIRVIEW*

1.1 *Les 3 Piliers*[4]

L'épicerie Les 3 Piliers a informé la Commission d'accès à l'information (ci-après « CAI ») de son intention de mettre en place un système de paiement par empreinte digitale pour ses clients, conformément à l'article 45 de la *Loi concernant le cadre juridique des technologies de l'information*[5], qui exige d'informer la CAI de la création d'une banque de caractéristiques ou de mesures biométriques. Cet article donne à la CAI le pouvoir de « rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne ». De plus, la CAI peut « suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée »[6].

Le système en question permettrait aux clients de payer leurs achats en appuyant simplement leur doigt sur un lecteur d'empreinte digitale. Ainsi, comme chaque empreinte est reliée à son numéro de compte, le client se verrait facturer ses achats par prélèvement automatique à la fin du mois.

Dans ses observations adressées à la CAI, Les 3 Piliers souligne qu'elle offrirait à ses clients ne souhaitant pas fournir leurs empreintes digitales l'option d'adhérer au système de paiement sans papier sur présentation de deux pièces d'identité, dont une avec photo.

4. *Les 3 Piliers Inc.*, 2020 QCCAI 1018507.
5. RLRQ, c. C-1.1 (ci-après « LCCJTI »).
6. *Id.*, art. 45 al. 3.

La particularité de cette affaire réside dans la nature des renseignements personnels en cause, soit des caractéristiques biométriques[7]. En effet, dans sa décision du 14 février 2020, la CAI précise que bien que le système que l'entreprise souhaite mettre en place ne conserve dans ses fichiers que des codes correspondant à une transcription numérique de l'empreinte digitale du client, cela n'en constitue pas moins une information qui permet d'identifier ce dernier et, par conséquent, un renseignement personnel[8]. En outre, la CAI ne manque pas de souligner le caractère unique, distinctif et permanent de l'empreinte digitale, ce qui en fait un renseignement personnel particulièrement sensible.

La CAI passe ensuite à l'application du critère de nécessité de la collecte de renseignements personnels proposée par l'entreprise. Elle reprend pour ce faire la grille d'analyse développée dans la décision *Laval (Société de transport de la Ville de)* c. *X.*[9], qui propose d'évaluer la nécessité à la lumière de la finalité poursuivie par l'entreprise et d'apprécier la proportionnalité de l'atteinte à la vie privée que peut constituer cette collecte au regard de cette fin[10].

Pour convaincre la CAI de la nécessité de procéder à la collecte des empreintes digitales de ses clients, Les 3 Piliers doit d'abord démontrer que cette collecte participe à la réalisation d'un objectif légitime, important et réel. En implantant son système de paiement par empreinte digitale, l'entreprise souhaite : 1) minimiser son empreinte écologique ; 2) améliorer l'expérience client en réduisant le temps d'attente aux caisses et 3) assurer une meilleure prévention de la fraude.

---

7. COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA (« CPVP »), *Des données au bout des doigts : la biométrie et les défis qu'elle pose à la protection de la vie privée*, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/>.
8. *Les 3 Piliers Inc.*, préc., note 4, par. 28 à 31.
9. [2003] C.A.I. 667 (C.Q.).
10. *Id.*, par. 33 et 44, tel qu'appliqué dans *Grenier* c. *Centre hospitalier universitaire de Sherbrooke*, [2010] QCCQ 9397 et *Synergie Hunt International inc.* c. *Trinque Tessier*, 2017 QCCQ 13747. Au sujet de l'évolution de l'interprétation jurisprudentielle de ce critère, voir Lukasz GRANOSIK, « Le critère de nécessité : son évolution, son importance, son impact et son application », (2014) 392 *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé* 85 et Pierre-Luc DÉZIEL, « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », (2019) 465 *Développement récents en droit à la vie privée* 3.

La CAI estime que les arguments avancés par Les 3 Piliers pour justifier la collecte des empreintes digitales de ses clients « s'apparentent davantage à des questions de commodité »[11] qu'à la poursuite d'un objectif impérieux. À cet égard, la CAI note l'absence d'éléments concrets permettant de démontrer l'impact du nouveau système sur l'empreinte écologique de l'entreprise ainsi que l'existence d'une réelle problématique en ce qui concerne le délai d'attente aux caisses et de la fraude.

Quant à la question de la proportionnalité de la collecte par rapport aux objectifs poursuivis par l'entreprise, la CAI précise que lorsqu'il est question de renseignements biométriques comme des empreintes digitales, il importe de considérer les conséquences préjudiciables pouvant résulter de la divulgation et de l'utilisation malveillante de ces renseignements dans l'appréciation de la nécessité de la collecte. En l'espèce, la CAI est d'avis que les risques et les conséquences associés à la collecte des empreintes digitales des clients « surpassent de manière importante les avantages pour l'entreprise »[12]. En outre, Les 3 Piliers n'a pas su démontrer en quoi d'autres solutions moins attentatoires, comme l'envoi de factures électroniques, ne lui permettraient pas d'atteindre ses objectifs. Il convient de mentionner que la CAI semble avoir tiré une inférence négative du fait que Les 3 Piliers n'ait pas procédé à l'évaluation des facteurs relatifs à la vie privée du système de paiement envisagé[13].

1.2 *Cadillac Fairview*

Dans une enquête dont les conclusions ont été rendues publiques le 28 octobre 2020, le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») et ses homologues de l'Alberta et de la Colombie-Britannique se sont penchés sur l'utilisation de la technologie d'analyse vidéo anonyme (ci-après « AVA ») par Cadillac Fairview afin de générer des informations démographiques sur les consommateurs dans ses centres commerciaux[14].

---

11. *Les 3 Piliers Inc.*, préc., note 4, par. 51.
12. *Id.*, par. 60.
13. *Id*.
14. 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*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2020-004.

L'enquête a révélé que Cadillac Fairview avait déployé la technologie d'AVA à même les bornes d'orientation à écran tactile qui permettent aux visiteurs de ses centres commerciaux de trouver des magasins et de s'orienter. Le fonctionnement de la technologie d'AVA se divise en trois temps : 1) la détection d'un visage humain par la caméra installée dans la borne d'orientation ; 2) la saisie d'une photographie du visage afin de générer une représentation numérique du visage et 3) l'estimation de l'âge et du sexe des visiteurs par l'analyse des représentations numériques. Chaque image de visage saisie par la caméra est stockée pour la durée de ce processus qui prend quelques millisecondes à accomplir.

Cadillac Fairfiew a fait valoir que la technologie d'AVA ne procédait pas à une « collecte » de renseignements personnels au sens de la loi en raison du fonctionnement en temps réel de la technologie. Plus précisément, Cadillac Fariview avançait qu'aucun renseignement n'était « enregistré » par la technologie d'AVA puisque celle-ci ne fait que capter un intrant (image du visage) pour produire de façon quasi automatique un extrant (estimation d'âge et de sexe). Or, comme elles sont anonymes, les données démographiques générées par l'AVA ne peuvent être utilisées, seules ou en combinaison avec d'autres informations, pour identifier un individu et elles devraient donc échapper à l'application des lois de protection des renseignements personnels. Par conséquent, l'entreprise soutenait qu'elle n'était pas tenue d'informer les visiteurs de ses centres commerciaux ni d'obtenir leur consentement.

Les commissaires n'ont pas retenu la thèse proposée par Cadillac Fairview et ont plutôt conclu à une collecte de renseignements personnels au sens des lois applicables. Selon eux, il ne fait aucun doute que les images de visages saisies par la technologie d'AVA grâce aux caméras installées sur les bornes d'orientation sont, en soi, des renseignements personnels. Les commissaires estiment que, Cadillac Fairview a tort lorsqu'elle affirme que la technologie d'AVA fonctionne « en temps réel » puisque les images de visages sont conservées en mémoire pendant la très courte période qui correspond au délai de traitement des données. Il y a donc bel et bien « collecte » de renseignements personnels biométriques malgré le fait que leur rétention soit de très courte durée.

Qui plus est, les commissaires sont d'avis que le processus menant à la création d'une représentation numérique du visage d'un individu constitue en soi une collecte de renseignements personnels « parce que ces renseignements proviennent uniquement d'une

personne identifiable particulière et pourrait servir (et sert) [*sic*] dans le cas présent de la technologie d'AVA à faire la distinction entre différentes personnes »[15]. Les représentations numériques générées par la technologie d'AVA doivent donc être considérées comme des renseignements personnels biométriques distincts des images de visages à partir desquelles elles sont produites. Cela étant dit, les commissaires ont reconnu que Cadillac Fairview n'avait pas utilisé les représentations numériques générées par l'AVA dans le but d'identifier ou d'authentifier un individu.

