Université de Montréal

Publicité comportementale en ligne :

Analyse de la complexité et de l'encadrement juridique applicable au secteur privé au Québec et au Canada

Par

Isabel Poirier

Faculté de droit

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de maîtrise

en droit des technologies de l'information

30 avril 2023

Résumé

Le présent mémoire traite de la publicité comportementale en ligne (ci-après « PCL ») suite à la récente et importante vague de resserrements législatifs, des décisions judiciaires et enquêtes du CPVP, ainsi qu'aux récentes modifications technologiques impactant les pratiques de PCL. À la manière d'un guide, il y est recensé, décrit et analysées les obligations des entreprises participants à la PCL sous l'angle du droit à la vie privée et à la protection des renseignements personnels. Les enjeux et les principales zones d'ombre problématiques y sont identifiés et analysés, tel le critère de nécessité, l'exigence d'anonymisation et l'obligation de consentement, en incluant les enseignements des récentes décisions et enquêtes du CPVP. Une comparaison avec le cadre règlementaire de l'Union européenne est proposée sur certains points jugés plus pertinents. Le présent mémoire inclut une réflexion non seulement sur les obligations clés et leur évolution récente et rapide au Québec et au Canada dans un contexte de resserrement à l'international, mais également sur la PCL en soi en émettant des questionnements et des pistes de réflexion pour l'amélioration des pratiques. Ainsi, ce mémoire contient un volet pratique prononcé et un volet théorique qui se nourrissent l'un de l'autre.

La partie I est un état des lieux où sont mises en lumière la complexité factuelle et juridique entourant la PCL, incluant une observation et une réflexion sur les interactions entre les différents acteurs (organisations, organismes d'autoréglementation, autorités de contrôle) et leur rôle dans la création et l'évolution des normes formelles et informelles. La partie II est consacrée à l'analyse des principales obligations incombant aux entreprises du secteur privé participant à la PCL en vertu de la LPRPDE et du Projet de loi C-27 au fédéral ainsi que des récentes modifications apportées par la Loi 25 au Québec en matière de protection des renseignements personnels. Finalement, la partie III propose une analyse de l'exercice de contrôle de l'utilisateur et des limites du consentement.

Mots-clés : Publicité comportementale en ligne, publicité ciblée par centres d'intérêt, ciblage publicitaire, droit à la vie privée, protection des renseignements personnels, droit des technologies de l'information

Abstract

This master's thesis is about online behavioral advertising (hereafter "OBA"). Like a guide, it lists, describes and analyzes the obligations of companies participating in the OBA from the perspective of the right to privacy and the protection of personal information. The issues and the main problematic gray areas are identified and analyzed, such as the criterion of necessity, the requirement of anonymization and the obligation of consent, including the lessons of recent decisions and investigations by the OPC. A comparison with the regulatory framework of the European Union is proposed on certain points deemed more relevant. This thesis includes a reflection not only on the key obligations and their recent and rapid evolution in Quebec and Canada in a context of international tightening, but also on the OBA itself by raising questions and lines of thought for improving practices. Thus, this dissertation contains a pronounced practical component and a theoretical component which feed off each other.

Part I is an inventory highlighting the factual and legal complexity surrounding the OBA, including an observation and reflection on the interactions between the different actors (organizations, self-regulatory bodies, supervisory authorities) and their role in the creation and evolution of formal and informal norms. Part II is devoted to the analysis of the main obligations incumbent on private sector companies participating in the OBA under PIPEDA and draft law C-27 at the federal level and Bill 25 in Quebec with regards to the protection of personal information. Finally, Part III analyzes the exercise of user control and the limits of consent.

Keywords: Online behavioral advertising, interest-based advertising, targeted advertising, privacy, protection of personal information, information technology law

Table des matières

Liste des figures

Liste des sigles et abréviations

CAI : Commission d'accès à l'information du Québec

CCQ : *Code civil du Québec*, RLRQ c CCQ-1991

CCPA : *California Consumer Privacy Act,* Ch.55, 2018, Sec.3

CNIL : Commission nationale de l'informatique et des libertés

CPVP : Commissariat à la protection de la vie privée du Canada

CRTC : Conseil de la radiodiffusion et des télécommunications canadiennes

GAFAM : *Google*, *Apple*, *Facebook* (*Meta*), *Amazon* et *Microsoft*

LCAP : *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la loi sur la concurrence, la loi sur la protection des renseignements personnels et les documents électroniques et la loi sur les télécommunications*, LC 2010, c 23

Loi sur le privé : *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1

Loi 25 : *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25

LPRPDE : *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5

OCDE : Organisation de coopération et de développement économiques

PCL : Publicité comportementale en ligne / Publicité basée sur les centres d'intérêt

PRP : Protection des renseignements personnels

Projet de loi 64 : *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Projet de loi 64, 1re session, 42e législature (Québec)

Projet de loi C-27 : *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Projet de loi C-27 (1re lecture), 1re session, 44e législature (Can.)

RGPD : Règlement général sur la protection des données

RPRP : Responsable à la protection des renseignements personnels

UE : Union européenne

Remerciements

Merci à ma famille, mes ami.es et mes collègues pour leur soutien. Merci à mes consœurs et confrères juristes qui contribuent à nourrir le débat d'idées et les réflexions. Un merci tout particulier au Pr. Vincent Gautrais, ainsi qu'à Simon Dutilly, Sylvie Lafrenière et Dominique Villeneuve, mes précieux alliés qui m'ont guidée, soutenue et inspirée.

Prologue

En 2007, Michel Serres, philosophe et historien des sciences, qualifiait la révolution numérique de troisième révolution dans l'histoire de l'humanité, succédant à celles causées par l'invention de l'imprimerie, et avant elle, de l'écriture.[1] Ces révolutions concernant l'information, le « couplage support-message » comme il le nomme, ont entraîné une transformation complète de la totalité de la culture et de la civilisation[2], c'est-à-dire notre façon de vivre, de penser, de réfléchir ainsi que nos rapports avec les autres.[3] Ainsi, il soutenait que les conséquences fondamentales de ces révolutions concernant traitement de l'information (le « doux »), sont la mondialisation, la transformation de la monnaie et du commerce, ainsi que les crises concernant la science, la pédagogie et des religions.[4] Il expliquait aussi que « [c]'est lorsqu'interviennent des révolutions concernant l'information que les civilisations basculent et se mettent en place de manière nouvelle. »[5] « Et donc, sur le temps, (…) nous vivons aujourd'hui une période comparable à celle que le Moyen-Orient a connu au 1er millénaire avant Jésus Christ ou que la Renaissance européenne a connu autour des 15e-16e siècles. C'est-à-dire qu'aujourd'hui, nous n'avons peut-être pas conscience de la nouveauté extraordinaire des temps dans lesquels nous vivons, nous pensons, nous réfléchissons et nous avons rapport les uns aux autres ».[6] Il ajoutait que cette révolution nous a même fait changer d'habitat : « Habiter dans un nouvel espace n'est pas innocent ; cela a des conséquences complexes du point de vue des relations humaines, de la politique et du droit. »[7]

Ainsi, depuis 2007, la révolution numérique s'est poursuivie, produisant ses effets transformatifs sur nos sociétés, tout en s'en nourrissant, et engendrant une effervescence technologique et législative. Toutefois, au-delà du droit et des avancées technologiques, il convient de prendre un

[1] Michel SERRES, « Les Nouvelles technologies : révolution culturelle et cognitive », Conférence de Michel Serres sur les nouvelles technologies lors du 40e anniversaire de l'INRIA (2007) en ligne : <https://www.youtube.com/watch?v=ZCBB0QEmT5g>
[2] *Id.*
[3] *Id.,* fin : 16 min 47 sec.
[4] *Id.*
[5] *Id.*
[6] *Id.,* fin : 16 min 47 sec.
[7] *Id.,* fin : 29 min 50 sec.

pas de recul et de regarder de manière objective et critique non seulement les possibilités et les opportunités qu'offrent la révolution numérique, mais d'identifier les dérives possibles pour les éviter.

INTRODUCTION

A. Plan

Le présent mémoire traite de la publicité comportementale en ligne (ci-après « PCL ») suite à la récente et importante vague de resserrements législatifs, des décisions judiciaires et enquêtes du CPVP, ainsi qu'aux récentes modifications technologiques impactant les pratiques de PCL. À la manière d'un guide, j'y recense, décris et analyse les obligations des entreprises participant à la PCL sous l'angle de la protection des renseignements personnels. Je prends soin d'identifier et d'analyser les enjeux et les principales zones d'ombre problématiques, tels l'anonymisation et le consentement. Une comparaison avec le cadre règlementaire de l'Union européenne est proposée sur certains points jugés plus pertinents. J'y propose également une réflexion non seulement sur les obligations clés et leur évolution récente et rapide au Québec et au Canada, mais également sur la PCL en soi en émettant des questionnements et des pistes de réflexion pour l'amélioration des pratiques. Ainsi, ce mémoire contient un volet pratique prononcé et un volet théorique qui se nourrissent l'un de l'autre.

Ainsi, la partie I (préliminaire) est un état des lieux où sont mises en lumière la complexité factuelle et juridique entourant la PCL, incluant une observation et une réflexion sur les interactions entre les différents joueurs dans l'industrie et leur contribution dans la création et l'évolution des normes formelles et informelles.

La partie II est consacrée à l'analyse des principales obligations incombant aux entreprises du secteur privé participant à la PCL en vertu de la LPRPDE[8] et du Projet de loi C-27[9] au fédéral et de la Loi 25 au Québec[10] en matière de protection des renseignements personnels.

Finalement, la partie III propose une analyse de l'exercice de contrôle de l'utilisateur et des limites du consentement.

Cela dit, constatant l'immense transversalité liée à la PCL, j'ai choisi d'approfondir les obligations des entreprises du secteur du privé sous l'angle précis du droit à la vie privée et de la protection des renseignements personnels. Bien qu'il s'agisse d'un sujet étroitement lié à l'intelligence artificielle, je ne traiterai pas spécifiquement du cadre législatif et de la partie 3 du Projet de loi C-27, *Loi sur l'intelligence artificielle et les données*, visant les systèmes d'intelligence artificielle et le traitement des données liées à ces systèmes, qui y est applicable.

B. Définition de la PCL et distinction par rapport aux autres types de ciblage à des fins publicitaires

Différencions d'entrée de jeu la PCL des autres types de ciblage publicitaire. La PCL, aussi appelée publicité ciblée par centres d'intérêt, était définie en 2015 par le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») « (…) comme le suivi et le ciblage des activités sur le Web des personnes, dans plusieurs sites et au fil du temps, afin de leur présenter des publicités adaptées à leurs intérêts présumés. »[11] Selon la DAAC, ce type d'activité de profilage, de

---

[8] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, <http://canlii.ca/t/6c2fl> (ci-après « LPRPDE »)

[9] *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Projet de loi C-27 (1re lecture), 1re session, 44e législature (Can.), en ligne : <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture > (ci-après « Projet de loi C-27 »)

[10] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25, en ligne : < https://canlii.ca/t/6d6s0 > (ci-après « Loi 25 »)

[11] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, décembre 2015, révisée le 13 août 2021, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/publicite-et-marketing/publicite-comportementale-et-publicite-ciblee/bg_ba_1206/> (consulté le 15 avril 2023)

personnalisation et de ciblage s'étend aux navigateurs Internet via l'utilisation des fichiers témoins (*cookies*), sur les applications mobiles via les identifiants de publicité, et sur les adresses courriel via les jetons d'identité.[12] Les données collectées sur les consommateurs peuvent donc inclure les données de navigation sur le Web (sur les sites Web visités), les données de consommation média (articles lus, vidéos regardées), les historiques de recherches (sur les moteurs de recherche), les données d'utilisation des applications, les achats, les réponses aux clics publicitaires et le contenu de communication incluant les courriels écrits via Gmail et les messages publiés sur les réseaux sociaux.[13]

Concernant le suivi du comportement de navigation des consommateurs, sont souvent utilisés les fichiers témoins de suivi, mais également les fichiers témoins « *flash* » et les empreintes digitales des appareils.[14]

Notons qu'il n'y a pas de définition de témoin de connexion ou de technologies similaires dans les lois québécoise et canadienne en matière de PRP, ni de jurisprudence l'interprétant.[15] Toutefois, les témoins de connexion de ciblage peuvent être classés dans la catégorie des témoins de connexion dits « non essentiels » puisqu'ils ne sont pas nécessaires au bon fonctionnement du site web.[16]

Ce qui distingue la PCL des autres types publicité en ligne est le fait « qu'elle vise la pertinence personnelle »[17] c'est-à-dire qu'elle soit perçue comme plus « personnellement pertinente »[18].

---

[12] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « Outils », en ligne : <https://youradchoices.ca/fr/outils> (consulté le 4 décembre 2022); et ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « Foire aux questions », en ligne : <https://youradchoices.ca/fr/faq> (consulté le 4 décembre 2022)

[13] Sophie C. BOERMAN, Sanne KRUIKEMEIER & Frederik J. ZUIDERVEEN BORGESIUS, « Online Behavioral Advertising: A Literature Review and Research Agenda », *Journal of Advertising* (2017) 46:3, 363-376, DOI: 10.1080/00913367.2017.1339368, par. 2 et 7, en ligne : <https://www.tandfonline.com/doi/full/10.1080/00913367.2017.1339368 > (consulté le 4 janvier 2023)

[14] *Id.*, par. 9

[15] Caroline JONNAERT et Élisabeth LESAGE-BIGRAS, « Cookies et vie privée : ce que toute organisation devrait savoir », *Infopresse* (22 juin 2022), par. 1 de la section « Définitions », en ligne : <https://www.infopresse.com/cookies-et-vie-privee-ce-que-toute-organisation-devrait-savoir/> (consulté le 24 février 2023)

[16] *Id.*

[17] Sophie C. BOERMAN, Sanne KRUIKEMEIER & Frederik J. ZUIDERVEEN BORGESIUS, *op. cit.* note 13, par. 10. Traduction libre de « *it aims at personal relevance* ».

[18] *Id*., par. 10. Traduction libre de « *perceived as more personnaly relevant* ».

En effet :

> « À l'ère du " *big data*", la gamme d'outils mis à la disposition du publicitaire pour procéder à ce profilage de masse s'est étendue. La traque peut avoir lieu sur l'ordinateur d'un internaute par l'utilisation de témoins de connexion, par l'inspection de paquets profonds, grâce à son adresse IP ou encore aux coordonnées GPS de son cellulaire. Ces techniques de traque n'évoluent pas en vase clos et sont souvent couplées avec d'autres données permettant d'obtenir de l'information démographique concernant l'utilisateur, pour ultimement le catégoriser à travers différents segments. Ces segments, généralement appelés des profils, sont des outils de connaissance qui permettent de mieux comprendre quels sont les types de comportements et non pas les raisons sous-tendant un comportement donné. L'internaute est donc ciblé à travers un profil bâti à son image menant alors à une personnalisation au plan individuel. »[19] [Références omises]

La PCL est donc à différencier des autres types de publicité en ligne, principalement :

- la publicité contextuelle, qui « repose sur le contenu de la page Web consultée, sur la consultation en cours d'une page Web ou d'une application, ou sur une requête de recherche »;[20]
- le reciblage publicitaire (*retargeting*), qui « (…) permet de cibler les visiteurs d'un site [Internet] qui n'ont pas converti en clients mais qui ont manifesté leur intérêt pour la marque ou les produits d'un site e-commerce ».[21] Concrètement, il fonctionne au moyen d'une balise JavaScript installée sur le site internet et permet de placer des fichiers témoins qui vont pouvoir identifier l'internaute sur les autres sites qu'il va visiter qui, une fois qu'ils l'auront reconnu, pourront lui proposer les contenus qu'il a visités précédemment dans un onglet publicitaire dédié (bannières *display*) pour l'inciter à accomplir l'action marketing recherchée, telle compléter son achat.[22]

---

[19] Virginie JETTÉ, *Traque-moi si je le veux. À la recherche d'un cadre juridique entourant la publicité comportementale*, mémoire de maîtrise, Montréal, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, 2017, p. 15, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/20384/Jette_Virginie_2017_memoire.pdf?sequence=2&isAllowed=y>

[20] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, *Foire aux questions*, en ligne : <https://youradchoices.ca/fr/faq> (consultée le 4 décembre 2022)

[21] « Reciblage publicitaire », dans WiziShop, en ligne : <https://www.wizishop.fr/lexique-ecommerce/reciblage-publicitaire> (consulté le 4 décembre 2022)

[22] *Id.*, et « Conversion », dans WiziShop, en ligne : <https://www.wizishop.fr/lexique-ecommerce/conversion> (consulté le 4 décembre 2022)

- la publicité géographique qui est faite « selon l'emplacement apparent »[23] ou qui est basée sur la localisation[24];
- la publicité aléatoire[25];
- la publicité qui inclut le nom des personnes.[26]

[23] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, DIRECTION DE L'ANALYSE DES TECHNOLOGIES, *Publicité comportementale en ligne (PCL),* Projet de recherche de suivi, juin 2015, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2015/oba_201506/> (consultée le 4 décembre 2022)
[24] Sophie C. BOERMAN, Sanne KRUIKEMEIER & Frederik J. ZUIDERVEEN BORGESIUS, *op. cit.,* note 13, par. 10.
[25] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, DIRECTION DE L'ANALYSE DES TECHNOLOGIES, *Publicité comportementale en ligne (PCL),* Projet de recherche de suivi, *op. cit.,* note 23.
[26] Sophie C. BOERMAN, Sanne KRUIKEMEIER & Frederik J. ZUIDERVEEN BORGESIUS, *op. cit.,* note 13.

PARTIE I – État des lieux sur la complexité factuelle et juridique

La multitude des parties prenantes dans l'écosystème de la publicité comportementale en ligne (ci-après « PCL »), l'évolution des différentes technologies employées et meilleures pratiques, les nombreux resserrements législatifs et réglementaires récents, le flou entourant certaines dispositions clés, ainsi que la présence de nombreuses autorités réglementaires et organismes de contrôle qui livrent leur interprétation et lignes directrices, sans qu'elles soient toujours harmonisées entre elles, rend ardue la compréhension des importantes obligations qui incombent aux entreprises privées qui participent à la PCL et leur opérationnalisation. De surcroît, l'évolution du contexte législatif et règlementaire étranger, principalement, pour les entreprises nord-américaines, celui de l'Union européenne (RGPD[27] et règlement *ePrivacy* à venir[28]) et de la Californie (CCPA[29]), doit être pris en compte par les entreprises d'ici pour permettre la planification et la mise en place de pratiques, politiques et mesures qui sont conformes à ces lois et règlements étrangers qui peuvent trouver application.

[27] *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 (général sur la protection des données)*, 2016, en ligne : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees#:~:text=R%C3%A8glement%20(UE)%202016%2F679,sur%20la%20protection%20des%20donn%C3%A9es> (ci-après « RGPD »)

[28] *Délibération n°2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n°2019-093 du 4 juillet 2019)*, 2019, en ligne : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179> (ci-après « Règlement *ePrivacy* »)

[29] *California Consumer Privacy Act,* Ch.55, 2018, Sec.3., en ligne : <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5> (ci-après « CCPA »)

Chapitre 1 - Complexité factuelle

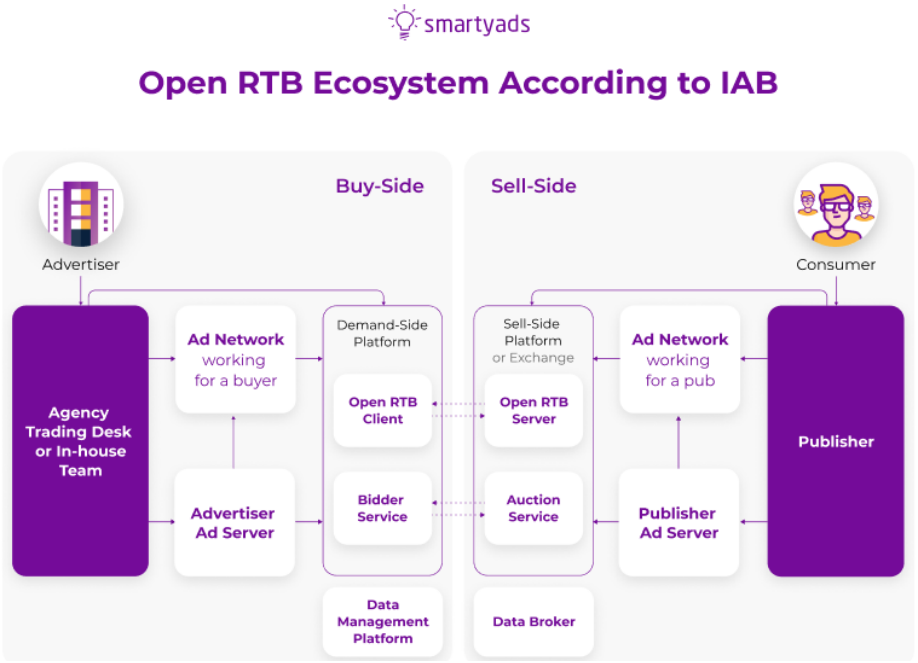
Un premier niveau de complexité est créé par un ensemble de facteurs : un vaste écosystème où coexistent et interagissent plusieurs parties prenantes aux intérêts variés, ainsi qu'à la création et au perfectionnement constant des technologies entourant le monde numérique ainsi que la PCL. De ces interactions et innovations naissent de nouvelles pratiques, normes et techniques, et ce, de manière continue.

1.1. Écosystème : pluralité de parties prenantes et d'intérêts

L'écosystème publicitaire numérique est vaste et complexe, constitué de diverses parties prenantes. Je me limiterai ici à en résumer les principales composantes nécessaires aux fins du présent mémoire. Cet écosystème de l'économie des données est en constante évolution, façonné par une dynamique particulière entre le durcissement du cadre législatif à l'échelle internationale, l'interprétation et l'application des lois par les organismes de contrôle, les besoins marketing et communicationnels des clients-annonceurs, les nombreux intervenants dans le marché de la donnée, le besoin de financement des créateurs de contenu et d'information, la créativité des agences de création et des agences média, l'opinion publique et la perspective consommateur, le développement des technologies et le leadership exercé par les GAFAM.

Figure 1. – *The Structure of the Advertising Ecosystem: Open RTB Ecosystem According to the International Advertising Bureau (IAB)*[30]

La figure ci-dessous illustre de manière simplifiée les différentes parties prenantes dans un système d'enchère en temps réel (*Real Time Biding* – RTB), étant « une manière de traiter les médias qui permet à une impression d'annonce individuelle de faire l'objet d'une enchère en temps réel. Cela se fait par le biais d'une enchère programmatique sur place, qui est similaire au fonctionnement des marchés financiers. Le RTB permet la publicité adressable ; la possibilité de diffuser des publicités directement auprès des consommateurs en fonction de leurs attributs démographiques, psychographiques ou comportementaux. »[31]



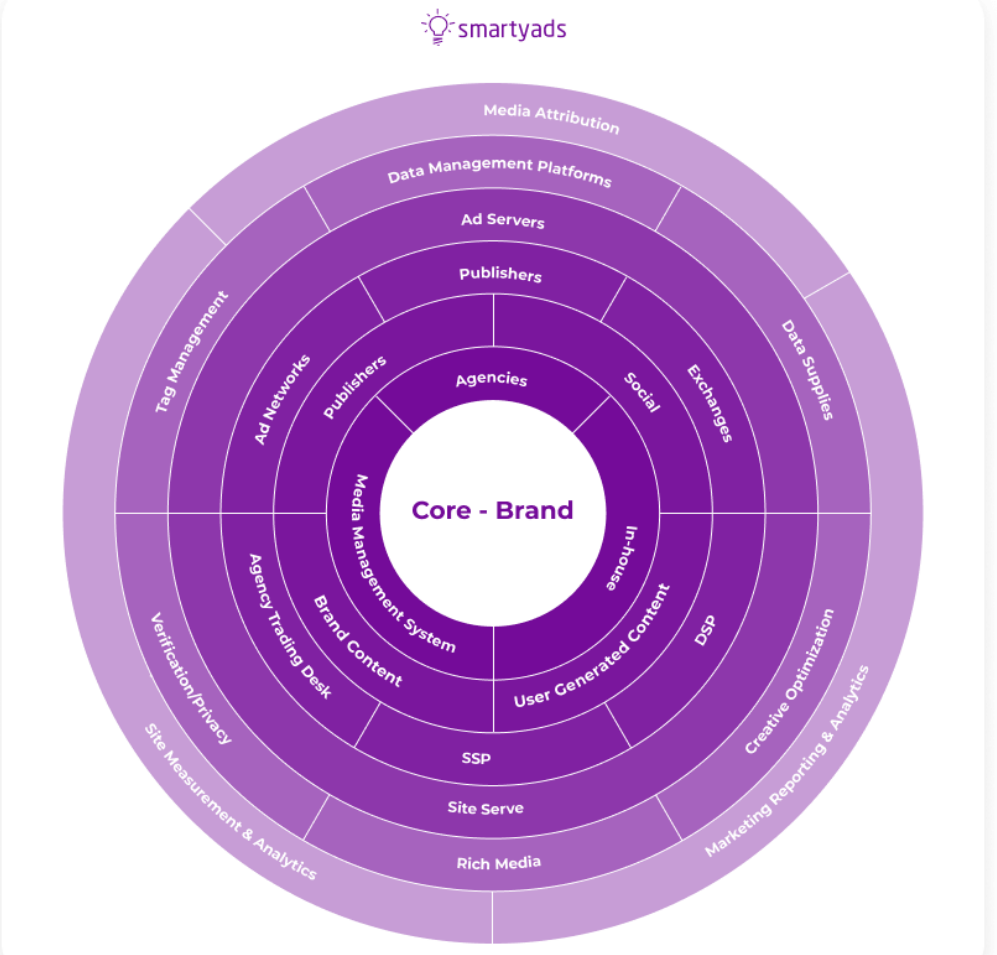
[30] Irina KOVALENKO, « Digital Advertising Ecosystem: Components », *Smartyads* (mis à jour le 9 septembre 2021), en ligne : <https://smartyads.com/blog/digital-advertising-ecosystem-components/> (consulté le 3 janvier 2023)

« Les premiers chercheurs en marketing ont commencé à étudier l'écosystème dès 2009. À l'époque, leur focus principal était sur les aspects achat et vente, et bien sûr l'attention de l'utilisateur. Une fois que les échanges publicitaires sont arrivés, l'achat de médias automatisé a commencé à se développer en ce que nous connaissons maintenant sous le nom de concept de publicité programmatique. Au cours de la dernière décennie, cette relation s'est transformée en un écosystème publicitaire complexe si vaste que certaines de ses visualisations incluent jusqu'à 13 secteurs de tailles et de formes différentes. » (Traduction libre)

[31] INTERNATIONAL ADVERTISING BUREAU, « OpenRTB », en ligne : <https://www.iab.com/guidelines/openrtb/#:~:text=Real%2Dtime%20Bidding%20(RTB),to%20how%20financial%20markets%20operate> (consulté le 24 avril 2023) (Traduction libre)

Figure 2. – *The Structure of the Advertising Ecosystem: The International Advertising Bureau (IBA) Arena*[32]

Cette deuxième figure quant à elle illustre la multiplication des différents acteurs de l'écosystème publicitaire numérique et allant bien au-delà des annonceurs et des consommateurs.



[32] *Id.*
« Une telle division décrit parfaitement le système du point de vue du processus de négociation des stocks, mais lorsqu'il s'agit de la communication réelle entre la marque et ses clients potentiels, il manque certainement quelques couches de soutien supplémentaires. L'International Advertising Bureau a développé sa propre illustration du système, nommée IAB Arena, qui décrit l'écosystème de la publicité en ligne du point de vue d'un spécialiste du marketing. L'illustration a six couches, réparties selon leurs rôles dans la construction de la relation entre les marques et leurs audiences. Ces activités sont le commerce de médias, la création de contenu, l'édition, la diffusion d'annonces, l'amélioration des médias et l'intelligence d'affaires. Chaque cercle comprend plusieurs joueurs avec la marque au centre d'un diagramme en tant qu'initiateurs de campagnes publicitaires numériques. Ces acteurs ont chacun leur propre rôle au sein du processus de diffusion d'annonces et de l'écosystème de la publicité numérique en général. » (Traduction libre)

Attardons-nous maintenant à la définition et au rôle de ces différents acteurs, qui nous permettra par la suite de mieux comprendre et analyser les différentes obligations des parties II et III ainsi que des problématiques et réflexions que j'y soulèverai.

1.1.1. Annonceurs

L'annonceur est défini comme « l'organisation ou l'entreprise à l'origine d'une opération de communication publicitaire ou marketing qui vise à promouvoir ses produits ou sa marque. »[33] La révolution numérique a apporté son lot de complexification pour ces derniers, en ayant engendré une multiplication des points de contact avec les consommateurs et transformé la façon dont nous communiquons, informons, éduquons, consommons. La PCL leur permet de cibler le bon groupe de personnes au bon moment et ainsi possiblement améliorer l'efficacité des campagnes et optimiser les investissements marketing. Par ailleurs, parmi les autres avantages escomptés pour les annonceurs canadiens, ont été soulevé en 2010 : 1) « la fidélisation de la clientèle [qui] va augmenter et sa frustration va diminuer à mesure que les Canadiennes et les Canadiens seront exposés à des publicités de moins en moins nombreuses et de plus en plus pertinentes »; 2) la « diminu[tion] [des] dépenses consacrées à la mise en marché, ce qui leur permettra d'investir davantage dans le développement de produits »; et 3) d'être « en mesure de rivaliser avec les entités internationales et en ligne comme eBay et Amazon pour les parts de marché »[34].

1.1.2. Consommateurs/Utilisateurs[35]

Il s'agit des internautes, des utilisateurs d'Internet[36] et d'applications mobiles. Suite à ses consultations de 2010, le CPVP identifiait à l'époque plusieurs inquiétudes des consommateurs par rapport au suivi en ligne, principalement : « la divergence quant à ce qui constitue ou non des renseignements personnels », « un manque de transparence à l'égard du suivi, du profilage et du ciblage des activités et de ce que cela suppose du point de vue de l'obtention d'un consentement

---

[33] B. BATHELOT, définition de « Annonceur », dans Définitions marketing, modifié le 19 avril 2022, en ligne : <https://www.definitions-marketing.com/definition/annonceur/> (consulté le 3 janvier 2023)
[34] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, *op. cit*., note 11, par. 7
[35] Infra, chapitre 6
[36] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, DIRECTION DE L'ANALYSE DES TECHNOLOGIES, *Publicité comportementale en ligne (PCL),* Projet de recherche de suivi, *op. cit.,* note 23

valable », le fait que le nombre d'entreprises participant à la PCL soit grand, mais inconnu et que ces entreprises soient « très peu connues des utilisateurs et [que] cette situation complique la détermination des responsabilités », et la question du consentement valable des enfants « qui sont de plus en plus jeunes à naviguer sur le Web et qui ne savent pas qu'ils font l'objet d'un suivi et encore moins de publicités ciblées ».[37]

1.1.3. Agences de communication marketing

Les agences média travaillent de pair avec les agences de création ou directement avec le client-annonceur. Elles offrent des services de planification médiatique afin d'assurer un mix média optimal pour les campagnes publicitaires ainsi que la négociation et l'achat des placements publicitaires auprès des différents médias.[38] Elles peuvent également collaborer à l'élaboration des campagnes qui comprennent de la créativité média.[39]

Les agences de création offrent divers services à leurs clients-annonceurs, principalement des services de création, de planification stratégique et de service-conseil. À ces services s'ajoutent souvent un ou plusieurs autres services : production publicitaire, développement de site web ou de microsites de campagne et optimisation de leur référencement pour les moteurs de recherche (SEO) de ceux-ci, développement d'applications mobiles, intégration avec la réalité augmentée et virtuelle, achat de publicités avec mots-clés sur les moteurs de recherche (SEM)), marketing de contenu (création et partage de contenu), médias sociaux (ex : gestion de communauté), *branding* et *design*, rédaction, marketing relationnel (implantation de système de gestion de relation clientèle (CRM), envoi d'infolettres, autres communications personnalisées et mise sur pied de programmes de fidélité), mise en marché et commercialisation, événementiel et l'expérientiel, relations publiques, planification et l'achat média.

[37] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, *op. cit.*, note 11.
[38] ASSOCIATION DES AGENCES DE COMMUNICATION CRÉATIVE, *Guide de sélection d'agence*, 2023 (à paraître)
[39] *Id.*

1.1.4. Fournisseurs de services

Historiquement, ce sont les fournisseurs de services Internet, les exploitants de navigateurs et les barres d'outils Web[40], lesquels « (…) offrent des services qui [leurs] permettent d'accéder à toutes ou à pratiquement toutes les URL consultées par [leurs] utilisateurs. »[41] À titre d'illustrations, pensons à *Google toolbar*, *Yahoo! Toolbar*, *Google Chrome*, *Firefox*, *Internet Explorer*, *Rogers*, Bell.[42] Un certain nombre d'entre eux, comme *Google*, sont également devenus des tierces parties et des parties premières avec le temps.

Par ailleurs, avec la croissance et la complexification des exigences règlementaires dans le monde, tout un secteur de l'industrie s'est créé. Pensons aux plateformes de gestion des consentements (*Consent Management Platforms* (CMP)) qui ont vu le jour ces dernières années et qui offrent des solutions *opt-in / opt-out* aux éditeurs (propriétaires de site web ou d'application) directement[43], ainsi qu'aux différentes entreprises qui offrent des services de consultation, de solutions informatiques et de programmes de conformité.[44]

1.1.5. Parties premières : Médias, plateformes éditrices et propriétaires de sites web et d'applications mobiles

Ces parties premières sont celles qui « possède[nt] ou contrôle[nt] un site Web avec lequel le consommateur interagit, par ex : les éditeurs »[45]. L'annonceur qui détient son propre site web est donc également un éditeur.[46] Ce sont donc elles qui vendent des espaces médias sur leurs plateformes aux tierces parties pour le placement d'annonces publicitaires des annonceurs. Elles

---

[40] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, *Programme canadien d'autoréglementation pour la publicité comportementale en ligne*, Webinaire d'introduction, 26 février 2015, en ligne : <https://assets.youradchoices.ca/pdf/DAAC-choixdepub-webinaire.pdf>, p. 29.
[41] *Id.*, p. 29.
[42] *Id*., p. 30.
[43] Geri KIROVSKA, « What is a Consent Management Platform (CMP) and Do You Need One? », *LiveRamp* (20 mars 2020) en ligne : <https://liveramp.com/blog/consent-management-platform-cmp/ > (consulté le 8 mars 2023)
[44] Par exemples : DAA, DAAC, IAB Tech Lab (https://iabtechlab.com/compliance-programs/)
[45] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, *Programme canadien d'autoréglementation pour la publicité comportementale en ligne*, Webinaire d'introduction, *op. cit.* note 40, p. 26
[46] EUROPEAN INTERACTIVE DIGITAL ADVERTISING ALLIANCE, « À propos de la publicité comportementale », en ligne : <https://www.youronlinechoices.com/fr/a-propos-de-la-publicite-comportementale/> (consulté le 4 janvier 2023)

peuvent donc collecter de la donnée pour leur propre usage, la vendre à un tiers, ou encore vendre de l'espace publicitaire.