Les commissaires mentionnent également que bien que les données démographiques générées par la technologie d'AVA ne constituent pas en soi des renseignements personnels, celles-ci sont susceptibles de le devenir lorsqu'elles sont conservées avec d'autres renseignements qui permettent de les identifier[16]. En l'espèce, les données démographiques générées par la technologie d'AVA étaient stockées, sans raison apparente, avec les représentations numériques des traits du visage et d'autres informations contextuelles, soit l'heure et le lieu où la photo d'origine avait été prise, sur une même base de données. De l'avis des commissaires, cette situation crée une possibilité sérieuse qu'une personne puisse être identifiée à partir de la combinaison de ces informations suivant le critère formulé par la Cour fédérale dans la décision *Gordon* c. *Canada (Santé)*[17].

Ainsi, selon le CPVP et ses homologues de l'Alberta et de la Colombie-Britannique, Cadillac Fairview aurait dû obtenir un consentement valable avant de recueillir et d'utiliser les renseignements personnels des visiteurs de ses centres commerciaux au moyen de la technologie d'AVA. D'ailleurs, les commissaires sont d'avis que ce consentement aurait dû être explicite considérant la sensibilité des renseignements biométriques ainsi que les attentes raisonnables des visiteurs de centres commerciaux qui ne s'attendent vraisemblablement pas à ce que leur visage soit photographié par une caméra discrète pendant qu'ils effectuent une recherche sur une borne d'orientation numérique. Les commissaires ont suggéré à Cadillac Fairview d'intégrer un encadré contextuel sur ses bornes d'orientation numérique afin d'expliquer aux visiteurs les implications en matière de vie privée associées à la technologie d'AVA et leur permettre de donner leur consentement sans toutefois qu'il s'agisse d'une condition d'accès au répertoire d'orientation.

---

15. *Id.*, par. 65.
16. Les commissaires adoptent l'approche préconisée par la Cour fédérale dans *Gordon* c. *Canada (Santé)*, 2008 CF 258.
17. *Id*.

1.3 Observations

Ces deux affaires témoignent du défi pour les organisations qui souhaitent optimiser l'expérience de leurs usagers à l'aide de technologies ayant recours à la biométrie. À l'heure où il est possible de payer ses achats simplement en présentant son téléphone intelligent, il n'est pas étonnant que plusieurs organisations souhaitent miser sur la technologie pour moderniser leurs services et les rendre plus efficaces. Cela étant, les commissaires estiment que les renseignements biométriques bénéficient d'un niveau de protection accru vu leur degré de sensibilité et les conséquences préjudiciables pour les individus advenant leur divulgation ou leur utilisation non autorisées.

Ainsi, ces deux décisions illustrent l'interprétation large et libérale de la définition de renseignements personnels par les commissaires à la protection de la vie privée. En effet, tant la saisie d'une marque biométrique pour une fraction de seconde que la conversion de cette marque sous une forme numérique ont été assimilées à une collecte de renseignements personnels aux yeux des autorités. En outre, la conservation de données qui ne constituent pas *a priori* des renseignements personnels avec des renseignements biométriques pourrait donner lieu à une « possibilité sérieuse » d'identification si l'on se fie à l'interprétation donnée par les commissaires au critère formulé dans la décision *Gordon*.

Par ailleurs, les organisations qui souhaitent recueillir des renseignements biométriques dans le cadre de projets visant à rendre la prestation de services plus efficace, plus personnalisée ou encore plus écologique devront présenter des éléments concrets à l'appui de leurs prétentions afin de démontrer la nécessité de cette collecte, et ce, même si les individus consentent explicitement à la collecte[18]. En effet, la sensibilité accrue des renseignements biométriques fait en sorte que l'atteinte à la vie privée liée à leur collecte et à leur utilisation est potentiellement plus grande. Ainsi, avant d'entreprendre un projet impliquant la collecte de données biométriques, il est pertinent de se demander si le projet envisagé est nettement plus utile à l'organisation (et aux personnes concernées) que potentiellement préjudiciable

18. Rappelons que la démonstration de la nécessité d'une collecte de renseignements personnels est une règle impérative qui ne peut être écartée même avec le consentement des personnes concernées, voir à ce sujet *Laval (Ville)* c. *X.*, préc., note 9, par. 70 ; Voir aussi *Skyventure Montréal*, 2013 QCCAI 101888 ; *X* et *EB Games*, 2013 QCCAI 081856, par. 17 ; *Garderie Cœur d'Enfant Inc.*, 2014 QCCAI 080272, par. 29 et *Banque Nationale du Canada*, 2016 QCCAI 110676, par. 43.

aux personnes concernées. Si des alternatives moins attentatoires existent, l'organisation devra être en mesure de démontrer en quoi celles-ci ne lui permettent pas d'atteindre les objectifs qu'elle poursuit.

S'agissant du consentement, nous sommes d'avis qu'il est possible de remettre en question les conclusions des commissaires dans l'affaire *Cadillac Fairview* selon lesquelles un consentement explicite doit être exigé pour toute collecte de renseignements biométriques. D'une part, la conclusion des commissaires selon laquelle les représentations numériques des traits du visage sont des renseignements biométriques se base sur le fait que ces renseignements sont dérivés de caractéristiques propres à un individu identifiable et pourraient être utilisés pour faire la distinction entre différentes personnes. Cette interprétation ne correspond toutefois pas strictement aux orientations du CPVP en matière d'utilisation de données biométriques[19], qui traite de celles-ci en lien avec des systèmes permettant l'identification ou l'authentification des individus[20]. En d'autres termes, nous ne sommes pas convaincus que des renseignements générés à partir de l'analyse de caractéristiques physiques doivent inévitablement être considérés comme des « renseignements biométriques » – et donc sensibles – s'ils ne sont pas utilisés en relation avec un système visant l'identification ou l'authentification d'une personne.

D'autre part, s'il est vrai que les individus ont une attente raisonnable en matière de vie privée lorsqu'ils fréquentent des lieux publics, on peut soutenir que celle-ci est néanmoins réduite dans les endroits où ils savent déjà qu'ils sont filmés par des caméras de surveillance, comme un centre commercial ou une épicerie[21]. Ainsi, il n'est pas clair selon nous que la collecte et l'utilisation d'images de personnes physiques doivent nécessairement justifier l'obtention d'un consentement explicite, particulièrement lorsque ces informations sont conservées pendant une très courte période, qu'elles ne font pas l'objet d'un visionnement constant et ne sont pas utilisées à des fins de reconnaissance faciale (c'est-à-dire d'identification ou d'authentification).

19. CPVP, préc., note 7.
20. COMMISSION D'ACCÈS À L'INFORMATION, *Biométrie : principes à respecter et obligations légales des organisations*, 2020, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_G_biometrie_principes-application.pdf>, p. 5.
21. *Eastmond* c. *Canadien Pacifique Ltée*, 2004 CF 852, par. 180.

2. À L'INTERSECTION DU DROIT DE LA CONCURRENCE ET DU DROIT AU RESPECT DE LA VIE PRIVÉE : LE RÈGLEMENT ENREGISTRÉ PAR FACEBOOK AU TRIBUNAL DE LA CONCURRENCE

2.1 Le règlement

Le 19 mai 2020, le Bureau de la concurrence (ci-après le « Bureau ») a annoncé un règlement avec Facebook au sujet d'allégations d'indications fausses ou trompeuses quant à la possibilité pour ses utilisateurs de limiter l'accès et la consultation de leurs renseignements personnels par l'entremise des paramètres de confidentialité[22]. En effet, le Commissaire de la concurrence (ci-après le « Commissaire ») a conclu que Facebook n'avait pas limité le partage des renseignements personnels de ses utilisateurs auprès de certains développeurs tiers de manière cohérente avec ses déclarations au sujet des fonctionnalités de protection des renseignements personnels de sa plateforme. Le Commissaire a également conclu que Facebook avait permis à certains développeurs tiers d'accéder aux renseignements personnels d'amis d'utilisateurs après que ceux-ci eurent installé certaines applications tierces, et ce, en contradiction avec des déclarations antérieures affirmant que cette pratique n'était plus autorisée[23]. Bien que Facebook conteste les allégations du Commissaire, l'entreprise s'est néanmoins engagée, en vertu du règlement, à payer une sanction administrative de 9 millions $, en plus de 500 000 $ en frais, et à respecter les dispositions de la *Loi sur la concurrence*[24] portant sur les pratiques commerciales trompeuses[25].

---

22. BUREAU DE LA CONCURRENCE, « Facebook payera une sanction de 9 millions de dollars pour régler les préoccupations du Bureau de la concurrence à propos d'indications trompeuses quant à la confidentialité », 19 mai 2020, en ligne : <https://www.canada.ca/fr/bureau-concurrence/nouvelles/2020/05/facebook-payera-une-sanction-de-9millions-de-dollars-pour-regler-les-preoccupations-du-bureau-de-la-concurrence-a-propos-dindications-trompeuses-qu.html>.
23. Facebook a annoncé en avril 2014 qu'elle n'autoriserait plus les développeurs tiers à collecter des données sur les amis des utilisateurs d'applications, mais cette pratique se serait poursuivie jusqu'en 2018 selon le CPVP et la FTC. Voir FEDERAL TRADE COMMISSION, « FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook », 24 juillet 2019, en ligne : <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.
24. L.R.C. (1985), ch. C-34.
25. TRIBUNAL DE LA CONCURRENCE, *Facebook, Inc. – Consentement enregistré*, 19 mai 2020, en ligne :<https://decisions.ct-tc.gc.ca/ct-tc/cdo/fr/item/471812/index.do>.

La *Loi sur la concurrence* interdit de donner au public une indication fausse ou trompeuse sur un point important pour promouvoir la fourniture d'un produit, la prestation d'un service ou des intérêts commerciaux[26]. La jurisprudence considère qu'une indication porte « sur un point important » lorsqu'elle est de nature à influencer le consommateur à acheter ou à utiliser le produit ou le service promu[27]. Concrètement, cela signifie inciter les consommateurs à prendre une décision qu'ils n'auraient peut-être pas prise en l'absence de l'information fausse ou trompeuse. Pour déterminer si une indication est fausse ou trompeuse sur un point important, il est tenu compte de l'impression générale donnée par les indications ainsi que du sens littéral de celles-ci[28] ; il n'est pas nécessaire d'établir qu'une personne a été trompée ou induite en erreur par cette représentation.

Dans l'édition de mars 2020 du *Recueil des pratiques commerciales trompeuses*[29], le Bureau s'est penché sur les modèles d'affaires qui reposent sur la collecte des données des consommateurs en échange de produits et de services numériques « gratuits ». Le Bureau y précise qu'un échange d'argent ou de produits tangibles n'est pas nécessaire pour qu'une indication soit visée par les dispositions de la *Loi sur la concurrence*. Ainsi, les transactions non monétaires comme l'accès à un service numérique en échange de données d'utilisation sont encadrées par les règles relatives à la publicité trompeuse. Selon le Bureau, les indications qui sont les plus susceptibles de poser problème dans le contexte des produits et services numériques « gratuits » sont celles qui créent une impression générale fausse ou trompeuse par rapport aux points suivants :

- Des données sur les consommateurs seront-elles recueillies ?
- Quelles données seront recueillies ?
- À quelle fréquence les données seront-elles recueillies ?
- Pourquoi les données seront-elles recueillies et comment seront-elles utilisées ?

---

26. *Loi sur la concurrence*, préc., note 24, art. 74.01.
27. *Commissaire de la concurrence* c. *Premier Career Management Group Corp.*, 2009 CAF 295, par. 20.
28. *Loi sur la concurrence*, préc., note 24, art. 52(4).
29. BUREAU DE LA CONCURRENCE, *Le recueil des pratiques commerciales trompeuses*, vol. 5, 4 mars 2020, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04520.html>.

- Les données seront-elles vendues à des tiers ou partagées avec des tiers ?

- Les données sur les consommateurs seront-elles conservées et comment seront-elles préservées et effacées ?

Ainsi, les entreprises qui collectent des renseignements personnels doivent s'assurer que leurs indications sont conformes au niveau de contrôle réel que les consommateurs peuvent avoir à leur égard. En ce qui concerne Facebook, il faut remonter quelques années en arrière pour faire la lumière sur les allégations d'indications fausses ou trompeuses qui font l'objet du règlement enregistré auprès du Tribunal de la concurrence en 2020.

2.2 Le rôle de Facebook dans le scandale Cambridge Analytica

En avril 2019, après une enquête conjointe, le CPVP et le Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique ont conclu que Facebook n'avait pas obtenu le consentement valide de ses utilisateurs avant de communiquer leurs renseignements personnels[30] à des développeurs d'applications tierces[31]. Au cœur de l'enquête se trouve l'application « This Is Your Digital Life » (ci-après « TYDL »), qui a été développée par Alexsandr Kogan afin de récolter les données de millions d'utilisateurs de Facebook pour le compte de la société Cambridge Analytica. Ces données ont mené à la création de profils psychologiques très détaillés dont s'est servi Cambridge Analytica pour envoyer des messages politiques ciblés.

En outre, en raison de l'interface de programmation d'applications utilisée par Facebook à l'époque, l'application TYDL a non seulement eu accès aux renseignements personnels des utilisateurs qui l'ont installée, mais également aux renseignements des amis de ces utilisateurs, sauf si ces derniers avaient désactivé de façon proactive le partage de leurs renseignements avec les applications utilisées par leurs amis.

---

30. En l'occurrence, le nom, le sexe, la date de naissance, la ville de résidence, la photo de profil, la photo de couverture, la liste d'amis et les pages « aimées » par l'utilisateur.
31. 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.*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2019-002.

De fait, les commissaires ont conclu que Facebook n'avait pas assumé sa responsabilité de veiller à la protection de la confidentialité des renseignements personnels en transférant plutôt celle-ci aux utilisateurs et aux développeurs d'applications. En effet, les commissaires ont jugé qu'en se fiant aux développeurs d'applications tierces pour obtenir le consentement valable des utilisateurs sans mettre en œuvre des mesures raisonnables pour s'assurer que ce consentement était véritablement obtenu et en s'appuyant sur le libellé vague et général de ses conditions d'utilisation, le réseau social a placé les utilisateurs dans une situation où ils ne pouvaient comprendre lesquels de leurs renseignements seraient communiqués, à quelles applications et à quelles fins. Cette situation s'est avérée particulièrement problématique dans le contexte où les renseignements de millions d'utilisateurs auraient été utilisés, à leur insu, afin d'influencer les électeurs convoités par les campagnes politiques des clients de Cambridge Analytica[32].

Or, les commissaires soulignent dans leurs conclusions d'enquête que bien avant les révélations liées à l'affaire Cambridge Analytica, Facebook avait fait de nombreuses déclarations jugées inexactes au sujet de la protection de la confidentialité des renseignements des utilisateurs de sa plateforme[33].

En outre, dans sa *Déclaration des droits et responsabilités* en vigueur à l'époque de l'enquête, le réseau social affirmait : « Le respect de votre vie privée nous tient à cœur » et « Nous exigeons des

32. Au sujet de cette affaire, voir Carole CADWALLADR, « Revealed: how US billionaire helped to back Brexit », *The Observer* (26 février 2017), en ligne : <https://www.theguardian.com/politics/2017/feb/26/us-billionaire-mercer-helped-back-brexit> ; Mattathias SCHWARTZ, « Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate », The Intercept (30 mars 2017), en ligne : <https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/> ; Carole CADWALLADR, « The Great British Brexit Robbery: How Our Democracy Was Hijacked », *The Guardian* (7 mai 2017), en ligne : <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> ; Carole CADWALLADR et Emma GRAHAM-HARRISON, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian* (17 mars 2018), en ligne : <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> ; Stephanie HANKEY, Julianne KERR MORRISSON et Ravi NAIK, *Data and Democracy in the Digital Age*, Londres, The Constitution Society, 2018, en ligne : <https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf> ; Christopher WYLIE, *Mindf*ck: Cambridge Analytica and the Plot to Break America*, New York, Random House, 2019.

33. CPVP, préc., note 31, par. 169-170.

applications qu'elles respectent la confidentialité de vos données » [traduction]. Il convient de rappeler que Facebook a fait l'objet d'une enquête du CPVP en 2009, qui avait révélé l'insuffisance des mesures mises en place pour prévenir l'accès non autorisé aux renseignements personnels des utilisateurs par des applications tierces. À l'époque, le CPVP avait recommandé à Facebook plusieurs mesures par rapport aux applications tierces, notamment :

- limiter l'accès des développeurs d'applications aux renseignements des utilisateurs qui ne sont pas nécessaires au fonctionnement de l'application ;

- informer les utilisateurs des renseignements recueillis par une application et des fins pour lesquelles ils sont utilisés ;

- obtenir un consentement explicite des utilisateurs pour que les développeurs aient accès à leurs renseignements ;

- interdire toute communication de renseignements d'utilisateurs n'ayant pas installé eux-mêmes une application[34].