Encore à ce jour, bon nombre de médias et d'éditeurs qui publient du contenu se financent en partie avec la publicité. Le modèle d'affaires par abonnement trouve aussi preneur, mais semble plus difficile à implanter, considérant que les utilisateurs sont habitués d'accéder à du contenu gratuitement. Toutefois, avec la disparition annoncée des cookies tiers (*third party cookies*), initiée par les grands joueurs, ce modèle est appelé à changer, forçant les parties premières à modifier leurs façons de faire[47], thème sur lequel reviendrai plus bas[48].

1.1.6. Tierces parties

Il s'agit du terme générique employé dans l'industrie qui englobe l'ensemble des entités qui « recueille[nt] et utilise[nt] des données sur le site Web d'une autre entité (c'est-à-dire [le] propriétaire) aux fins de la PCL; [elles] livre[nt] des annonces sur de tels sites Web en fonction des données PCL, par exemple : réseaux publicitaires et entreprises de données »[49]. À titre d'illustrations, pensons à *Tribal Fusion*, *Bright Roll*, *Casale Media*, *Suite 6ixty 6ix*, *bluekai*, et *RightMedia* de Yahoo![50].

Plus précisément, les réseaux publicitaires mettent en relation les sites et les éditeurs avec les annonceurs[51]. Quant à elles, les entreprises de données sont multiples : sociétés de courtage de données (*Data Brokers*), plateformes de gestion des données (*Data Management Platform – DMP*)[52], plateformes mettant en relation des annonceurs et les éditeurs (*Demand Side Platform – DSP*)[53], plateformes servant à maximiser les revenus de vente publicitaire sur le site des éditeurs (*Sell Side Platform - SSP*)[54], plateformes d'enchère publicitaire (*Advertising Exchange*) servant

[47] Notamment dans : Andréa LUBECK, « Disparition des cookies tiers : Soyez prêts! », *Grenier Magazine*, vol. 6, n°24 (6 avril 2021) p.4 et 5, en ligne : <https://magazines.grenier.qc.ca/magazine-parution/2021-04-06/#4/>
[48] Infra, 1.2.
[49] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, *Programme canadien d'autoréglementation pour la publicité comportementale en ligne*, Webinaire d'introduction, *op. cit.,* note 40, p. 27
[50] *Id.*, p. 28.
[51] EUROPEAN INTERACTIVE DIGITAL ADVERTISING ALLIANCE, « À propos de la publicité comportementale », *op. cit*., note 46
[52] *Id.*
[53] *Id.*
[54] *Id.*

d'espace d'achat-vente de publicité[55] en temps réel, agrégateurs de données collectant des données multi sources pour créer des groupes d'intérêts nommés « segments », par exemple les acheteurs de voitures,[56] serveurs de publicité qui sont dotées d'une technologie diffusant de la publicité sur le site web[57] ou l'application, équipes de *trading desk* en agence média (ATD) qui travaillent avec les DSP pour gérer les campagnes[58], etc.

1.1.7. Organismes de contrôle : hausse de ces organismes et du besoin de collaboration

J'inclus ici les autorités de contrôle dans cet écosystème puisqu'elles occupent un rôle grandissant et contribuent à modifier leurs pratiques. En effet, elles enquêtent de plus en plus sur les parties premières et émettent différentes normes informelles (interprétations, positions, lignes directives) sur lesquelles tendent à s'aligner les organismes d'autoréglementation et les différents acteurs, comme nous le verrons plus bas. En outre, elles se font confier par les législateurs des pouvoirs grandissant de sanction, tant dans le Projet de loi C-27 que dans la Loi 25. Elles ont donc un rôle et un impact important dans l'application du cadre législatif et règlementaire touchant la PCL au Canada. J'y reviendrai tout au long de ce mémoire.

Voyons-en ici les principales. Au premier rang, le Commissariat à la protection de la vie privée (ci-après « CPVP ») a pour mission « de protéger et de promouvoir le droit à la vie privée. (…) [Il] veille au respect de la *Loi sur la protection des renseignements personnels*[59], laquelle porte sur les pratiques de traitement des renseignements personnels utilisées par les ministères et organismes fédéraux, et de la LPRPDE, la loi fédérale sur la protection des renseignements personnels dans le secteur privé. »[60]

---

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, en ligne : <http://canlii.ca/t/6c2m5>
[60] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « À propos du Commissariat », en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/> (consulté le 4 janvier 2023)

Au niveau fédéral, nous retrouvons également le Bureau de la concurrence chargé de l'application de la *Loi sur la concurrence*[61], qui est l'« organisme indépendant d'application de la loi qui protège la concurrence et en fait la promotion au bénéfice des consommateurs et des entreprises au Canada. »[62]

Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) quant à lui est chargé notamment de l'application de la loi canadienne antipourriel (LCAP)[63], qui prévoit certaines dispositions concernant les fichiers témoins.

Au niveau provincial, quatre provinces se sont dotées d'un commissariat chargé des questions de vie privée : la Commission d'accès à l'information (CAI) du Québec[64], le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario[65], l'*Office of the Information and Privacy Commissioner of Alberta (OIPC)*[66] et l'*Office of the Information and Privacy Commissioner for British Columbia (OIPC)*[67].

Soulignons ici la nécessaire collaboration qui doit s'opérer entre les organismes de contrôle. À titre d'exemple au Canada, un protocole d'entente existe entre le CRTC, le Bureau de la concurrence et le CPVP ayant pour objet leur coopération et leur coordination dans le cadre de l'application de la loi canadienne antipourriel.[68]

Par ailleurs, le CPVP est autorisé à communiquer des renseignements à des États étrangers ayant des attributions similaires en matière de protection de renseignements personnels ou étant

---

[61] *Loi sur la concurrence*, LRC 1985, c C-34, en ligne : <https://canlii.ca/t/6cdtb>
[62] GOUVERNEMENT DU CANADA, « Bureau de la concurrence Canada », en ligne : <https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr> (consulté le 4 janvier 2023)
[63] GOUVERNEMENT DU CANADA, « Conseil de la radiodiffusion et des télécommunications canadiennes », en ligne : <https://crtc.gc.ca/fra/internet/anti.htm> (consulté le 4 janvier 2023)
[64] https://www.cai.gouv.qc.ca/
[65] https://www.ipc.on.ca/?lang=fr
[6666] https://www.oipc.ab.ca/
[67] https://www.oipc.bc.ca/
[68] *Protocole d'entente sur la coopération, la coordination et l'échange d'information entre le Commissaire à la concurrence, le Conseil de la radiodiffusion et des télécommunications canadiennes et la Commissaire à la protection de la vie privée du Canada dans le cadre de l'exécution de leur mandat au titre de la loi canadienne antipourriel*, 23 janvier 2014, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/loi-canadienne-anti-pourriel/mou_casl_2014/> (consulté le 4 janvier 2023), art. 1(1).

chargés de réprimer des comportements essentiellement semblables à ceux constituant des contraventions au sens de la LPRPDE.[69] Il s'agit ici d'un élément de complexité tant factuel que juridique.

De plus, le CPVP peut également conclure des accords et des ententes avec les commissariats provinciaux visant à coordonner les activités de leurs bureaux respectifs, à effectuer des recherches ou à élaborer des lignes directrices, des documents, des contrats, des documents types portant sur la protection des renseignements personnels, et visant à leur communiquer des renseignements utiles à l'examen d'une plainte ou d'une vérification ou à l'exercice des attributions du CPVP en matière de protection de renseignements personnels.[70]

Illustrant ce dernier point, une entente de collaboration en 2019 est intervenue entre le CPVP et la CAI dans l'enquête concernant l'incident de confidentialité vécu récemment par Desjardins.[71] De plus, le Commissariat de la Colombie-Britannique et le CPVP avaient procédé à une enquête conjointe visant les activités d'*AggregateIQ Data Services Ltd*.[72] Dans cette enquête, le CPVP résume cette approche collaborative ainsi :

> « Cette enquête conjointe, la deuxième effectuée cette année par les deux commissariats, est une nouvelle illustration de la réalité collaborative de l'application des lois sur la protection des renseignements personnels. Cela est vrai non seulement entre les deux commissariats, mais aussi entre les organismes de réglementation de la protection de la vie privée à l'échelle mondiale. Bien que les lois dans le monde sur la protection des renseignements personnels ne soient pas identiques – et elles ne le seront jamais –, elles sont généralement enracinées dans des principes communs relatifs à l'équité dans le traitement de l'information qui, comme cela était pertinent dans ce cas-ci, accordent une grande importance au consentement en pleine connaissance de cause des personnes, que

[69] LPRPDE, art. 23.1(1) et (2).
[70] *Id*., art. 23(2) et (3).
[71] 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*, Conclusions en vertu de la LPRPDE n°2020-005, 14 décembre 2020, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2020/lprpde-2020-005/> (consulté le 5 janvier 2023), par. 19.
[72] 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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, 26 novembre 2019, en ligne : <https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-004/> (consulté le 5 janvier 2023)

ce soit à la collecte, à l'utilisation ou à la communication de leurs renseignements personnels et à la protection de ces renseignements.

Par conséquent, les organismes de réglementation collaboreront de plus en plus à l'échelle nationale et internationale pour s'assurer que le droit à la vie privée des personnes, y compris ceux relatifs au consentement et aux mesures de sécurité, sont respectés d'un territoire de compétence à l'autre; ce que nous examinons dans ce cas-ci. Les deux commissariats se sont engagés à faire leur part pour relever ce défi. »[73]

[Mes soulignements]

Le législateur fédéral dans le Projet de loi C-27 maintient cette vision et accroit les pouvoirs du CPVP en matière de coopération avec ses homologues étrangers :

> « Reconnaissant la nature internationale inhérente aux efforts de protection des données, l'article 120 de la LPVPC donnera au Commissaire de nouveaux pouvoirs concernant la divulgation de certains renseignements aux législateurs étrangers en matière de protection des renseignements personnels. Il est intéressant de noter que ces pouvoirs incluront la capacité de conclure des accords de coopération avec les autorités étrangères, ce qui peut impliquer: une coopération pour l'application des lois sur la protection des données et la gestion des plaintes, l'élaboration de directives, normes et autres documents relatifs à la protection des renseignements personnels, la conduite et la publication de recherches, le partage de connaissance et d'expertise et la détermination de questions d'intérêt commun. »[74] [Mon soulignement]

D'une perspective québécoise, espérons que le CPVP et la CAI collaboreront non seulement au niveau des enquêtes, mais idéalement sur la rédaction de lignes directrices communes et de documents types communs dans un souci d'harmoniser et de clarifier la mise en application des obligations clés de la loi québécoise et de la loi qui découlera du Projet de loi C-27, plus précisément concernant la question de la nécessité d'obtenir consentement sous forme implicite ou explicite dans un contexte de PCL, question que j'approfondirai à la partie III[75].

---

[73] *Id*., « Message des commissaires » par. 12 et 13

[74] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, Borden Ladner Gervais - Perspectives, juin 2022, p. 29, en ligne: <https://www.blg.com/fr/insights/2022/06/canadas-consumer-privacy-protection-act-bill-c27-impact-for-businesses> (consulté le 11 mars 2023)

[75] Infra, 6.2.1.

1.1.8. Associations d'industrie et organismes d'autoréglementation

Au Canada, comme ailleurs dans le monde, nous retrouvons de nombreuses associations et regroupements dans l'industrie des communications marketing qui contribuent à la recherche, à l'amélioration des pratiques et à la création de standards.

En matière de PCL, l'Alliance de la publicité numérique du Canada / *Digital Advertising Alliance of Canada* (DAAC)[76] a été créée par les principales associations de l'industrie : le Bureau de la publicité interactive du Canada / *Interactive Advertising Bureau of Canada* (IAB Canada)[77], l'Association des agences de communication créative (A2C)[78], l'*Institute of Canadian Agencies* (ICA)[79], l'Association canadienne des annonceurs / *Association of Canadian Advertisers* (ACA)[80], les Normes de la publicité / *Ad Standards*[81], le Conseil des directeurs médias du Québec (CDMQ)[82], l'Association canadienne du marketing / *Canadian Marketing Association* (CMA)[83], et le *Canadian Media Director's Council* (CMDC)[84].

La DAAC, comme ses homologues américaine (DAA) et européenne (EDAA), considère et plaide que la PCL offre des avantages pour les utilisateurs, soit de donner accès à du contenu gratuit en ligne et de livrer de la publicité susceptible d'être plus pertinente.[85] En effet, l'industrie est généralement favorable à la PCL, soutenant que « la publicité en ligne finance l'accès gratuit au contenu en ligne et permet aux opérateurs de petits sites web de demeurer concurrentiels et de créer du contenu gratuit et spécialisé » en plus de « contribuer à "alimenter Internet" et stimule[r] l'économie numérique »[86]. IAB Canada ajoutait même qu'il « considère les publicités comme un service précieux offert aux consommateurs, plutôt que comme une interruption de leur

[76] https://youradchoices.ca/
[77] https://www.iabcanada.com/fr/
[78] https://a2c.quebec/
[79] http://theica.ca/
[80] https://acaweb.ca/fr/
[81] https://adstandards.ca/fr/accueil/
[82] http://cdmq.ca/fr
[83] https://www.thecma.ca/
[84] https://www.cmdc.ca/
[85] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « Foire aux questions « Quels sont les avantages que m'offre la publicité ciblée par centre d'intérêt en ligne ? », en ligne : <https://youradchoices.ca/fr/faq> (consulté le 3 janvier 2023)
[86] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, *op. cit.*, note 11, par. 6 et 7.

expérience de navigation, si ces publicités correspondent étroitement aux intérêts des consommateurs »[87], ce qui est le fondement de la PCL.

Ajoutons également les différentes associations de défense de droits et intérêts des consommateurs, tel Option Consommateurs au Québec, et les associations *None Of Your Business* (NOYB) et La Quadrature du Net (LQDN) en Europe, qui jouent un rôle important dans la vigie et l'analyse des pratiques, l'information et l'éducation des consommateurs, ainsi que dans l'exercice d'importants recours collectifs principalement à l'égard des grandes entreprises qui font le commerce de la données, telles *Google* et *Facebook*[88]. Leur rôle est central dans cet exercice de mise en équilibre entre les différents droits et intérêts en présence.

1.2. L'impact des grands joueurs « hybrides » sur les technologies et les pratiques utilisées en PCL

Ces acteurs de premier plan jouent un rôle majeur dans la composition et le fonctionnement de l'écosystème de la PCL. Ils peuvent cumuler plusieurs fonctions (première partie, tierce partie et fournisseurs de services).

Sous l'influence des grands joueurs que nous appellerons ici « hybrides » puisqu'ils portent différents chapeaux (partie première, tierce partie, fournisseurs de services), les technologies et les techniques de ciblage, profilage et personnalisation employées se développent rapidement, mais ont aussi vécu une réforme à l'échelle de l'industrie entière dans la dernière année. Nous parlons ici de l'adoption du régime de consentement positif de iOS14 et de l'arrivée des cohortes d'intérêts et de la fin des cookies tiers par *Google Chrome*. Ces changements annoncés en 2021 sur leurs politiques et outils technologiques de traitement de données ont transformé le *modus operandi* et les meilleures pratiques de l'industrie en matière de ciblage publicitaire.

[87] *Id.*, par. 6.
[88] Infra, 2.1.6., 4.1.1., 5.2.3., 6.2.3. et 6.3.2.

1.2.1. *Apple* et changement en matière de publicité mobile ciblée : Implantation du régime de notification et d'obtention du consentement exprès/positif

Au moment de la présentation de iOS14.5, iPadOS14.5 et tvOS14.5 en 2021, *Apple* affirmait que « [l]e droit à la vie privée est fondamental, et la confidentialité est au cœur de tout ce que nous faisons.»[89] La multinationale s'engageait à ce que les utilisateurs soient notifiés et que leur consentement soit obtenu préalablement à la collecte, l'utilisation et le transfert de leurs données par ou via chacune des applications utilisées (ex : *Facebook*).[90] iOS 14.5, iPadOS14.5 et tvOS14.5 ont donc comme particularité de demander aux utilisateurs leur consentement pour chaque application pour autoriser les éditeurs à accéder à leur identifiant publicitaire (*IDentifier for Advertising* (IDFA)). Cela dit, les utilisateurs de iOS14 peuvent préautoriser le suivi par les applications en allant sous le paramètre Confidentialité / Suivi.[91]

Ainsi, par défaut, les propriétaires d'applications mobiles disponibles dans l'*AppStore* ne peuvent pas traiter les données d'un utilisateur à moins d'avoir reçu le consentement de ce dernier, suivant une demande simple, mais suffisamment détaillée, via le *AppTrackingTransparency framework* d'*Apple*, l'autorisant à le suivre et à accéder à son identifiant publicitaire.[92]

Regardons plus attentivement en quoi consistent les changements mis en place par Apple. En premier lieu, précisons que l'action de suivi selon *Apple* inclut notamment les actions suivantes :

- « L'affichage de publicité ciblée sur l'application basée sur des données collectées sur des apps et des sites web appartenant à des tiers
- Le partage de données de géolocalisation et de listes courriels à des courtiers de données (*data brokers*)
- Le partage de listes courriels, identifiants à des fins publicitaires (IDFA) ou autres identifiants en faveur d'un réseau publicitaire qui utilisera cette information pour recibler ces utilisateurs dans d'autres applications ou pour trouver des utilisateurs similaires

[89]APPLE, « iOS 16 », en ligne : <https://www.apple.com/ca/fr/ios/ios-14/> (consulté le 7 avril 2021)
[90] « Transparence du suivi par les apps : Dès le début de 2021, vous recevrez un message chaque fois qu'une app cherche à suivre votre activité sur les apps ou sites web d'autres entreprises à des fins publicitaires, ou à partager vos informations avec des sociétés de courtage de données. Vous pourrez alors accorder votre permission ou non. » APPLE, « iOS 16 », en ligne : <https://www.apple.com/ca/fr/ios/ios-14/> (consulté le 7 avril 2021)
[91] APPLE, « iOS 16 », en ligne : <https://www.apple.com/ca/fr/ios/ios-14/> (consulté le 7 avril 2021)
[92] APPLE, « User Privacy and Data Use », en ligne: <https://developer.apple.com/app-store/user-privacy-and-data-use/> (consulté le 6 janvier 2023)

- Le placement d'un *Software Development Kit* (SDK ou *devkit*)[93] de tiers dans l'application, lequel combine de la donnée d'utilisateur provenant de l'application avec de la donnée utilisateur provenant d'autres applications détenues par des tiers, dans le but de fournir de la publicité ciblée ou de mesurer l'efficacité de publicités, et ce même si un SDK n'est pas utilisé à ces fins. Par exemple, en utilisant un SDK d'analyse qui réutilise les données qu'il collecte à partir de l'application pour activer la publicité ciblée dans les applications d'autres développeurs. »[94]

Les cas énoncés par *Apple* qui ne constituent pas un suivi visé, et donc ne nécessitant pas d'aviser et d'obtenir le consentement préalable des utilisateurs sont :

- « Lorsque les données de l'utilisateur ou de l'appareil de votre application sont liées à des données de tiers uniquement sur l'appareil de l'utilisateur et ne sont pas envoyées hors de l'appareil de manière à identifier l'utilisateur ou l'appareil.
- Lorsque le courtier de données avec lequel vous partagez des données utilise les données uniquement à des fins de détection de fraude, de prévention de la fraude ou à des fins de sécurité. Par exemple, utiliser un courtier de données uniquement pour empêcher la fraude par carte de crédit.
- Lorsque le courtier de données est une agence d'information sur les consommateurs et que les données sont partagées avec elle à des fins (1) de rapport sur la solvabilité d'un consommateur, ou (2) d'obtenir des informations sur la solvabilité d'un consommateur dans le but précis de déterminer le crédit. »[95]

De plus, *App Store* fournit désormais des renseignements pour faciliter la compréhension des pratiques et de la politique de confidentialité d'une application avant son téléchargement.[96] Ainsi, l'exemple donné montre une conception graphique simplifiée : résumé des pratiques de confidentialité déclarées par le développeur de l'application en question, hyperliens vers plus d'informations, pictogrammes des types de données qui pourront être utilisées pour le suivi des activités à travers les applications et sites web tiers.)[97]

Ce qui est intéressant par ailleurs, est de constater que le nouveau système d'*Apple* est fondé sur le principe de *Privacy by design* : Ainsi, *Apple* ne fournit pas d'IDFA tant que le développeur du site

[93] Christopher SANDOVAL, « What is the Difference Between an API and an SDK ? » *Nordic APIS* (2 juin 2016), en ligne : < https://nordicapis.com/what-is-the-difference-between-an-api-and-an-sdk/> (consulté le 6 janvier 2023)
[94] APPLE, « User Privacy and Data Use », en ligne : <https://developer.apple.com/app-store/user-privacy-and-data-use/> (consulté le 6 janvier 2023) (Traduction libre)
[95] *Id*.
[96] APPLE, « iOS 16 », en ligne : <https://www.apple.com/ca/fr/ios/ios-14/> (consulté le 7 avril 2021)
[97] *Id*.

n'a pas fourni la preuve de l'obtention du consentement.[98] Il ne se limite pas à un système dont le respect fonctionne sur des obligations contractuelles.

De plus, *Apple* a créé un second identifiant, soit le *ID for Vendors* (IDFV), à des fins d'analyses à travers les applications du même fournisseur de contenu, mais ne peut être jumelé avec d'autres données si le consentement de l'utilisateur n'a pas été obtenu.[99]

Finalement, *Apple* a ajouté une fonctionnalité intéressante, soit l'indicateur d'enregistrement qui

> « s'allume en haut de votre écran chaque fois qu'une app utilise votre microphone ou votre caméra. Et dans le Centre de contrôle, vous voyez si une app y a eu recours dernièrement. »[100]

De plus, *Apple* a ajouté la possibilité de partager une localisation approximative plutôt que la localisation exacte.

Avec tous ces changements, nous pouvons conclure que la multinationale manifeste l'intention de se positionner sur le marché comme un joueur plus conscient des enjeux liés à la protection de la vie privée et soucieux de mettre en place les bonnes pratiques en matière de transparence et de choix des utilisateurs dans un contexte publicitaire. Inutile de préciser que cette réforme a créé une onde de choc dans l'industrie a dû s'ajuster en conséquence.[101] Cela dit, il n'en demeure pas moins qu'il est un GAFAM dont le fonds de commerce n'est plus seulement la vente d'ordinateurs, de téléphones cellulaires et d'autres appareils, mais que dans ce contexte qu'il détient une énorme quantités de données dont des renseignements personnels très sensibles incluant des données biométriques (ex. empreinte digitale du pouce, voix, visage), qu'il doit protéger contre les nombreuses tentatives d'attaques informatiques notamment.

Nous pouvons également déduire que ce nouveau positionnement de marque est attribuable à une volonté de garder la confiance des consommateurs, mais également des autorités

---

[98] APPLE, « User Privacy and Data Use », Using the AppTrackingTransparency Framework, en ligne : <https://developer.apple.com/app-store/user-privacy-and-data-use/> (consulté le 7 avril 2021)
[99] *Id.*
[100] *Id.*
[101] Pour un exemple de réponse de l'industrie, lire : Shannon LEWIS, « Industry Response to Apple iOS », *Canadian Media Directors Council (CMDC)* (20 janvier 2021) en ligne : <https://www.cmdc.ca/news-mentor/apple> (consulté le 7 avril 2021)

réglementaires et organismes de contrôle, qui observent attentivement -avec raison- les GAFAM, tout particulièrement *Facebook* (Meta) et *Google* au Canada et au Québec, dont je verrai les principaux exemples récents dans ce mémoire.

Du côté d'*Apple*, ce dernier avait fait l'objet d'une enquête de la part du CPVP en 2014 au terme de laquelle elle avait dû fournir des précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée.[102] À l'époque, *Apple* utilisait déjà un identifiant unique (UDID) attribué à chaque appareil iOS avant la vente de l'appareil, pour suivre les activités de son utilisateur. Cet identifiant pouvant être jumelé au compte associé à l'UDID, le CPVP avait considéré que l'UDID se qualifiait de renseignement personnel au sens de la LPRPDE. De plus, puisque ce renseignement personnel était communiqué à des développeurs d'applications tiers pour envoyer de la publicité ciblée, le CPVP avait jugé insuffisante que la divulgation de ce traitement n'ait lieu que dans les déclarations générales de la politique de confidentialité de *Apple*. Afin d'être conforme aux attentes du CPVP en matière d'application de la LPRPDE, il avait alors été demandé à *Apple* d'aviser les utilisateurs plus clairement et directement, soit au moyen d'un avis appelé « juste à temps », clair et visible. En cours d'enquête, *Apple* a cessé d'utiliser l'UDID pour le remplacer par un nouvel identifiant à des fins publicitaires (AdID) et a modifié iOS7 de manière à « permettre à l'utilisateur de trouver plus facilement les boutons de réglage des fonctions de confidentialité pour réinitialiser l'AdID et choisir de ne pas recevoir de publicités ciblées »[103], le tout à la satisfaction du CPVP.

1.2.2. *Google* : Initie le virage vers l'ère post-*cookies* tiers

Une autre annonce majeure a ébranlé l'industrie en 2021 : *Google* annonçait qu'il retirait les fichiers témoins tiers sur *Chrome*, et de ce fait, annonçait le début de la fin de l'ère des *cookies* tiers.[104] Cette entrée en vigueur a finalement été repoussée à 2022, puis à nouveau à la mi

---

[102] CPVP, *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE n° 2013-017, 20 novembre 2013, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-017/ > (consulté le 7 avril 2021)

[103] *Id.*, p. 1.

[104] Erin JEFFERY, « Advertising without Third-Party Cookies: Frequently Asked Questions », *AX INSIGHTS* (6 janvier 2023), en ligne : <https://audiencex.com/advertising-without-third-party-cookies-frequently-asked-questions/ > (consulté le 16 août 2022)

2024[105], afin de lancer sur *Chrome* leur nouvel *Privacy Sandbox APIs*[106] et permettre à l'industrie de se préparer à la transformation majeure qui en découle.

En effet, *Google* déclare avoir pris la décision de changer de technologie et de fonctionnement en matière de publicité numérique afin de respecter les préoccupations et les attentes des utilisateurs en matière de suivi et de vie privée ainsi que de l'évolution des restrictions imposées par l'encadrement législatif.[107] Se disant soucieuse de préserver un Internet ouvert et accessible, *Google* a décidé de procéder à ce virage en remplaçant les cookies tiers, non pas en créant des identifiants-utilisateurs individuels, mais en mettant un système basé sur des API préservant la confidentialité et la constitution de groupes appelés « cohortes » dans lesquels seront regroupés et « cachés » des individus partageant des intérêts communs :

> « Advances in aggregation, anonymization, on-device processing and other privacy-preserving technologies offer a clear path to replacing individual identifiers. In fact, our latest tests of FLoC show one way to effectively take third-party cookies out of the advertising equation and instead hide individuals within large crowds of people with common interests. Chrome intends to make FLoC-based cohorts available for public testing through origin trials with its next release this month, and we expect to begin testing FLoC-based cohorts with advertisers in Google Ads in Q2. Chrome also will offer the first iteration of new user controls in April and will expand on these controls in future releases, as more proposals reach the origin trial stage, and they receive more feedback from end users and the industry.
>
> This points to a future where there is no need to sacrifice relevant advertising and monetization in order to deliver a private and secure experience. »[108]

Malgré les efforts énoncés par ces grandes entreprises de données et l'intention dont ils témoignent de modifier leurs pratiques pour atteindre un meilleur équilibre droit à la vie privée – monétisation des données – accès au contenu Internet gratuit[109], les écarts et les dérives sont

---

[105] Anthony CHAVEZ, « Expanding testing for the Privacy Sandbox for the Web », *Google The Keyword* (27 juillet 2022), en ligne: <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> (consulté le 16 août 2022)
[106] *Id.*
[107] David TEMKIN, « Charting a course towards a more privacy-first web », *Google Ads & Commerce Blog* (3 mars 2021), en ligne: <https://blog.google/products/ads-commerce/a-more-privacy-first-web/> (consulté le 16 août 2022)
[108] *Id.*
[109] Par exemple : *Id.*

toujours possibles, tant d'un point de vue du droit à la vie privée que des autres droits protégés. Ils font encore l'objet de poursuites et de recours collectifs depuis de nombreuses années tant ici qu'à l'étranger, tout particulièrement *Facebook* et *Google*.

Par exemple, encore récemment au Québec, un recours collectif a été autorisé en décembre 2022 contre *Facebook* pour ciblage publicitaire discriminatoire (discrimination algorithmique)[110] et un autre a été autorisé en juillet 2022 contre *Google* pour « collect[e] et utilis[ation] à des fins commerciales [d]es renseignements des membres du groupe qui naviguent en mode de navigation privée lorsque ceux-ci utilisent les Services *Google* ou visitent des sites Internet ayant recours aux Outils *Google* »[111]. J'y reviendra sur cette dernière affaire aux parties II et III[112].

Ainsi, force est de constater que ces grands joueurs, qui étaient et sont toujours dans la mire - avec raison- des législateurs et des autorités de contrôle, ceux-là mêmes qui étaient l'une des raisons initiales pour renforcir le cadre législatif en place au niveau national et à l'international, tendent à modifier certaines de leurs pratiques. Certains le font assurément mieux que d'autres.

Il est intéressant de constater le jeu d'influence qui s'opère, l'interaction continue entre les actions et les innovations de ces grands joueurs avec les actions des législateurs et organismes de contrôle. Il est d'autant plus intéressant de constater que l'opinion publique est un puissant moteur de changement tant pour les marques, que les entreprises de l'industrie de la donnée et les gouvernements.

---

[110] À l'égard de certains groupes de personnes comme des femmes et des travailleurs plus âgés de recevoir des annonces d'emploi. Exemple : *Beaulieu* c. *Facebook inc*., 2022 QCCA 1736 (CanLII), en ligne : <https://canlii.ca/t/jtpzj> (consulté le 24 avril 2023) ; Kirill KUDRYATSEV, « La Cour d'appel du Québec approuve un recours collectif contre Facebook », *Agence France-Presse, Le Devoir* (4 janvier 2023) en ligne : <https://www.ledevoir.com/societe/justice/776725/la-cour-d-appel-du-quebec-approuve-un-recours-collectif-contre-facebook> (consulté le 6 janvier 2023)

[111] Joannie LANGLOIS, « Action collective autorisée contre Google », *SOQUIJ BLOGUE* (20 juillet 2022) en ligne : <https://blogue.soquij.qc.ca/2022/07/20/action-collective-autorisee-contre-google/> (consulté le 6 janvier 2023)

[112] Voir Infra 6.2.2.

1.2.3. Changement des pratiques

Puisque l'industrie publicitaire se dirige vers un ciblage sans *cookies* tiers,[113] les différents experts en publicité reconnaissent que les éditeurs doivent dorénavant se tourner vers l'optimisation de leurs propres cookies ainsi que par le développement de partenariats.[114] Le modèle d'accessibilité du contenu sur base d'abonnement pourrait aussi prendre de l'ampleur.[115]

Par ailleurs, l'industrie prend un virage vers les technologies alternatives proposées (c'est-à-dire migration vers *Google Analytics 4*, utilisation de *Privacy Sandbox – Federated Learning of Cohorts (FloC)*, *Privacy Sandbox – Fledge*, *Facebook Conversion API*, *Customer Data Platform (CDP)*, et *Clean Room*).[116] L'industrie ira également vers un développement des autres formes de ciblage existantes comme le reciblage (*retargeting*) de cohortes (vs d'individus) et le ciblage contextuel, un développement des listes de données par les premières parties et un développement des partenariats entre éditeurs et annonceurs.[117]

Bien que le changement constitue une transformation en profondeur des pratiques établies, plusieurs intervenants choisissent d'y voir l'opportunité de mieux utiliser la donnée, de parler aux consommateurs d'une manière axée sur la qualité plutôt que sur la quantité, voire de faire de la confidentialité, un positionnement de marque comme l'a fait *Apple*. [118]

Ainsi, ce changement majeur s'inscrit dans un besoin plus large de favoriser la transparence, de rehausser le niveau de confidentialité des données et de rehausser la responsabilité des

---

[113] Audrey SCHOMER, « Publisher Ad Monetization After the Third-Party Cookie », *eMarketer* (8 mars 2021), en ligne : <https://www.emarketer.com/content/publisher-ad-monetization-after-third-party-cookie> (consulté le 6 janvier 2023)
[114] *Id.*
[115] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, ASSOCIATION CANADIENNE DES ANNONCEURS et CANADIAN MEDIA DIRECTORS' COUNCIL, Webinaire « The State of Identity in Online Advertising: A focus on Canada » (18 novembre 2021), en ligne : <https://us02web.zoom.us/webinar/register/rec/WN_eOwaoTPvQ06KD4ou2-P69g?meetingId=cTkoaRCDuJaZ3NdEJ692itXotvoaXujIkxdL-Znve5E8ANR-8X3b7cMHCaXLHgzF.fmZJTpE4HTO0w-ct&playId=&action=play&_x_zm_rtaid=rWB24S9kQzG8yRg4Cf5MWg.1640274121136.cc5166f33d54d31228dbb4a51d104a3d&_x_zm_rhtaid=743>
[116] Simon CAILLÉ, Conférence virtuelle « Quel avenir dans un monde sans cookie », *Dialekta* (30 novembre 2021), en ligne : <https://dialekta.com/fr/conferencier-quel-avenir-pour-les-annonceurs-dans-un-monde-sans-cookie/>
[117] *Id.*
[118] *Id.*

entreprises dans l'utilisation des renseignements personnels.[119] En effet, les notions de « gouvernance en matière de données » (*data governance*), de conservation des données (*data retention*), de minimisation de la collecte de données (*data minimisation*), sont des concepts de plus en plus populaires au sein des différents forums de l'industrie, notamment au dernier Sommet de la *European Interactive Digital Adversiting Alliance* (EDAA)[120]. Lors de ce Sommet, le concept de « technologie responsable » était très présent dans les discussions. Plus encore, dans une perspective où la monétisation des données représente un marché immense et très convoité et que pour continuer d'en tirer profit, directement ou indirectement, M. Guido Scorza, de l'Autorité italienne de la protection des données, rappelait que les entreprises doivent percevoir la protection des données comme une ressource en soit, plutôt que comme un coût ou une dépense[121].