Selon les commissaires, la mise en œuvre superficielle et inefficace des recommandations formulées dans le rapport d'enquête de 2009, telle qu'illustrée par les faits à l'origine de l'enquête de 2019, représente non seulement « un abus de confiance très grave vis-à-vis des utilisateurs de Facebook, mais aussi un manquement grave quant au respect continu, par Facebook, des lois sur la protection des renseignements personnels du Canada »[35].

2.3 Observations

Le règlement enregistré par Facebook auprès du Tribunal de la concurrence illustre la complémentarité du droit au respect de la vie privée et du droit de la concurrence, deux domaines qui sont rarement abordés conjointement au Canada. En effet, selon le Commissaire, les lacunes de Facebook dans l'application de plusieurs principes établis

34. *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques par Elizabeth Denham Commissaire adjointe à la protection de la vie privée du Canada*, Rapport de conclusions en vertu de la LPRPDE nº 2009-008, par. 211.
35. CPVP, préc., note 31, par. 181.

dans le *Code type sur la protection des renseignements personnels*[36], notamment la responsabilité dans la gestion des renseignements personnels, l'obtention d'un consentement valable et la mise en place de mesures de sécurité adéquates, ont eu des répercussions au-delà des sanctions prévues par la LPRPDE. À cet égard, voir le Bureau de la concurrence travailler main dans la main avec les commissaires à la protection de la vie privée signifie que malgré les pouvoirs d'application limités de ces derniers à l'heure actuelle, les contraventions aux lois relatives à la protection des renseignements personnels peuvent avoir des conséquences sérieuses.

Ainsi, pour éviter toute violation des règles relatives à la publicité fausse ou trompeuse, les organisations dont le modèle d'affaires repose sur la collecte et l'analyse des données numériques auraient intérêt à adopter des mesures périodiques, notamment procéder à l'évaluation des facteurs relatifs à la vie privée de leurs systèmes, pour s'assurer que leurs politiques de confidentialité, leurs documents de marketing et leurs autres déclarations représentent de façon juste leurs pratiques en matière de collecte, d'utilisation, de communication de conservation et de destruction des renseignements personnels des consommateurs, ainsi que le niveau de contrôle réel que les consommateurs ont sur ces activités.

3. LES MENACES INTERNES À LA SÉCURITÉ DE L'INFORMATION : RETOUR SUR L'AFFAIRE *DESJARDINS*

3.1 Un incident de confidentialité sans précédent

Le 14 décembre 2020, le CPVP et la CAI ont rendu publiques les conclusions de leurs enquêtes sur l'incident de confidentialité annoncé par le Mouvement Desjardins en juin 2019[37]. Réalisées en collaboration, ces deux enquêtes ont révélé que les renseignements personnels compromis ont d'abord été copiés, par des employés agissant dans le cadre de leurs fonctions, depuis deux entrepôts de données dont

36. Constituant l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c. 5 (ci-après « LPRPDE »).
37. CPVP, *Enquête sur la conformité à la LPRPDE de Desjardins suite à l'atteinte aux mesures de sécurité des renseignements personnels entre 2017 et 2019*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2020-005, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2020/lprpde-2020-005/> et *Fédération des caisses Desjardins du Québec*, 2020 QCCAI 1020846-S.

l'accès était limité vers un répertoire partagé par le département de marketing. En conséquence,, des employés qui n'avaient normalement pas les autorisations nécessaires pour accéder à ces informations confidentielles ont pu y avoir accès. Ainsi, entre mars 2017 et mai 2019, un employé malveillant, qualifié de « personne-ressource »[38] par ses collègues, a copié les renseignements se trouvant sur le répertoire partagé vers plusieurs clés USB en contravention avec l'accord de confidentialité signé dans le cadre de son emploi chez Desjardins. Les renseignements auraient par la suite été vendus à des tiers[39]. L'accès non autorisé s'est déroulé sur une période de 26 mois avant que Desjardins n'en soit informée par les autorités policières de la Ville de Laval.

Il importe de mentionner que Desjardins est assujettie à la fois à la *Loi sur la protection des renseignements personnels dans le secteur privé*[40] (ci-après « LPRPSP ») pour ce qui est de ses activités au Québec[41] et à la LPRPDE en raison des activités qu'elle exerce dans d'autres provinces ne disposant pas d'une loi jugée essentiellement similaire à la LPRPDE[42]. La LPRPDE trouve également application dans le cadre des opérations commerciales de Desjardins qui impliquent des transferts interprovinciaux ou internationaux de renseignements personnels[43]. Ainsi, le CPVP et la CAI ont tous deux analysé la conformité des pratiques de Desjardins en matière de protection des renseignements personnels à la lumière de la loi qu'ils sont chargés d'appliquer.

L'analyse effectuée par le CPVP et la CAI peut se résumer en trois questions principales :

1. Desjardins a-t-elle mis en place les mesures de sécurité nécessaires pour assurer la sécurité des renseignements personnels qu'elle détient ?

38. CPVP, préc., note 37, par. 41.
39. Félix SÉGUIN, Hugo JONCAS et Andrea VALERIA, « Le suspect du vol de données chez Desjardins n'était qu'un pion », *TVA Nouvelles*, 10 octobre 2019, en ligne : <https://www.tvanouvelles.ca/2019/10/10/vol-dinfos-personnelles-chez-desjardins-le-suspect-netait-quun-pion> ; Éric PLOUFFE, « Fuite de données chez Desjardins : un acheteur de listes devant un tribunal », *Radio-Canada*, 27 octobre 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1744759/tribunal-administratif-francois-baillargeon-bouchard>.
40. RLRQ, c. P-39.1.
41. *Fédération des caisses Desjardins du Québec*, préc., note 37, par. 27.
42. CPVP, préc., note 37, par. 18.
43. *Id*.

2. Desjardins a-t-elle respecté les exigences en matière de conservation et de destruction des renseignements personnels ?

3. Les mesures d'atténuation offertes par Desjardins aux personnes touchées étaient-elles adéquates pour protéger leurs renseignements personnels contre une utilisation non autorisée par des tiers malveillants ?

3.1.1 Mesures de sécurité

Tant la LPRPSP que la LPRPDE prévoient que les entreprises doivent adopter des mesures de sécurité afin de protéger les renseignements personnels qu'elles détiennent[44]. Ces mesures doivent être proportionnelles au degré de sensibilité des renseignements, à leur quantité et à leur finalité d'utilisation. Selon les deux commissaires, les renseignements personnels compromis peuvent être qualifiés de sensibles, que ce soit par nature (ex. : numéro d'assurance sociale, habitudes transactionnelles) ou en raison de la possibilité que ceux-ci soient utilisés par des fraudeurs pour usurper l'identité des individus[45]. Ainsi, Desjardins devait mettre en place des mesures de sécurité particulièrement rigoureuses afin d'assurer la protection de ces renseignements.

Les mesures visant la protection de l'information confidentielle se divisent généralement en trois catégories, soit :

- les mesures physiques (ex. : restriction de l'accès à certains locaux, verrouillage des classeurs) ;

- les mesures administratives (ex. : formation et sensibilisation des employés, politiques et directives en matière de sécurité de l'information, droits d'accès restreints aux fichiers) ;

- les mesures techniques (ex. : mots de passe, chiffrement, journalisation)[46].

---

44. LPRPSP, préc., note 40 et LPRPDE, préc., note 36, annexe 1, principe 4.7.
45. CPVP, préc., note 37, par. 38 ; *Fédération des caisses Desjardins du Québec*, préc., note 37, par. 35.
46. LPRPDE, préc., note 36, annexe 1, principe 4.7.3 ; Voir aussi Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Montréal, Éditions Yvon Blais, 2010, p. 42.

En outre, les menaces à la sécurité de l'information peuvent être internes – comme dans le cas qui nous occupe – ou externes – comme dans la décision *Equifax*, que nous aborderons à la prochaine section. Les menaces internes malveillantes sont particulièrement difficiles à prévenir puisqu'elles sont l'œuvre d'employés qui connaissent bien les systèmes de l'organisation et qui savent tirer profit de leurs faiblesses. L'enquête du CPVP a d'ailleurs révélé qu'au moment de l'incident, la majorité du budget consacré par Desjardins à la sécurité de l'information visait à prévenir et à combattre les menaces externes[47].

Bien que Desjardins ait adopté un cadre de gestion comportant un arsenal de directives, politiques et procédures liées à la protection des renseignements personnels, la mise en œuvre de plusieurs de ces politiques s'est avérée déficiente selon le CPVP et la CAI. Par exemple, le *Standard de sécurité sur la protection des données de Desjardins* prévoit que seul le personnel autorisé peut consulter, modifier ou communiquer les données stockées par l'organisation. Ce document précise également que le responsable d'une base de données qui contient de l'information confidentielle doit s'assurer que les accès et permissions y sont gérés de façon à assurer la confidentialité. Or, l'enquête a mis au jour un transfert de renseignements confidentiels depuis un entrepôt de données à accès restreint vers un répertoire accessible à des employés ne disposant pas des autorisations requises. En outre, la politique relative au *Mouvement sur l'utilisation des technologies* interdit le stockage de renseignements personnels sur des appareils n'appartenant pas à l'organisation. Pourtant, l'enquête des commissaires a révélé que le blocage des ports USB n'était pas activé, ce qui a permis à l'employé malveillant de transférer les renseignements personnels des membres sur ses appareils de stockage amovibles personnels.

La formation et la sensibilisation des employés à l'égard des enjeux relatifs à la sécurité de l'information font partie des mesures qu'une organisation doit prendre pour prévenir les menaces internes. Selon les commissaires, le fait que des employés dûment autorisés aient déposé des renseignements confidentiels dans des répertoires partagés en contravention évidente avec les directives et politiques de Desjardins soulève des doutes quant au niveau de sensibilisation réel des employés. Considérant que « [l]e facteur humain est le maillon le plus faible dans un système de sécurité informatique »[48], les lacunes au

47. CPVP, préc., note 37, par. 39.
48. *Id.*, par. 58.

chapitre de la formation du personnel et l'absence d'une « culture de vigilance »[49] au sein de l'organisation sont des facteurs qui ont considérablement facilité l'atteinte aux mesures de sécurité selon le CPVP.

En ce qui concerne les mesures techniques, les enquêtes ont révélé que la surveillance mise en place par Desjardins au moment de l'incident était essentiellement passive, c'est-à-dire que l'analyse et la corrélation des journaux d'activités ne s'effectuaient qu'après que des alertes aient été déclenchées. Or, le CPVP note : « Une organisation comme Desjardins, qui traite un volume important de transactions concernant des renseignements personnels sensibles, doit se doter d'un système de surveillance active »[50]. Par ailleurs, Desjardins était au courant des vulnérabilités de ses systèmes au cours de la période pendant laquelle l'incident s'est déroulé puisque plusieurs audits, tant internes qu'externes, avaient identifié des risques en matière de sécurité d'information. En outre, les commissaires ont constaté que Desjardins a tardé à adopter plusieurs recommandations contenues dans ces rapports d'audit, comme le blocage des ports USB et le déploiement complet d'une stratégie de prévention de la perte de données (« data loss prevention » ou DLP)[51].

3.1.2 Conservation et destruction

En vertu du principe de limitation, les organisations ne doivent conserver des renseignements personnels que pour la durée nécessaire à la réalisation des fins pour lesquelles ils les ont recueillies[52]. Ainsi, lorsque la finalité d'un renseignement personnel est accomplie, l'organisation doit, sous réserve d'autres exigences pouvant être prévues par la loi[53], détruire ou anonymiser les renseignements personnels qu'elle détient[54].

Les enquêtes du CPVP et de la CAI ont révélé que près de 4 millions de dossiers étaient inactifs, c'est-à-dire que Desjardins n'avait plus aucune relation avec les membres en question, lorsque

---

49. *Id.*, par. 41.
50. *Id.*, par. 80.
51. CPVP, préc., note 37, par. 81 ; *Fédération des caisses Desjardins du Québec*, préc., note 37, par. 66.
52. LPRPDE, préc., note 36, annexe 1, principe 4.5 ; LPRPSP, préc., note 40, art. 12.
53. Par exemple, les lois fiscales exigent la conservation des documents de nature financière pour une durée de sept ans, voir *Loi sur l'administration fiscale*, RLRQ, c. A-6 002, art. 35.1 et *Loi de l'impôt sur le revenu*, L.R.C. (1985), ch. 1 (5e suppl.), art. 230(4).
54. LPRPDE, préc., note 36, annexe 1, principe 4.5.3.

l'employé malveillant y a accédés[55]. Au moment de l'incident, Desjardins était en train de développer son calendrier de conservation, de sorte que l'institution n'avait pas de procédure en place afin d'assurer la destruction des renseignements personnels une fois leur finalité accomplie. Cette affaire illustre que la conservation de renseignements personnels pour une durée plus longue que nécessaire par une organisation augmente le risque auquel elle s'expose advenant un incident de confidentialité.

3.1.3 Mesures d'atténuation

L'adoption de mesures de sécurité propres à assurer la protection des renseignements personnels s'accompagne d'une obligation de prendre des mesures d'atténuation à la suite d'un incident de confidentialité afin de réduire le risque de préjudice pour les personnes touchées[56].

À cet égard, les commissaires notent que Desjardins a rapidement mis sur pied un plan d'action offrant aux membres touchés plusieurs mesures, notamment :

- Un site Web et un centre d'appel destiné aux questions des membres sur l'incident et sur les mesures de protection associées ;
- Un Plan de protection pour tous les membres actuels et futurs de Desjardins[57] ;
- Un accès illimité à leur dossier de crédit auprès de TransUnion.

---

55. CPVP, préc., note 37, par. 89 ; *Fédération des caisses Desjardins du Québec*, préc., note 37, par. 73.
56. CPVP, *Enquête sur la conformité d'Equifax Inc. et d'Equifax Canada à la LPRPDE à la suite de l'atteinte à la sécurité des renseignements personnels en 2017*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2019-001, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-001>, par. 148, voir aussi LPRPDE, préc., note 36, art. 10.1 et *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64, art. 2(1)e).
57. Ce Plan comprend quatre éléments : 1) une protection permanente permettant un remboursement complet de toute perte causée par des transactions non autorisées dans les comptes de clients ; 2) une protection qui donne droit au remboursement des frais engagés dans des démarches de restauration d'identité ; 3) une assistance directe et personnalisée dans les démarches de réhabilitation en cas de vol d'identité et 4) la surveillance quotidienne du dossier de crédit par Equifax avec des alertes en cas d'activité ou de modification de la cote de crédit. Voir CPVP, préc., note 37, par. 105.

Le CPVP a souligné que les mesures d'atténuation mises en place par Desjardins à la suite de l'incident « dépassent, de manière significative, celles offertes par d'autres organisations à la suite des fuites importantes »[58].

3.2 Observations

L'incident de confidentialité impliquant Desjardins est porteur de leçons pour les organisations qui détiennent un volume considérable de renseignements personnels de leurs clients.

Le premier enseignement est sans contredit l'importance ne pas sous-estimer les menaces internes à la sécurité de l'information. En effet, l'accès non autorisé aux renseignements personnels qui s'est produit chez Desjardins est loin d'être un cas isolé étant donné qu'environ 60 % des atteintes aux mesures de sécurité sont causés par une menace interne, selon une étude réalisée par IBM[59].

En outre, l'adoption de politiques et de directives en matière de sécurité de l'information n'est pas suffisante pour prévenir les menaces internes si elle ne s'accompagne pas d'une formation et d'une sensibilisation effective du personnel. Les exigences prévues aux politiques doivent également se refléter dans les mesures physiques et techniques mises en place par l'organisation. Ainsi, selon les commissaires, le blocage des ports USB aurait permis d'éviter l'exfiltration de renseignements personnels sur des appareils de stockage amovibles. Les enquêtes des commissaires soulignent également que les organisations qui traitent une grande quantité de renseignements personnels doivent se doter de mécanismes permettant d'assurer une surveillance active des technologies utilisées par leurs employés. À ce titre, la prévention de la perte de données (« data loss prevention » ou DLP), l'analyse des comportements des utilisateurs et entités (« user and entity behaviour analytics » ou UEBA) et le système de gestion de l'information et des événements de sécurité (« security information and event management » ou SIEM) sont au nombre des solutions recommandées.

L'affaire *Desjardins* est également un rappel que la meilleure mesure de sécurité qu'une organisation peut adopter est de ne pas

58. *Id.*, par. 106.
59. Marc VAN ZADELHOFF, « The Biggest Cybersecurity Threats Are Inside Your Company », *Harvard Business Review*, 19 septembre 2016, en ligne : <https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company>.

conserver des renseignements personnels non nécessaires[60]. Pour ce faire, les organisations doivent être en mesure d'identifier les renseignements personnels qu'elles conservent ainsi que leur finalité. Procéder à une cartographie des renseignements personnels détenus par l'organisation est un bon point de départ en ce sens. Il est également important de mettre en place une procédure visant à assurer la destruction ou l'anonymisation automatique des renseignements personnels à la fin de leur cycle de vie.