[119] *Id.*

[120] Notamment lors du Sommet de la *European Interactive Digital Adversiting Alliance* (EDAA), « From choices to voices : Transparency in action », Londres, 15 novembre 2021, en ligne : <https://www.edaasummit.eu/>
Note : Ce Sommet réunit les experts, entreprises et organismes d'autoréglementation en matière de ciblage en ligne à travers le monde

[121] Lors du Sommet de la *European Interactive Digital Adversiting Alliance* (EDAA), « From choices to voices : Transparency in action », Londres, 15 novembre 2021, en ligne : <https://www.edaasummit.eu/>

Chapitre 2 - Complexité juridique

Après avoir brossé le portrait de la complexité factuelle entourant la PCL, examinons maintenant sa complexité juridique, étant soumise à une pluralité de normes formelles et informelles, ainsi qu'aux lignes directrices et positions des autorités de contrôle, et ce au niveau provincial, fédéral et international. Les lois nationales étrangères doivent effectivement être prise en compte considérant les flux de données transfrontières propres à la PCL. Finalement, il convient de souligner qu'un autre élément ajoutant à cette complexité est la structuration des normes en soi.

2.1 Pluralité de normes formelles au Canada applicables au secteur privé

La PCL est assujettie non seulement aux lois en matière de droit à la vie privée, mais aussi aux lois en matière de droit de la concurrence, de droit de la protection du consommateur et de droit commun. Je propose ici d'en décrire les principales exigences, afin de démontrer que cette pluralité normative ajoute à la complexité du cadre juridique applicable à la PCL. À preuve, le récent recours collectif intenté par Option Consommateurs au Québec contre *Google* se fonde sur l'ensemble des lois applicables au Québec et au Canada[122]. L'analyse concernant la complexité propre aux exigences prévues à la LPRPDE, au Projet de loi C-27 et à la Loi 25 est développée sous les parties II et III de ce mémoire.

2.1.1. Droit à la vie privée et protection des renseignements personnels au Canada et au Québec

Au Canada, le droit à la vie privée est un droit quasi constitutionnel dont l'une des dimensions est la protection des renseignements personnels, actuellement encadré au niveau fédéral par une loi visant les organismes publics[123] et par la LPRPDE s'appliquant au secteur privé. Ces deux lois seront bientôt regroupées sous une même loi, conformément au Projet de loi C-27.

---

[122] *Option Consommateurs* c. *Google*, 2022 QCCS 2308 (CanLII), par. 1, en ligne : <https://canlii.ca/t/jq114> (consulté le 12 février 2023)
Infra, 2.1.6., 6.1., 6.2.3. et 6.3.2.

[123] *Loi sur la protection des renseignements personnels* (LPRP), L.R.C. 1985, ch. P-21

La LPRPDE actuellement en vigueur « établit des règles de base pour la gestion des renseignements personnels dans le secteur privé [et] vise à concilier le droit individuel au respect de la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins commerciales légitimes. »[124]

Elle repose sur dix principes structurants énoncés à son Annexe 1, soit la responsabilité, la détermination des fins, le consentement, la limite à la collecte, la limite à l'utilisation, communication et conservation, l'exactitude, la sécurité, la transparence, l'accès aux renseignements personnels et la possibilité de porter plainte. Elle est complétée par le Règlement concernant les atteintes aux mesures de sécurité de 2018[125]. Ces principes demeurent les piliers sur lesquels repose la réforme proposée par le Projet de loi C-11 puis C-27. La Loi 25 au Québec et le RGPD sont également bâtis sur les mêmes principes-piliers autour desquelles viennent s'articuler les différents droits et obligations qu'ils mettent en place.

La LPRPDE a d'abord fait l'objet d'une révision qui a donné lieu au dépôt, en novembre 2020, du projet de *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois* (Projet de loi C-11)[126]. Son cheminement a été interrompu après l'étape de la première lecture à la Chambre des communes[127], puis a été relancé en juin 2022 sous une version modifiée et bonifiée[128], soit le projet de *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et*

---

[124] Miguel BERNAL-CASTILLERO et Nancy HOLMES, *Les loi fédérales du Canada sur la protection de la vie privée*, Bibliothèque du Parlement, *Publications de recherche*, 1er janvier 2013, révisée le 17 novembre 2020, par. 4, en ligne : <https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/200744E> (consulté le 15 janvier 2023)

[125] *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64, en ligne : <https://canlii.ca/t/6b62r> (consulté le 7 janvier 2023)

[126] *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois*, Projet de loi C-11 (Première lecture), 2e session, 43e législature (Can.), en ligne : <https://parl.ca/DocumentViewer/fr/43-2/projet-loi/C-11/premiere-lecture >

[127] PARLEMENT DU CANADA, « C-11 », LEGISinfo, en ligne : <https://www.parl.ca/legisinfo/fr/projet-de-loi/43-2/c-11>

[128] Le Projet de loi C-27 a été bonifié par rapport au Projet de loi C-11, notamment par l'ajout de la partie III qui introduit la *Loi sur l'intelligence artificielle des données*

apportant des modifications corrélatives et connexes à d'autres lois (Projet de loi C-27)[129]. Les dispositions finales qui modifieront l'actuelle LPRPDE devraient donc être connues prochainement. J'y reviendrai dans les parties II et III.

Au Québec, le droit à la vie privée est un droit protégé par l'article 5 de la Charte des droits et libertés de la personne[130]. De plus, il s'agit de la première province canadienne à s'être doté dès 1994 d'une loi spécifique en matière de protection des renseignements personnels. Un resserrement important a ensuite eu lieu avec le Projet de loi 64 déposé en juin 2020[131], dont a découlé la Loi 25 qui entre en vigueur en trois phases, soit en septembre 2022, septembre 2023 et septembre 2024. La réforme apportée par la Loi 25 a eu pour effet de renforcir le cadre législatif québécois et, par le fait même, de réaffirmer la position québécoise plus stricte par rapport au modèle fédéral canadien actuellement en vigueur. En effet, dès l'annonce du Projet de loi 64, la ministre Lebel mettait l'accent sur l'intention de s'aligner avec le standard européen (RGPD)[132] en donnant plus de contrôle à l'utilisateur.

Comme le soulignent Gautrais et Laville,

> « […] en matière de protection des renseignements personnels, le règlement européen constitue à la fois un modèle et un incitatif à adopter de pareilles mesures. »[133]

Se faisant, ils remarquent que

> « [s]i l'uniformisation des règles est un atout évident, elle risque en revanche de lisser les différences culturelles qui ne manquent pas de poindre entre les États. Ces différences

[129] *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Projet de loi C-27 (Première lecture), 1re session, 44e législature (Can.), en ligne : <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture >
[130] *Charte des droits et libertés de la personne*, RLRQ c C-12, en ligne : <https://canlii.ca/t/6dmsf> (consulté le 24 février 2023)
[131] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Projet de loi 64, 1re session, 42e législature (Québec), en ligne : <https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html?appelant=MC>
[132] Fanny LÉVESQUE, « Données personnelles : une loi avec plus de mordant », *La Presse* (12 février 2020) en ligne : <https://www.lapresse.ca/actualites/politique/202002/11/01-5260568-donnees-personnelles-une-loi-avec-plus-de-mordant.php>
[133] Vincent GAUTRAIS et Henry LAVILLE, « Pour une gouvernance participative des données personnelles au Québec » dans Mathilde HAUTEREAU-BOUTONNET et Cyril SINTEZ, Mélanges en l'honneur de Catherine Thibierge, 2023, p. 11, par. 1 (à paraître)

apparaissent d'abord substantiellement, certains pays étant plus enclins à faire prévaloir la protection des renseignements personnels que d'autres. »[134]

2.1.2. Loi sur la concurrence

En plus des lois spécifiques au droit à la vie privée et à la protection des renseignements personnels, la PCL, comme les autres formes de publicité, est assujettie à de nombreuses autres lois et règlements contenant des dispositions s'appliquant à la publicité en général, telle la Loi sur la concurrence[135]. Nous nous y attardons ici en traitant des points les plus directement pertinents.

La disposition centrale de cette loi s'appliquant à la publicité est celle qui interdit que la publicité contienne des indications fausses ou trompeuses sur un point important. Ainsi, le paragraphe 1 de l'article 52 de la loi prévoit que « [n]ul ne peut, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'utilisation d'un produit, soit des intérêts commerciaux quelconques, donner au public, sciemment ou sans se soucier des conséquences, des indications fausses ou trompeuses sur un point important. »

Afin de déterminer s'il y a infraction à l'article 52, le Bureau de la concurrence rappelle qu'il faut non seulement tenir compte du sens littéral des indications contenues dans l'annonce, mais également de l'impression générale que donne l'annonce dans son ensemble.[136]

En effet, le Bureau rappelle que la Cour suprême du Canada en 2012 est venue préciser que « les tribunaux ne doivent pas aborder une publicité écrite comme un contrat commercial, c'est-à-dire la lire plusieurs fois, en s'attachant à tous ses détails pour en comprendre toutes les subtilités. Une seule lecture d'ensemble devrait suffire pour apprécier l'impression générale donnée par une publicité écrite. »[137] Par ailleurs, le Bureau de la concurrence constate que « [b]on nombre d'indications qui cherchent à tromper les consommateurs en ligne créent une impression générale fausse ou trompeuse parce que l'annonceur n'a pas divulgué de façon appropriée les

---

[134] *Id*., p. 11 par. 2, référant à « Vincent GAUTRAIS, « "Made in Canada" : Distinctions culturelles de la protection des renseignements personnels canadienne », (2021) 33 *Les Cahiers de propriété intellectuelle* 1365, 1406.
[135] *Loi sur la concurrence*, LRC 1985, c C-34, en ligne : <https://canlii.ca/t/6dj9g> (consulté le 22 janvier 2023)
[136] BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, Volume 1, 10 juin 2015, par. 2.2, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03946.html>
[137] *Richard* c. *Time Inc*., 2012 CSC 8, [2012] 1 RCS 265, 2012 CSC 8 (CanLII), par. 56, cité par BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, *op. cit*., note 136 , par. 2.3.2.

renseignements dont les consommateurs ont besoin pour faire des choix éclairés. L'état véritable des activités, s'il est divulgué, est souvent caché dans des avertissements en petits caractères ou dissimulé par le formatage ou l'emplacement dans le contexte de l'annonce générale. »[138]

Le Bureau observe des problèmes importants et fréquents liés à la divulgation, dont premièrement, l'utilisation des avertissements et petits caractères à mauvais escient. L'utilisation de la technique du prix partiel (*drip-pricing*) consiste à afficher un prix accrocheur qui ne représente pas le coût total réel pour l'achat du produit ou service, puisque certains coûts liés à l'achat sont délibérément réduits ou cachés dans de petits caractères de sorte que le consommateur ne réalise le prix réel qu'au moment de passer la transaction.[139]

À titre d'exemple, en 2011, Bell Canada a dû modifier toutes ses publicités jugées trompeuses dans un délai de 60 jours et payer la sanction administrative maximale prévue par la Loi sur la concurrence, soit 10 millions de dollars.[140] En effet, dans cette affaire, Bell faisait la promotion de différents services, mais « [l]es prix annoncés n'étaient en fait pas disponibles, étant donné que des frais obligatoires supplémentaires étaient cachés aux consommateurs dans des modalités en petits caractères ».[141]

Lors de la révision de la loi, dont les modifications sont entrées en vigueur en juin 2022, l'indication de prix partiel (c'est-à-dire indiquer un prix qu'un client ne peut atteindre parce qu'il y a des frais supplémentaires fixes obligatoires) a été explicitement reconnue comme une pratique commerciale préjudiciable et assimilée à une indication fausse ou trompeuse au sens des articles 52 et 74.01 de la loi.[142]

---

[138] BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, *op. cit.* note 136, par. 1.4.
[139] *Id.*, par. 1.4.2.
[140] BUREAU DE LA CONCURRENCE, Archivé – « Le Bureau de la concurrence conclut une entente avec Bell Canada exigeant que Bell paie 10 millions de dollars pour publicité trompeuse » (28 juin 2011), en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03388.html >
[141] BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, *op. cit.* note 136, par. 2.6.
[142] BUREAU DE LA CONCURRENCE, *Guide des modifications apportées en 2022 à la Loi sur la concurrence*, 24 juin 2022, en ligne : <https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/comment-nous-favorisons-concurrence/education-sensibilisation/publications/guide-modifications-apportees-2022-loi-concurrence#sec04 > (consulté le 22 janvier 2023)

Par ailleurs, constitue une infraction à la loi la dissimulation de modalités d'achat dans de petits caractères ou au cœur d'une rédaction obscure, telles l'acceptation du consommateur à un abonnement annuel ou encore la renonciation au contrôle de ses renseignements personnels.[143] Ainsi, si les annonceurs souhaitent ou doivent avoir recours aux avertissements en petits caractères dans leurs annonces publicitaires, ils doivent respecter les principes fondamentaux de cet usage, lesquels se résument ainsi :

- Le recours aux petits caractères est considéré légitime par le Bureau de la Concurrence si ces derniers ont pour objet d'ajouter des renseignements utiles à des indications qui sont déjà vraies et exactes.[144] [Mes soulignements] *A contrario*, ils ne peuvent servir à « restreindre, contredire ou annuler d'une certaine façon le message auquel il[s] se rapporte[nt] »[145] par exemple pour rectifier un message principal faux ou trompeur.[146]
- Quant à leur forme et emplacement, ils ne peuvent ni « créer de confusion ou être difficiles à comprendre »,[147] ni « être cachés entre des lignes de texte dense en petits caractères ou […] présentés autrement de telle sorte que leur véritable sens soit obscur. »[148]

Finalement, le Bureau reconnait lui-même le défi que peut poser le fait de la publicité conçue et transférable en différents formats, plateformes et appareils.[149] Conséquemment, bien que la tâche ne soit pas facile, il n'en demeure pas moins qu'il faille s'assurer que les avertissements soient en tout temps présents, visibles, accessibles facilement et compréhensibles de sorte qu'ils « soient consultés et compris de manière à [ne pas] déformer l'impression générale créée par une annonce en ligne »[150].

[143] BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, *op. cit.* note 136, par. 1.4.3.
[144] *Id.*, par. 2.3.1.
[145] *Id.,* par. 2.3.2.
[146] *Id.,* par. 2.3.2. À titre d'exemple, le Bureau mentionne l'affaire *Commissioner of Competition* v. *Yellow Page Marketing*, 2012 ONSC 927 (CanLII).
[147] *Id.*, par. 2.3.2.
[148] *Id.*, par. 2.3.2.
[149] *Id.*, par. 2.5.
[150] *Id.*, par. 2.5.

Une autre pratique problématique en lien avec la divulgation est la pratique de la désinformation populaire planifiée. En effet, le Bureau remarque l'existence de cette pratique qui consiste à diffuser des annonces qui ont l'apparence d'articles provenant de sources d'information indépendantes, tels des critiques d'experts, des billets de blogues ou des témoignages de consommateurs.[151] Il déplore, avec raison, que des avis de faux consommateurs soient utilisés pour bonifier l'évaluation de la marque et/ou de son produit/service ou encore pour dévaloriser et nuire à un compétiteur.[152] Il constate que ces avis proviennent d'employés ou de personnes ou d'entreprises payées par l'annonceur pour produire ces commentaires, avis, cotes ou critiques.[153] Ainsi, afin de permettre au consommateur d'être en mesure de prendre une décision libre et éclairée concernant un produit/service/marque, le Bureau rappelle que la critique doit être non seulement authentique, mais également impartiale, autrement tout lien important (rémunération, contrepartie versée ou autre) doit être divulgué par l'expert, le blogueur ou l'influenceur le cas échéant. En conséquence, il recommande que « [l]es annonceurs, ou les personnes avec qui ils entretiennent un lien important, qui songent à afficher des critiques de consommateurs sur leurs propres produits ou sur ceux de leurs concurrents devraient peut-être se demander si ces critiques créent l'impression générale qu'elles représentent l'expérience et l'opinion authentiques de consommateurs impartiaux. Lorsqu'ils réfléchissent à l'impression qui est créée, les annonceurs devraient tenir compte du contexte dans lequel les critiques risquent d'être affichées. Pendant cet examen du contexte, ils devraient notamment se demander si l'on peut faire une distinction entre la critique et la divulgation d'un lien important. »[154] [Mes soulignements]

Pour guider l'industrie dans l'application de ces règles, notons que l'organisme canadien d'autoréglementation d'industrie, les Normes canadiennes de la publicité[155], proposent des lignes directrices sur les manières concrètes recommandées (formes, emplacements) de divulguer un

[151] *Id.*, par. 1.4.1.
[152] *Id.,* par. 3.4.
[153] *Id.*, par. 3.4.
[154] *Id.*, point 3.4, par. 10.
[155] Infra, 2.2.2.

lien important entre un influenceur et un annonceur afin d'éviter que la publicité soit considérée comme trompeuse[156].

La divulgation du lien entre l'annonceur et l'entité qui émet une opinion est également une exigence commune dans d'autres juridictions, tels les États-Unis, l'Australie et le Royaume-Uni.[157] Aux États-Unis plus précisément, elle est comprise dans les lignes directrices émises par la *Federal Trade Commission* (FTC) aux États-Unis concernant le marketing d'influence, lesquelles demandent la « divulg[ation] [de] tout lien entre la personne faisant une recommandation et le spécialiste du marketing du produit qui aurait une incidence sur l'importance que les gens accordent à la recommandation »[158]. [Mes soulignements.]

Est donc primordiale la préservation d'un lien de confiance entre les consommateurs et l'information qu'ils trouvent tant en ligne qu'ailleurs. Cette dernière passe nécessairement par la protection de la transparence et de la véracité des informations données aux consommateurs, non seulement quant au produit/service/marque lui-même, mais également quant à l'authenticité des commentaires émis sur ceux-ci et susceptibles d'influencer les consommateurs dans leur prise de décision.

2.1.3. Loi canadienne antipourriel

La loi canadienne antipourriel[159] (LCAP) est la loi fédérale canadienne encadrant spécifiquement l'envoi de messages électroniques commerciaux (MEC) et l'installation de programmes d'ordinateur.

Encadrement des messages électroniques commerciaux :

[156] NORMES CANADIENNES DE LA PUBLICITÉ, COMITÉ DIRECTEUR SUR LE MARKETING D'INFLUENCE, *Lignes directrices sur la divulgation*, révisé automne 2020, en ligne : <https://adstandards.ca/fr/ressources/marketing-dinfluence/> (consulté le 29 avril 2023)

[157] BUREAU DE LA CONCURRENCE, *Recueil des pratiques commerciales trompeuses*, *op. cit.* note 136, point 3.5.

[158] *Id.*, point 3.4, par. 10, ayant comme source : FEDERAL TRADE COMMISSION, *The FTC's Endorsement Guides : What People are Asking*, septembre 2017, mis à jour le 27 août 2020, en ligne: <https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking>

[159] *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la loi sur la concurrence, la loi sur la protection des renseignements personnels et les documents électroniques et la loi sur les télécommunications*, LC 2010, c 23, en ligne : <https://canlii.ca/t/6b07x> (consulté le 29 janvier 2023)

Dans un premier temps, elle interdit l'envoi de message électronique commercial qui n'a pas été sollicité par son destinataire, c'est-à-dire sans avoir au préalable obtenu le consentement exprès conforme[160] ou tacite du destinataire du MEC.[161]L'émetteur ne peut pas solliciter ce consentement via un MEC puisque cette demande est considérée par la LCAP comme étant un MEC en soi[162]. Cette loi reconnaît qu'un consentement tacite à la réception d'un MEC peut être présumé, notamment lorsque l'émetteur du MEC communique avec son destinataire dans le cadre d'une relation d'affaires en cours ou de moins de deux ans[163], par exemple découlant d'une transaction commerciale déjà réalisée par le destinataire auprès de l'entreprise émettrice du MEC[164].

La LCAP définit largement un MEC comme étant

> « (…) le message électronique dont il est raisonnable de conclure, vu son contenu, le contenu de tout site Web ou autre banque de données auquel il donne accès par hyperlien ou l'information qu'il donne sur la personne à contacter, qu'il a pour but, entre autres, d'encourager la participation à une activité commerciale et, notamment, tout message électronique qui, selon le cas :
>
> a) comporte une offre d'achat, de vente, de troc ou de louage d'un produit, bien, service, terrain ou droit ou intérêt foncier;
>
> b) offre une possibilité d'affaires, d'investissement ou de jeu;
>
> c) annonce ou fait la promotion d'une chose ou possibilité mentionnée aux alinéas a) ou b);
>
> d) fait la promotion d'une personne, y compris l'image de celle-ci auprès du public, comme étant une personne qui accomplit — ou a l'intention d'accomplir — un des actes mentionnés aux alinéas a) à c). »[165]

[160] Tel que défini à l'art. 10 de la LCAP
[161] LCAP, art. 6(1).
[162] LCAP, art. 1(3) : « Le message électronique comportant une demande de consentement en vue de la transmission d'un message visé au paragraphe (2) est aussi considéré comme un message électronique commercial. »
[163] LCAP, art. 10(9) et (10).
[164] CRTC, *Lignes directrices sur le consentement tacite dans le cadre de la Loi canadienne anti-pourriel (LCAP)*, dernière modification le 4 septembre 2015, en ligne : <https://crtc.gc.ca/fra/com500/guide.htm> (consulté le 5 février 2023)
[165] LCAP, art. 1(2), définition de « message électronique commercial ».

Ainsi, une annonce publicitaire envoyée à une adresse électronique, c'est-à-dire à un compte courriel, de messagerie instantanée, de téléphone ou autre compte similaire[166], qu'elle soit textuelle, sonore, vocale ou visuelle[167], tombe sous le champ d'application de la LCAP. Dès lors, elle devra non seulement contenir les mentions obligatoires prévues par la LCAP, c'est-à-dire les renseignements règlementaires permettant d'identifier l'émetteur et la personne au nom de qui il a envoyé le MEC le cas échéant et les coordonnées permettant de contacter ces personnes[168], mais également un mécanisme d'exclusion conforme permettant au destinataire de ne plus recevoir de tel message à l'avenir[169] et effectif dans les dix jours ouvrables[170].

Cette interdiction s'applique à un contexte de marketing relationnel (aussi appelé marketing direct), et moins à un contexte de PCL, mais pourrait trouver application dans un contexte de PCL si la publicité résulte ou inclut l'envoi de message se qualifiant de MEC au sens de la loi, tel que résumé plus haut, tel un courriel, un message transmis dans une boite de messagerie privée sur les réseaux sociaux ou encore un message texte.

Encadrement de l'installation de programmes d'ordinateur

Dans un deuxième temps, la LCAP interdit l'installation de programme d'ordinateur dans le cadre d'activités commerciales sans obtention préalable d'un consentement exprès du propriétaire de l'ordinateur.[171] Cela vise à priori les logiciels malveillants, mais pourrait également trouver application dans un contexte de PCL dans la mesure où elle fonctionne – encore – grâce à la collecte de fichiers témoins.

[166] LCAP, art. 1 (1), définition de « adresse électronique ».
[167] LCAP, art. 1 (1), définition de « message électronique ».
[168] LCAP, art. 6(2)a) et b), complétés par le *Règlement sur la protection du commerce électronique (CRTC)*, DORS/2012-36, en ligne : <https://canlii.ca/t/69fmr> (consulté le 10 février 2023), art. 2.
[169] LCAP, art. 6(2)c) et art. 11(1), complétés par le *Règlement sur la protection du commerce électronique (CRTC)*, DORS/2012-36, en ligne : <https://canlii.ca/t/69fmr> (consulté le 10 février 2023), art. 3.
[170] LCAP, art. 11(3) et (4)b).
[171] LCAP, art. 8(1)a).

La LCAP réfère à la définition du Code criminel pour définir ce qu'est un programme d'ordinateur, c'est-à-dire un « [e]nsemble de données informatiques qui représentent des instructions ou des relevés et qui, lorsque traitées par l'ordinateur, lui font exécuter une fonction. »[172]

Dans la liste des fonctions des programmes visés par la LCAP, celle permettant la collecte de renseignements personnels sur l'ordinateur est expressément incluse et vient d'ailleurs au premier rang :

> Art. 10(5) Fonctions
>
> « (5) Les fonctions visées au paragraphe (4) sont celles mentionnées ci-dessous dont la personne qui sollicite le consentement sait qu'elles auront pour effet de faire fonctionner l'ordinateur d'une façon contraire aux attentes raisonnables du propriétaire ou de l'utilisateur autorisé de celui-ci et dont il entend qu'elles aient cet effet :
>
> a) la collecte de renseignements personnels sur l'ordinateur;
>
> b) l'entrave au contrôle de l'ordinateur par le propriétaire ou l'utilisateur autorisé de celui-ci;
>
> c) la modification des paramètres, préférences ou commandements déjà installés ou mis en mémoire dans l'ordinateur ou l'entrave à leur utilisation, à l'insu du propriétaire ou de l'utilisateur autorisé de l'ordinateur;
>
> d) la modification des données déjà mises en mémoire dans l'ordinateur ayant pour effet d'empêcher, d'interrompre ou d'entraver l'accès ou l'utilisation légitimes de ces données par le propriétaire ou l'utilisateur autorisé de celui-ci;
>
> e) la communication de l'ordinateur, sans l'autorisation de son propriétaire ou utilisateur autorisé, avec un autre ordinateur ou dispositif;
>
> f) l'installation d'un programme activé par un tiers à l'insu du propriétaire ou de l'utilisateur autorisé de l'ordinateur;
>
> g) toute autre fonction précisée dans les règlements. »[173]
>
> [Mes soulignements]

[172] *Code criminel*, LRC 1985, c C-46, en ligne : <https://canlii.ca/t/6dzjf> (consulté le 10 février 2023), art. 342.1(2), auquel réfère la LCAP art. 1(1) définition de « programme d'ordinateur ».

[173] LCAP, art. 10(5).

Concernant cette fonction de collecte de renseignements personnels, le CRTC donne l'exemple d'« [u]ne application ou un logiciel qui a été installé [qui] recueille des identifiants d'utilisateur, comme des noms d'utilisateur et des mots de passe. »[174]

Concernant l'obligation de consentement, la LCAP formule différemment cette exigence lorsqu'elle parle de programme d'ordinateur. En effet, a priori, elle prévoit qu'un consentement exprès doit être obtenu[175]. Ainsi, un consentement exprès est obligatoire et la demande de consentement doit préciser les fins pour lesquelles le consentement est demandé, les informations permettant d'identifier la personne qui sollicite le consentement et tout autre renseignement requis par règlement[176], le tout en termes simples et clairs.[177] De surcroît, la demande de consentement doit préciser la fonction et l'objet du programme en question[178], et, lorsqu'il s'agit d'une des fonctions listées à l'article 10(5), décrire les éléments du programme qui effectuent ces fonctions tels la nature, l'objet et les conséquences prévisibles sur le fonctionnement de l'ordinateur, le tout en termes clairs et facilement lisibles dans un endroit qui n'est pas le contrat de licence.[179] Lorsqu'il s'agit d'une fonction énumérée à l'article 10(5), comme la collecte de renseignements personnels, le règlement DORS/2012-36 précise que les éléments du programme qui effectuent ses fonctions doivent être « portés à l'attention de la personne auprès de qui le consentement est sollicité séparément des autres renseignements fournis dans la demande de consentement et la personne qui sollicite le consentement doit obtenir de cette personne une confirmation écrite attestant qu'elle comprend et accepte que le programme effectue les fonctions mentionnées.»[180]

---

[174] CRTC, *Exigences de la Loi canadienne anti-pourriel concernant l'installation de programmes informatiques*, date de modification : 2020-09-18, en ligne : <https://crtc.gc.ca/fra/internet/install.htm> (consulté le 10 février 2023)
[175] LCAP, art. 8(1)a).
[176] En référence au *Règlement sur la protection du commerce électronique (CRTC)*, DORS/2012-36, art. 4, en ligne : <https://canlii.ca/t/69fmr> (consulté le 10 février 2023)
[177] LCAP, art. 10(1).
[178] *Id.*, art. 10(3).
[179] *Id.*, art. 10(4).
[180] *Règlement sur la protection du commerce électronique (CRTC)*, DORS/2012-36, en ligne : <https://canlii.ca/t/69fmr> (consulté le 10 février 2023), art. 5.

Toutefois, la LCAP ajoute qu'il peut y avoir une présomption de consentement exprès lorsque le programme est un témoin de connexion[181] et qu'il est raisonnable de croire, d'après son comportement, que la personne consent à l'installation du programme :

> art. 10 « Présomption de consentement exprès
>
> (8) La personne est réputée consentir expressément à l'installation d'un programme d'ordinateur si, à la fois :
>
> a) le programme est, selon le cas :
>
> - (i) un témoin de connexion,
> - (ii) un code HTML,
> - (iii) un JavaScript,
> - (iv) un système d'exploitation,
>
> (v) tout autre programme qui ne peut être exécuté que par l'entremise d'un autre programme auquel elle a déjà expressément consenti à l'installation ou à l'utilisation,
>
> (vi) tout autre programme précisé par règlement;
>
> b) il est raisonnable de croire, d'après son comportement, qu'elle consent à l'installation du programme. » [182]

Ainsi, la LCAP ne permet pas l'obtention d'un consentement tacite pour l'installation de programme d'ordinateur, contrairement à l'envoi de MEC, mais prévoit qu'un consentement exprès peut être présumé (réputé) selon les circonstances. À cet effet, le CRTC est venu préciser :

> « Il importe de souligner que vous n'êtes réputé avoir le consentement pour installer ces types de programmes [énumérés à 10(8)] que si le comportement de la personne montre qu'elle consent à l'installation. Par exemple, si la personne désactive JavaScript de son navigateur, vous ne seriez pas réputé avoir le consentement en vertu de la LCAP puisque le comportement de la personne n'indiquerait pas que celle-ci consent à l'installation de ce type de programme. De la même manière, si la personne désactive les témoins de

[181] Le CRTC définit ainsi un témoin de connexion : « Un témoin de connexion, aussi appelé simplement témoin, est un programme informatique non exécutable qui ne peut pas transporter de virus et installer un maliciel. Tel qu'il est précisé ci-dessus, la LCAP prévoit que la personne est réputée consentir à l'installation d'un témoin si le comportement de la personne est tel qu'il est raisonnable de croire qu'elle consent. » CRTC, *Exigences de la Loi canadienne anti-pourriel concernant l'installation de programmes informatiques*, modifié le 18 septembre 2020, en ligne : <https://crtc.gc.ca/fra/internet/install.htm> (consulté le 10 février 2023)

[182] LCAP, art. 10(8).

connexion dans son navigateur, vous ne seriez pas réputé avoir le consentement d'implanter des témoins de connexion. »[183] [Mon soulignement]

Soulignons qu'« [i]l n'existe cependant aucune indication claire sur la conduite qui serait considérée comme « raisonnable » pour présumer du consentement. »[184] Ainsi, il y a place a interprétation sur cette question.

À la lumière de l'analyse ci-dessus, dans un contexte de PCL, si nous devions nous baser uniquement sur la LCAP, un consentement implicite pourrait être considéré comme étant valide tant et aussi longtemps que la personne ne désactive pas les témoins de connexion dans son ou ses navigateurs Internet. Il est possible d'affirmer que cette façon de penser est commune à celle développée par le CPVP dans sa position de principe concernant la PCL que nous verrons plus bas.

Constatons ici que les principes de transparence et de consentement, balisés par les concepts d'attentes raisonnables, de demande de consentement détaillée et de manière simple, claire et accessible, sont communs avec les lois en vigueur en matière de protection de la vie privée.

2.1.4. Loi sur la protection du consommateur du Québec et Code civil du Québec

Le Titre II « Pratiques de commerce » de la Loi sur la protection du consommateur du Québec (LPC)[185] prévoit plusieurs obligations et interdictions visant les activités des commerçants, fabricants et publicitaires, et plusieurs dispositions visant spécifiquement les messages publicitaires. À l'instar de la loi fédérale sur la concurrence et du Code des Normes de la publicité, la LPC interdit principalement toute représentation fausse ou trompeuse à un consommateur et prévoit différentes dispositions concernant la présentation des informations tant sur le commerçant que sur le produit ou le service annoncé, notamment qu'elles doivent être vraies et exactes, et qu'elles doivent présentées de manière claire, lisible et compréhensible. S'ajoutent à ces dispositions les précisions apportées par règlements, notamment le Règlement d'application

[183] CRTC, *Exigences de la Loi canadienne anti-pourriel concernant l'installation de programmes informatiques*, modifié le 18 septembre 2020, en ligne : <https://crtc.gc.ca/fra/internet/install.htm> (consulté le 10 février 2023)
[184] Caroline JONNAERT et Élisabeth LESAGE-BIGRAS, « Cookies et vie privée : ce que toute organisation devrait savoir », *op. cit.,* note 15
[185] *Loi sur la protection du consommateur*, RLRQ c P-40.1, art. 215 à 253, en ligne : <https://canlii.ca/t/6dr0n> (consulté le 12 février 2023)

sur la LPC, qui traite notamment de publicité destinée aux enfants.[186] Ainsi, la publicité destinée aux enfants est en principe interdite aux enfants de moins de treize ans. Lorsque le Règlement d'application de la LPC le permet exceptionnellement, ce règlement prévoit les différentes conditions quant au contenu du message publicitaire.

Le Code civil du Québec (CCQ) trouve également application en matière de publicité et de PCL. Ainsi, le Chapitre troisième « Du respect de la réputation et de la vie privée » du Titre Deuxième « De certains droits de la personnalité », encadre spécifiquement le droit à la vie privée d'une personne[187]. Ainsi, l'article 35 prévoit le droit au respect de la vie privée et le protège contre les atteintes non autorisées par la loi ou le consentement de la personne concernée. Le CCQ prévoit aussi spécifiquement que le fait de surveiller la vie privée par quelque moyen que ce soit peut être considéré comme une atteinte à la vie privée.[188] L'article 37 prévoit :

> « Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation. »

Les articles 38 à 41 quant à eux prévoient un droit d'accès et de consultation de la personne aux renseignements contenus à un dossier qui la concerne, ainsi que le droit d'y faire rectifier un renseignement inexact, incomplet ou équivoque ou encore de faire supprimer un renseignement périmé ou non justifié.

Des obligations de même nature et fondée sur des principes semblables sont également présentes dans les lois spécifiques à la protection des renseignements personnels, que nous

---

[186] *Règlement d'application de la Loi sur la protection du consommateur*, RLRQ c P-40.1, r 3, en ligne : <https://canlii.ca/t/6dq40> (consulté le 12 février 2023), Section II (art. 87 à 91).
La publicité destinée aux enfants est en principe interdite aux enfants de moins de treize ans. Lorsque le Règlement d'application de la LPC le permet exceptionnellement, ce règlement prévoit les différentes conditions quant au contenu du message publicitaire.

[187] *Code civil du Québec*, RLRQ c CCQ-1991, en ligne : <https://canlii.ca/t/6dzcm> (consulté le 12 février 2023), art. 35 à 41.

[188] CCQ, art. 36(1)4°.

étudierons plus loin. Toutefois, constatons ici que le CCQ parle de renseignements et non de renseignements personnels, et donc que les CCQ a une portée plus large en ce sens.