Finalement, l'affaire *Desjardins* fournit un exemple probant de ce que constitue une réaction appropriée d'une organisation à la suite d'un incident de confidentialité. En effet, tant la CAI que le CPVP ont souligné que les mesures d'atténuation mises en place par Desjardins étaient à la hauteur de la gravité de la situation.

4. ACTIONS COLLECTIVES À LA SUITE D'UN INCIDENT DE CONFIDENTIALITÉ : LA DÉCISION *EQUIFAX*

4.1 *Li* c. *Equifax Inc.*

Le 7 septembre 2017, Equifax Inc. a annoncé que plus de 143 millions de personnes à travers le monde, dont environ 19 000 Canadiens, avaient été victimes d'un accès non autorisé à leurs renseignements personnels à la suite d'une cyberattaque[61]. Les Canadiens touchés auraient vu leur nom, leur adresse, leur date de naissance et leur numéro d'assurance sociale être compromis par cet incident de confidentialité.

Peu de temps après l'annonce de l'incident, M. Daniel Li dépose une demande d'autorisation pour exercer une action collective pour le compte de « [t]outes les personnes au Québec qui, en tout temps avant le 7 septembre 2017, avaient des renseignements personnels ou de crédit recueillis par Equifax et entreposés par cette dernière ET qui étaient à risque de perte de ces renseignements à la suite d'un accès non autorisé survenu entre mai et juillet 2017, ou tout sous-groupe à

60. Dans l'affaire *TJX*, le CPVP a reconnu que la collecte et la conservation des numéros de permis de conduire des clients qui effectuaient des retours de marchandises n'étaient pas nécessaires au sens de la loi, voir CPVP, *TJX Companies Inc. / Winners Merchant International L.P.*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2007-389, par. 7.

61. EQUIFAX, « Equifax Announces Cybersecurity Incident Involving Consumer Information », 7 septembre 2017, en ligne : <https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628>.

être déterminé par le Tribunal »[62]. Le recours du demandeur repose essentiellement sur trois fondements juridiques :

- la responsabilité extracontractuelle d'Equifax de veiller à la protection des renseignements personnels et financiers des membres du groupe, en vertu de l'article 1457 du *Code civil du Québec*[63] (ci-après « C.c.Q. ») ;

- la violation du droit au respect de la vie privée et de la réputation des membres du groupe garanti par les articles 3, 35 et 37 C.c.Q. résultant de la communication ou du défaut d'empêcher la communication à des tiers des renseignements personnels des membres du groupe ;

- la violation du droit à la vie privée et à la non-communication des renseignements confidentiels des membres du groupe garanti par les articles 5 et 9 de la *Charte des droits et libertés de la personne*[64] (ci-après « Charte québécoise »).

Le demandeur réclame des dommages compensatoires et punitifs en réparation du préjudice subi par l'accès non autorisé par un tiers aux renseignements personnels des membres du groupe. Plus précisément, le préjudice allégué par le demandeur se divise en trois éléments, soit :

- les dépenses, troubles et inconvénients associés à l'accès non autorisé, dont l'annulation de cartes de crédit et l'achat de services de protection d'identité comme le suivi du crédit ;

- le préjudice moral lié au stress ressenti par le fait de se savoir à risque d'être victime d'un vol ou d'une fraude d'identité ; et

- les « autres pertes » [traduction] liées à l'incident de confidentialité.

Dans son analyse du critère d'apparence de droit[65], le juge Donald Bisson de la Cour supérieure conclut que les faits allégués dans la demande d'autorisation sont suffisants pour démontrer *prima facie* que l'incident de confidentialité résulte d'une faute d'Equifax, soit de ne pas avoir pris les mesures nécessaires pour protéger

62. *Li* c. *Equifax Inc.*, 2019 QCCS 4340, par. 1.
63. *Code civil du Québec*, RLRQ, c. CCQ-1991.
64. *Charte des droits et libertés de la personne*, RLRQ, c. C-12.
65. *Code de procédure civile*, RLRQ, c. C-25.01, art. 575(2).

les renseignements personnels du demandeur et des membres du groupe[66]. Le juge est également satisfait des allégations du demandeur selon lesquelles la communication ou le défaut de prévenir la communication à des tiers de renseignements confidentiels sans l'autorisation des membres du groupe constitue une violation du droit au respect de la réputation et de la vie privée[67].

Toutefois, pour ce qui est des dommages subis par le demandeur, la Cour rappelle qu'au stade de l'autorisation, le recours n'existe pas encore sur une base collective[68]. C'est donc à la lumière de la situation personnelle du demandeur que la Cour doit déterminer si la cause est défendable[69]. Ainsi, le tribunal constate que non seulement le demandeur n'a pas été victime d'un vol d'identité, mais il n'a pas non plus déboursé d'argent pour l'achat de services de protection d'identité. Bref, selon le juge Bisson, le « préjudice » allégué par le demandeur repose sur « [un] risque futur et de[s] dépenses à venir »[70].

Or, le droit québécois ne reconnaît pas la possibilité d'obtenir compensation pour un préjudice incertain et hypothétique[71]. Comme l'a rappelé la Cour supérieure dans la décision *Zuckerman* c. *Target Corporation*[72], le suivi qu'un particulier fait de ses comptes bancaires et de ses cartes de crédit constitue une activité normale et non un « trouble et inconvénient » pour lequel il peut obtenir réparation. Par contre, le fait de se procurer, à ses frais, un plan de suivi de son dossier de crédit, d'entreprendre des démarches pour annuler des cartes de paiement ou de faire rectifier sa cote de crédit à la suite de transactions non autorisées sont des événements qui peuvent donner ouverture à un droit à l'indemnisation. Par exemple, au stade de l'autorisation, une dépense de 19,95 $ pour des services de surveillance du crédit a été considérée comme un préjudice indemnisable dans la décision *Zuckerman*[73], tout comme l'extension d'un programme de surveillance de crédit (dont la première année était payée par l'entreprise défenderesse) au coût de 6,90 $ dans l'affaire *Lévy* c. *Nissan Canada inc.*[74].

---

66. *Li* c. *Equifax Inc.*, préc., note 62, par. 23.
67. *Id*.
68. *Bouchard* c. *Agropur Coopérative*, 2006 QCCA 1342, par. 109.
69. *Sofio* c. *Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820, par. 10.
70. *Li* c. *Equifax Inc.*, préc., note 62, par. 27.
71. Art. 1611 C.c.Q.
72. 2017 QCCS 110.
73. *Id.*, par. 76.
74. *Lévy* c. *Nissan Canada inc.*, 2019 QCCS 3957, par. 108.

En ce qui concerne le préjudice moral, ou « mental distress », allégué par le demandeur, la Cour précise qu'en l'absence de détails supplémentaires permettant de mieux caractériser la situation, ce dommage ne saurait s'élever au-dessus des « désagréments, angoisses et craintes ordinaires que toute personne vivant en société doit régulièrement accepter fût-ce à contrecœur »[75]. En d'autres termes, et pour reprendre les mots de la Cour suprême dans l'arrêt *Mustapha* c. *Culligan du Canada Ltée*[76], le stress et l'anxiété occasionnés par l'accès non autorisé aux renseignements personnels du demandeur représentent des « contrariétés mineures et passagères n'équivalent pas à un préjudice personnel et, de ce fait, ne constituent pas un dommage »[77].

La Cour rejette également la réclamation de dommages punitifs pour violation illicite et intentionnelle du droit à la vie privée et du droit à la non-divulgation des renseignements confidentiels, vu que la demande ne contient aucun détail ou fait permettant de justifier une telle allégation[78]. Le tribunal arrive donc à la conclusion que le recours intenté par M. Li n'a pas d'apparence de droit et doit être rejeté.

4.2 Observations

Dans le contexte où le nombre d'organisations visées par des cyberattaques ne cesse d'augmenter[79], la judiciarisation des incidents de confidentialité est une tendance qui ne risque pas de s'estomper. En ce sens, la décision *Li* c. *Equifax inc.* est importante puisqu'elle précise les conditions nécessaires pour qu'une action collective intentée en réponse à un incident de confidentialité puisse avoir une apparence sérieuse de droit.

Ainsi, au regard de la faute, la démonstration de l'insuffisance des mesures de sécurité censées prévenir l'accès non autorisé aux renseignements personnels détenus par une organisation ne semble pas être un fardeau particulièrement difficile à satisfaire pour la

75. *Li* c. *Equifax Inc.*, préc., note 62, par. 31 citant *Mustapha* c. *Culligan du Canada Ltée*, 2008 CSC 27, par. 9.
76. 2008 CSC 27.
77. *Mustapha* c. *Culligan du Canada Ltée*, préc., note 75, par. 9.
78. *Li* c. *Equifax Inc.*, préc., note 62, par. 41.
79. RISK BASED SECURITY, « 2020 Year End Data Breach QuickView Report », 2020, en ligne : <https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report>.

partie demanderesse. Cela n'est toutefois pas suffisant pour que le recours soit autorisé puisque le demandeur doit également faire la démonstration *prima facie* qu'il a personnellement subi un préjudice indemnisable, c'est-à-dire un dommage qui soit réel, non hypothétique et qui dépasse les contrariétés de la vie courante. En ce sens, les organisations auraient tout intérêt à mettre en place un plan de contingence efficace advenant un incident de confidentialité, incluant notamment la prestation rapide d'un service de suivi du dossier de crédit aux individus touchés afin de réduire le risque de litiges en matière de responsabilité.

Par ailleurs, il pertinent de souligner que la Cour supérieure a accordé peu de considération au rapport de conclusions d'enquête du CPVP publié le 9 avril 2019[80], qui concluait que la plainte concernant Equifax était fondée vu les multiples lacunes de l'entreprise au chapitre des mesures de sécurité et son laxisme dans l'application de ses propres politiques de conservation des renseignements personnels. Fait notable, le CPVP indique dans ses conclusions qu'en raison du caractère sensible des renseignements personnels compromis, l'incident de confidentialité d'Equifax crée un « risque réel de préjudice » pour les personnes concernées en cas d'utilisation non autorisée par des acteurs malveillants[81]. La décision de la Cour supérieure constitue donc un rappel clair de l'étanchéité des rapports qu'entretient le droit civil avec les instances administratives.

La décision *Li* c. *Equifax inc.* illustre également le caractère distinctif du régime québécois en en matière d'autorisation d'actions collectives fondées sur des incidents de confidentialité. En effet, depuis l'arrêt *Jones* v. *Tsige* de la Cour d'appel de l'Ontario, qui a reconnu le droit d'action fondé sur la notion d'« intrusion upon seclusion » en common law[82], une action collective peut être autorisée en Ontario malgré l'absence de perte financière réelle puisque ce fondement juridique autorise l'octroi de dommages symboliques. C'est d'ailleurs ce qui s'est produit dans le recours intenté en Ontario contre Equifax sur la base du même incident de confidentialité[83].

80. CPVP, préc., note 56.
81. *Id.*, par. 20.
82. *Jones* v. *Tsige*, 2012 ONCA 32.
83. *Agnew-Americano* v. *Equifax Canada Co.*, 2019 ONSC 7110.

5. RÉPUTATION EN LIGNE : L'AFFAIRE *RATEMDS*

5.1 RateMDs.com

Une dentiste exerçant en Colombie-Britannique a déposé une plainte au CPVP après avoir découvert un profil à son sujet sur le site Web www.ratemds.com (ci-après « RateMDs »). Le profil en question contient le nom de la plaignante, son domaine d'exercice, le nom et l'adresse de sa clinique ainsi que plusieurs avis, tant positifs que négatifs, sur sa pratique. La plaignante allègue que RateMDs a enfreint la LPRPDE en publiant ses renseignements personnels sans son consentement et en refusant d'agréer à sa demande de retirer les renseignements, y compris les avis des clients.

RateMDs se décrit comme « un site Web d'évaluation de professionnels de la santé destiné à permettre aux patients de classer et d'évaluer les professionnels de la santé auxquels ils font appel afin que d'autres patients puissent prendre des décisions plus éclairées au sujet de leurs soins de santé »[84]. Pour atteindre cet objectif, RateMDs permet à ses utilisateurs de créer le profil d'un professionnel de la santé contenant son nom, son sexe, sa spécialité, sa pratique principale et ses coordonnées professionnelles[85]. Une fois le profil créé, RateMDs permet aux anciens patients de soumettre anonymement leurs avis sur la pratique et la personnalité du professionnel de la santé. Selon RateMDs, ces avis ont pour but d'aider les gens à trouver un professionnel de la santé dans leur région[86].

RateMDs offre à ses utilisateurs, y compris aux professionnels de la santé, l'option de signaler un avis au personnel du site Web, qui peut retirer tout avis jugé inapproprié. RateMDs affirme toutefois qu'aucun avis n'est retiré sur la base de la seule plainte d'un professionnel qui le juge injuste à ses yeux[87]. RateMDs offre également aux professionnels de la santé l'option de souscrire à un abonnement payant qui leur permet, entre autres, de masquer jusqu'à trois avis jugés suspects et de mettre en avant des avis favorables. Selon le site Web, cette fonctionnalité, appelée « Ratings Manager », n'équivaut pas à exiger un paiement pour procéder au retrait des renseignements personnels d'un professionnel de la santé[88].

---

84. CPVP, *Un site d'évaluation des professionnels de la santé cesse de facturer le retrait des avis, une « zone interdite » de la LPRPDE*, Conclusions en vertu de la LPRPDE nº 2020-002, par. 8.
85. *Id.*, par. 10.
86. *Id.*, par. 13.
87. *Id.,* par. 21.
88. *Id.*, par. 28.

5.2 L'analyse du CPVP

La première question qui s'est posée est la nécessité, pour RateMDs, d'obtenir le consentement de la plaignante pour la publication de ses renseignements personnels. Le CPVP indique que les renseignements de la plaignante publiés sur le site Web se divisent en deux catégories, soit : ses coordonnées d'affaires (c.-à-d. son nom et l'adresse ainsi que le numéro de téléphone de sa clinique), d'une part, et les avis des utilisateurs du site au sujet de sa pratique professionnelle, d'autre part.

En ce qui concerne les coordonnées d'affaires de la plaignante, le CPVP est d'avis que celles-ci ne peuvent bénéficier de l'exemption prévue à l'article 4.01 de la LPRPDE puisqu'en l'espèce, elles ne sont pas utilisées « uniquement pour entrer en contact ou pour faciliter la prise de contact »[89] avec la plaignante dans le cadre de son emploi, de son entreprise ou de sa profession. En effet, l'objectif avoué de RateMDs n'est pas de faciliter le contact avec les professionnels de la santé, mais de permettre aux patients potentiels de « prendre une décision éclairée ». Ainsi, le CPVP souligne qu'une des conséquences possibles de la consultation du profil d'un professionnel sur RateMDs est qu'une personne décide de ne *pas* communiquer avec un professionnel de la santé en raison des avis qui y sont publiés[90].

Le CPVP est cependant d'avis que les coordonnées d'affaires de la plaignante peuvent se qualifier au regard d'une autre exception reconnue par la LPRPDE, soit celle concernant les « renseignements réglementaires auxquels le public a accès »[91]. Il s'agit des cinq catégories de renseignements spécifiquement identifiées dans le *Règlement précisant les renseignements auxquels le public a accès*[92], soit les renseignements personnels figurant dans :

- un annuaire téléphonique accessible au public ;
- un répertoire à caractère professionnel ou d'affaires qui est accessible au public ;
- un registre public dont la loi exige la tenue ;

89. LPRPDE, préc., note 36, art. 4.01.
90. CPVP, préc., note 84, par. 37.
91. LPRPDE, préc., note 36, art. 7(1)d) ; 7(2)c.1) et 7(3)h.1).
92. DORS/2001-7.

- les dossiers d'un organisme judiciaire ou quasi judiciaire et auxquels le public a accès et
- une publication, sous forme imprimée ou électronique, qui est accessible au public[93].

Ainsi, étant donné que les coordonnées d'affaires de la plaignante publiées sur son profil RateMDs se retrouvent à la fois dans le registre du College of Dental Surgeons of British Columbia, dans les Pages Jaunes et dans des répertoires en ligne de professionnels ou d'entreprises[94], le CPVP conclut que RateMDs n'a pas à obtenir le consentement de la plaignante pour la collecte, l'utilisation ou la communication de ses renseignements[95].