En cas d'atteinte, une personne pourrait invoquer la responsabilité extracontractuelle sous 1457 CCQ ou la responsabilité contractuelle sous 1458 CCQ selon le cas, afin de trouver réparation[189].

2.1.5. Autres lois fédérales, provinciales et sectorielles

Ajoutons à cette liste les autres lois et règlements au Canada qui s'appliquent à la publicité la Loi sur les marques de commerce[190] et la Loi sur le droit d'auteur[191], et également les différentes lois en matière de protection des renseignements personnels propres à certains secteurs d'activité telle la Loi sur les banques[192] et les lois provinciales sur les caisses de crédit.[193] Finalement, s'ajoutent les différentes lois et règlements étrangers qui s'appliquent lorsque les renseignements personnels sortent de nos frontières[194].

2.1.6. Importante décision judiciaire à venir au Québec concernant l'application des différentes lois dans un contexte de PCL

Le droit à la vie privée a été reconnu et interprété à plusieurs reprises au Canada et au Québec. Toutefois, nous ne disposons pas encore de jurisprudence pertinente portant spécifiquement sur le sujet des témoins de connexion et les technologies similaires au Québec ni au Canada.[195] Faute de décision émanant des cours de justice, les rapports de conclusion des différentes enquêtes effectuées par le CPVP viennent prendre une place importante dans l'interprétation et l'application des règles entourant la PCL et les pratiques de ciblage publicitaire de manière

[189] Infra, 2.1.6. et 6.2.2.
[190] *Loi sur les marques de commerce*, LRC 1985, c T-13, en ligne : <https://canlii.ca/t/6d5fr> (consulté le 22 janvier 2023). Plus particulièrement à son article 50.
[191] *Loi sur le droit d'auteur*, LRC 1985, c C-42, en ligne : <https://canlii.ca/t/6cdt9> (consulté le 22 janvier 2023)
[192] *Loi sur les banques*, LC 1991, c 46, en ligne : <https://canlii.ca/t/6dj9l> (consulté le 12 février 2023)
[193] Pour une liste complète des lois en vigueur, lire : CPVP, *Aperçu des lois sur la protection des renseignements personnels au Canada*, novembre 2017, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/#heading-0-0-3-1 > (consulté le 12 février 2023)
[194] Infra, 2.5 et 5.4.
[195] Et corroboré par Caroline JONNAERT et Élisabeth LESAGE-BIGRAS, « Cookies et vie privée : ce que toute organisation devrait savoir », *op. cit.,* note 12, par. « Jurisprudence »

générale. Je propose d'étudier les conclusions de ces rapports dans les sections II et III du présent mémoire.

Néanmoins, cela changera bientôt au Québec puisqu'une importante demande d'action collective contre *Google*, concernant spécifiquement les services de publicité comportementale en ligne offerts par *Google* à ses clients annonceurs, a été autorisée à l'été 2022. La décision au mérite qui suivra sera déterminante puisque plusieurs définitions et concepts centraux y seront revus en détail à la lumière des différentes lois applicables au Québec et au Canada dans un contexte de profilage et de ciblage publicitaire, principalement la définition de renseignements personnels, les paramètres d'un consentement valable, et la détermination de la nature des dommages applicables et leur l'évaluation, de pair avec la notion de valeur de renseignements personnels.

En résumé, dans cette affaire, Option Consommateurs s'est vue autorisée par la Cour supérieure d'exercer une action collective pour le compte du groupe constitué de

> « [t]oute personne domiciliée au Québec ayant utilisé un service offert par *Google* qui ne nécessite pas la création d'un compte *Google*, tel que *Google Search* ou *Google Maps*, ou ayant navigué sur un site Web utilisant un des outils offerts par *GOOGLE* tels que *Google Analytics*, *Google Ad Manager* ou le bouton d'ouverture de session « *Sign in with Google* ».[196] [Mes soulignements]

Le cœur de la problématique alléguée par Option Consommateurs, et acceptée par le Tribunal, est que *Google* traiterait des renseignements, qui se qualifient de renseignements personnels au sens de la loi, des utilisateurs des outils et services *Google*, sans leur consentement, afin d'offrir des services de publicité comportementale à ses clients annonceurs. De plus, l'exemple de la personne désignée au recours est plus problématique, puisqu'elle aurait utilisé à plusieurs reprises la fonction « Ne pas suivre » et le mode de navigation privée lorsqu'elle naviguait sur les sites Web tiers utilisant *Google Analytics* et *Google Ad Manager*.[197]

En conséquence, la demanderesse allègue toutes les violations statutaires possibles en vertu du droit québécois et fédéral applicable, c'est-à-dire : les articles 6, 8, 13, 14 de la Loi 25, le troisième principe de l'annexe 1 de la LPRPDE, les articles 8 et 9 de la LCAP, les articles 5 et 49 de la Charte

[196] *Option Consommateurs* c. *Google*, 2022 QCCS 2308 (CanLII), par. 1, en ligne : <https://canlii.ca/t/jq114> (consulté le 12 février 2023)
[197] *Id.*, par. 25.

des droits et libertés de la personne[198], les articles 41, 219 et 228 (en appliquant le test de l'article 218) de la LPC[199] et les articles 52 et 36 de la Loi sur la concurrence[200]. Selon Option Consommateurs, les violations à la Loi 25, à la LPRPDE et à la LCAP constituent des fautes qui fondent la responsabilité extracontractuelle de *Google* au sens de l'article 1457 du CCQ à l'égard des membres du groupe à l'action collective.[201]

Dans son jugement sur demande d'autorisation d'exercer l'action collective, la Cour supérieure conclut que les renseignements traités par *Google* sont bien des renseignements personnels au sens de l'article 2 de la Loi 25[202], que le consentement des consommateurs pour pouvoir les traiter est requis[203] et que la demanderesse a fait la démonstration de la faute par *Google* de ne pas respecter la Loi 25, la LPRPDE et la LCAP,[204] fondant la responsabilité extracontractuelle de *Google* en vertu de 1457 du CCQ, ainsi que la violation à la LPC et à la Loi sur la concurrence quant à la navigation en mode privé.

La décision au mérite traitera de tous ces aspects, en plus de celui de l'existence et de l'évaluation des dommages patrimoniaux et extrapatrimoniaux demandés par la demanderesse. L'issue de cette affaire qui fera jurisprudence aura un impact non seulement sur *Google*, mais sur l'industrie en général puisqu'elle utilise largement les différents outils déployés par *Google*. Je reviendrai plus en détail sur ces différents aspects abordés par cette décision[205].

2.2 Interprétations et lignes directrices du CPVP et de la CAI, et leur rôle de premier plan

Les lignes directrices, les positions, les énoncés de principe et les guides d'interprétation et d'application émanant des différents organismes de contrôle comme le CPVP, la CAI, le Bureau

[198] *Charte des droits et libertés de la personne*, RLRQ c C-12, en ligne : <https://canlii.ca/t/6dmsf> (consulté le 24 février 2023)
[199] *Option Consommateurs* c. *Google*, *op. cit.*, note 196, par. 119 à 137.
[200] *Id.*, par. 138 à 143.
[201] *Id.*, par. 58 et ss.
[202] *Id.*, par. 64.
[203] *Id.*, par. 67.
[204] *Id.*, par. 67, 81 et 92.
[205] Infra, 6.1., 6.2.3. et 6.3.2.

de la concurrence et le CRTC occupent un rôle de premier plan dans l'application des lois dont ils ont la responsabilité. Concernant l'application des lois en matière de vie privée au fédéral et au Québec, les interprétations et les lignes directrices du CPVP et de la CAI s'avèrent également centrales, à plus forte raison considérant l'accroissement de leurs pouvoirs prévu dans le Projet de loi C-27 et dans la Loi 25.

Commissariat à la protection de la vie privée du Canada

Les quatre priorités stratégiques déclarées du CPVP liées à la vie privée et à la PRP sont :

1- L'économie des renseignements personnels, en poursuivant le but de « [r]enforcer la protection de la vie privée et la confiance des gens pour qu'ils puissent participer avec assurance à l'économie innovante du numérique. »[206]
2- La surveillance du gouvernement, visant à « [c]ontribuer à l'adoption et à l'application de lois et d'autres mesures qui ont manifestement pour effet de garantir tant la sécurité nationale que la protection de la vie privée. »[207]
3- La réputation et la protection de la vie privée, dont l'objectif est d'« [a]ider à créer un environnement en ligne où les gens pourront se servir d'Internet pour explorer leurs intérêts et se développer comme personnes sans craindre que leur trace numérique n'entraîne un traitement injuste. »[208]
4- Le corps comme source d'information, afin de « [p]romouvoir le respect de la vie privée et de l'intégrité du corps humain comme véhicule de nos renseignements personnels les plus intimes. »[209]

Incidemment, le CPVP a émis plusieurs lignes directrices, positions et guides au cours des dernières années, significativement plus abondantes et étoffées que celles de la CAI en matière de PCL et de PRP, afin d'expliquer son interprétation des différentes dispositions de la LPRPDE.

---

[206] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les priorités stratégiques liées à la vie privée*, dernière modification : 14 décembre 2018, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/priorites-strategiques-liees-a-la-vie-privee-du-commissariat/les-priorites-strategiques-liees-a-la-vie-privee/> (consulté le 4 janvier 2023)
[207] *Id.*
[208] *Id.*
[209] *Id.*

Ceux touchant plus particulièrement la PCL sont les Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne (2011)[210], la *Position de principe sur la publicité comportementale en ligne* (2015)[211], les *Lignes directrices pour l'obtention d'un consentement valable* (2018)[212], ainsi que ses divers rapports de conclusion d'enquête publiés au fil des ans.[213]

Dans sa position de principe sur la PCL, le CPVP émet son opinion et ses recommandations sur des points majeurs, principalement sur le fait que selon lui, les renseignements collectés dans le processus de PCL constituent en principe des renseignements personnels et que la PCL peut constituer une fin acceptable au sens de la LPRPDE si elle respecte certains paramètres : transparence, obtention d'un consentement implicite avec possibilité de retrait du consentement s'il ne s'agit pas de renseignements personnels sensibles, sécurité des renseignements et destruction ou anonymisation lorsque la fin poursuivie est accomplie.[214]

Ainsi, ces interprétations et directives viennent définir le cadre applicable en matière de PCL sur lequel s'aligne l'industrie, en ayant pour but de préciser la portée et l'application de la LPRPDE. Elles influencent également les entreprises du secteur privé et les organismes d'autoréglementation d'industrie dans l'élaboration de leurs propres politiques et meilleures pratiques.

À travers ses lignes directrices et positions de principes, mais également ses recommandations quant à la modernisation de la LPRPDE, il se dégage une approche qu'il est raisonnable de qualifier « de nuancée » dans la mesure où le CPVP reconnaît toute l'importance de protéger la vie privée et les renseignements personnels, tout en reconnaissant l'utilité de la publicité en ligne et en

---

[210] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, décembre 2011, révisé le 13 août 2021, en ligne : <https://www.priv.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 1er mars 2023)

[211] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, *op. cit.*, note 11

[212] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices pour l'obtention d'un consentement valable*, mai 2018, révisé le 13 août 2021, 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 1er mars 2023)

[213] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Section *Enquête visant les entreprises*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/?q%5B0%5D=28&Page=1> (consulté le 1er mars 2023)

[214] Infra, parties II et III.

adoptant un ton neutre lorsqu'il fait état des préoccupations et des pratiques dont lui a fait part l'industrie[215]. Un exemple de cette approche de compromis est sa position concernant la validité possible d'un consentement négatif (*opt-out*) dans un contexte de PCL lorsque certaines balises ont été respectées. J'y reviendrai à la partie III[216].

Par ailleurs, soulignons que le CPVP est très actif en termes d'éducation et d'information, avec ses nombreuses publications incluant des guides, et de services d'accompagnement aux entreprises, avec son nouveau programme de collaboration avec la Direction de services-conseils à l'entreprise et les entreprises qui en font la demande[217].

Commission d'accès à l'information

La CAI, quant à elle, manifeste une approche plus stricte et alignée avec les valeurs pro-vie privée de l'Europe. En effet, dans son guide portant sur le profilage et la publicité ciblée publié en 2013[218], elle s'adressait davantage aux consommateurs qu'aux entreprises en donnant des explications générales sur le profilage et le ciblage et exposait les enjeux en lien avec cette pratique. Par la suite, dans son rapport quinquennal de 2016, elle dénonçait l'érosion de la notion de vie privée et de sa composante informationnelle qu'est la protection des renseignements personnels[219], et recommandait au législateur québécois de moderniser ses lois en matière de protection des renseignements personnels dans le but de resserrer le cadre juridique applicable aux secteurs public et privé « compte tenu de l'informatisation des secteurs public et privé, de l'omniprésence de nouveaux modèles d'affaires et de communication, du fait d'Internet et des réseaux sociaux ou encore de la surveillance accrue des États ».[220] Un tel resserrement était assurément nécessaire, mais il est raisonnable de croire que les interprétations et les recommandations qu'émettra la CAI seront probablement teintées de cette position alignée sur

---

[215] Par exemple, dans COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne, op. cit.,* note 11.
[216] Infra, 6.2.1.1.
[217] Voir : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/services-conseils-entreprises/
[218] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, octobre 2013, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FI_profilage.pdf > (consulté le 30 janvier 2023)
[219] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rétablir l'équilibre, Rapport quinquennal 2016*, septembre 2016, p. 73, en ligne : < https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf > (consulté le 3 mars 2023), faisant référence à l'arrêt *R.* c. *Dyment*, [1988] 2 R.C.S. 417.
[220] *Id*.

la vision européenne. Un exemple est l'interprétation récemment publiée par la CAI de l'article 8.1 de la Loi 25. En effet, alors qu'un flou persiste dans la Loi 25 concernant la validité d'un consentement tacite en matière de PCL, la CAI est venue préciser dans ses explications sur 8.1 qu'un consentement exprès devra avoir été obtenu pour activer les fonctions de profilage et de ciblage. Je développerai sur cet aspect dans la partie III[221].

Par ailleurs, soulignons que les lignes directrices contenues dans ce guide de la CAI demeurent générales et

> « n'offre[nt] pas d'informations spécifiques sur la façon de réglementer l'utilisation des témoins de connexion ou autres technologies similaires, et vise[nt] davantage à informer le public sur le marketing direct et la publicité ciblée. »[222]

Ce guide est toujours en cours de révision et la nouvelle version devant inclure les mises à jour nécessaires en lien avec la Loi 25 n'est toujours pas publiée, bien que la phase 1 de la loi soit entrée en vigueur. Toutefois, l'information générale et les interprétations sommaires concernant les dispositions de la Loi 25 sont publiées au fur et à mesure de leur approbation par la CAI dans les différentes sections de l'Espace évolutif.

Espérons qu'une plus grande ouverture à prendre en considération les connaissances, la réalité, voire certaines des préoccupations de l'industrie, puisse s'observer dans les années à venir, principalement le besoin d'une plus grande clarté et prévisibilité des normes applicables, et idéalement un espace de concertation pour proposer des recommandations visant à préciser les dispositions problématiques de la loi, comme le proposent Gautrais et Laville[223]. L'approche participative mise de l'avant par ces deux auteurs serait un exercice intéressant et potentiellement mutuellement bénéfique dans la mesure où « les recommandations reflète[raient] un certain degré d'expertise et de consensus parmi les acteurs participants au

[221] Infra, 6.2.1.2.
[222] Caroline JONNAERT et LESAGE-BIGRAS, « Cookies et vie privée : ce que toute organisation devrait savoir », *op. cit.,* note 15.
[223] Vincent GAUTRAIS et Henry LAVILLE, « Pour une gouvernance participative des données personnelles au Québec », *op. cit*, note 133, p. 14.

projet »[224] et donc susceptible d'augmenter l'effectivité de la loi et l'atteinte des objectifs qu'elle dessert.

2.3 Pluralité et rôle des normes informelles au Canada

Une pluralité de normes informelles importantes trouve également application au Canada et au Québec, dont les normes émanant des différents programmes d'autoréglementation de l'industrie, reconnues par l'industrie publicitaire au Canada et au Québec.

2.3.1. Programmes d'autoréglementation de l'industrie spécifiques à la publicité

S'ajoutent à cette liste les principes mis de l'avant par les organismes d'autoréglementation d'industrie.

Il s'agit d'initiatives d'autoréglementation de l'industrie canadienne des communications et du marketing afin de se doter de paramètres concrets et de meilleures pratiques notamment dans le but de se conformer aux différents lois et règlements en vigueur dans le secteur, principalement Loi sur la concurrence et la LPRPDE. Les plus importantes sont le Code canadien des Normes canadiennes de la publicité[225], le programme d'autoréglementation Choix de pub et *Political Ad*[226] et les lignes directrices sur la divulgation en matière de marketing d'influence[227].

Le Code canadien des Normes canadiennes de la publicité a été mis sur pied en 1963 dans le but de « répondre aux besoins des consommateurs et de la société »[228]. Le Code détermine quels sont les critères pour qu'une publicité puisse se qualifier de vraie, intègre et exacte[229] et donc en

---

[224] *Id.*, p. 14.
[225] LES NORMES CANADIENNES DE LA PUBLICITÉ, *Code canadien des normes de la publicité*, (révisé juillet 2019) en ligne : < https://adstandards.ca/fr/code-canadien/code-en-ligne/ > (consulté le 3 mars 2023)
[226] Le programme *Political Ad* ayant été mis sur pied spécialement pour la publicité électorale afin d'accroître la transparence requise à un sain exercice démocratique et alignée avec la Loi électorale du Canada : https://politicalads.ca/
[227] LES NORMES CANADIENNES DE LA PUBLICITÉ, COMITÉ DIRECTEUR SUR LE MARKETING D'INFLUENCE, *Lignes directrices sur la divulgation*, révisé automne 2020, en ligne : <https://adstandards.ca/wp-content/uploads/Ad-Standards-Influencer-Marketing-Steering-Committee-Disclosure-Guidelines_FALL2020_FR.pdf > (consulté le 3 mars 2023)
[228] https://adstandards.ca/fr/code-canadien/
[229] https://adstandards.ca/fr/code-canadien/

respect des principes énoncés par la Loi sur la concurrence du Canada. Il est administré par les Normes de la publicité, organisme chargé de préapprouver les publicités et du traitement des plaintes conformément aux principes du Code[230]. Par ailleurs, cet organisme sans but lucratif offre aux annonceurs une procédure alternative de règlement de différends s'apparentant à l'arbitrage permettant aux parties de faire trancher de manière confidentielle une situation litigieuse par un comité d'experts de l'industrie.[231]

Le programme d'autoréglementation Choix de Pub (*Ad Choices*) quant à lui est une initiative de l'Alliance de la publicité numérique du Canada (DAAC), spécifiquement conçu pour encadrer la PCL, et regroupe les principales associations de l'industrie[232]. Ce programme est dans son essence similaire à ceux en place aux États-Unis (DAA), en Union européenne (EDAA) et en Argentine (APDA)[233], mais est adapté aux particularités canadiennes. Il promeut les pratiques de publicité responsable, plus particulièrement via les principes directeurs de responsabilité, de transparence et de contrôle. Il offre aux entreprises participantes un outil permettant d'opérationnaliser une partie de leurs obligations légales, c'est-à-dire celle de divulgation et de permettre aux consommateurs de retirer leur consentement. L'outil en question prend la forme d'un logo notifiant le consommateur lorsqu'il y a collecte et/ou utilisation de renseignements personnels à des fins de PCL, lui permet de voir quelles sont les entreprises impliquées et lui offre la possibilité de retirer son consentement à recevoir de la PCL émanant des entreprises participantes au programme. De manière plus détaillée, les principales obligations qui incombent aux entreprises participant au programme sont[234] :

- Faire en sorte que les individus soient avisés, d'une manière claire, compréhensible et évidente, et non cachée dans une politique de protection de confidentialité ou de protection des renseignements personnels;

[230] LES NORMES CANADIENNES DE LA PUBLICITÉ, « Les plaintes », en ligne : < https://adstandards.ca/fr/plaintes/ > (consulté le 3 mars 2023)
[231] LES NORMES CANADIENNES DE LA PUBLICITÉ, « Procédure en matière de différends publicitaires », en ligne : <https://adstandards.ca/fr/plaintes/differends-publicitaires/ > (consulté le 3 mars 2023)
[232] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « Au sujet de la DAAC », en ligne : <https://youradchoices.ca/fr/au-sujet > (consulté le 3 mars 2023)
[233] ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « AdChoices in Canada », Webinaire, 18 mars 2021
[234] *Id.*

- Les organisations participantes doivent être transparentes et communiquer avec les usagers;
- Les usagers doivent être informés avant ou au moment de la collecte de données. L'information sur toutes les parties impliquées doit être disponible;
- Les individus doivent facilement pouvoir retirer leur consentement;
- Le retrait de consentement est immédiat et permanent;
- L'information collectée est limitée à des renseignements personnels non sensibles;
- Les renseignements personnels sont détruits dès que possible ou désidentifiés.

Le programme comprend également un système de traitement des plaintes qui permet à un consommateur de signaler toute infraction aux principes du programme auprès des Normes de la publicité qui enquêtera ensuite et indiquera les corrections à apporter à ses pratiques le cas échéant.

Ainsi, cette culture d'autoréglementation dans une industrie fortement règlementée permet de développer, mettre en place et moderniser rapidement des outils d'opérationnalisation et des meilleures pratiques qui peuvent aller au-delà du cadre législatif en vigueur, de manière susceptible d'être mieux adaptée à la réalité des organisations qui s'engagent à les appliquer.

En outre, ces programmes ont recours aux modes alternatifs de résolution de conflit et, se faisant, offrent une alternative aux plaintes déposées auprès des organismes de contrôle et aux recours devant les tribunaux, plus coûteux et plus longs. En outre, ces programmes d'autoréglementation d'industrie jouent aussi un rôle de vigie des changements technologiques et réglementaires, de représentants dans les discussions avec les différentes instances et intervenants, de vulgarisateurs et de contributeurs à la littéracie digitale, d'organisateurs de forums d'échanges, en plus d'être créateurs de normes.

Comme le soulignait Guido Scorza de l'Autorité italienne de la protection des données en 2021, il a un besoin de réglementation et d'autoréglementation, les deux étant complémentaires.[235]

[235] Allocution de Guido SCORZA, Garante per la protezione dei dati personali (Autorité italienne de la protection des données), lors du Sommet international de novembre 2021 de la *European Interactive Digital Adversiting Alliance* (EDAA), en ligne : < https://edaa.eu/2021-edaa-summit-talks-up-the-importance-of-transparency-and-trust-in-digital-advertising/ >

Selon lui, l'autoréglementation devient complémentaire au droit positif, de par sa capacité à s'adapter plus rapidement aux évolutions technologiques que le droit étatique, et permettant ainsi au droit étatique de jouer son rôle de mettre les bases, d'énoncer les grands principes et de garantir une application uniforme. Parlant plus spécifiquement de la protection de la vie privée, il constatait que l'application d'un régime *one-stop-shop*, c'est-à-dire le système unifié sous le RGPD, prenait effectivement plus de temps à se modifier.

Ainsi, ces normes issues de l'industrie sont certainement complémentaires, mais il faut prendre soin d'identifier et de tenir compte de leurs limites. Comme résument et concluent Gautrais et Laville :

> « Le recours à la normativité informelle a donc deux facettes. On attribue d'abord aux normes informelles certaines vertus ce qui explique leur apparition dans la loi : elles sont dotées d'une grande efficacité et flexibilité, en plus d'être le fruit d'une certaine expertise. Le caractère privé de cette normativité l'empêche, toutefois, de satisfaire à certains intérêts plus vastes. En effet, l'intérêt public, la participation des tiers, l'ouverture démocratique, la transparence et le contrôle de ces normes ne sont garantis. Le PL64 établit une corégulation dans le PL64 par le biais de la délégation législative, ce qui peut s'interpréter comme une tentative de palier aux défauts de la normativité informelle, en permettant aux autorités publiques d'avoir un certain contrôle sur ce processus. **Or, le processus semble inachevé : la loi n'explicite en rien la manière dont cette co-régulation doit s'opérer concrètement**. Notre thèse est ici de défendre l'idée selon laquelle un renforcement des exigences procédurales en incluant un processus de participation dans l'élaboration de cette normativité informelle permettrait de renforcer la légitimité procédurale de cette dernière. En somme, c'est une affaire de mesure où il faut insérer dans la normativité les considérations publiques sans perdre les caractéristiques qui font son attrait. »[236]

2.4 Complexité inhérente à la structuration des normes

Dans la continuité de cette réflexion, un sujet étroitement lié à celui du rôle des normes informelles privées est celui de la structuration des normes formelles. En effet, cette structure qualifiée de « mille-feuille normatif » par Gautrais et Laville[237], ajoute une couche de complexité

[236] Vincent GAUTRAIS et Henry LAVILLE, « Pour une gouvernance participative des données personnelles au Québec », *op. cit.*, note 133, p. 13 et 14.
[237] *Id.*, p. 4.

au cadre juridique applicable à la pratique de la PCL et à la PRP de manière générale. Cette structure se caractérise par l'introduction de références croisées dans lesquelles les lois en matière de vie privée réfèrent à des règlements, existant ou à venir, et/ou à des meilleures pratiques, et/ou à normes techniques (telle la norme ISO), et/ou à des documents internes (politiques d'entreprise, registre, guides, directives).

Gautrais et Laville, se penchant sur le Projet de loi 64 plus spécifiquement, y ont constaté la présence marquée de délégations normatives et les ont classés en deux catégories. Les premières sont les délégations à des normes communautaires, qui peuvent prendre la forme de référence aux meilleures pratiques d'un secteur cible, par exemple pour anonymiser les renseignements personnels et pour documenter le traitement des renseignements personnels[238]. Ces délégations à des normes communautaires peuvent aussi prendre la forme de renvois à des directives ou à des guides que les entreprises doivent mettre en place pour rencontrer leurs obligations légales[239]. Dans ces deux cas, les auteurs relèvent que

> « […] le législateur recherche [ainsi] l'effectivité de la règle de droit, en déléguant la production de certaines normes aux groupes cibles [c'est-à-dire les secteurs cibles ou les entreprises cibles selon le cas], qui doivent alors les élaborer en respectant les objectifs posés par la loi et les rendre publiques. »[240]

Ces auteurs ajoutent :

> « En procédant ainsi, le législateur vise deux choses : d'abord, il pense que dans un domaine aussi complexe que celui des technologies de l'information, l'usage de normes confectionnées et connues de ces secteurs d'activité permettra d'orienter plus facilement le comportement des individus que l'approche législative classique ; ensuite, et surtout, il invite les secteurs ciblés à élaborer des normes qui viennent prendre en compte les exigences législatives à la protection des renseignements personnels. Cette approche a été mise en évidence lors de l'identification du phénomène de la *Lex informatica*, de la *Lex electronica*, où l'on a cherché à comprendre de quoi était constitué l'écosystème normatif des technologies de l'information. »[241] [Références omises]

[238] *Id.*, p. 5, en faisant référence aux articles 28, 119 et 103 du Projet de loi 64.
[239] *Id.*, p. 6, en faisant référence aux articles 15 et 103 du Projet de loi 64.
[240] *Id.*, p. 6, en faisant référence aux articles 15 et 103 du Projet de loi 64 à titre d'exemples.
[241] *Id.*, p. 5 et 6.

Les secondes sont les délégations à des normes étatiques[242] où le législateur a plutôt choisi d'enjoindre le gouvernement à prendre des mesures qui compléteront sa volonté -comme le règlement devant déterminer les critères et modalités d'anonymisation des données[243]-, ou bien de lui accorder la faculté de préciser la législation[244].

En conséquence, les entreprises et organisations assujetties à de telles lois contenant de telles délégations normatives, comme la Loi 25, doivent tenir compte de toutes ces précisions externes à la loi. De surcroit, dans un contexte de réforme législative comme celle de la Loi 25, elles doivent modifier leurs pratiques et prendre des décisions importantes, malgré l'attente de précisions règlementaires et l'incertitude par rapport à la conformité des normes développées par leur industrie ou à venir.

2.5 Circulation transfrontalière des données : élément extraterritorial ajoutant à la complexité

Une caractéristique importante de la PCL est le fait qu'elle implique des flux de données complexes et transférés hors de ses frontières d'origine. Ainsi, les consommateurs peuvent être situés hors des frontières québécoises et canadiennes (par exemple pour dans le cadre d'une campagne faisant la promotion du Canada comme destination touristique auprès des Européens). De plus, de nombreux outils, solutions et partenaires marketing fréquemment utilisés par les entreprises d'ici sont américains (ex : solution infonuagique, *Google Analytics*, messagerie courriel, réseaux sociaux, etc.). Ainsi, un renseignement personnel peut traverser plusieurs frontières dans le cadre de son traitement et cycle de vie.

Ainsi, s'ajoute aux éléments de complexité énoncés ci-dessus, le fait que le secteur privé canadien et québécois doit aussi prendre en considération les lois étrangères qui trouvent application lorsqu'il y a traitement de renseignements personnels de personnes étant situées en territoire étranger.

---

[242] *Id*., p. 4, 5 et 6.

[243] *Id*., p. 6, en faisant référence aux articles 119 et 15 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. 1993, c. P-39.1.

[244] *Id*., p. 6.

Je résumerai ci-dessous la question de l'application du cadre européen, étant le plus important cadre étranger à prendre en considération d'une perspective nord-américaine.

Concernant les transferts transfrontaliers de renseignements personnels de Canadiens et de Québécois hors du Canada, je propose d'approfondir cet élément de complexité sous la partie II du présent mémoire. J'y traiterai des obligations incombant aux entreprises, ainsi que de la zone grise concernant le champ d'application territorial de la LPRPRE ou de la Loi 25 à ces transferts.

2.5.1. Application de la réglementation de l'UE

RGPD

La récente vague de resserrement des règles en matière de PRP a été initiée en mai 2018 par l'UE avec l'entrée en application du RGPD. L'UE s'est alors positionnée comme l'une des juridictions les plus strictes à l'égard du secteur privé en matière de PRP. Cette réforme poursuivait trois grands objectifs, soit de : « 1. Renforcer les droits de la personne, notamment par la création d'un droit à la portabilité des données personnelles et de leurs dispositions aux personnes mineures; 2. Responsabiliser les acteurs en traitant des données (responsables de traitement et sous-traitants); 3. Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées. »[245]

Son impact fût grand tant pour les organisations de l'UE que des autres juridictions, incluant celles du Canada et du Québec, puisque le champ d'application territorial du RGPD s'étend hors de ses frontières, du moment qu'il s'agit de données à caractère personnel de personnes physiques situées sur le territoire de l'UE[246].

[245] CNIL, *Règlement européen sur la protection des données : ce qui change pour les professionnels*, 10 juillet 2018, en ligne : <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels > (consulté le 22 janvier 2023)

[246] RGPD, art. 3(1) et (2), en ligne : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1 > (consulté le 22 janvier 2023)

En effet, ce cadre règlementaire renforci s'applique à tous les responsables de traitement et leurs sous-traitants qui ne sont pas établis dans l'UE, mais qui procèdent au traitement[247] des données à caractère personnel relatives à des personnes qui se trouvent sur le territoire de l'UE « lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. »[248] La pratique de la PCL est donc assujettie à ces dispositions dans ce contexte.

Ainsi, le RGPD prévoit que « le transfert de données hors de l'Union européenne (UE) et de l'Espace économique européen (EEE) est possible, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques. »[249]

Règlement ePrivacy sur les fichiers témoins et les métadonnées

Par ailleurs, le RGPD sera bientôt complété par le Règlement *ePrivacy*, remplaçant la directive *ePrivacy* de 2002, plus spécifique aux cookies et aux métadonnées. La date d'entrée en application du Règlement *ePrivacy* a encore été repoussée[250], principalement en raison d'une divergence d'opinions importante qui persiste entre le Conseil de l'Union européenne et les éditeurs de sites -dont le modèle d'affaires repose sur le consentement des utilisateurs- concernant l'encadrement juridique du *Cookie Wall*.[251] Le concept de *Cookie Wall* est le fait

[247] RGPD, art. 4(2) : Définition de « traitement » : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction », en ligne : < https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1 > (consulté le 22 janvier 2023)

[248] RGPD, art. 3(2), en ligne : < https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1 > (consulté le 22 janvier 2023)

[249] CNIL, *Transférer des données hors de l'UE*, en ligne : <https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue > (consulté le 16 août 2022).
Voir les règles d'entreprise contraignantes, Infra, p. 84.

[250] Julie PACI, « Tout savoir sur la nouvelle directive ePrivacy pour s'y préparer au mieux », *Mailjet* (6 novembre 2022) en ligne : <https://www.mailjet.com/fr/blog/bonnes-pratiques-emailing/directive-eprivacy/#chapter-2> (consulté le 7 janvier 2023)

[251] GESTE, « EPrivacy : La phase de trilogue peut enfin commencer ! » (26 février 2022) en ligne : <https://geste.fr/eprivacy-la-phase-de-trilogue-peut-enfin-commencer/> (consulté le 7 janvier 2023)

d'offrir une option de navigation aux internautes qui acceptent les cookies qui est différente de ou des option(s) de navigation, payante ou autre, offertes aux internautes refusant ces *cookies*.[252]

Règlement européen sur les services numériques (DSA)

Soulignons également un important et nécessaire règlement qui visera les GAFAM directement. Ainsi, sera applicable dès février 2024, le Règlement européen sur les services numériques (DSA).[253] Ce règlement est applicable dès 2023 pour les très grandes plateformes en ligne et les très grands moteurs de recherche c'est-à-dire utilisés par plus de 45 millions d'Européens par mois comme les GAFAM.[254] Il vise les fournisseurs d'accès internet, les services d'informatique en nuage, les différentes plateformes en ligne incluant les réseaux sociaux, et les très grandes plateformes en ligne et les très grands moteurs de recherche, et vise essentiellement la lutte contre les contenus illicites, la croissance de la transparence en ligne, ainsi que l'atténuation des risques et réponse aux crises.[255]

Ce règlement vient contribuer à assainir la pratique de la PCL puisqu'il renforce plusieurs exigences clés notamment en rehaussant le niveau de transparence requis. Dès lors, les plateformes visées par le règlement devront

> « expliquer le fonctionnement des algorithmes qu'elles utilisent pour recommander certains contenus publicitaires en fonction du profil des utilisateurs. Les très grandes plateformes et les très grands moteurs de recherche auront l'obligation de proposer un système de recommandation de contenus non fondé sur le profilage. Elles devront en outre mettre à disposition du public un registre des publicités contenant diverses informations (qui a parrainé l'annonce, comment et pourquoi elle cible tels individus...). [De plus,] [l]a publicité ciblée pour les mineurs sera interdite pour toutes les plateformes, de même que la publicité basée sur des données sensibles comme la religion ou l'orientation sexuelle (sauf consentement explicite). »[256] [Mes soulignements]

[252] *Id.* ; Infra, 6.2.3.
[253] VIE PUBLIQUE, « Le règlement européen sur les services numériques (DSA) vise une responsabilisation des plateformes » (dernière modification : 26 octobre 2022), par. 1 et 2, en ligne : <https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act > (consulté le 22 janvier 2023)
[254] *Id.*, par. 6.
[255] *Id.*
[256] *Id.*, par. 14 et 15.