Concernant les avis des utilisateurs de RateMDs au sujet de leur expérience avec un professionnel de la santé, le CPVP est d'avis que ceux-ci constituent des renseignements personnels aussi bien de la plaignante que des utilisateurs qui les ont publiés[96]. Cette interprétation est cohérente avec la jurisprudence de la Cour d'appel fédérale qui a confirmé que de mêmes renseignements peuvent être « personnels » pour plusieurs personnes[97]. Cette qualification a pour conséquence d'obliger RateMDs à obtenir le consentement des utilisateurs et des professionnels pour publier les avis sur son site Web. Or, le CPVP souligne que « lorsque les intérêts des personnes sont en conflit, cela sera rarement possible »[98].

Le CPVP se livre ensuite à un exercice de pondération des intérêts en jeu, à savoir le droit des patients au partage de leur expérience avec un professionnel de la santé, le droit des professionnels au respect de leur vie privée et de leur réputation, ainsi que l'intérêt du public d'accéder à de l'information pertinente. Le CPVP arrive à la conclusion que de donner préséance à l'absence de consentement de la plaignante serait préjudiciable par rapport aux intérêts en jeu[99]. Ainsi, RateMDs n'avait pas besoin d'obtenir le consentement de la personne pour publier les avis d'anciens patients à son sujet.

---

93. *Id.*, art. 1.
94. CPVP, préc., note 84, par. 43.
95. *Id.*, par. 44.
96. *Id.*, par. 49 à 51.
97. *Canada (Commissaire à l'information)* c. *Canada (Ministre de la Citoyenneté et de l'Immigration)*, 2002 CAF 270, par. 15 et *Wyndowe* c. *Rousseau*, 2008 CAF 39, par. 50.
98. CPVP, préc., note 84, par. 53.
99. *Id.*, par. 58.

Le CPVP se penche ensuite sur la question de la transparence et de la raisonnabilité des pratiques de RateMDs au regard des principes établis dans la LPRPDE. Dans le premier cas, le CPVP conclut que RateMDs a enfreint le principe 4.8 de la LPRPDE[100] en n'indiquant pas clairement aux professionnels de la santé leur droit de demander la correction ou la modification des renseignements les concernant lorsqu'ils estiment que ceux-ci sont inexacts, incomplets ou ne sont pas à jour[101].

Dans le second cas, le CPVP rappelle que la publication de renseignements personnels dans le but de réclamer un paiement aux individus pour leur retrait est considérée comme une des « zones interdites » par le paragraphe 5(3) LPRPDE selon le *Document d'orientation sur les pratiques inacceptables du traitement des données : interprétation et application du paragraphe 5(3)*[102]. Ainsi, à l'instar de la Cour fédérale, qui a reconnu, dans la décision *Globe24h*[103], que les activités d'une organisation qui consistaient à republier des décisions de tribunaux canadiens afin de faire payer les gens pour procéder à leur retrait étaient contraires au paragraphe 5(3), le CPVP a considéré que le « Ratings Manager » de RateMDs constitue « un exemple clair d'une pratique inappropriée de "paiement pour retrait", en contravention du paragraphe 5(3) de la Loi »[104]. En effet, une personne n'estimerait pas acceptable qu'une plateforme qui autorise la publication d'avis négatifs sur des professionnels de la santé génère des revenus en demandant à ces mêmes professionnels une somme d'argent pour procéder au retrait des avis en question[105].

5.3 Observations

L'affaire *RateMDs* est l'exemple typique d'une situation factuelle assez banale qui soulève pourtant des questions juridiques importantes.

---

100. Le principe 4.8 de l'annexe 1 de la LPRPDE prévoit : « Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne ».
101. *Id.*, par. 72.
102. CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : interprétation et application du paragraphe 5(3)*, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/>.
103. *A.T.* c. *Globe24h.com*, 2017 CF 114.
104. CPVP, préc., note 84, par. 80.
105. *Id*.

Premièrement, la décision du CPVP nous renseigne sur la portée de deux exemptions importantes à la LPRPDE : celle pour les coordonnées d'affaires et celle pour les renseignements publiquement accessibles. Dans le premier cas, le CPVP confirme que l'article 4.01 LPRPDE doit être interprété restrictivement ; cette exception ne peut donc s'appliquer que si les coordonnées d'affaires servent exclusivement à faciliter la prise de contact avec un professionnel. Par ailleurs, il est pertinent de mentionner que le Québec s'apprête à introduire une exception similaire, quoique moins restreinte, dans la LPRPSP[106]. Dans le second cas, l'exemption pour les renseignements publiquement accessibles ne semble pas être soumise à une telle restriction. Ainsi, dans la mesure où cette exception exige que les renseignements accessibles au public soient collectés, utilisés ou divulgués pour un but particulier – généralement celui pour lequel l'information se retrouve dans le registre ou le répertoire en question –, cette condition pourra être remplie même s'il ne s'agit pas du seul but poursuivi par l'organisation avec ces renseignements. En outre, étant donné que les renseignements ont été ajoutés sur RateMDs par les utilisateurs, le CPVP semble implicitement admettre que les organisations n'ont pas à recueillir les renseignements auxquels le public a accès directement auprès de la source désignée par la réglementation afin de bénéficier de l'exception.

Deuxièmement, la décision RateMDs réaffirme le fait que les avis, commentaires et évaluations au sujet d'une personne sont à la fois les renseignements personnels de la personne visée et ceux de la personne qui les publie. D'ailleurs, lorsque les intérêts de ces deux personnes sont concurrents, les organisations doivent donc se livrer à une pondération avant de donner la priorité aux intérêts de l'un plutôt qu'à ceux de l'autre. Il s'agit d'un exercice délicat dans la mesure où les intérêts des organisations peuvent aussi entrer en ligne de compte (par exemple, une organisation a généralement intérêt à garder du contenu sur sa plateforme).

Un troisième élément clé est l'obligation pour les organisations de faire preuve de transparence et d'ouverture quant à ses politiques et pratiques en matière de gestion des renseignements personnels. En

106. Le projet de loi nº 64 propose d'ajouter à l'art. 1 LPRPSP une précision selon laquelle la loi ne s'applique pas « aux renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail » : voir *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 2, art. 93.

effet, il ne suffit pas d'avoir une procédure en place qui permet aux individus de faire rectifier leurs renseignements ; encore faut-il que ces personnes soient informées de leurs droits et des moyens pour les exercer. Pour ce faire, les organisations ont intérêt à utiliser un langage clair dans leurs politiques de protection de la vie privée et à les rendre disponibles aux personnes concernées dans un format facilement accessible.

De façon plus fondamentale, l'affaire *RateMDs* illustre que la LPRPDE n'est pas un outil adapté pour trancher les conflits qui opposent le droit à la vie privée de certaines personnes aux droits et aux intérêts d'autres personnes et du public en général. En effet, la décision du CPVP donne préséance aux « droits » des utilisateurs de la plateforme sur celui des professionnels de la santé. Or, à notre avis, il est loin d'être clair que les patients d'un professionnel de la santé possèdent un « droit » au partage de leurs expériences personnelles sur un site Web comparativement au droit des professionnels au respect de leur vie privée et de leur réputation qui, lui, est bien réel[107]. En outre, la prise en considération de critères comme le droit à la liberté d'expression et le droit du public à l'information dans l'interprétation et l'application de la législation en matière de protection des renseignements personnels dans le secteur privé risque selon nous de causer des maux de tête aux organisations qui doivent répondre à des demandes d'accès ou de rectification. Par ailleurs, nous trouvons curieux que le CPVP se soit livré à un tel arbitrage au lieu de considérer l'applicabilité de l'exception pour la collecte et l'utilisation de renseignements personnels à des fins journalistiques, qui aurait permis d'exclure les avis publiés sur RateMDs du champ d'application de la LPRPDE[108].

CONCLUSION

Avec la réforme en cours des lois relatives à la protection des renseignements personnels au Québec et au fédéral, le paysage des décisions judiciaires et administratives en matière de protection de la vie privée pourrait changer grandement dans les prochaines années.

S'il est adopté dans son état actuel, le projet de loi québécois donnerait à la CAI le pouvoir d'imposer aux entreprises des sanctions administratives pécuniaires de plusieurs millions de dollars et accorderait aux individus la possibilité d'intenter des poursuites en

107. Art. 35 C.c.Q.
108. LPRPDE, préc., note 36, art. 4(2)c).

dommages-intérêts sur la base d'une violation à la LPRPSP. Le projet de loi fédéral changerait aussi le mode d'application de la loi fédérale avec la création du Tribunal de la protection des renseignements personnels et des données et la possibilité pour le CPVP d'imposer des ordonnances de conformité.

Ces nouveaux pouvoirs entraîneront probablement en davantage de contestation judiciaire des décisions des commissaires et favoriseront le développement d'une jurisprudence plus riche en matière de protection de la vie privée et des renseignements personnels.