2.5.2. Précarité du statut d'adéquation partielle du Canada

Le Canada bénéficie actuellement d'une décision d'adéquation partielle de la Commission européenne, adoptée en 2001[257], ce qui signifie que le Canada est reconnu comme adéquat, mais pour certains traitements spécifiques seulement, c'est-à-dire ceux réalisés dans le cadre d'activités commerciales couverts par la LPRPDE.[258] En conséquence, ces traitements ne nécessitent pas d'encadrement spécifique, contrairement aux autres transferts de données personnelles qui nécessitent un encadrement via des outils de transfert[259], tels les règles d'entreprise contraignantes (BCR), les clauses contractuelles types (CCT) de la Commission européenne, les arrangements administratifs et les dérogations pour des situations particulières.[260]

Les modifications proposées par le Projet de loi C-27 seront déterminantes pour le maintien de ce statut. En effet, selon Glover et Hantho :

> « Sauf [si le Canada] modifie sa législation fédérale sur la protection des renseignements personnels avant le prochain examen (qui est effectué tous les quatre ans, le prochain devant commencer en mai 2020), on s'attend généralement à ce que le Canada ne conserve pas son statut d'adéquation actuel. En l'absence de décision d'adéquation, une évaluation de l'impact du transfert doit être réalisée (…) »[261]

---

[257] *2002/2/CE: Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques* [notifiée sous le numéro C(2001) 4539], en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32002D0002> (consulté le 25 avril 2023) ;
Daniel G.C. GLOVER et Ella HANTHO, « 2021/2022 Bilan et perspective en Cyber/Données : Modifications prévues aux lois sur la protection de la vie privée au Canada », McCarthy Tétrault (28 février 2022), en ligne : <https://www.mccarthy.ca/fr/references/blogues/techlex/20212022-bilan-et-perspectives-en-cyberdonnees-modifications-prevues-aux-lois-sur-la-protection-de-la-vie-privee-au-canada > (consulté le 6 mars 2023)

[258] CNIL, *La protection des données dans le monde*, en ligne : <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde> (consulté le 16 août 2022)

[259] *Id.*

[260] *Id.*

[261] Daniel G.C. GLOVER et Ella HANTHO, « 2021/2022 Bilan et perspective en Cyber/Données : Modifications prévues aux lois sur la protection de la vie privée au Canada », *op. cit*., note 257, par. 10.

2.5.3. Complexité liée aux transferts subséquents vers les États-Unis

De plus, les entreprises canadiennes doivent porter attention aux transferts subséquents de ces données d'Européens vers les États-Unis. En effet, ce pays n'est plus un pays reconnu comme adéquat depuis que son statut d'adéquation a été annulé en juillet 2020 par la Cour de justice de l'Union européenne dans l'arrêt *Schrems II*[262].

Cet arrêt marquant est venu invalider le régime de transferts de données entre l'Union européenne et les États-Unis dans le cadre du *Privacy Shield*[263], en raison de l'absence de limitation adéquate quant à l'accès par les autorités américaines aux données personnelles en vertu des programmes de surveillance, et de l'absence de recours suffisants et effectifs pour les individus concernés. Voici les principaux passages résumant les enjeux en cause et le raisonnement de la Cour :

> « (…) cette juridiction nourrit des doutes sur le point de savoir si le droit des États-Unis assure effectivement le niveau de protection adéquat requis à l'article 45 du RGPD, lu à la lumière des droits fondamentaux garantis aux articles 7, 8 et 47 de la Charte [des droits fondamentaux de l'Union européenne]. En particulier, ladite juridiction considère que le droit de ce pays tiers ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa réglementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences. À ce dernier égard, elle ajoute que l'instauration du médiateur du bouclier de protection ne peut, selon elle, remédier à ces lacunes dès lors que ce médiateur ne saurait être assimilé à un tribunal, au sens de l'article 47 de la Charte. »[264]
>
> « La Cour a déjà jugé que la communication de données à caractère personnel à un tiers, tel qu'une autorité publique, constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. Il en va de même de la conservation de données à caractère personnel ainsi que de l'accès auxdites données en vue de leur utilisation par les autorités publiques, indépendamment du point de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible, ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence (…) »[265]

---

[262] *Data Protection Commissioner* c. *Facebook Ireland Ltd et Maximillian Schrems*, Cour de justice de l'Union européenne, 16 juillet 2020, en ligne : <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=4594815>

[263] CNIL, *Invalidation du Privacy shield : les suites de l'arrêt de la CJUE*, en ligne : <https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue > (consulté le 16 août 2022)

[264] *Data Protection Commissioner* c. *Facebook Ireland Ltd et Maximillian Schrems*, *op. cit*., note 266, par. 168.

[265] *Id.,* par. 171.

> « En l'occurrence, la constatation opérée par la Commission dans la décision BPD selon laquelle les États-Unis assurent un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par le RGPD, lu à la lumière des articles 7 et 8 de la Charte, a été remise en cause au motif, notamment, que les ingérences résultant des programmes de surveillance fondés sur l'article 702 du FISA et sur l'E.O. 12333 ne seraient pas soumises à des exigences assurant, dans le respect du principe de proportionnalité, un niveau de protection substantiellement équivalent à celui garanti par l'article 52, paragraphe 1, seconde phrase, de la Charte. »[266]
>
> « Il apparaît ainsi que l'article 702 du FISA ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non-américaines potentiellement visées par ces programmes. Dans ces conditions, (…), cet article n'est pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui garanti par la Charte, telle qu'interprétée par la jurisprudence rappelée aux points 175 et 176 du présent arrêt, selon laquelle une base légale qui permet des ingérences dans les droits fondamentaux doit, pour satisfaire au principe de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné et prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales.»[267]
>
> « Ainsi, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte »[268].
>
> [Références omises, mes soulignements]

De plus, dans cette affaire, la Cour a aussi reconnu que l'obligation de vérifier si le droit positif du pays tiers respecte le niveau et les garanties minimales requises et de prendre les mesures supplémentaires requises incombe tant à l'entreprise qui transfert les données qu'à celle qui les reçoit :

> « (…) en règle générale, les Clauses Contractuelles Types (CCT) peuvent toujours être utilisées pour transférer des données vers un pays tiers (qu'il s'agisse des États-Unis ou d'un autre pays tiers). Cependant, la CJUE a souligné qu'il incombe à l'exportateur et à l'importateur de données d'évaluer en pratique si la législation du pays tiers permet de

[266] *Id.,* par. 178.
[267] *Id.,* par. 180.
[268] *Id.,* par. 187.

> respecter le niveau de protection requis par le droit de l'UE et les garanties fournies par les CCT. Si ce niveau ne peut pas être respecté, les entreprises doivent prévoir des mesures supplémentaires pour garantir un niveau de protection essentiellement équivalent à celui prévu dans l'Espace économique européen, et elles doivent s'assurer que la législation du pays tiers n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité. »[269] [Mes soulignements]

En conséquence, la Commission nationale de l'informatique et des libertés (CNIL) conclut qu'un transfert de données d'Européens vers les États-Unis nécessite plusieurs vérifications et documentation préalables, incluant la recension des transferts de données personnelles liés aux outils numériques de l'organisation, la vérification des outils numériques et des contrats, la complétion d'un outil de suivi des transferts hors de l'Union européenne, et la mise en place d'un plan d'action.[270] Elle recommande donc de mettre en place des règles d'entreprise contraignantes (*Binding Corporate Rules* (BCR)), c'est-à-dire « (…) une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne »[271] et des clauses contractuelles types de la Commission européenne[272].

En somme, dans un contexte de PCL, si des renseignements personnels d'Européens sont transférés vers le Canada, puis retransférés vers des outils ou des tiers-prestataires de services américains, alors ce transfert devrait être fait en conformité avec les exigences de la règlementation européenne.

Notons que le statut d'adéquation n'a pas encore été rétabli, mais que les États-Unis font des démarches actives en ce sens. En effet, ils ont proposé un nouveau cadre juridique à la Commission européenne, le *Executive Order* qui remplacerait le *Privacy Shield*, venant renforcir les garanties concernant la collecte et l'utilisation des données personnelles par les services

---

[269] CNIL, *Les règles d'entreprise contraignantes (BRC)*, en ligne : <https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr > (consulté le 16 août 2022)

[270] CNIL, *Responsable de traitement : comment identifier et traiter des transferts de données hors de UE ?*, 23 juin 2021, en ligne : <https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue > (consulté le 16 août 2022)

[271] CNIL, *Les règles d'entreprise contraignantes (BRC)*, *op. cit.*, note 269.

[272] CNIL*, Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne*, 21 décembre 2022, en ligne : <https://www.cnil.fr/fr/transfert-de-donnees-les-clauses-contractuelles-types-cct-de-la-commission-europeenne> (consulté le 5 mars 2023)

secrets américains[273], dans le but de rétablir une décision d'adéquation auprès de la Commission européenne. En décembre 2022, la Commission a publié un projet de décision dans lequel elle inclut des annexes, et a demandé au *European Data Protection Board* d'émettre son opinion à ce sujet.[274] Dans son avis concernant le projet de décision d'adéquation de la Commission européenne relative à la protection adéquate des données à caractère personnel en vertu du cadre Union européenne-États-Unis sur la protection des données, le Conseil européen de la protection des données reconnait les améliorations significatives qui sont proposées, mais émet plusieurs réserves :

> « The EDPB welcomes substantial improvements such as the introduction of requirements embodying the principles of necessity and proportionality for U.S. intelligence gathering of data and the new redress mechanism for EU data subjects. At the same time, it expresses concerns and requests clarifications on several points. These relate, in particular, to certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism. The EDPB would welcome if not only the entry into force but also the adoption of the decision were conditional upon the adoption of updated policies and procedures to implement Executive Order 14086 by all U.S. intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share its assessment with the EDPB. » [275] [Mon soulignement]

Ce dossier est donc à suivre, en parallèle de celui du Canada, suite à l'adoption du Projet de loi C-27. Je reviendrai plus bas sur la question des transferts hors Québec vers les États-Unis et l'évaluation des facteurs relatifs à la vie privée[276].

---

[273] CNIL, *Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne*, 1er mars 2023, en ligne : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation > (consulté le 12 mars 2023)

[274] EUROPEAN DATA PROTECTION BOARD, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 28 février 2023, par. 1 et 2, en ligne : <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_fr > (consulté le 12 mars 2023)

[275] CNIL, *Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne*, 1er mars 2023, par. 1, en ligne : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation > (consulté le 12 mars 2023)

[276] Infra, 5.4.

PARTIE II – Obligations des entreprises participant à la PCL en vertu des lois québécoise et canadienne fédérale en matière de PRP

Ayant brossé le portrait de la complexité factuelle et juridique de la PCL lors de la première partie de ce mémoire, je propose maintenant de décrire les différentes obligations incombant au secteur privé en comparant la LPRPDE, le Projet de loi C-27 et la Loi 25. J'y intègre une analyse des ambiguïtés problématiques à l'opérationnalisation des obligations incombant aux organisations.

Chapitre 3 - Étape préalable : Identification et qualification des renseignements traités

Attardons-nous d'abord à l'étape préalable et cruciale de classification et de qualification des données, puisque ce sont les données qui se qualifient de renseignements personnels qui sont visées par les lois en matière de PRP.

3.1. Définition de renseignements personnels

3.1.1. Définitions en vertu des lois en matière de PRP : basées sur le caractère identifiable de l'individu

Le concept de renseignement personnel est énoncé de manière large à l'article 2 de la LPRPDE. En effet, est un renseignement personnel : « Tout renseignement concernant un individu identifiable. »[277] Le mot clé ici étant donc le terme « identifiable ». Cette même définition a été

[277] LPRPDE, art. 2(1), définition de « renseignement personnel ».

reprise dans la Partie 1 du Projet de loi C-27[278]. Notons, comme le fait remarquer le CPVP, que la Cour fédérale, dans *Gordon c. Canada (ministre de la Santé),* a aussi conclu qu'

> « un renseignement concerne un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles »[279].

Au niveau québécois, la précédente loi québécoise sur le secteur privé référait également déjà au même principe d'identification en prévoyant que : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »[280]. Par la suite, cette définition a été élargie dans la Loi 25, se lisant maintenant ainsi : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier. »[281] De plus, la loi précise qu'elle

> « s'applique à ces renseignements, que leur conservation soit assurée par l'entreprise ou par un tiers, quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles : écrite, graphique, sonore, visuelle, informatisée ou autres. »[282]

Les sections II et III de la loi (collecte de renseignements personnels et caractère confidentiel des renseignements personnels), ne s'appliquent pas :

- « à un renseignement personnel qui a un caractère public en vertu de la Loi »[283]
- « 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

---

[278] *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, Projet de loi C-27 (1re lecture), 1re session, 44e législature, Partie 1 *Loi sur la protection de la vie privée des consommateurs,* art. 2(1), définition de « renseignement personnel », en ligne : < https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture > (consulté le 16 mars 2023)

[279] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit*., note 11, par. 1 de la question 1 « L'information en question constitue-t-elle des renseignements personnels tels qu'ils sont définis à l'article2 de la LPRPDE? », citant *Gordon* c. *Canada (ministre de la Santé)*, 2008 CF 258

[280] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, <http://canlii.ca/t/6bk26>, art. 2

[281] Loi 25, art. 2.

[282] *Id*., art. 1, par. 2.

[283] *Id.*, art. 1, par. 5.

que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail. »[284] [Mon soulignement]

La définition de renseignement personnel dans le RGPD quant à elle se distingue par sa rédaction plus précise. Elle est encore plus englobante, tout comme sa définition de traitement, faisant d'elle une loi au champ d'application plus large que celui de la LPRPDE[285]. En effet, se dit d'une « donnée à caractère personnel » au sens du RGPD « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».[286] [Mes soulignements]

Ainsi, contrairement à la LPRPDE, au Projet de loi C-27 et à la Loi 25, la protection offerte par le RGPD couvre toutes ces données à caractère personnel, comme les coordonnées d'affaires, sans

[284] *Id.,* art. 1, par. 5 *in fine.*

[285] Le fait que le domaine d'application du projet de RGPD était très large a d'ailleurs été critiqué par le professeur Gautrais : « Nous croyons qu'il importe de ne pas avoir peur de reconnaitre que la vision excessivement large, comme l'OCDE l'a d'ailleurs récemment reconnu, est susceptible de poser problème. En protégeant à outrance, même des données qui ne présentent aucune sensibilité, qui ont parfois un caractère partiellement ou totalement public, on applique donc un corpus de règles à des informations qui ne mériteraient peut-être pas pareille protection; on est aussi susceptible de limiter les prérogatives prévues dans d'autres domaines du droit, pour rien. Il est aussi loisible de se demander si cette protection mal ciblée ne fait pas oublier les atteintes véritables qui elles méritent assurément d'être contrôlées, réparées et condamnées. Si nous prenons l'exemple précédemment cité des sites de notation de professeurs, le couplage d'un nom et d'une profession (Vincent Gautrais + professeur) rentre sans aucun doute dans une telle définition de renseignement personnel. Sous réserve de lois qui ont pris le soin de spécifiquement extraire de leur domaine d'application certaines informations publiques presque par essence, il ne fait doute qu'une telle information soit assujettie à la loi, et ce, en dépit de son caractère inoffensif. Est-il donc si nécessaire d'appliquer un corpus de règles au complet à des informations si anodines ? ». Dans Vincent GAUTRAIS, « Proposition de Règlement général sur la protection des données : un regard d'ailleurs », dans Nathalie MARTIAL-BRAZ (dir.), *La proposition de règlement européen relatif aux données à caractère personnel*, Collection Trans Europe Experts, Société de législation comparée, Paris, 2014, pp. 464-493, par. 27, en ligne : <https://www.gautrais.com/publications/proposition-de-reglement-general-sur-la-protection-des-donnees-un-regard-dailleurs/ https://www.cyberjustice.ca/publications/proposition-de-reglement-general-sur-la-protection-des-donnees-un-regard-dailleurs/>

[286] RGPD, art. 4(1).

égard à l'existence ou non d'un risque de dommage, de préjudice, comme le remarquait le professeur Gautrais à l'époque de la proposition du RGPD[287].

Somme toute, ces lois adoptent une définition très large et englobante. Ce caractère large avait d'ailleurs été critiqué en 2012 par Me Gratton :

> « Based on the definition of personal information, information is only covered by [data protection laws] if the information in question can "identify" an individual, which is the usual metric for establishing appropriate limits within data protection regimes. I maintain that this metric can be over-inclusive, under inclusive, and that there are various uncertainties surrounding this notion of "identifiable individual". But I believe that this metric remains relevant when evaluating the type of harm that may take place at the "disclosure" level, although the fact that the information is "identifiable" is only one of the three criteria that are relevant when evaluating the subjective kind of harm that may take place at this level. »[288]

3.1.2. Interprétation des autorités de contrôle et décision récente concernant *Google* : définition large axée sur la finalité

Le CPVP considère qu'est un renseignement personnel tout renseignement qui, seul ou jumelé à d'autres données, permet d'identifier un individu.[289] Selon lui, il s'agit en général de renseignements qui portent sur la race, la nationalité, l'origine ethnique, la religion, l'âge, l'état civil, les antécédents médicaux, scolaires ou professionnels, les transactions financières, l'ADN, les numéros d'identification (tels le numéro d'assurance sociale et le numéro de permis de conduire), et les points de vue et opinions d'une personne.[290] *À contrario*, il reconnait que ne sont généralement pas considérés comme des renseignements personnels :

---

[287] Vincent GAUTRAIS, « Proposition de Règlement général sur la protection des données : un regard d'ailleurs », *op. cit.*, note 285, par. 28.
[288] Éloïse GRATTON, *Redefining personal information in the context of the Internet*, Thèse de doctorat, Montréal, Faculté de droit, Université de Montréal, 2012, p. 294-295, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/19676/Gratton_Eloise_2012_these.pdf?sequence=4&isAllowed=y>
[289] CPVP, *Aperçu des lois sur la protection des renseignements personnels au Canada*, *op. cit.*, note 193, par. 4.
[290] *Id.*, par. 5.

- « Des renseignements qui ne concernent pas un individu, soit parce que le lien avec cette personne est trop vague ou trop distant (p. ex. un code postal s'applique à un vaste secteur où se trouve de nombreuses résidences).
- Des renseignements sur une organisation notamment une entreprise.
- Des renseignements anonymisés, pourvu qu'il ne soit pas possible de les relier à une personne identifiable.
- Certains renseignements sur des fonctionnaires comme leur nom, le titre du poste qu'ils occupent.
- Les coordonnées d'affaires d'une personne qu'une organisation recueille, utilise ou communique uniquement pour entrer en contact avec elle dans le cadre de son emploi, de son entreprise ou de sa profession.
- L'information gouvernementale. À l'occasion, les gens communiquent avec nous pour obtenir des renseignements gouvernementaux. Il ne s'agit pas de renseignements personnels. Pour obtenir des renseignements du gouvernement, veuillez communiquer avec le commissaire à l'information du Canada. »[291]

Concernant les renseignements traités spécifiquement dans un contexte de PCL[292], le CPVP s'est positionné en les qualifiant de renseignements personnels, en s'appuyant sur une vision qu'il qualifie de large et contextuelle[293]. Ainsi, il s'appuie sur le but poursuivi et les résultats possibles pour justifier sa conclusion :

> « Par conséquent, dans le contexte de la PCL, compte tenu du fait que le but derrière la collecte de renseignements est de créer des profils de personnes qui, à leur tour, permettent d'offrir des publicités ciblées; compte tenu des moyens puissants disponibles pour recueillir et analyser les bits de données disparates et la possibilité sérieuse d'identifier les personnes concernées, et compte tenu du caractère potentiellement très personnalisé de la publicité en résultant, on peut raisonnablement penser que les renseignements en cause dans la publicité comportementale touchent à la protection de renseignements personnels et, dans les circonstances, ils doivent être considérés comme " identifiables ". Même si une telle évaluation devrait être effectuée au cas par cas, il n'est

[291] *Id.,* par. 6.

[292] La DAAC fait une liste des renseignements souvent utilisés en PCL : « les informations de géolocalisation, incluant des données GPS, les identifiants d'appareils (ex : adresse IP, adresse MAC), les données de parcours de navigation, historique de navigation, signets, etc., les données générées par l'utilisateur de réseaux sociaux (ex : commentaires, évaluations, mentions J'aime, mentions Je n'aime pas, Fil de nouvelles Twitter, interactions avec le service aux consommateurs), la combinaison de plusieurs informations disparates permettant de construire un profil détaillé ». ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, Webinaire « AdChoices in Canada », 18 mars 2021 (traduction libre tirée de l'anglais)

[293] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit.,* note 11, par. 7 et 8.

> pas déraisonnable de considérer cette information comme des " renseignements personnels " de prime abord. » [294] [Mes soulignements]

De plus, le CPVP ajoute une précision importante dans cette position, à l'effet que « [l]es renseignements découlant du suivi servent à modifier l'expérience de navigation de l'utilisateur. Même si les données sont rassemblées par groupes d'utilisateurs à des fins de ciblage, l'appartenance à un groupe se fonde sur des renseignements sur les comportements individuels. »[295]

Ainsi, du moment où divers renseignements sont utilisés à des fins de livraison de PCL, ils sont considérés par le CPVP comme des renseignements personnels protégés par la LPRPDE. Cette interprétation contextuelle est également adoptée par la CAI, qui, dans son document sur le profilage et la publicité ciblée (2013), considère d'emblée que les renseignements traités à des fins de PCL sont des renseignements personnels.[296]

La Cour supérieure dans la décision de 2022 autorisant l'action collective d'Option Consommateurs contre *Google*, adopte également une telle approche contextuelle et large en tenant compte des fins pour lesquelles les renseignements ont été collectés :

> « Le but ouvertement reconnu de Google est ainsi d'offrir **un contenu personnalisé** à ses utilisateurs, ce qui inclut un contenu publicitaire personnalisé. Or, logiquement, selon le Tribunal, il va de soi que Google ne peut pas offrir ce contenu personnalisé si elle est incapable d'identifier et de reconnaitre ses utilisateurs. C'est ce qu'elle fait, notamment par l'utilisation d'« identifiants uniques » [termes utilisés dans sa Politique de confidentialité de Google], qui permettent de relier chacune des informations listées ci-haut autour d'un pôle unique. »[297]

Elle refuse la définition qu'elle qualifie de « très étroite » de *Google*[298] qui considère plutôt, tel que le reflète sa Politique de confidentialité, que des renseignements ne sont pas des

---

[294] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit.,* note 11, par. 7 de la question « 1. L'information en question constitue-t-elle des renseignements personnels tels qu'ils sont définis à l'article 2 de la LPRPDE ? »
[295] *Id*., note de bas de page 10.
[296] CAI, *Le profilage et la publicité ciblée*, *op. cit.,* note 218.
[297] *Option Consommateurs* c. *Google*, *op. cit*., note 196, par. 38.
[298] *Id.* par. 40.

renseignements personnels « (…) s'ils ne permettent plus d'identifier un utilisateur ou de faire référence à celui-ci de manière personnelle. »[299] [Mon soulignement]. Ainsi, comme *Google* fonctionne en regroupant les individus dans des groupes d'intérêts, et que ce sont ces groupes d'intérêts qui sont ciblés à des fins de PCL, *Google* soutient plutôt que les renseignements des individus qui s'y retrouvent ne sont pas des renseignements personnels.

Il faudra donc attendre la décision au mérite afin de savoir si la Cour adhèrera à l'interprétation large et contextuelle adoptée jusqu'à ce jour par les autorités de contrôle, ou si elle adoptera la logique mise de l'avant par *Google*.

Soulignons qu'une telle approche de qualification des renseignements personnels axée sur la finalité, mais tenant peu compte des risques de préjudice a été critiquée par Me Gratton dans sa thèse de 2012 :

> « My contribution in providing guidance on this notion of "identifiability" in the context of the Internet and related technologies is two-fold. First, the notion of "identifiable individual" should be interpreted differently depending on the purpose behind the data handling activity regulated by the [data privacy laws]. Regulating the "disclosure" and the "use" of personal information serve very different ends; protecting against subjective harm in the case of the former and objective harm for the latter. Accordingly, interpreting the notion of "identifiability" will vary in light of the data handling activity at stake. Secondly, when evaluating the risk of harm pertaining to the disclosure of personal information, we need to interpret this notion in light of the other two criteria which are relevant when evaluating the overall subjective harm following disclosure: the "intimate" nature of the information, and its "availability". For instance, the higher the risk of harm based on the previous criteria (data revealing "intimate" information which may or may not have been previously "available"), the less stringent the link between data and an identifiable individual for certain information to qualify as "personal". »[300]

[299] *Id.,* par. 39.
[300] Éloïse GRATTON, *Redefining Personal Information in the Context of the Internet*, *op. cit*., note 288, p. 298.

3.2. Analyse de la définition et de la qualification des données anonymisées et dépersonnalisées

Il s'agit d'un point important à approfondir, particulièrement dans un contexte de PCL. En effet, si un renseignement est correctement anonymisé, cela pourrait constituer une solution intéressante répondant à plusieurs préoccupations partagées tant par le législateur, les autorités de contrôle, les entreprises et les individus, notamment en matière de sécurité en diminuant le risque de vol d'identité lorsqu'un incident de sécurité, et en matière d'anonymat en contribuant à rendre acceptable le maintien d'un régime de consentement implicite dans un contexte de PCL au Canada. Les obligations de sécurité et d'obtention de consentement sont approfondies plus loin aux sections II et III de ce mémoire.

Toutefois, nous verrons comment l'anonymisation réelle, telle que définie et interprétée, est loin d'être chose facile à réaliser, considérant tant les moyens technologiques que les pratiques actuelles.

3.2.1. L'anonymisation selon la loi fédérale et la loi québécoise

Évolution de la définition d'anonymisation au fédéral, et exclusion à venir de l'application de la loi

En guise d'introduction générale à cette section, révisons la terminologie générale employée. J'aborderai dans l'ordre la définition de la LPRPDE, du Projet de loi C-27 et de la Loi 25.

Analysant les différents types de désidentification, soit l'anonymisation et la dépersonnalisation (ou pseudonymisation), Barry Sookman en 2020, résumait ainsi ces différences terminologiques et conceptuelles observées dans le RGPD, la LPRPDE et la CCPA :

> « The term "de-identified" is often used as a general term that includes privacy and security processes that renders personal information as either "anonymized" or "pseudonymized". "Pseudonymization" commonly refers to a de-identification method that removes or replaces direct identifiers from a data set, leaves in place data that could be used to indirectly identify a person. This data is generally still subject to privacy laws.[1] "Anonymization", by contrast, generally refers to a stronger form of de-identification which (depending on the formulation) makes re-identification impossible,

> reasonably unlikely, or not reasonably expected. This data is generally considered to be outside of general privacy law obligations.[2] »[301] [Mes soulignements]

Ainsi, l'anonymisation des données s'entend généralement d'un processus irréversible contrairement à la pseudonymisation. Un renseignement seulement pseudonymisé se retrouve donc encore à bénéficier de la protection de la LPRPDE, contrairement à un renseignement validement anonymisé.

Au niveau fédéral, la LPRDPE actuellement en vigueur ne parle pas de l'anonymisation spécifiquement, mais seulement de la dépersonnalisation. Toutefois, le Projet de loi C-27, à son article 2(1), intègre une définition de l'anonymisation, étant l'action de

> « [m]odifier définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues, des renseignements personnels afin qu'ils ne permettent pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit. (*anonymize)* ». [Mes soulignements].

En conséquence, si cet article était adopté tel quel, le législateur canadien viendrait ainsi rehausser son standard actuel, tout en ayant recours aux meilleures pratiques généralement reconnues, à l'instar de l'article 23 de la Loi 25, cette dernière ajoutant toutefois à ces meilleures pratiques des critères à être déterminés par un éventuel règlement[302]. Nous pouvons nous attendre à ce qu'il recommande ou reconnaisse éventuellement certaines normes informelles techniques de type ISO qui pourraient rencontrer le niveau requis par l'article 2(1), conformément aux pouvoirs qui lui sont conférés à l'article 77 du Projet de loi C-27.

Concernant cette référence aux meilleures pratiques, Teresa Scassa se fait très critique de ce choix de délégation normative en reprochant l'absence de référence à un règlement, contrairement à ce que la province de Québec a fait dans la Loi 25 en référant à un règlement et

---

[301] Barry SOOKMAN, « CPPA: identifying the inscrutable meaning and policy behind the de-identifying provisions », (7 décembre 2020), *Barry Sookman*, par. 2, en ligne : <https://www.barrysookman.com/2020/12/07/cppa-identifying-the-inscrutable-meaning-and-policy-behind-the-de-identifying-provisions/ > (consulté le 19 mars 2023). À la note 1, Sookman réfère aux définitions de pseudonymisation du RGPD et de *California Consumer Privacy Act* de 2018. À la note 2, Sookman réfère à Mike HINTZE et al., « Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR », *Privacy Analytics* (août 2017)

[302] Infra, p. 99.

aux meilleures pratiques[303]. Elle soutient plutôt que les organismes de règlementation devraient jouer un rôle dans l'établissement des normes pour l'anonymisation et la dépersonnalisation.[304]

Cela étant dit, plusieurs conséquences découlent de cette qualification de renseignement anonymisé, la première et la plus lourde de conséquences étant d'exclure ce renseignement « non personnel » à l'application de la loi fédérale. En effet, l'article 5(5) du Projet de loi C-27 précise qu'« [i]l est entendu que la présente loi ne s'applique pas à l'égard des renseignements personnels qui ont été anonymisés ». En conséquence, si cet article du Projet de loi est adopté tel quel, les renseignements anonymisés seront expressément exclus de la définition de renseignements personnels protégés par la loi. Il s'agit d'une précision importante qui est toutefois absente dans la Loi 25, laissant ainsi planer un certain doute sur l'application de la loi à la collecte de renseignements personnels anonymisés[305], ce qui est problématique pour les organisations québécoises et les organisations ayant des activités pancanadiennes.

La logique qui sous-tend cette approche du législateur fédéral a été exprimée par le Commissaire à l'information et à la protection de la vie privée de l'Ontario (IPC) :

> « L'anonymisation protège la vie privée des particuliers puisqu'une fois que les renseignements personnels ont été anonymisés, l'on considère que l'ensemble de données ne contient plus de renseignements personnels. Lorsqu'un ensemble de données est exempt de renseignements personnels, son utilisation ou sa divulgation ne peut aucunement contrevenir aux droits à la vie privée des particuliers. En conséquence, les dispositions touchant la protection de la vie privée de la *Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)* ou de la *Loi sur l'accès à l'information municipale et la protection de la vie privée (LAIMPVP)* ne s'appliqueraient pas aux renseignements anonymisés. »[306]

[303] Teresa SCASSA, « Anonymization and De-identification in Bill C-27 », *Teresa Scassa - Blog*, (6 juillet 2022), en ligne: <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80 > (consulté le 24 mars 2023)
[304] *Id*., par. 19.
[305] Infra, p. 99-100.
[306] COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *L'anonymisation et autres mesures de protection de la vie privée*, par. 2, en ligne : https://www.cipvp.ca/protection-de-la-vie-privee-organismes/lanonymisation-et-autres-mesures-de-protection-de-la-vie-privee/ > (consulté le 19 mars 2023)

Une autre conséquence notable liée à cette qualification de renseignement anonymisé est d'y attacher l'obligation de documenter les mesures en lien avec l'anonymisation prévue à l'article 6 du Projet de loi C-27[307] :

> « La personne qui exerce une activité règlementée et qui, dans le cadre de cette activité, traite ou rend disponibles des données anonymisées établit, conformément aux règlements, des mesures concernant :
>
> a) la manière d'anonymiser des données;
>
> b) l'utilisation ou la gestion des données anonymisées.» [Mes soulignements]

Ainsi, si une organisation arrive à qualifier les données en question de données anonymisées, elle devra documenter comment elle les a anonymisées et comment elles sont utilisées et gérées, le tout conformément à un ou plusieurs règlements à venir. Elle devra être en mesure de démontrer qu'elle s'est ainsi correctement acquittée de son obligation générale de responsabilité et être en mesure de démontrer sa démarche et ses conclusions auprès des autorités de contrôle le cas échéant. Remarquons ici qu'il sera important que le ou les règlements auxquels réfère l'article 6 soit publié avant l'entrée en vigueur de la nouvelle loi, afin que les entreprises puissent s'y référer et s'y conformer à temps, contrairement à ce que nous observons au Québec où ce type de délégation a été incluse, mais où le règlement se fait toujours attendre.

Concernant l'exclusion des renseignements anonymisés de la définition de renseignements personnels protégés par la loi, Teresa Scassa apporte une réflexion très pertinente en lien avec le non-assujettissement des renseignements anonymisés à la loi. Elle affirme son désaccord avec cette exclusion et soutient qu'un régime de gouvernance devrait demeurer applicable aux données relatives à des humains, même si elles ont été anonymisées :

> « Emerging and evolving concepts of collective privacy take the view that there should be appropriate governance of the use of human-derived data, even if it has been anonymized. Another argument for keeping anonymized data in scope relates to the importance of

[307] Cette documentation des processus est d'ailleurs commune avec les standards, dont la norme ISO/IEC 27559 « visant à identifier et à atténuer les risques tout au long du cycle de vie des données anonymisées. » : Luk ARBUCKLE, « A new standard for anonymization », IAPP (14 mars 2023), en ligne : <https://iapp.org/news/a/a-new-standard-for-anonymization/> (consulté le 27 avril 2023) (Traduction libre);
ISO, « ISO/IEC 27559 :2002. Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework », en ligne : <https://www.iso.org/standard/71677.html> (consulté le 27 mars 2023)

> oversight, given re-identification risks. Placing anonymized data outside the scope of data protection law is contrary to the recent recommendations of the ETHI Standing Committee of the House of Commons following its hearings into the use of de-identified private sector mobility data by the Public Health Agency of Canada. ETHI recommended that the federal laws be amended "to render these laws applicable to the collection, use, and disclosure of de-identified and aggregated data". Aggregated data is generally considered to be data that has been anonymized. The trust issues referenced by ETHI when it comes to the use of de-identified data reinforce the growing importance of notions of collective privacy. It might therefore make sense to keep anonymized data within scope of the legislation (with appropriate exceptions to maintain incentives for anonymization) leaving room for governance of anonymization. »[308] [Mes soulignements, références omises]

Ces préoccupations sont très importantes. Cela dit, le niveau requis par la loi et par le CPVP (que je verrai au point 3.2.2) est assez élevé pour que peu de renseignements se qualifient en réalité « d'anonymisés » pour le moment. J'y reviendrai brièvement au point 3.2.3.

Évolution de la définition d'anonymisation au Québec et régime applicable

Passons maintenant à la Loi 25. Au niveau de son application, contrairement au régime fédéral, la loi québécoise n'exclut pas expressément les renseignements anonymisés de la définition de renseignements personnels et donc de l'application générale de la loi. Le seul endroit dans la loi où il est question d'anonymisation est l'article 23 traitant de l'anonymisation comme option à la destruction si elle est conforme aux meilleures pratiques reconnues et au règlement à venir, et si elle dessert des fins légitimes. Il n'est donc pas clair si l'anonymisation permet de se soustraire à l'application de la loi dès l'étape de la collecte, par exemple dans un contexte de PCL.

En effet, pour trouver une définition d'anonymisation dans la nouvelle loi québécoise, nous devons nous diriger vers la section traitant de la destruction des renseignements personnels, où l'anonymisation y est décrite comme une alternative à cette destruction une fois arrivé l'accomplissement de la finalité visée.

Cela dit, il apparaît illogique que l'ensemble des obligations de la Loi 25 s'appliquent à des renseignements dûment anonymisés considérant la définition même de renseignements personnels, qui réfère au caractère identifiable d'un individu, directement ou indirectement.

[308] Teresa SCASSA, « Anonymization and De-identification in Bill C-27 », *op. cit,* note 303, par. 8.

Néanmoins, il serait pertinent que cette précision concernant l'anonymisation soit apportée dans d'éventuelles lignes directrices de la CAI ou du règlement à venir émanant du gouvernement provincial afin de dissiper tout doute. De plus, le dénouement de l'affaire *Option Consommateurs* c. *Google*[309] et l'analyse de la Cour sur la définition de renseignements personnels pourrait apporter un certain éclairage sur la question.

Toutefois, si l'anonymisation permet de sortir du champ d'application de loi, il sera fort difficile d'y parvenir vu les critères énoncés à l'article 23. Cet article énonce les paramètres suivants concernant l'anonymisation comme option à la destruction des renseignements personnels :

> « Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser pour l'utiliser à des fins sérieuses et légitimes, sous réserve d'un délai de conservation prévu par une loi.
>
> Pour l'application de la présente loi, un renseignement concernant une personne physique 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.
>
> Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement. » [Mes soulignements]

Remarquons que la définition inclut quatre critères assez restrictifs : 1) les fins de l'utilisation doivent être sérieuses et légitimes, donc sujettes à l'évaluation de l'autorité de contrôle; 2) il ne doit plus être possible et de façon irréversible d'identifier directement ou indirectement la personne, donc l'anonymisation doit être permanente ; 3) le processus d'anonymisation doit satisfaire tant aux meilleures pratiques généralement reconnues qu'aux critères et modalités déterminés par un règlement à venir.

Le recours à la double délégation normative[310] (meilleures pratiques et règlement) pourrait poser problème si les normes des meilleures pratiques et du règlement s'avéraient contradictoires ou incompatibles, notamment en raison de l'évolution plus rapide des meilleures pratiques que dudit

[309] Supra, 2.1.6. et 3.1.2.; Infra, 6.2.2.
[310] Supra, 2.4.

règlement. Toutefois, aucun règlement n'a encore été publié, ce qui est un enjeu pour les entreprises qui doivent pourtant se conformer à l'article 23 à compter du 22 septembre 2023.

Ainsi, comme le remarquent notamment Gautrais et Laville, le flou entourant la définition d'anonymisation est problématique :

> « Ainsi, plutôt que d'assurer une certaine flexibilité de la législation, le caractère flou de la loi combiné à la double problématique de la terminologie employée dans la loi et les normes informelles et les champs d'application respectifs des normes font douter de l'efficacité du PL64. » [311]

Comparaison avec la définition de dépersonnalisation au fédéral

Au niveau fédéral, la LPRPDE ne définit pas la dépersonnalisation, mais en fait mention dans le cadre du principe de limite à la conservation des renseignements personnels énoncé à 4.5.3 de son annexe 1 qui se lit comme suit :

> « On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels. »[312] [Mes soulignements]

Le Projet de loi C-27 vient apporter une certaine lumière sur la question en proposant une définition de la dépersonnalisation comme étant l'action de « [m]odifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement. (*de-identify*) »[313]. [Mes soulignements]. Il ajoute que

> « [p]our l'application de la présente loi, à l'exception des articles 20 et 21, des paragraphes 22(1) et 39(1), des articles 55 et 56, du paragraphe 63(1) et des articles 71, 72, 74, 75 et 116, les renseignements personnels qui ont été dépersonnalisés sont considérés comme étant des renseignements personnels. » [Mes soulignements].

[311] Vincent GAUTRAIS et Henry LAVILLE, « Pour une gouvernance participative des données personnelles au Québec », *op. cit*, note 133, p. 9.
[312] LPRPDE, annexe 1, art. 4.5.3.
[313] LPRPDE, art. 2.

Ainsi, les renseignements dépersonnalisés demeurent des renseignements personnels et les entreprises les traitant doivent respecter l'ensemble des obligations prévues à la loi, sauf dans le contexte limité des articles énumérés à 2(3), c'est-à-dire :

- L'article 20 autorisant l'utilisation sans consentement si pour fin de dépersonnalisation;
- L'article 21 autorisant l'utilisation sans consentement si pour fin de recherche, analyse et développement;
- Une transaction commerciale éventuelle au sens de l'article 22(1);
- Les fins socialement bénéfiques visées à l'article 39(1);
- L'obligation de procéder au retrait des renseignements à la demande l'individu de l'article 55;
- L'obligation de maintien de l'exactitude des renseignements de l'article 56;
- L'obligation de donner accès aux renseignements sur demande de l'article 63(1);
- L'obligation de rectification des renseignements sur demande de l'article 71;
- La communication de renseignements personnels conformément à un cadre de mobilité des données de l'article 72;
- Les articles 74 et 75 spécifiques aux renseignements dépersonnalisés concernant la proportionnalité des procédés techniques et administratifs, et l'interdiction de réidentification;
- Les attributions du commissaire de l'article 116.

Soulignons ici que bien que les renseignements dépersonnalisés demeurent des renseignements personnels au sens du Projet de loi C-27, ils bénéficient toutefois d'un régime « allégé » d'une perspective organisation. En effet comme le constatait le cabinet BLG, « les renseignements qui ont été dépersonnalisés ne seront pas considérés comme des renseignements personnels aux fins du droit de retrait, du droit d'accès et de rectification ainsi qu'au droit à la mobilité des renseignements. Le droit d'être informé des systèmes décisionnels automatisés continue cependant de s'appliquer aux renseignements dépersonnalisés (art. 2(3) de la LPVPC). »[314]

Ainsi, le cabinet BLG concluait que

> « [l]'examen de ces exceptions révèle un cadre soigneusement étudié qui répond aux défis que soulève le traitement de renseignements personnels dépersonnalisés lorsqu'ils sont

[314] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 21 par. 2.

> traités de la même manière que des renseignements personnels standards. (…) Collectivement, ces articles motiveront les organisations à dépersonnaliser les renseignements personnels avant de les utiliser pour des fins de recherche et de développement (plutôt que d'obtenir le consentement et d'utiliser les renseignements personnels dans leur forme originale) en rendant inapplicables plusieurs obligations qui rendraient la dépersonnalisation difficile en pratique. »[315]

Teresa Scassa quant à elle, se fait plutôt critique de cette définition :

> « In the context of the new definition of 'de-identify', it is jarring, since de-identification according to the new definition *requires only the removal of direct identifiers*. What this, perhaps, means is that although the definition of de-identify only requires removal of direct identifiers, actual de-identification might mean something else. This is not how definitions are supposed to work. »[316]

Revenons sur les articles 74 et 75 du Projet de loi relatifs aux renseignements dépersonnalisés.

Le premier prévoit que

> « [l]orsque l'organisation dépersonnalise des renseignements personnels, elle veille à ce que les procédés techniques et administratifs utilisés soient proportionnels aux fins auxquelles ces renseignements sont dépersonnalisés et à la nature sensible des renseignements personnels. » [Mes soulignements].

Le deuxième ajoute que la réidentification d'un individu à partir d'un renseignement personnel dépersonnalisé est interdite, sauf dans les six cas d'exception prévus, soit :

> « a) pour vérifier l'efficacité des mesures de sécurité mises en place;
>
> b) pour se conformer aux exigences prévues sous le régime de la présente loi ou à celles du droit fédéral ou provincial;
>
> c) pour vérifier l'équité et l'exactitude des modèles, des processus et des systèmes élaborés à l'aide des renseignements dépersonnalisés;
>
> d) pour vérifier l'efficacité de ses processus de dépersonnalisation;
>
> e) à une fin ou dans une situation approuvées par le Commissaire en vertu de l'article 116;
>
> f) tout autre cas prévu par règlement. » [Mes soulignements]

[315] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 23 et 24.
[316] Teresa SCASSA, *op. cit*., note 303.

Ainsi, une organisation, à plus forte raison dans un contexte de PCL, n'est donc pas autorisée à réidentifier une personne à partir de renseignements dépersonnalisés, sauf pour exercer les mesures de contrôle et de vérification en lien avec ces procédés techniques et administratifs (art. 74) énumérées à l'article 75. Avec raison,

> « [c]es dispositions reconnaissent implicitement le risque inhérent à la repersonnalisation associée à certaines formes de dépersonnalisation, et vise à équilibrer l'utilisation de ces renseignements et les protections/restrictions qui devraient être mises en place pour minimiser un tel risque. »[317]

Soulignons également deux éléments importants par rapport aux exigences de l'article 75 : Elles imposent un important fardeau documentaire (alinéas a, c, d et e), susceptible d'évoluer dans le temps et d'inclure de nouvelles exigences règlementaires (alinéa f) ou émanant du Commissaire directement suite à une demande de dérogation spéciale (alinéa e), et elles renforcent la volonté de coopération entre les différents organismes de contrôle fédéraux et provinciaux[318].

Nouvelle définition de dépersonnalisation au Québec

Résumons ici la situation québécoise. La Loi 25 prévoit pour la dépersonnalisation, à l'instar du Projet de loi C-27, l'élimination des identifiants directs[319]. En effet, l'article 12 a été modifié afin d'intégrer des précisions sur la dépersonnalisation en spécifiant qu'un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée[320]. Remarquons que

> « [c]ette définition correspond essentiellement à la notion de renseignements " pseudonymisés ", tel que ce terme est généralement compris (sous le RGPD, notamment) : la suppression de tous les " identifiants directs " (par exemple, le

[317] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 23, par. 3.
[318] Supra, 1.1.7.
[319] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 23, par. 1.
[320] Loi 25, art. 12(3).

> nom, le numéro d'assurance sociale), tout en laissant intacts les " identifiants indirects " (date de naissance, sexe). »[321]

Une fois qu'un renseignement peut être considéré comme ayant été dépersonnalisé, la Loi 25 prévoit l'obligation spécifique de prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de ces renseignements[322]. Les entreprises devront donc correctement documenter leur exercice de qualification des renseignements traités ainsi que les mesures mises en place pour limiter les risques de réidentification. Pour le reste, l'ensemble des obligations prévues par la loi demeurent applicables aux renseignements dits dépersonnalisés, puisqu'ils demeurent des renseignements personnels bénéficiant de l'entière protection de la loi, comme nous l'avons vu plus haut.

Soulignons que le régime de gouvernance auquel sont soumis les renseignements dépersonnalisés au Québec est très similaire à celui proposé par le Projet de loi C-27, bien que ce dernier ait été rédigé de manière plus détaillée, permettant d'emblée aux entreprises de mieux comprendre les éléments concrets à opérationnaliser.

3.2.2. Précisions et imprécisions apportées par les autorités de contrôle

Regardons maintenant l'apport des autorités de contrôle dans l'évolution de la définition de l'anonymisation et leur rôle à venir considérant la récente réforme législative au Québec et la réforme en cours au fédéral.

---

[321] Éloïse GRATTON et al., « Amendements proposés à la loi québécoise sur la protection des renseignements personnels : Conséquences sur les entreprises », *Borden Ladner Gervais / Perspectives* (15 juin 2020), en ligne : < https://www.blg.com/fr/insights/2020/06/proposed-amendments-to-quebec-privacy-law-impact-for-businesses > (consulté le 23 mars 2023)

[322] Loi 25, art. 110 modifiant l'art. 12(5).

Au fédéral

Dans le contexte d'application de la LPRPDE, alors que la LPRPDE ne prévoit pas de définition d'anonymisation, comme nous l'avons plus haut, le CPVP a adopté en 2017 une définition qu'il a intégrée à la liste des exclusions à la définition de renseignements personnels :

- « Des renseignements qui ne concernent pas un individu, soit parce que le lien avec cette personne est trop vague ou trop distant (p. ex. un code postal s'applique à un vaste secteur où se trouvent de nombreuses résidences).
- Des renseignements sur une organisation notamment une entreprise.
- Des renseignements anonymisés, pourvu qu'il ne soit pas possible de les relier à une personne identifiable.
- Certains renseignements sur des fonctionnaires comme leur nom, le titre du poste qu'ils occupent.
- Les coordonnées d'affaires d'une personne qu'une organisation recueille, utilise ou communique uniquement pour entrer en contact avec elle dans le cadre de son emploi, de son entreprise ou de sa profession.
- L'information gouvernementale (...) »[323] [Mon soulignement]

Par la suite, comme le constatait Sookman en 2020, « [t]he Federal Privacy Commissioner has historically advanced the "serious possibility" of identification or re-identification test to determine when personal information becomes anonymous. »[324] [Mon soulignement] À ce critère appliqué par le CPVP s'ajoute celui des attentes raisonnables en matière de vie privée qui occupe également une place de premier plan dans l'approche d'interprétation des autorités, comme le constatait aussi Sookman :

> « The weight of federal and provincial authority, however, has adopted the more practical "reasonable expectations" test. Under this formulation, information is still about an "identifiable" individual "if it is reasonable to expect that an individual can be identified from the information in issue including when combined with information from sources otherwise available".[4] If it is not, the compliance obligations under PIPEDA do not apply. »[325] [Mes soulignements]

[323] CPVP, *Aperçu des lois sur la protection des renseignements personnels au Canada*, *op. cit.* note 193.
[324] Barry SOOKMAN, « CPPA: identifying the inscrutable meaning and policy behind the de-identifying provisions », *op. cit*., note 301, par. 6.
[325] *Id*., par. 7.

Or, par la suite, le CPVP a appliqué une interprétation plus stricte et une définition plus précise dans son examen des répercussions sur la vie privée de l'application Alerte COVID. Dans ces explications, le CPVP y exprime le niveau très élevé auquel il s'attendait pour qu'une organisation puisse prétendre avoir dûment anonymisé un renseignement conformément à la LPRPDE :

> « Cependant, au cours de notre examen, nous avons remarqué qu'un élément dans l'avis de confidentialité et dans les indications était inexact, selon nous, si bien qu'il n'aurait pas été possible pour les utilisateurs de donner un consentement valable. On y attestait que les données recueillies par l'application étaient « confidentielles et anonymes ». Cette affirmation passe sous silence le fait qu'il existe un risque de réidentification, même s'il est très faible. Le véritable anonymat, techniquement parlant, exigerait l'impossibilité totale et permanente d'inverser les processus relatifs aux données concernées, ce qui rendrait impossible de déceler la source des renseignements personnels et donc de réidentifier les individus (note 6). Autrement dit, pour rendre les données véritablement anonymes, elles doivent être dépouillées de tout élément qui pourrait les relier à un individu (note 7). Notre compréhension est que bien que l'identification des utilisateurs soit très **improbable**, elle n'est pas **impossible**. Par conséquent, l'utilisation de l'application ne devrait pas être décrite comme étant totalement anonyme. Les données personnelles sont désidentifiées à certaines étapes et les utilisateurs ont des identités pseudonymes à d'autres étapes, mais de telles techniques dans le système ne devraient pas être décrites comme offrant l'anonymat. Nous avons recommandé que toutes les références à l'anonymat soient retirées de l'avis de confidentialité et des indications au cours du processus d'inscription. Santé Canada et le gouvernement du Canada ont accepté notre recommandation et retiré ces références. »[326] [Mes soulignements]

Note 4 : Voir, *Canada (Information Commissioner)* v. *Canadian Transportation Accident Investigation & Safety Board*, 2006 FCA 157 in interpreting the *Privacy Act*, en ligne : <https://www.canlii.org/en/ca/fca/doc/2006/2006fca157/2006fca157.html?autocompleteStr=Canada%20(Information%20Commissioner)%20v.%20Canadian%20Transportation%20Accident%20Investigation%20%26%20Safety%20Board&autocompletePos=1>

[326] CPVP, *Examen des répercussions sur la vie privée de l'application Alerte COVID*, 31 juillet 2020, 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/urgences-sanitaires/rev_covid-app/ > (consulté le 19 mars 2023)

Note 6 : Paul, OHM, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization » (13 août 2009), *UCLA Law Review*, Vol. 57, p. 1701, 2010, pp. 1772-1774, en ligne : <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>;
Voir aussi Ira S. RUBINSTEIN et Woodrow HARTZOG, « Anonymization and Risk » 91 *Wash. L. Rev.* 703 (2016), p. 710-714, en ligne: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4948&context=wlr >

Note 7 : Commissariat à l'information du Royaume-Uni, *Anonymization: Managing Data Protection Risk Code of Practice*, novembre 2012, p. 16, en ligne : <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>;
Voir aussi GROUPE DE TRAVAIL ARTICLE 29 SUR LA PROTECTION DES DONNÉES, *Avis 05/2014 sur les techniques d'anonymisation*, 10 avril 2014, p. 5, en ligne : <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf>

Le CPVP a ainsi exprimé comment il a déjà rehaussé son niveau d'attente de manière à exiger qu'il soit dorénavant impossible de réidentifier une personne physique. Considérant la définition à venir dans le Projet de loi C-27, nous pouvons nous attendre à ce que le CPVP maintienne cette position suite à l'adoption de C-27.

Au Québec

Du côté de la CAI, les lignes directrices concernant l'anonymisation devront être émises afin d'assurer l'effectivité de ce volet de la Loi 25. En l'absence de telles lignes directrices, la question se pose à savoir si les entreprises canadiennes et québécoises se tourneront vers les lignes directrices existantes émanant d'autres autorités de contrôle, tels les commissariats à la vie privée de l'Ontario[327], du Royaume-Uni[328] et de Singapour[329], afin d'orienter leurs actions. Considérant l'approche généralement stricte de la CAI eu égard à la PRP, il est raisonnable de s'attendre à des lignes directrices qui le reflèteront, et qui plus est, seront alignées ou fortement inspirées de l'approche européenne.[330] Pour le moment, les précisions sommaires publiées par la CAI sont disponibles non pas dans l'onglet « anonymisation » de l'espace évolutif, mais dans le Guide d'accompagnement pour réaliser une évaluation des facteurs relatifs à la vie privée (EFVP).

---

[327] Les lignes directrices du Commissaire à l'information et à la protection de la vie privée de l'Ontario, qui incluent les procédés essentiels pour la suppression des renseignements personnels dans les ensembles de données : en ligne : COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *De-identification Guidelines for Structured Data*, juin 2016, en ligne : <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf> (consulté le 27 avril 2023)

[328] INFORMATION COMMISSIONER'S OFFICE, *Anonymisation and pseudonymisation guidance*, en ligne : <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/> (consulté le 27 avril 2023)

[329] PERSONAL DATE PROTECTION COMMISSION SINGAPORE, *Guide to Basic Anonymisation*, 31 mars 2021, en ligne : <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf> (consulté le 27 avril 2023)

[330] GOUVERNEMENT DU QUÉBEC, *Anonymisation*, dernière mise à jour le 23 février 2023, en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/anonymisation> (consulté le 2 avril 2023)
De plus, ces trois critères sont les mêmes que ceux publiés par le G29 en UE en 2014 dans son avis décrivant les principales techniques d'anonymisation et expliquant comme les mettre en œuvre. Lire : CNIL, *Le G29 publie un avis sur les techniques d'anonymisation*, 16 avril 2014, en ligne : <https://www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation> (consulté le 24 mars 2023)

La CAI y reprend le critère d'impossibilité et d'irréversibilité, mais ne précise pas les méthodes auxquelles elle fait référence :

> « Des renseignements sont dépersonnalisés ou anonymisés s'il est impossible d'identifier une personne à partir du jeu de données. La garantie d'anonymat est obtenue à la suite de l'application d'une ou de plusieurs méthodes. L'anonymisation doit être irréversible. »[331]

Toutefois, le gouvernement du Québec, dans le contexte de l'application de l'article 73 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[332], visant les organismes publics, modifié par la Loi 25, explique qu'un processus d'anonymisation doit notamment respecter trois critères, étant : 1) l'individualisation (« il ne doit pas être possible d'isoler une personne ni de l'identifier directement ou indirectement »); 2) la corrélation (« il ne doit pas être possible de relier des ensembles de données distincts qui concernant une même personne »); et 3) l'inférence (« il ne doit pas être possible de déduire de nouvelles informations sur une personne »)[333]. Il précise également qu'il existe différentes techniques pour empêcher l'identification indirecte d'une personne, tel la randomisation et la généralisation[334]. Il ajoute par ailleurs que dans certains cas toutefois, l'anonymisation peut s'avérer impossible à effectuer par exemple si le besoin nécessite des renseignements très précis[335].

3.2.3. Questionnement sur l'existence de l'anonymisation et défis pour les entreprises assujetties à la loi québécoise

En prenant connaissance du niveau d'anonymisation exigé ci-dessus, nous pouvons nous questionner à savoir si l'anonymisation peut ou pourra réellement exister dans la pratique. Force

---

[331] CAI, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, 10 mars 2021, p. 9 note de bas de page 16, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf > (consulté le 24 mars 2023)

[332] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ C A-2.1, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html?autocompleteStr=loi%20sur%20l%27acc%C3%A8s&autocompletePos=1> (consulté le 2 avril 2023)

[333] GOUVERNEMENT DU QUÉBEC, *Anonymisation*, *op. cit.*, note 330, par. 2 de la section « Techniques d'anonymisation ».

[334] *Id.*, par. 5 de la section « Techniques d'anonymisation ».

[335] *Id.*, par. 4 de la section « Techniques d'anonymisation ».

est de constater que nous pourrions surtout continuer à observer différentes approches de dépersonnalisation plutôt que d'anonymisation.

En effet, il est constaté à ce jour que

> « (…) l'anonymisation est difficile à obtenir et que la plupart des organisations ne sont malheureusement pas qualifiées pour développer leur propre processus d'anonymisation. Qui plus est, au fil des ans, des chercheurs[336] ont démontré que les données anonymisées ne peuvent jamais être totalement anonymes[337]. »[338]

Ainsi dans la pratique,

> « [l]a plupart des entreprises procèdent généralement à la dépersonnalisation plutôt qu'à l'anonymisation des données. Cela signifie que les noms et les identifiants évidents sont supprimés, mais que le reste des données est laissé intact. »[339]

Certains sont encore plus perplexes face à possibilité d'atteindre une réelle anonymisation :

> « Or, la question de l'anonymisation demeure infiniment complexe (…). Toute personne travaillant dans des environnements numériques sait que l'anonymisation totale est une utopie. " Dans les lois canadiennes, on parle plutôt de risque raisonnable d'identification des individus. En ce qui concerne la loi québécoise, on attend toujours des lignes directrices plus claires de la part de la Commission d'accès à l'information, mais nous

---

[336] Alex HERN, « Anonymised' data can never be totally anonymous, says study », THE GUARDIAN (23 juillet 2019), en ligne: <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds>, cité par : Vanessa DESCHÊNES, « Dépersonnalisé, anonymisé, agrégé, pseudonymisé; mais de quoi parlez-vous! », *ROBIC / Publications*, (10 décembre 2020), en ligne : <https://www.robic.ca/publications/depersonnalise-anonymise-agrege-pseudonymise-mais-de-quoi-parlez-vous/> (consulté le 23 mars 2023)

[337] Martin SCAIANO, Grant MIDDLETON, Luk ARBUCKLE, Varada KOLHATKAR, Liam PEYTON, Moira DOWLING, Debbie S. GIPSON, Khaled EL EMAM, « A unified framework for evaluating the risk of re-identification of text de-identification tools », *Journal of Biomedical Informatics*, Volume 63, 2016 aux pages 174-183, en ligne : <https://www.sciencedirect.com/science/article/pii/S1532046416300697> (consulté le 7 décembre 2020); Simon, G. E., Shortreed, S. M., Coley, R. Y., Penfold, R. B., Rossom, R. C., Waitzfelder, B. E., Sanchez, K., & Lynch, F. L., *Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care Records*, EGEMS (Washington, DC); Volume 7,1 6; 2019, en ligne : <https://egems.academyhealth.org/articles/10.5334/egems.270/>, (consulté le 7 décembre 2020); Emam, K. E., Dankar, F. K., Vaillancourt, R., Roffey, T., & Lysyk, M, *Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records*., The Canadian journal of hospital pharmacy, Volume 62,4, 2009, pages 307-19, en ligne : <https://www.sciencedirect.com/science/article/pii/S1532046416300697> (consulté le 7 décembre 2020).

Cités par: Vanessa DESCHÊNES, « Dépersonnalisé, anonymisé, agrégé, pseudonymisé; mais de quoi parlez-vous! », *ROBIC / Publications*, (10 décembre 2020), en ligne : <https://www.robic.ca/publications/depersonnalise-anonymise-agrege-pseudonymise-mais-de-quoi-parlez-vous/> (consulté le 23 mars 2023)

[338] Vanessa DESCHÊNES, « Dépersonnalisé, anonymisé, agrégé, pseudonymisé; mais de quoi parlez-vous! », *op. cit.,* note 337.

[339] *Id*.

> savons que la notion d'anonymisation et que les degrés d'anonymisation requis varient beaucoup en fonction de l'industrie dans laquelle ils s'appliquent. " »[340]

Toutefois, comme le faisait remarquer Vanessa Deschênes, « [m]ême si la dépersonnalisation n'équivaut pas à une anonymisation, elle demeure une technique utile de minimisation des données et une mesure de sécurité »,[341] qui peut être intéressante notamment pour « entrainer un modèle d'intelligence artificielle en utilisant un apprentissage automatique »[342]. Par ailleurs, elle propose d'explorer d'autres techniques « afin de "transformer" les renseignements personnels en renseignements personnels non identifiables et ainsi rester conformes »[343], « telles que la "confidentialité différentielle"[14], le "chiffrement homomorphe" ou les "ensembles de données artificiels" »[344].

Cela dit, rappelons que dans un contexte de PCL, il serait très surprenant que les renseignements puissent un jour être considérés comme des renseignements anonymisés et échapper à l'application de la loi, et ce, peu importe la technique employée, considérant que les autorités de contrôle adoptent une interprétation contextuelle, comme nous l'avons vu à 3.1 ci-dessus, qui tient compte de la finalité pour laquelle les renseignements sont collectés et traités. Dans sa position de principe de 2015-2021 sur la PCL, le CPVP écrivait :

> **« Position :** Adoptant une vision large et contextuelle de la définition de renseignements personnels, le Commissariat estime qu'en général, l'information recueillie à des fins de PCL constitue des renseignements personnels, *étant donné* que le but de la collecte de renseignements est de créer des profils de personnes qui, à leur tour, permettent d'offrir des publicités ciblées, de puissants moyens disponibles pour recueillir et analyser les bits

---

[340] Antoine GUILMAIN et François SENÉCAL, « Collecte de données et éthique : des enjeux à décoder », *École des dirigeants, HEC Montréal* (octobre 2022), en ligne : <https://ethique-conformite.hec.ca/communaute/collecte-de-donnees-et-ethique-des-enjeux-a-decoder/?_ga=2.51290281.1260303918.1669831872-1693310516.1669831872&_gl=1*ss1dub*_ga*MTY5MzMxMDUxNi4xNjY5ODMxODcy*_ga_FPW0B8V0CE*MTY2OTgzMTg3Mi4xLjEuMTY2OTgzMTkzNy42MC4wLjA. > (consulté le 19 mars 2023)

[341] Vanessa DESCHÊNES, « Dépersonnalisé, anonymisé, agrégé, pseudonymisé; mais de quoi parlez-vous! », *op. cit*., note 337.

[342] *Id*.

[343] *Id*.

[344] *Id*.

Note 14 : « Termes généralement utilisés en anglais : "differential privacy", "homomorphic encryption" et "synthetic datasets"»

de données disparates et la possibilité bien réelle d'identifier les personnes concernées et du caractère potentiellement très personnalisé de la publicité en résultant. »[345]

Soulignons de plus que de nombreux défis d'opérationnalisation attendent les entreprises québécoises en lien avec cette question d'anonymisation et de dépersonnalisation. Premièrement, comme nous l'avons vu plus haut, il subsiste une différence majeure entre le Projet de loi C-27 et la Loi 25, du fait que les renseignements anonymisés sont exclus de la définition de renseignements personnels dans le premier, mais inclus dans le second. En effet, alors que ces entreprises doivent s'aligner avec la loi québécoise (et traiter tout renseignement d'un humain, même anonymisé, comme un renseignement personnel protégé par la loi), leurs partenaires et sous-traitants nationaux ou étrangers, eux, s'aligneront plutôt sur la loi fédérale. Cela est un élément important que les entreprises d'ici ne devront pas négliger. En effet, elles devront mieux questionner leurs partenaires et sous-traitants davantage, voire mieux les sélectionner, et demeurer critiques de la qualification que ces derniers font des renseignements qui leur sont transférés, par exemple en vérifiant si des renseignements agrégés ont été erronément qualifiés d'anonymisés. Cet exercice risque toutefois d'être complexe à réaliser dans certains cas. En deuxième lieu, elles devront mieux comprendre les différentes techniques de dépersonnalisation et d'anonymisation, documenter leurs choix et les mesures de protection mises en place pour empêcher la réidentification le cas échéant.

[345] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit.,* note 11, par. 8 sous la question 1 « L'information en question constitue-t-elle des renseignements personnels tels qu'ils sont définis à l'article2 de la LPRPDE? »

Chapitre 4 – Obligations liées aux types d'opérations en cause : finalités, limitation et exactitude

Regardons maintenant en quoi consistent les obligations incombant aux entreprises en lien avec le type d'opérations en cause, soit l'obligation de détermination préalable des finalités et de leur caractère acceptable / approprié, l'obligation de limiter la collecte aux renseignements uniquement nécessaires à l'accomplissement de ces fins et de les détruire une fois ces fins accomplies, et finalement l'obligation d'exactitude de ces renseignements.

4.1. Détermination préalable des finalités et de leur caractère acceptable / approprié

Examinons comment les lois en matière de PRP au fédéral et au Québec définissent cette obligation et comment elle évolue au sein d'une approche d'interprétation souple et dynamique au niveau fédéral, et plus stricte au niveau québécois.

Tant la LPRPDE actuelle, que son Projet de loi C-27, ainsi que la Loi 25 et la Loi sur le privée[346] qui la précède, exigent que les finalités et les nouvelles finalités le cas échéant soient déterminées et documentées préalablement à tout traitement de renseignements personnels et que ces fins soient divulguées de manière claire et transparente aux consommateurs / individus / personnes concernées avant leur traitement au niveau québécois ou au plus tard au moment de la collecte au niveau du Projet de loi C-27[347].

Toutefois, ces finalités doivent impérativement être raisonnablement considérées comme appropriées (au fédéral) ou acceptables (au Québec), comme le rappelaient d'ailleurs la CAI en 2013 et le CPVP en 2018. En effet, parlant de profilage et de publicité ciblée sous l'ancienne loi québécoise sur le secteur privé, la CAI rappelait que « [l]'entreprise ne doit collecter que les

[346] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, en ligne : <https://canlii.ca/t/6ddvs> (ci-après « Loi sur le privé »)
[347] LPRPDE, art. 5(3) et annexe I, art. 4.2, 4.2.1 et 4.5.1 ; Projet de loi C-27, art. 7(2) et 12(1); loi 25, art. 4 et 5

renseignements nécessaires à l'objet du contrat, elle ne peut donc recueillir d'autres renseignements, et ce, même avec votre consentement. »[348] Du côté du CPVP, il rappelait, dans l'affaire *Profile Technology Ltd*., que :

> « Le paragraphe 5(3) limite les fins pour lesquelles une organisation peut recueillir, utiliser ou communiquer des renseignements personnels à celles « qu'une personne raisonnable estimerait acceptables dans les circonstances ». Cette condition s'applique qu'importe qu'un consentement ait été obtenu ou non et même lorsque le consentement n'est pas nécessaire (par exemple, lorsque l'information est « accessible au public » conformément au *Règlement*). »[349] [Mon soulignement]

Il est important de noter que le Projet de loi C-27 vient détailler, à son article 12, les critères qui seront à prendre en considération pour déterminer si une fin peut être considérée comme acceptable ou non. Ainsi, tant la finalité que la manière dont le traitement est fait doivent être considérées comme acceptables par une personne raisonnable dans les circonstances[350], en tenant compte de la nature sensible des renseignements personnels le cas échéant, de l'existence de besoins commerciaux légitimes de l'organisation, du degré d'efficacité du traitement pour y répondre, de l'existence ou non de moyens portant une atteindre moindre à la vie privée tout en permettant l'atteinte des fins visées moyennant un coût et des avantages comparables, et de la proportionnalité entre l'atteinte à la vie privée et les avantages pour l'organisation par rapport aux mesures mises en place par l'organisation pour atténuer les effets de cette atteinte[351].

Ainsi, remarquons que le Projet de loi C-27 intègre ici le test de l'arrêt *Oakes*[352] sous la forme des critères listés à l'article 12(1) et (2). En effet, rappelons que jusqu'à maintenant, tel que constaté par le professeur Déziel, trois (3) approches d'interprétation du critère de nécessité ont été utilisées par les tribunaux, soit : 1) l'interprétation stricte et littérale selon laquelle les renseignements, pour être jugés nécessaires, doivent être indispensables ; 2) l'interprétation

---

[348] CAI, *Le Profilage et la publicité ciblée*, *op. cit*, note 218, p. 2, par. 5

[349] CPVP, *La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée, Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002*, 12 juin 2018, par. 110, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-002/ > (consulté le 26 mars 2023)

[350] Projet de loi C-27, art. 12(1).
L'obligation de transparence et de divulgation sont développées au point 5.2 ci-dessous.

[351] Projet de loi C-27, art. 12(2).

[352] *R.* c. *Oakes,* 1986 CanLII 46 (CSC), [1986] 1 R.C.S. 103

contextuelle et relative qui tient compte des besoins des organisations ; et 3) l'interprétation souple et dynamique qui mise plutôt sur un exercice de pondération des intérêts de l'organisation et du droit à la vie privée de la personne, inspiré du test en deux (2) étapes de l'arrêt *Oakes*[353].[354]

Déziel met en lumière que ce test de l'arrêt *Oakes* consiste dans un premier temps à « établir si la collecte vise un objectif important et légitime et, ensuite, déterminer si l'incidence que peut avoir cette collecte sur le droit à la vie privée de la personne est raisonnable ».[355] [Mes soulignements]. De surcroit, pour conclure au caractère raisonnable de l'atteinte, il faudra prouver trois (3) éléments, soit :

> « l'existence d'un lien rationnel entre les objectifs visés par la collecte et la nature des renseignements collectés, la capacité de la collecte à ne porter qu'une atteinte minimale au droit à la vie privée de la personne, et la proportionnalité entre les effets de la collecte sur le droit à la vie privée des personnes et l'intérêt de l'entreprise ou de l'organisme public à atteindre les objectifs visés par l'utilisation des renseignements personnels.»[356]

De plus, le professeur Déziel remarquait que le CPVP a utilisé une variante de ce test en deux étapes dans son rapport d'enquête de 2018 concernant l'utilisation de données *Facebook* par l'entreprise *Profile Technology Ltd*. mentionné ci-dessus, et l'obligation de traitement à des fins raisonnables énoncée à l'article 5(3) de la LPRPDE.[357] En effet, dans cette affaire, des plaintes de Canadiens avaient été déposées auprès du CPVP contre l'entreprise de Nouvelle-Zélande *Profile Techonology Ltd*[358] puisqu'elle avait collecté à leur insu leurs renseignements de profil *Facebook* (nom, prénom, date de naissance, nom d'utilisateur, photo, situation amoureuse, politique, situation concernant les communications, lieu, écoles, groupes et clubs, noms des amis, choix musicaux, QI estimatif, influence sociale, allégations concernant les comportements sociaux) pour leur créer des profils individuels ou de groupe sur la plateforme de rencontre

---

[353] *Id.,* par. 70 et s.
[354] 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 », dans Barreau du Québec, Service de la formation continue, Développements récents en droit à la vie privée (2019), vol 465, Montréal (QC), Éditions Yvon Blais, 2019, 1, p. 9 à 14, en ligne : <https://edoctrine.caij.qc.ca/developpements-recents/465/369051329>
[355] *Id*., p.13 et 14.
[356] *Id*., p. 14.
[357] *Id*., p. 14.
[358] CPVP, *La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée, Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002*, *op. cit*., note 349.

www.profileengine.com de l'entreprise *Profile Technology*.[359] Cette dernière affirmait que, suite à un contrat exécuté pour le compte de *Facebook* (fourniture d'un puissant moteur de recherche), *Facebook* aurait accepté que *Profile Technologie* ait accès aux renseignements que les utilisateurs *Facebook* avaient consenti à rendre publics et accessibles sur les moteurs de recherche.[360] *Profile Technology* affirmait également qu'il n'est qu'un moteur de recherche comme *Google*, et non une plateforme de rencontre en soi. Les arguments de l'entreprise ont évidemment été refusés par le CPVP qui conclut que :

> « 113. Enfin, nous constatons que le mis en cause utilise et divulgue des renseignements de profils qui sont périmés ou qui ne sont plus publics sur *Facebook*. Le fait qu'il puisse le faire, en partie en raison d'un différend contractuel avec Facebook, ne rend pas cette pratique appropriée. Cela illustre seulement que le mis en cause n'est pas en mesure de refléter la nature dynamique de l'information telle qu'elle apparait sur Facebook ou de respecter le contrôle que les propriétaires de profils *Facebook* exercent sur ces renseignements.
>
> 114. À notre avis, la perte de vie privée résultant de l'utilisation par le mis en cause des renseignements issus des profils est disproportionnée par rapport aux avantages découlant de cette pratique, à savoir le développement et l'alimentation de son réseau social à partir de données provenant d'un autre réseau social et leurs utilisations sans autorisation. De plus, le mis en cause aurait pu alimenter son réseau social d'une manière moins envahissante pour la vie privée, en permettant aux individus de fournir leurs renseignements directement à cette fin.
>
> 115. Par conséquent, nous estimons que la création et l'affichage d'une réplique statique de la page *Facebook* d'une personne dans le but de développer et d'alimenter le site Web du mis en cause, page qui demeure hors du contrôle de la personne et qui n'est pas modifiée, mise à jour ou supprimée comme celle-ci le souhaite, n'est pas une fin qu'une personne raisonnable estimerait acceptable dans les circonstances, conformément au paragraphe 5(3) de la LPRPDE. »[361]

En somme, avec l'intégration des critères listés à l'article 12(1) et (2) du Projet de loi C-27, il y aura continuité dans l'application des critères déjà appliqués par la jurisprudence et par le CPVP.

Au Québec, la CAI semble également appliquer le test en deux étapes de *Oakes*, mais d'une manière plus restrictive. En effet, elle reconnait que le « critère de nécessité est un principe

[359] *Id.*, par. 1 et 13.
[360] *Id.*, par. 15.
[361] *Id.,* par. 113 à 115.

fondamental »[362] et que ce « principe doit s'interpréter au regard de la finalité poursuivie par l'entreprise privée »[363]. Toutefois, elle a récemment publié sur son site Internet, qu'elle considère qu'un renseignement personnel sera jugé nécessaire

> « si la finalité poursuivie est légitime, importante, urgente et réelle et si l'atteinte au droit à la vie privée consécutive à la collecte, la communication ou la conservation de chaque élément de renseignement est proportionnelle à cette finalité (c.-à-d. la collecte des renseignements est-elle rationnellement liée aux objectifs visés, l'atteinte au droit à la vie privée est-elle minimisée et la divulgation du renseignement requis est-elle nettement plus utile à l'entreprise que préjudiciable à la personne concernée).
>
> Dans le secteur privé, en cas de doute, un renseignement personnel est réputé non nécessaire. »[364] [Mes soulignements]

Remarquons ici qu'elle est venue ainsi ajouter les critères d'urgence et d'utilité qui surpasse les effets préjudiciables. De plus, remarquons que la présomption de non-nécessité est présente dans la loi québécoise, mais sous l'article 9 interdisant à une organisation de refuser une demande de bien ou de service si une personne refuse de consentir à fournir un renseignement personnel. Appliquée à la PCL, cette interprétation de la CAI pourrait mener à conclure que les renseignements personnels traités dans un contexte de PCL ne sont pas nécessaires.

4.1.1. Évaluation du caractère acceptable de la PCL et ses limites

Concernant le traitement à des fins de PCL spécifiquement, la CAI n'a pas émis de position concernant la finalité de PCL. En effet, en lisant son document de 2013 concernant le profilage et la publicité ciblée[365], sa note commentant le rapport de 2016 d'Option Consommateurs[366], et ses précisions récentes apportées dans l'Espace évolutif sur les technologies de ciblage et

[362] CAI, « La collecte de renseignements personnels », par. 2, en ligne : <https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/ > (consulté le 26 mars 2023)
[363] *Id.*, par. 3.
[364] *Id.*, par. 3 et 4.
[365] CAI, *Le profilage et la publicité ciblée*, *op. cit*., note 218.
[366] CAI, *Publicité ciblée et protection des renseignements personnels*, en ligne : <https://www.cai.gouv.qc.ca/publicite-ciblee-et-protection-des-renseignements-personnels/ > (consulté le 25 mars 2023)

profilage[367], nous pouvons constater qu'elle ne développe pas spécifiquement sur la question à savoir si la PCL constitue ou non une fin légitime, mais elle rappelle les balises principales à respecter, qui sont essentiellement les mêmes que celles décrites par le CPVP en 2015 (2021), sauf lorsqu'elle précise que le recours à des technologies de profilage devra faire l'objet d'un consentement positif préalable[368]. J'y reviendrai dans la partie III de ce mémoire[369].

Le CPVP quant à lui a publié une position de principe à l'égard de la PCL en 2015 (révisée en 2021), dans laquelle il expliquait que la PCL pouvait constituer une finalité acceptable en vertu de l'article 5(3) de la LPRPDE lorsque cette activité respecte les balises proposées par le CPVP :

> « **Position :** Étant donné que certains utilisateurs peuvent être mal à l'aise à l'idée d'être "suivis" sur le Web, tout en jugeant utiles les publicités adaptées à leurs intérêts, et compte tenu du fait que les services sont généralement gratuits et que les utilisateurs doivent s'attendre à ce que certains renseignements personnels soient nécessaires pour accéder aux services et à l'information, la PCL peut être considérée comme une fin acceptable pour la collecte, l'utilisation ou la communication de renseignements personnels, du point de vue d'une personne raisonnable. Toutefois, la publicité comportementale en ligne ne devrait pas être considérée comme une condition permettant aux personnes d'utiliser Internet en général. Les sites Web peuvent compter sur d'autres formes de publicité. Un consentement valable et des limites sur les types de renseignements recueillis et utilisés à des fins de profilage sont nécessaires. La protection de l'information est également cruciale, tout comme l'est la limitation de la durée de conservation des données. »[370]

Ainsi, cet énoncé de position semble un compromis qui semble réussir à mettre en équilibre les différents enjeux, intérêts et besoins en présence dans l'écosystème numérique. Elle inclut la réalité économique et transactionnelle du web, tout en respectant le concept d'expectative de vie privée d'une personne raisonnable.

---

[367] CAI, « Technologie d'identification, de localisation ou de profilage », en ligne : <https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/technologie-identification-localisation-profilage/> (consulté le 25 mars 2023)

[368] « En d'autres mots, ces technologies ne pourront être activées par défaut; ce sera à la personne concernée de les activer si elle le souhaite. » CAI, « Technologie d'identification, de localisation ou de profilage », en ligne : <https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/technologie-identification-localisation-profilage/> (consulté le 25 mars 2023).

[369] Infra, 6.2.1.2.

[370] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit.,* note 11, par. 8, sous la question « L'offre de publicités ciblées en fonction des comportements est-elle une fin acceptable aux termes du paragraphe 5(3) de la LPRPDE et constitue-t-elle une condition de services ? »

Un exemple récent montre que la publicité ciblée a été considérée comme une fin non acceptable dans les circonstances, à savoir l'affaire *Tim Hortons*. Dans cette affaire, une enquête a été menée conjointement par le CPVP et les autorités provinciales de PRP du Québec, de l'Alberta et de la Colombie-Britannique, sur la collecte massive et en continu de données de géolocalisation d'utilisation par *Tim Hortons* (*Restaurant Brands International Inc*.) et ce en utilisant l'application américaine *Radar*.[371] La conformité de l'entreprise à la loi fédérale, québécoise, albertaine et de Colombie-Britannique en matière de PRP applicables au secteur privé a été analysé.

L'enquête a révélé que dans la pratique, le suivi avait lieu en tout temps, et que *Radar* envoyait en moyenne à *Tim Hortons* environ 10 événements par utilisateur par jour[372], et ce, même si l'application était fermée et que la personne soit au Canada ou à l'étranger.[373] Deuxièmement, l'enquête a révélé que le traitement était contraire à ce qui était expliqué dans les FAQ, qui précisaient plutôt que la collecte avait lieu seulement lors l'application est ouverte.[374] De plus, les politiques sur la PRP de *Tim Hortons* ont été jugées trop vagues puisqu'elles mentionnaient seulement « que *Tim Hortons* pouvait utiliser les renseignements de l'utilisateur, y compris les données de localisation, pour faciliter la communication d'annonces publicitaires ciblées, et la transmission de promotions et d'offres. »[375]

Ainsi, concernant la question précise de l'acceptabilité des finalités, les commissariats sont venus à la conclusion que la collecte de données de localisation détaillées (données de localisation *Radar*) en continu - se qualifiant de renseignements sensibles - et leur transmission aux serveurs du fournisseur de services tiers *Radar*, aux fins de traitement pour *Tim Hortons*, ne saurait constituer une fin qu'une personne raisonnable estimerait acceptable dans les circonstances, ni raisonnable en raison d'un intérêt légitime[376]. Le CPVP résume les éléments considérés ainsi :

---

[371] CPVP, *Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons*, Conclusions en vertu de la LPRPDE n°2022-001, 1er juin 2022, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2022/lprpde-2022-001/ > (consulté le 1er avril 2023)
[372] *Id.*, par. 28.
[373] *Id.*, par. 18.
[374] *Id*., par. 21.
[375] *Id*., par. 19 *in fine*.
[376] Et contrevenant ainsi à l'art. 5(3) de la LPRPDE, à l'art. 5 de la LPRPSP du Québec, à l'art. 11 de la PIPA de l'Alberta, et à l'article 11 de la PIPA de la Colombie-Britannique. *Id*., par. 50 *in fine*.

> « En effet, le but initialement poursuivi par *Tim Hortons* était de « fournir des annonces publicitaires ciblées, afin de mieux promouvoir son café et ses produits connexes, mais [elle] n'a jamais utilisé les données à cette fin identifiée. Dans les faits, l'usage que faisait *Tim Hortons* des données était très limité, puisque l'entreprise avait décidé de mettre l'accent sur d'autres priorités commerciales peu de temps après avoir mis à jour l'application. De plus, l'entreprise utilisait les données de manière agrégée et dépersonnalisée, afin de réaliser des analyses limitées concernant les tendances des utilisateurs.
>
> Nous sommes d'avis que *Tim Hortons* n'a pas recueilli et utilisé les données de localisation détaillées à des fins appropriées dans les circonstances. D'une part, *Tim Hortons* n'avait pas un besoin légitime de recueillir de grandes quantités de données de localisation détaillées de nature sensible et l'entreprise n'a jamais utilisé ces données aux fins prévues. Par ailleurs, les conséquences associées à la collecte de ces données par l'application, dont la vaste majorité étaient recueillies alors que l'application n'était pas ouverte, représentaient une atteinte à la vie privée des utilisateurs qui n'était pas proportionnelle aux avantages potentiels que *Tim Hortons* aurait pu espérer tirer d'une promotion plus ciblée de son café et de ses produits connexes. »[377] [Mes soulignements]

En somme, les données de géolocalisation ont été qualifiées de sensibles, la collecte a été jugée trop vaste par rapport aux besoins légitimes de l'entreprise et aux fins initialement prévues, et l'atteinte à la vie privée qui en résulte a été jugée disproportionnée par rapport aux avantages que *Tim Hortons* aurait pu tirer du ciblage publicitaire. Dès lors, les utilisateurs de l'application ne pouvaient validement consentir au traitement de ses renseignements personnels pour une finalité non appropriée, raisonnable ou légitime au sens des lois en matière de PRP[378].

Il sera intéressant de voir l'impact du Projet de loi C-27 et de l'évolution de la perception de la personne raisonnable sur les balises tracées par cette position (consentement, transparence, sécurité, nécessité et conservation).

Néanmoins, la question risque de se complexifier dans un contexte de traitement par intelligence artificielle où un nombre massif de données est traité et va même jusqu'à créer des nouvelles données.

[377] *Id.*, par. 5 et 6 de la section « Aperçu ».
[378] *Id.*, par. 7 de la section « Aperçu ».

4.2. Limitation des données collectées et conservées : Réflexion sur le critère de nécessité et sur le virage vers une culture de *Data Minimization*

Au Canada, la LPRPDE, le Projet de loi C-27 et la Loi 25 prévoient que seuls les renseignements personnels nécessaires à l'accomplissement de la finalité déterminée doivent être collectés et faire l'objet du traitement.[379]

Il est donc impératif d'évaluer et de se limiter aux renseignements personnels réellement nécessaires à l'accomplissement des fins légitimes qui ont été prédéterminées par l'entreprise, par exemple la collecte, le transfert ou l'utilisation de renseignements personnels à des fins de PCL. Incidemment, un exercice important de réflexion et de tri devient nécessaire afin de réduire au maximum la quantité et le type de renseignements personnels traités.

Comme le rappelait le professeur Déziel en 2019, la détermination de la portée de la limitation dépend de la définition de nécessité et de l'évaluation du caractère légitime et raisonnable des fins visées par la collecte.[380] Ainsi, dans un contexte de personnalisation et de profilage, il développait la réflexion suivante :

> « Puisque l'objectif visé par le traitement de l'information est d'offrir une expérience personnalisée à l'utilisateur, l'ensemble des intérêts, préférences, opinions ou attributs de la personne sont susceptibles de s'avérer pertinents, voire nécessaires, pour mieux connaitre cette personne. »[381] Conséquemment, « [o]n aura compris que, dès lors qu'une fin de personnalisation ou de profilage est identifiée et évoquée, le concept de nécessité risque d'être vidé de tout sens. Dans la mesure où l'objectif visé est d'offrir à l'utilisateur une expérience personnalisée et de lui recommander un contenu qui corresponde à ses goûts, intérêts et préférences, tous les renseignements qui portent sur cet utilisateur peuvent être a priori présentés comme étant nécessaires à l'atteinte de cette fin. Ainsi, même en adoptant des pratiques et des schémas de collecte qui s'inscrivent dans une perspective maximaliste, il demeure possible pour les entreprises de défendre l'idée selon laquelle le concept de nécessité est respecté. Toutefois, il devient par le fait même

[379] LPRPDE, annexe I, art. 4.4 et 4.4.1; PL C-27, art. 13; Loi 25, art. 5.

[380] 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 », *op. cit.,* note 354, p.16.

[381] *Id*., p. 18

largement artificiel et inefficace. Le défi lancé est d'autant plus redoutable que, […], la jurisprudence n'a pas encore fixé de définition claire et précise du concept de nécessité. »[382] [Mes soulignements]

En effet, les dérives sont possibles et les abus assurément présents, causés par ignorance ou négligence. Toutefois, l'industrie exprime la volonté de modifier ses pratiques et de saisir l'opportunité d'intégrer le principe de *Data Minimization* (ou de minimisation des données) dans ses processus[383]. En effet, cette expression qui nous vient du RGPD - qui faire référence à la collecte uniquement des données personnelles qui sont adéquates, pertinentes et nécessaires au regard des finalités de traitement définies au moment de la collecte -[384], est de plus en plus employée dans l'industrie[385], étant associée aux éléments constituant la « publicité responsable », la « technologie responsable » et la saine gouvernance des données. Il s'agit effectivement d'un changement de culture important, mais qui a beaucoup de potentiel. Pour y arriver, les entreprises participant à la PCL auront à questionner et évaluer quels sont les renseignements réellement nécessaires plutôt que superflus dans un contexte de PCL.

Toujours est-il que d'une perspective d'industrie, une réflexion devra s'amorcer sur la quantité, la nature et la qualité des renseignements à collecter. Il s'agit d'une opportunité non seulement pour améliorer les pratiques marketing et leur performance, mais également pour réduire les risques de vol d'identité pouvant découler d'un incident de confidentialité.

---

[382] *Id.*, p. 20.

[383] Notamment lors du Sommet 2021 de l'EDAA, bloc 8 « Une perspective d'entreprise : défis et opportunités de demain », où plusieurs représentants d'entreprises ont invité les diverses parties prenantes de l'industrie à faire plus et mieux avec moins de renseignements, et en respectant l'ensemble des législations applicables.

[384] RGDP, art. 5(1)c); CNIL, *Fiche n°7 : Minimiser les données collectées*, en ligne : <https://lincnil.github.io/Guide-RGPD-du-developpeur/#Fiche_n%C2%B07%C2%A0:_Minimiser_les_donn%C3%A9es_collect%C3%A9es> (consulté le 26 mars 2023)

[385] Notamment lors du Sommet 2021 de l'EDAA, bloc 8 « Une perspective d'entreprise : défis et opportunités de demain », où plusieurs représentants d'entreprises ont invité les diverses parties prenantes de l'industrie à faire plus et mieux avec moins de renseignements, et en respectant l'ensemble des législations applicables.

4.3. Obligation de limiter la conservation de renseignements personnels

De manière connexe, la LPRPDE, le Projet de loi C-27 et la Loi 25 prévoient l'obligation de documenter le calendrier de conservation des données et de supprimer les renseignements personnels une fois atteinte la finalité poursuivie, dans le but de conserver un minimum de renseignements personnels par la suite[386]. À titre d'illustration, mentionnons l'affaire *AggregateIQ* dans laquelle le CPVP avait confirmé que l'entreprise de données « doit supprimer tous les renseignements personnels sous sa garde ou sous son contrôle qui ne sont plus nécessaires à des fins juridiques ou commerciales. » [387]

Soulignons toutefois une différence importante entre le Projet de loi C-27 qui parle de procéder dès que possible au retrait des renseignements personnels à son article 53(1), alors que la Loi 25 exige plutôt la destruction ou l'anonymisation des renseignements à son article 23. Or, comme nous l'avons également vu plus haut, il est complexe de réellement anonymiser des renseignements personnels, et plusieurs organisations doivent être en mesure de conserver des données à des fins statistiques, d'analyse, de production de rapport ou d'amélioration des processus. L'atteinte de l'anonymisation sera particulièrement importante pour y arriver[388].

Remarquons toutefois que la destruction n'est pas chose simple par ailleurs et n'est pas détaillée dans la Loi 25 ni dans le Projet de loi C-27. Dès lors, il est possible de se référer aux normes ISO ou CEI prévoyant différentes procédures ou mécanismes documentés pour l'élimination des données personnelles permettant d'atteindre différents niveaux de destruction[389]. Ces normes incluent des techniques d'élimination des données variant selon « le type de support, la nature

[386] LPRPDE, annexe I, art. 4.5, 4.5.2, 4.5.3; Projet de loi C-27, art. 53(1); Loi 25, art. 23(1).
[387] CPVP, *Enquête conjoint 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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n° 2019-004, *op. cit*., note, 72, « Constatations et recommandations », par. 107.
[388] Supra, 3.2.3.
[389] Guillaume LAPIERRE et Mélissa PELLETIER, « Les répercussions de la Loi 25 en droit des affaires » dans Barreau du Québec, Service de la formation continue, Développements récents en droit des affaires (2022), vol 519, Montréal (QC), Éditions Yvon Blais, 2022, 189, p. 208, par. 3, en ligne : https://edoctrine.caij.qc.ca/developpements-recents/519/c-10c7f1df-e4ab-42f8-8219-0ebaeee7d256 > (consulté le 23 avril 2023)

et l'étendue des données à éliminer, l'existence ou non de métadonnées associées aux données et les caractéristiques physiques du support sur lequel les données sont stockées »[390].

Soulignons également une autre difficulté propre à la PCL, c'est-à-dire qu'en vertu du Projet de loi C-27, l'entreprise « qui utilise des renseignements personnels pour prendre une décision concernant un individu conserve ces renseignements suffisamment longtemps pour permettre à l'individu de présenter une demande [d'accès et de rectification] au titre de l'article 63 »[391].

Cette obligation de limitation à la conservation est également importante afin de réduire les risques d'incidents de confidentialité ou de sécurité qui pourraient survenir, tel que l'illustre bien malheureusement la récente affaire Desjardins. En effet, dans cette affaire, parmi les nombreux manquements relevés par le CPVP figure la contravention au principe de conservation des données. Pour remédier aux manquements aux principes de conservation et de sécurité, il recommandait notamment à Desjardins de finaliser son calendrier de conservation des données et sa procédure de destruction, et d'y préciser les motifs à l'appui des durées de conservation établies par Desjardins et de dépersonnaliser ou supprimer les renseignements personnels une fois arrivés à la fin de leur période de conservation déterminée.[392]

4.4. Exactitude et exercice des autres droits des consommateurs en vertu des lois sur la protection des renseignements personnels

Pour les fins du présent mémoire, je résumerai ici très sommairement en quoi consiste cette obligation d'exactitude, choisissant de me concentrer sur les éléments plus complexes et problématiques des lois en matière de PRP dans une perspective de PCL.

[390] *Id.*
[391] Projet de loi C-27, art. 54.
[392] 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,* Conclusions en vertu de la LPRPDE n° 2020-005, *op. cit*., note 71, par. 124 b) et c).

En vertu de la LPRPDE, du Projet de loi C-27 et de la Loi 25[393], les renseignements personnels doivent être exacts, complets et à jour, et leur fréquence de mise à jour et d'exactitude variera en fonction du contexte, c'est-à-dire principalement en fonction de la finalité qu'ils desservent et des intérêts de la personne concernée.

Dans un contexte de PCL, les entreprises ont tout intérêt à avoir des données exactes et à jour, afin que la PCL qui est livrée soit la plus pertinente possible. Soulignons toutefois, que ce qui complexifie les choses d'un point de vue entreprise, est le fait qu'une adresse IP peut être utilisée par plusieurs membres d'une même famille utilisant le même appareil par exemple. De plus, dans un contexte propre au marketing et à la publicité, remarquons également l'importance cruciale d'assurer l'exactitude des renseignements personnels surtout si se développait davantage et se généralisait la pratique de la tarification dynamique segmentée par exemple (étant un des types de *Dynamic Pricing* basée sur les segments d'audiences[394])[395].

Par ailleurs, soulignons l'importance d'assurer une telle exactitude, puisque de celle-ci permet l'exercice de contrôle et des droits importants généralement conférés aux individus dans les lois en matière de PRP au Canada, au Québec et à l'international, soit le droit de retirer son consentement[396], le droit d'accès aux renseignements le concernant (droit à la portabilité des données)[397], le droit de rectification d'un renseignement inexact, incomplet ou équivoque[398], le droit de retrait ou de suppression des renseignements personnels[399], le droit à la cessation de la diffusion, à la désindexation (droit à l'oubli) et à la réindexation[400]. Elle est en conséquence

[393] LPRPDE, annexe I, art. 4.6, 4.6.1, 4.6.2 et 4.6.3; Projet de loi C-27, art. 56(1), (2) et (3); Loi 25, art. 28 et 28.1.
[394] Jay FUCHS, « Dynamic Pricing : The Complete Guide », HUBSPOT (7 septembre 2022), en ligne : <https://blog.hubspot.com/sales/dynamic-pricing#:~:text=Dynamic%20pricing%20%E2%80%94%20also%20known%20as,and%20time%20until%20the%20flight.> (consulté le 26 mars 2023)
Infra, 6.3.
[395] Infra, 6.3.1.
[396] Projet de loi C-27, art. 17.
[397] LPRPDE, annexe I, art. 4.9 (neuvième principe - accès aux renseignements personnel); Projet de loi C-27, art. 63 et 72; Loi 25, art. 8(1)3°), (3) et (4), 27 à 41.
[398] LPRPDE, annexe I, art. 4.9.5 (correction d'un renseignement inexact ou incomplet); Projet de loi C-27, art. 63; Loi 25, art. 12.1(3°), 27 à 41.
[399] Projet de loi C-27, art. 55; Loi 25, art. 35 et 28.
[400] Loi 25, art. 28.1(1) et (2).

étroitement liée aux obligations documentaire, de transparence et d'obtention de consentement incombant aux entreprises, que je développerai plus bas.

Chapitre 5 - Obligations liées aux mesures à mettre en place

Voyons maintenant les obligations liées aux mesures à mettre en place, c'est-à-dire les exigences en matière de responsabilité, de transparence, de sécurité des renseignements personnels, de transfert transfrontalier des renseignements personnels, ainsi que de documentation.

5.1. Implantation d'une culture de responsabilité : ses fondements

La série de resserrements des obligations amorcée depuis 2018 en Europe et au Canada - et ce bien que la LPRPDE et les lois provinciales en matière de protection des renseignements personnels existaient déjà - a touché tout particulièrement les entreprises sur secteur privé, leurs pratiques marketing et leurs affaires. En effet, au fil de ces resserrements législatifs et règlementaires, il est devenu de plus en plus complexe et pressant pour les entreprises de se préparer à ces nouveaux standards rehaussés internationalement. Outre les sanctions, amendes administratives et les risques de poursuites au pénal, la non-conformité des entreprises non rigoureuses aux opportunités d'affaires auprès de plusieurs grands clients qui doivent s'assurer que leurs partenaires et fournisseurs seront des alliés dans la gestion des risques juridiques, économiques et réputationnels.

Incidemment, les meilleures pratiques de l'industrie et les programmes d'autoréglementation[401] s'adaptent et évoluent en fonction du cadre règlementaire et législatif, des développements technologiques et de l'évolution de la perception des consommateurs, comme je l'ai abordé en première partie de ce mémoire.

Plus spécifiquement, sous l'angle de la PCL, la hausse des exigences incombant aux organisations en matière de protection des renseignements personnels force plusieurs entreprises à être plus

[401] À titre d'exemple, la DAAC a révisé ses principes directeurs en octobre 2022, en renforçant et explicitant les principes d'éducation, de transparence, de contrôle du consommateur, de sécurité de données, des données sensibles et de responsabilité : ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA (DAAC), *Principe canadiens d'autorèglementation de la publicité ciblée par centre d'intérêt*, document révisé en octobre 2022, en ligne : <https://assets.youradchoices.ca/pdf/principles/DAAC-AdChoices-Principles-French.pdf> (consulté le 29 mars 2023)

rigoureuses et à revoir leurs façons de faire en matière de traitement des renseignements personnels. Cela impacte non seulement leur gouvernance en matière de données, mais également leur gouvernance des technologies de l'information et leur gouvernance des systèmes d'information[402].

5.1.1. Culture de responsabilité des données collectées et de reddition de comptes

Le premier principe de l'Annexe 1 de la LPRPDE, la responsabilité, est une des assises les plus importantes de cette loi, tout comme elle l'est dans le Projet de loi C-27 et dans la Loi 25. Toutefois, des différences de formulation entre les différentes lois et projet de loi sont à souligner.

L'actuelle formulation dans la LPRPDE est la suivante : « Une organisation est responsable des renseignements personnels dont elle a la gestion (…) ». [Mon soulignement] L'Office québécois de la langue française définit la gestion comme étant la « [m]ise en œuvre de tous les moyens techniques, humains et matériels d'une entreprise ou d'un organisme afin d'atteindre de manière efficace les objectifs organisationnels préalablement fixés. »[403] Le Larousse quant à lui définit la gestion comme étant l'« [a]ction ou manière de gérer, d'administrer, de diriger, d'organiser quelque chose; période durant laquelle quelqu'un gère une affaire : La gestion d'un stock. »[404]

Le Projet de loi C-27, à son article 7(1), vient préciser que la première obligation de toute organisation, est la responsabilité de celle-ci à l'égard des renseignements personnels « qui relèvent d'elle »[405], c'est-à-dire, « (…) qui décide de les recueillir et établit les fins pour lesquelles

[402]« La gouvernance des technologies de l'information s'occupe de l'utilisation efficace de l'informatique pour améliorer l'efficacité et la productivité des entreprises ou des organisations. La gouvernance des systèmes d'information a pour but d'améliorer le fonctionnement des systèmes d'information des entreprises et, plus généralement des organisations. Elle concerne non seulement la Direction du Système d'Information, mais aussi tous les métiers de l'entreprise qui concourent à la création de valeur grâce aux systèmes d'information. » WIKIPÉDIA, « Gouvernance des technologies de l'information », en ligne : <https://fr.wikipedia.org/wiki/Gouvernance_des_technologies_de_l%27information> (consulté le 17 août 2022)
[403] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), Vitrine linguistique, Fiche terminologique, « Gestion », en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26543848> (consulté le 6 juillet 2022)
[404] LAROUSSE, « Gestion », en ligne : <https://www.larousse.fr/dictionnaires/francais/gestion/36853 > (consulté le 6 juillet 2022)
[405] Projet de loi C-27, art. 7(1).

ils sont recueillis, utilisés ou communiqués, qu'elle les recueille, utilise ou communique elle-même ou qu'un fournisseur de services le fasse pour elle. »[406] [Mes soulignements]

La Loi 25 quant à elle, sous la nouvelle section I.1 intitulée « Responsabilités relatives à la protection des renseignements personnels », fait plutôt référence au concept de « détention » : « Toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient. »[407] [Mon soulignement]

À titre d'illustration récente, rappelons l'affaire *Tim Hortons* vue plus haut, où le CPVP, la CAI et les commissariats de l'Alberta et de Colombie-Britannique ont remarqué des lacunes importantes au niveau de la responsabilisation de l'entreprise *Tim Hortons*, dont a découlé plusieurs infractions à la loi :

> « (…) bien que nous n'ayons pas non plus réalisé un examen approfondi du programme global de gestion de la protection de la vie privée de *Tim Hortons*, nous sommes d'avis que la nature de certaines infractions relevées dans le cadre de notre enquête laisse entrevoir un manque plus général de responsabilisation. Qu'il suffise de souligner, à titre d'exemple, (i) la collecte par Tim Hortons de quantités très considérables de renseignements personnels sensibles pendant plus d'un an sans n'avoir jamais utilisé ces renseignements pour ses fins visées; et (ii) les tentatives de Tim Hortons d'obtenir un consentement par le truchement de demandes de permission qui présentaient un caractère nettement différent d'une plateforme mobile à l'autre et qui ne cadraient pas avec le fonctionnement réel de l'application. Nous sommes d'avis que des évaluations des effets sur la protection de la vie privée menées à des étapes clés auraient permis à *Tim Hortons* de cerner et de traiter de façon proactive un certain nombre ou la totalité des infractions relevées dans le cadre de notre enquête, avant que les renseignements des utilisateurs soient recueillis. »[408] [Mes soulignements]

Ainsi, une entreprise avisée et responsable doit plutôt faire l'inventaire des données collectées, utilisées et communiquées, et limiter la quantité de données collectées puis conservées proportionnellement aux besoins réels de l'entreprise par rapport à ces données. En amont, elle doit correctement s'acquitter de son obligation d'identifier les finalités de la collecte, les renseignements réellement nécessaires à la réalisation de ses fins, ainsi que la durée de

[406] Projet de loi C-27, art. 7(2).
[407] Loi 25, art. 3.1 al. 1.
[408] CPVP, « Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons, Conclusions en vertu de la LPRPDE n°2022-001 », *op. cit.*, note 371, par. 9 de la section « Aperçu ».

conservation requise, tel que nous l'avons vu plus haut concernant les obligations liées aux finalités, à la limitation et à la conservation[409]. Le tout doit être structuré au sein d'un programme de gestion de la protection de la vie privée, tel que recommandé par le CPVP, le Commissariat de la Colombie-Britannique et le Commissariat de l'Alberta[410].

Du côté du RGPD, la définition de responsable de traitement est précisée dans les lignes directrices de 2021 émises par le *European Data Protection Board.* Cette définition est davantage alignée avec la définition du Projet de loi C-27, puisque l'organisation responsable est celle qui *a priori* a déterminé les fins et les moyens du traitement des données à caractère personnel, sans nécessairement y avoir accès :

> « (…) dans la pratique, il s'agit généralement de l'organisation en tant que telle et pas d'une personne au sein de celle-ci (…) qui fait office de responsable du traitement. Un responsable de traitement est un organisme qui *décide* de certains éléments essentiels du traitement. La responsabilité du traitement peut être définie par la loi ou découler d'une analyse des éléments ou circonstances factuels de l'espèce. Certaines activités de traitement peuvent être considérées comme étant naturellement liées au rôle d'une entité (un employeur vis-à-vis de son personnel, un éditeur envers ses abonnés ou une association à l'égard de ses membres). Très souvent, les clauses contractuelles peuvent aider à identifier le responsable du traitement, bien qu'elles ne soient pas toujours déterminantes. Un responsable du traitement détermine les finalités et les moyens du traitement, à savoir le pourquoi et le comment de ce dernier. Le responsable du traitement doit décider à la fois des finalités et des moyens. Toutefois, certains aspects plus pratiques de la mise en œuvre (les « moyens non essentiels ») peuvent être laissés à la discrétion du sous-traitant. Il n'est pas nécessaire que le responsable du traitement ait réellement accès aux données faisant l'objet du traitement pour être considéré comme un responsable du traitement. »[411] [Mes soulignements]

Par ailleurs, toujours sous le RGPD, il peut y avoir des responsables conjoints du traitement « (…) lorsque plus d'un acteur intervient dans le traitement. (…) Le critère essentiel pour qu'il y ait

---

[409] Supra, 4.1., 4.2. et 4.3.

[410] CPVP, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA et OFFICE OF THE INFORMATION & PRIVACY COMMISIONER OF BRITISH COLUMBIA, *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, avril 2012, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/gl_acc_201204/> (consulté le 1er avril 2023)

[411] EUROPEAN DATA PROTECTION BOARD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, *Version 2.0*, adoptées le 7 juillet 2021, p. 3, en ligne : en ligne : <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr>

responsabilité conjointe du traitement est la participation conjointe de deux entités ou plus dans la détermination des finalités et des moyens d'une opération de traitement. »[412] En ce sens, il peut s'agir d'une « décision commune » ou encore de « décisions convergentes » adoptées par ces entités, c'est-à-dire qui « se complètent et sont nécessaires à la réalisation du traitement de telle sorte qu'elles ont un effet concret sur la détermination des finalités et des moyens du traitement ».[413] [Mes soulignements]

En résumé, sous le RGPD, la détermination des fins et des moyens est déterminante pour identifier le responsable ou les responsables conjoints, et l'accès aux données n'est pas nécessaire. Le Projet de loi C-27 s'aligne en partie avec cette vision du responsable en désignant l'entité qui prend la décision et qui détermine les fins, ce qui est plus clair à mon avis que de faire référence au concept de gestion, actuellement utilisé dans la LPRPDE. La nouvelle loi québécoise quant à elle est énoncée de manière différente en liant le concept de responsabilité à la notion de détention des renseignements personnels.

Au final, sous l'ensemble de ces lois, force est de constater qu'en pratique, dans un contexte de PCL, afin de clarifier et d'opérationnaliser le tout entre les différentes parties prenantes à la PCL, les obligations et les responsabilités de chacune des entités devront être précisées dans les contrats conclus entre elles afin d'encadrer leur relation d'affaires. Ces contrats devront préciser quels types de données sont traitées et quels sont les rôle et responsabilité de chacun dans cette activité de traitement (PCL), tout en incluant les durées de conservation et les finalités pour lesquelles les données pourront être traitées en toute légalité[414]. La responsabilité de s'assurer que le traitement est conforme aux lois applicables et de prendre les mesures contractuelles nécessaires auprès de ses fournisseurs de services incombe à l'entreprise qui détermine les fins de traitement. Je reviendrai sur la question des entreprises tierces qui fournissent des services à l'entreprise responsable[415].

[412] *Id*., p. 3, par. 6.
[413] *Id*., p. 3, par. 6.
[414] Comme le confirment notamment et tout récemment l'affaire *Home Depot* (Infra, 5.2.1, 5.2.2., 5.4.2. et 6.2.1.4.) et l'affaire *Tim Hortons* (Supra, 4.1.1., et Infra, 5.2.2., 5.2.3. et 6.2.1.4.)
[415] Infra, 6.2.2.

De ce principe de responsabilité consacré, découlent diverses obligations : la mise en place d'une politique de gouvernance en matière de PRP, qui elle-même inclut la prise de moyens de prévention en matière de bris de confidentialité et d'incident de sécurité. Ce changement de culture doit être initié par la haute direction et aller jusqu'à la formation adéquate des employés. Autrement, les « (…) les manquements liés à la mise en œuvre de procédures ainsi que ceux liés à la formation du personnel constituent une contravention au principe de la responsabilité et plus précisément, au principe 4.1.4 de la LPRPDE. »,[416] comme le rappelait le CPVP dans son rapport d'enquête concernant l'affaire Desjardins.

Concernant l'importance du rôle et de la responsabilité de la haute direction, le CPVP s'exprime ainsi :

> « S'il est souhaitable pour les organisations de faire confiance à leurs employés, cela doit être accompagné par des mesures de surveillance, et de contrôle. Cela s'accompagne aussi d'une culture de reddition de comptes. À cet effet, l'implication des plus hautes sphères de la gestion est primordiale dans la mesure où tout changement culturel doit être initié et adopté par les leadeurs de l'organisation. (…) tous les acteurs impliqués dans le traitement et la protection des renseignements personnels doivent assumer pleinement leurs rôles et leurs responsabilités. D'où l'importance de les doter des ressources techniques nécessaires ainsi que des formations requises. »[417] [Mes soulignements]

5.1.2. Désignation d'un responsable à la protection des RP (RPRP)

Au Québec, la Loi 25 vient introduire explicitement le principe de responsabilité avec l'obligation pour chaque personne exploitant une entreprise de désigner un responsable de la protection des renseignements personnels (RPRP), mais par défaut, ce rôle incombera au plus haut dirigeant de l'entreprise.[418] Le titre et les coordonnées de ce dernier devront être publiés dans la politique de confidentialité disponible sur le site web de l'entreprise et cette personne aura la charge de s'assurer que la loi est respectée et mise en œuvre[419], mais c'est l'entreprise qui demeure

[416] 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,* Conclusions en vertu de la LPRPDE n°2020-005, *op. cit*., note 71, par. 85.
[417] *Id*.
[418] Loi 25, art. 3.1., al. 2.
[419] Loi 25, art. 3.1., al. 3 et al. 2.

responsable de la protection des renseignements[420]. Concrètement, le RPRP devra minimalement « approuver les politiques et pratiques en matière de renseignements personnels que l'entreprise doit établir et mettre en œuvre (art. 3.2 al. 1) », « participer aux évaluations des facteurs relatifs à la vie privée (EFVP) (3.3. alinéa 2) et suggérer des mesures afin d'assurer la protection des renseignements personnels impliqués dans le projet (art. 3.4) » et

> « consigner toute communication à une entreprise ou organisme public susceptible de diminuer le préjudice causé par un incident de confidentialité (art. 3.5 al. 2) et prendre part à l'évaluation du préjudice causé par un incident de confidentialité (art. 3.7). »[421]

Au fédéral, avec le Projet de loi C-27, l'obligation est formulée de manière différente. En effet, l'article 8(1) prévoit qu'un ou plusieurs individus peuvent être désignés pour être « chargés des questions relatives aux obligations qui lui incombent sous le régime de la présente loi » et que « [l]es coordonnées d'affaires des individus désignés sont fournies à toute personne par l'organisation sur demande ».[422] Il est intéressant de souligner ici que contrairement au nouveau régime québécois qui exige la divulgation sur le site Internet de l'entreprise si elle en détient un, l'identité de ces responsables sous le régime fédéral n'a pas à être publiée d'emblée.

Soulignons qu'en Union européenne, une telle désignation est encouragée par la CNIL, mais obligatoire en vertu du RGPD dans les trois cas suivants : 1) les autorités et organismes publics; 2) « les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle »; et 3) « les organismes dont les activités de base les amènent à traiter à grande échelle des données dites " sensibles " (…) ou relatives à des condamnations pénales et infractions ».[423]

---

[420] Loi 25, art. 3.1., al. 1.

[421] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, Borden Ladner Gervais, mis à jour en octobre 2022, , p. 8, par. 3 (Tâches), en ligne : <https://www.blg.com/fr/insights/2021/11/quebec-privacy-law-reform-a-compliance-guide-for-organizations> (consulté le 13 avril 2023)

[422] Projet de loi C-27, art. 8(1).

[423] CNIL, « Règlement européen : le Délégué à la protection des données, c'est obligatoire ? », Section Besoin d'aide, en ligne : <https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-le-delegue-la-protection-des-donnees-cest-obligatoire#:~:text=La%20d%C3%A9signation%20d'un%20D%C3%A9l%C3%A9gu%C3%A9,des%20personnes%20%C3%A0%20grande%20%C3%A9chelle> (consulté le 29 mars 2023)

Une telle désignation m'apparait nécessaire afin de permettre la mise en œuvre des différentes obligations incombant aux entreprises et maximiser ainsi l'effort de prévention des incidents de confidentialité et de mise en conformité de manière générale.

En pratique, la gouvernance interne d'une organisation aurait tout avantage à créer un comité multidisciplinaire interne (par exemple : responsable des TI, conseiller juridique interne, RPRP, responsable des ressources humaines, un membre de la haute direction) éventuellement appuyée de firmes-conseils externes (par exemple : expert en cybersécurité et cybervigilance, cabinet juridique spécialisé en PRP), pour s'assurer d'analyser la question de la PRP d'une perspective générale et de permettre son opérationnalisation de la manière la plus efficace possible.

5.2. Obligation de transparence et d'information : défis et zones grises

Il est aujourd'hui évident que

> « [la] dissimulation [du suivi des activités en ligne, de la collecte de données comportementales et de la diffusion d'informations] peut être préjudiciable et contraire à l'éthique, car les consommateurs ne sont pas conscients des mécanismes de persuasion qui impliquent la PCL ».[424]

Pensons non seulement à l'utilisation de la PCL à des fins de promotion et de vente de produits et services, mais également à son utilisation à des fins sociales et politiques où les conséquences d'un manque de transparence sont évidemment d'une tout autre nature et envergure, allant jusqu'à perturber l'exercice démocratique.

Ainsi, la transparence est un autre concept clé en matière de vie privée et de protection des renseignements personnels, surtout en matière de PCL. Il est indissociable du concept de validité du consentement du consommateur. Je propose ici une analyse de l'obligation de transparence, puis approfondirai l'obligation de consentement à la partie III.

[424] SOPHIE C. BOERMAN, SANNE KRUIKEMEIER & FREDERIK J. ZUIDERVEEN BORGESIUS, « Online Behavioral Advertising: A Literature Review and Research Agenda », *op. cit.*, note 13, par. 10 (Traduction libre)

5.2.1. Évolution au Canada : Examen de la LPRPDE, du Projet de loi C-27 et des enseignements de l'affaire *Home Depot*

Au niveau fédéral, le principe de consentement à 4.3 de l'annexe 1 de la LPRPDE prévoit que « [t]oute 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. » De plus, 4.3.2 ajoute que

> « [s]uivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.» [Mes soulignements]

Ainsi, il est impensable qu'un consentement valable puisse être présumé et invoqué par une organisation qui n'aurait pas dévoilé à la personne concernée qu'il y aura communication à un tiers de renseignements personnels, à des fins tout autres que celles divulguées et donc normalement anticipées par une personne raisonnable dans les mêmes circonstances. C'est pourtant ce qui arriva dans le cas de *Home Depot*[425]. Je propose de m'y attarder, s'agissant d'une récente enquête du CPVP touchant directement une pratique marketing.

Dans cette affaire, le CPVP avait reçu une plainte émanant d'un client de *Home Depot* concernant le transfert non divulgué et conséquemment non autorisé de ses renseignements personnels, en l'occurrence l'adresse courriel hachée et l'historique d'achats hors ligne, à *Meta* via l'outil « Conversions hors ligne » lui permettant de faire « concorder le courriel avec le compte *Facebook* du client et de compar[er] les renseignements sur les achats hors ligne aux publicités sur *Facebook* à l'intention du client afin de mesurer l'efficacité de ces dernières »[426]. Cet outil permettait ainsi à *Home Depot* « de mesurer les répercussions des campagnes publicitaires en ligne de *Home Depot* »[427], c'est-à-dire

---

[425] CPVP, *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, Conclusions en vertu de la LPRPDE n°2023-001, 26 janvier 2023, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2023/lprpde-2023-001/#fn4> (consulté le 31 mars 2023)
[426] *Id.*, par. 7.
[427] *Id.*, par. 30.

> « i) de comprendre la part de leurs activités hors ligne qui peut être attribuable aux publicités [sur les plateformes *Meta*]; ii) de mesurer le retour réalisé hors ligne sur les dépenses publicitaires [sur les plateformes Meta]; et iii) de rejoindre des gens hors ligne [sur les plateformes *Meta*] et de diffuser des publicités en fonction de leurs actions hors ligne. »[428] Il permettait ainsi à Meta de présenter des « rapports globaux à *Home Depot*, y compris les ventes en magasin qui peuvent être attribuables à une campagne publicitaire précise [sur les plateformes *Meta*]. »[429]

Les renseignements étaient retransmis sous forme agrégée et demeuraient donc des renseignements personnels.[430]

Dans un deuxième temps, cet outil permettait en contrepartie à *Meta* « d'utiliser les renseignements du client à ses propres fins commerciales, y compris les publicités ciblées, qui ne se rattachent pas à *Home Depot* »[431], plus précisément « de créer des auditoires semblables dans le but de diffuser, par ses technologies, des publicités auprès de personnes ayant un profil semblable aux clients hors ligne »[432].

Le problème dans cette affaire se situe au niveau de l'absence de divulgation de cette communication à *Meta*, et donc de l'absence de consentement des clients pour le faire. En effet, au moment de payer à la caisse en magasin, le client se faisait demander s'il souhaitait recevoir un reçu papier ou électronique à son adresse courriel. Si le client demandait un reçu électronique et qu'il avait un compte *Facebook*, alors le lien pouvait être établi.[433] Le problème ici est que l'enquête du CPVP révèle qu'aucune mention de cette communication n'était faite explicitement au client de sorte qu'il n'était pas en mesure de le soupçonner[434]. Ainsi, le CPVP considère :

> « Les renseignements en question n'étaient pas forcément sensibles dans les circonstances de cette affaire, mais nous estimons que lorsqu'ils demandent un reçu électronique en magasin, 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* afin de mesurer les répercussions des campagnes publicitaires en ligne de *Home Depot*, ou ils n'ont aucune raison de le soupçonner. Ils ne s'attendent raisonnablement

[428] *Id.*, par. 3.
[429] *Id.*, par. 8.
[430] Supra, 3.2.
[431] CPVP, *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, Conclusions en vertu de la LPRPDE n°2023-001, *op. cit*, 425, Aperçu, par. 2.
[432] *Id.*, par. 3 *in fine*.
[433] *Id.*, par. 7.
[434] *Id.*, par. 30.

> pas non plus à ce que les mêmes renseignements soient communiqués à *Meta*, la plus grande société de médias sociaux au monde et l'une des plateformes de publicité en ligne les plus importantes au monde, et soient utilisés aux fins commerciales de *Meta*, y compris les publicités ciblées, qui ne se rattachent pas à *Home Depot*. »[435] [Mes soulignements]

De surcroit, ne suspectant pas cette communication, les consommateurs ne pouvaient retirer leur consentement.[436] Donc le fait que ce retrait était théoriquement possible n'était pas un argument recevable selon le CPVP.[437]

Le CPVP rappelle ensuite ses lignes directrices concernant un consentement valable[438] qui

> « stipulent qu'il est nécessaire d'informer les personnes de toutes les fins auxquelles les renseignements sont recueillis, utilisés ou communiqués. Il faut énoncer ces fins dans un langage clair, en évitant les formulations vagues comme " améliorer le service ". De plus, une information enfouie dans une politique de confidentialité ou des modalités d'utilisation n'est en réalité d'aucune utilité aux personnes qui ont peu de temps et d'énergie à consacrer à leur analyse. »[439] [Mes soulignements]

Elles prévoient également qu'

> « afin que le consentement soit considéré comme valide ou valable, les organisations doivent informer les personnes de leurs pratiques en matière de protection de la vie privée de manière détaillée et en des termes faciles à comprendre. Par conséquent, les organisations doivent fournir l'information sur leurs pratiques de gestion des renseignements personnels sous une forme facilement accessible. »[440] [Mes soulignements]

Or en l'espèce, les mentions présentes dans la Déclaration sur la confidentialité de *Home Depot*, accessibles sur demande, et de surcroit trop imprécises, ne pouvaient constituer une divulgation valide et suffisante pour fonder un consentement tacite du client pour les fins ci-haut expliquées.[441]

En outre, le CPVP conclut que :

---

[435] *Id.*, par. 30.
[436] *Id.*, par. 33.
[437] *Id.*, par. 35.
[438] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212.
[439] CPVP, *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, Conclusions en vertu de la LPRPDE n°2023-001, *op. cit*, note 425, par. 38.
[440] *Id.*, par. 39.
[441] *Id.*, par. 40 et 41.

> « lorsqu'ils demandent un reçu électronique, les clients ne sont ni avisés de la communication de leurs renseignements personnels à Meta ni dirigés vers les déclarations sur la confidentialité de *Home Depot* ou de *Meta* [,] [l]eurs attentes se limitent tout simplement à ce qu'on leur a dit, c'est-à-dire qu'ils recevront un reçu électronique de leur transaction. Par conséquent, nous estimons que les clients n'auraient aucune raison de consulter les documents mentionnés ci-dessus sur la confidentialité pour obtenir de plus amples renseignements au sujet d'une pratique dont ils ignorent l'existence. Pourtant, selon le modèle de consentement de *Home Depot*, il incombe aux clients de rechercher de façon proactive ces politiques en ligne ou d'en demander une copie papier auprès d'un associé en magasin. Or, il ne s'agit aucunement ici du déploiement par *Home Depot* d'« efforts raisonnables », au sens du principe 4.3.2, visant à voir à ce que les clients soient au courant des fins auxquelles leurs renseignements seront utilisés et communiqués. Par conséquent, *Home Depot* ne peut se fonder sur sa Déclaration sur la confidentialité ou celle de *Meta* pour corroborer l'obtention d'un consentement valable à l'égard de la pratique en question. »[442] [Mes soulignements]

Home Depot ne pouvait non plus invoquer une « lassitude du consentement » pour justifier ses pratiques[443].

Dans les circonstances, il est tout de même surprenant que *Home Depot* et *Meta* aient pu penser que cette pratique aurait pu passer le test des attentes raisonnables des consommateurs et le test des efforts raisonnables auxquels est soumise l'entreprise.

Cela étant dit, au final, le CPVP a recommandé à *Home Depot* de :

> « i. donner dès le départ les principaux renseignements, soit au moment où les clients demandent un reçu électronique, dont i) les renseignements précis qui seront communiqués à *Meta*; ii) le fait que ces renseignements serviront à mesurer l'efficacité des campagnes publicitaires de *Home Depot* sur *Facebook*; iii) le fait que *Meta* (*Facebook*) utilisera les renseignements à leurs propres fins, y compris à des fins de ciblage; et iv) le fait que les clients ont le choix de retirer leur consentement à un moment ultérieur;
>
> ii. intégrer dans sa Déclaration sur la confidentialité une explication plus détaillée de la pratique ainsi que la méthode de retrait d'un consentement. »[444] [Mes soulignements]

Home Depot a par la suite cessé d'utiliser l'outil « Conversions hors ligne » et s'est engagé à suivre les recommandations du CPVP si elle décidait de recommencer à utiliser l'outil[445].

---

[442] *Id.*, par. 43.
[443] *Id.*, par. 44.
[444] *Id.*, par. 47 iii).
[445] *Id.*, par. 48.

Il est en effet bien connu que le défi que représente la mesure de performance des campagnes et du retour sur les investissements médias est une des préoccupations majeures dans l'industrie des communications marketing, ce qui explique ce genre d'outils. Toutefois, il n'est pas permis de le faire en cachette et d'outrepasser les attentes raisonnables de l'utilisateur, surtout en ce qui concerne l'utilisation de renseignements à des fins secondaires, ce qui semble être un angle mort de plusieurs entreprises. L'industrie doit donc continuer de s'ajuster et d'améliorer ces pratiques en matière de transparence et de consentement si elle souhaite garder la confiance nécessaire des consommateurs à son égard. Ainsi, toute collecte, utilisation et transfert de renseignements personnels à des fins de profilage et de ciblage publicitaire doivent être divulgués de manière claire au préalable. Ainsi, comme le résume BLG :

> « Si la décision n'empêche pas les organisations de compter sur un consentement tacite pour toutes les formes de marketing et d'analytique, elle met en lumière l'importance de fournir des avis préalables sur le recours auxdites pratiques, de fixer des limites claires quant à l'usage que les partenaires peuvent faire des informations, et de permettre aux clients de retirer facilement leur consentement à l'utilisation de leurs informations à des fins secondaires. »[446] [Mes soulignements]

Projet de loi C-27

Soulignons que le Projet de loi C-27 a été rédigé de manière plus précise et détaillée que 4.3 de l'annexe I de la LPRPDE, précisant la liste des éléments qui doivent être divulgués et la façon dont ils doivent l'être. Les entreprises seront ainsi mieux renseignées sur les ententes du législateur, mais pourront constater le travail d'analyse et de documentaire important qui les attend, si elles n'ont pas encore procédé à l'exercice.

Dans un premier temps, l'entreprise doit rendre facilement accessibles et en langage clair ses politiques et pratiques mises en place pour assurer sa conformité à la loi.[447] Elle doit en outre rendre accessibles l'ensemble des renseignements listés à 62(2), soit : la description des types de

[446] Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, « Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée », *Borden Ladner Gervais, Perspective* (20 février 2023), par. 6 de la section « Contexte », en ligne : <https://www.blg.com/fr/insights/2023/02/digital-marketing-and-analytics-lessons-for-canadian-retailers-using-offline-conversion-tools > (consulté le 31 mars 2023)
[447] Projet de loi C-27, art. 62(1).

renseignements personnels qui relèvent d'elle, une explication générale sur leur usage, une explication sur la façon dont l'organisation applique les exceptions à l'obligation du consentement et une description des activités dans lesquelles elle a un intérêt légitime, une explication générale de son usage de systèmes décisionnels automatisés pour faire des prédictions, des recommandations ou prendre des décisions pouvant avoir une incidence sur les individus, l'existence de transfert ou des communications interprovinciaux ou internationaux avec répercussion prévisible sur la vie privée, les périodes de conservation des renseignements personnels sensibles, la manière de présenter une demande de retrait ou une demande d'accès et les coordonnées d'affaires de la personne désignée pour recevoir les demandes de renseignements et les plaintes.[448]

5.2.2. Obligation renforcie au Québec sous la Loi 25

La Loi 25 est venue également rehausser l'obligation de transparence et de divulgation avec des exigences similaires à l'article 62 du Projet de loi C-27, mais en ajoutant la précision de l'alinéa 2 concernant le nom du tiers pour qui la collecte est faite ou à qui il est nécessaire de communiquer les renseignements. Cet ajout vient s'aligner avec les conclusions adoptées par les commissariats dans l'affaire *Home Depot*. Afin d'en saisir toute l'ampleur, je le reproduis intégralement ici :

> « 107. L'article 8 de cette loi est remplacé par les suivants :
>
> 8. La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lors de la collecte et par la suite sur demande, l'informer :
>
> 1° des fins auxquelles ces renseignements sont recueillis;
> 2° des moyens par lesquels les renseignements sont recueillis;
> 3° des droits d'accès et de rectification prévus par la loi;
> 4° de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis.
>
> Le cas échéant, la personne concernée est informée du nom du tiers pour qui la collecte est faite, du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins visées au paragraphe 1° du premier alinéa et de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.
>
> Sur demande, la personne concernée est également informée des renseignements personnels recueillis auprès d'elle, des catégories de personnes qui ont accès à ces

[448] Projet de loi C-27, art. 62(2).

> renseignements au sein de l'entreprise, de la durée de conservation de ces renseignements, ainsi que des coordonnées du responsable de la protection des renseignements personnels.
>
> L'information doit être transmise à la personne concernée en termes simples et clairs, quel que soit le moyen utilisé pour recueillir les renseignements. » [Mes soulignements]

En sus, il convient de souligner l'important ajout de 8.1 qui touche directement la transparence et le consentement en matière de profilage et de ciblage publicitaire et l'utilisation de la géolocalisation :

> « 8.1. En plus des informations devant être fournies suivant l'article 8, la personne qui recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci doit, au préalable, l'informer :
>
> 1° du recours à une telle technologie;
>
> 2° des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.
>
> Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne. (....) ».
>
> [Mes soulignements]

Bien que j'approfondirai l'aspect consentement et le nouvel article 8.1 à la Partie III[449], pour continuer sur le volet transparence, remarquons ici que le fait d'ajouter l'exigence concrète et précise d'avoir à divulguer le recours à des technologies permettant l'identification, la localisation ou le profilage permettra d'éviter des situations problématiques comme l'ont vécu récemment *Tim Hortons* et *Home Depot* par exemple. Cet ajout vient concrétiser une nouvelle exigence qui s'aligne avec les standards européen et californien. En conséquence, comme le remarquait la DAAC, cette modification à loi québécoise « donnera vraisemblablement lieu à des " avis sur les témoins " qui sont désormais de plus en plus utilisés dans les publicités Web en Amérique du

[449] Infra, 6.1.3.

Nord — et qui proviennent de la Directive sur les témoins de l'UE et qui sont également requis en vertu de la *California Consumer Privacy Act.* »[450] Il s'agit d'ailleurs d'une recommandation de la CAI introduite dans ses rapports quinquennaux de 2016 et de 2011 où elle proposait déjà de prendre exemple sur l'Union européenne concernant l'obligation d'intégrer un bandeau comme moyen pour renforcer l'obligation d'information.[451] Je développerai sur le sujet des avis à la section sur le consentement valable de ce mémoire[452].

De plus, mentionnons que l'obligation de transparence a également été rehaussée avec le nouvel article 12.1 de la Loi 25 qui requière de divulguer l'utilisation de renseignements personnels afin de rendre une décision fondée exclusivement sur un traitement automatisé au plus tard au moment où la personne est informée de cette décision. Sur ce point, il convient de souligner que :

> « L'expression " traitement automatisé " n'est pas définie dans la Loi 64. D'éventuelles lignes directrices de la CAI seront donc essentielles pour circonscrire la portée des exigences introduites à l'article 12.1. Bien que les modifications introduites par la Loi 64 semblent viser la prise de décision automatisée au moyen d'algorithmes technologies d'intelligence artificielle (IA) et dont l'incidence sur les droits individuels est majeure, le libellé de cette disposition est rédigé de façon suffisamment large pour inclure toutes sortes d'autres processus automatisés de prise de « décision ». Par exemple, l'article 12.1 n'exclut pas la décision, prise à l'issue d'un processus automatisé, de présenter une offre, un produit ou un service à un individu en fonction de son activité en ligne ou de ses intérêts (par ex. la publicité ciblée). »[453] [Mes soulignements]

Ainsi, cet aspect devra être soigneusement analysé par les entreprises participant à la PCL.

5.2.3. Examen du standard européen et leçons tirées de l'affaire *Google* de 2019

Afin de bien comprendre cette obligation renforcie au Québec et au Canada, analysons la situation sous l'angle du régime du RGPD dont ces juridictions se sont inspirées, et plus

[450] DAAC, « Réforme de la LPRPDE et propositions provinciales en matière de protection de la vie privée », (3 décembre 2020), par. 20, en ligne : <https://youradchoices.ca/fr/actualites/2020/12/3/rforme-de-la-lprpde-et-propositions-provinciales >
[451] CAI, *Rétablir l'équilibre, Rapport quinquennal 2016*, *op. cit*, note 219, p. 83 et 84.
[452] Infra, 6.1.3.3.
[453] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit*., note 421.

précisément à travers une décision phare de 2019 en Europe concernant *Google* et ses pratiques publicitaires. Cette décision a permis de tirer des enseignements concrets sur la mise en application de l'obligation de transparence, et de ses sous-critères, l'accessibilité, la clarté et la compréhensibilité, que je propose de mettre en lumière ici.

En janvier 2019, la CNIL, réunie en sa Formation restreinte, adoptait une importante décision sanctionnant *Google LLC.* Étaient à l'origine de cette décision deux plaintes déposées par l'association *None Of Your Business* (NOYB) et par l'association La Quadrature du Net (LQDN), soit respectivement à l'effet que 1) :

> « les utilisateurs de terminaux mobiles Android sont tenus d'accepter la politique de confidentialité et les conditions générales d'utilisation des services de *Google* et qu'à défaut d'une telle acceptation, ils ne pourraient utiliser le terminal »

et 2) :

> « *Google* ne dispose pas de bases juridiques valables pour mettre en œuvre les traitements de données à caractère personnel à des fins d'analyse comportementale et de ciblage publicitaire ».[454]

La Formation restreinte s'est penchée sur la question à savoir s'il y avait bien conformité ou manquement aux obligations de transparence et d'information telles que détaillées aux articles 12(1) et 13(1) du RGPD, lesquels prévoient :

Art. 12(1) RGPD :

> « Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14[455] ainsi que pour procéder à toute communication

[454] *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.*, par. 6 et 7 de la section « Faits et procédure », en ligne : <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038032552> (consulté en juillet 2022)

[455] L'article 13 liste les informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée et l'article 14 liste les informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

au titre des articles 15 à 22[456] et de l'article 34[457] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. (…) » [Mes soulignements]

Art. 13(1) RGPD :

« 1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition; »[458][Mes soulignements]

[456] L'article 15 prévoit le droit d'accès de la personne concernée à ses données à caractère personnel et liste les informations qui doivent lui être communiquées à sa demande. L'art. 16 prévoit le droit de rectification), l'art. 17 prévoit le droit à l'effacement (« droit à l'oubli »), l'art. 18 prévoit le droit à la limitation du traitement, l'art. 19 prévoit l'obligation de notification en ce qui concernant la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement, l'art. 20 prévoit le droit à la portabilité des données, l'art. 21 prévoit le droit d'opposition, l'art. 22 prévoit les dispositions en matière de décision individuelle automatisée, y compris le profilage.

[457] L'article 34 prévoit la communication à la personne concernée lorsqu'il y a eu violation de données à caractère personnel.

[458] En outre, le paragraphe 1 est complété par les paragraphes 2, 3 et 4 de cet article.
Le paragraphe 2 liste les informations complémentaires et nécessaires à fournir pour garantir un traitement équitable et transparent, c'est-à-dire a) la durée de conservation, b) les différents droits des individus (droits d'accès, de rectification ou d'effacement, à la limitation du traitement de s'opposer au traitement, à la portabilité des données), c) le droit de retrait du consentement, d) le droit d'introduire une réclamation auprès de l'autorité

Examinons maintenant l'analyse faite par la Formation restreinte concernant les exigences d'accessibilité et de clarté et compréhensibilité de l'information.

Accessibilité de l'information

S'appuyant sur les lignes directrices sur la transparence et sur la position du G29, la Formation restreinte conclut que *Google* n'a pas rencontré ses obligations de transparence et d'information en vertu du RGPD.[459] En effet, dans son analyse, elle enseigne que pour qu'une information soit considérée comme aisément accessible au sens du RGPD, il faut :

1) Être assez précis sur la façon dont les données à caractère personnel seront traitées de sorte que :

> « la personne concernée devrait <u>être mesure de déterminer à l'avance ce que la portée et les conséquences du traitement</u> englobent afin de <u>ne pas être prise au dépourvu à un stade ultérieur</u> quant à la façon dont ses données à caractère personnel ont été utilisées »[460] [Mes soulignements]

2.« [D]éfinir <u>séparément et de façon claire les principales conséquences</u> du traitement : autrement dit, <u>quel sera réellement l'effet du traitement</u> spécifique décrit »[461]

3.Que l'architecture générale de l'information soit ergonomique et permette que les informations soient facilement trouvables.[462] *A contrario*, elles ne peuvent pas être éparpillées dans plusieurs documents, contenues dans de longs textes juridiques à analyser et/ou à comparer, aux termes de plusieurs clics, accessibles à différents moments de la relation avec la plateforme.[463] Ainsi, si, pour connaitre les informations qui sont collectées pour la finalité de traitement de personnalisation de la publicité, l'utilisateur doit accomplir plusieurs actions (cliquer sur plusieurs liens, aller chercher différents documents sous différents onglets) et combiner plusieurs

---

de contrôle, e) sur quoi repose l'exigence de fourniture de données à caractère personnel (règlement ou contrat) et les conséquences de la non-fourniture de ces données, f) l'existence d'une prise de décision automatisée dont le profilage et les conséquences de ce traitement pour la personne concernée.
Le paragraphe 3 quant à lui exige de divulguer la possibilité de traitement ultérieur à une autre fin.

[459] *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*., *op. cit.,* note 454, p. 8.

[460] *Id*., p. 8.

[461] *Id*., p. 8.

[462] *Id*., p. 8.

[463] *Id*., p. 8.

ressources documentaires (Document Règles de confidentialité, Document Conditions d'utilisation, Plus d'options, En savoir plus), pour avoir une information complète, alors il s'agit d'un « parcours dénué de tout caractère intuitif »[464] rendant difficilement trouvables les informations recherchées.[465]

Or, dans le cas de *Google*, pour accéder aux informations relatives au ciblage publicitaire, à la géolocalisation et aux durées de conservation, cinq, six et quatre actions sont respectivement nécessaires à l'utilisateur, ce qui est considéré comme trop par la Formation restreinte.[466] Elle conclut donc que « la multiplication des actions nécessaires, combinée à un choix de titres non explicites ne satisfait pas aux exigences de transparence et d'accessibilité de l'information »[467] ce qui constitue « un défaut global d'accessibilité des informations ».[468]

Clarté et compréhensibilité de l'information

Par ailleurs, pour satisfaire aux obligations de transparence et d'information, en plus d'être accessible, la Formation restreinte rappelle que l'information doit également être claire et compréhensible. Ce dernier caractère « doit s'apprécier en tenant compte de la nature de chaque traitement en cause et de son impact concret sur les personnes concernées. »[469]

Cette obligation s'étudie à la lumière de différents sous-critères, soit les sources des données traitées, la nature et catégorisation des données traitées, la description des finalités poursuivies et des données collectées, la mention de la base juridique du traitement, la précision quant à la durée de conservation des données et le moment de la divulgation des informations. Je propose de les résumer ici.

Concernant les sources des données traitées : La Formation restreinte constate d'abord que les données collectées par *Google* proviennent de plusieurs sources, soit des différents produits et

[464] *Id.*, p. 8.
[465] *Id.*, p. 8.
[466] *Id.*, p. 8.
[467] *Id.*, p. 8.
[468] *Id.*, p. 8.
[469] *Id.*, p. 8.

plateformes *Google* (*Android, Gmail, YouTube, Google Chrome*) et des fichiers témoins *Google Analytics* déposés sur les sites tiers utilisant les services *Google*.[470] Ainsi,

> « au moins vingt services proposés par la société sont susceptibles d'être impliqués dans les traitements, pouvant concerner des données telles que l'historique de navigation web, l'historique d'usage des applications, les données stockées localement sur l'équipement (telles que les carnets d'adresses), la géolocalisation de l'équipement, etc. Dès lors, un grand nombre de données est traité dans le cadre de ces services via ou en lien avec le système d'exploitation *Android*. »[471]

Concernant la nature et la catégorisation des données traitées : La Formation restreinte constate que les données de source interne, de nature diverse, qui sont collectées et traitées par *Google* peuvent être classifiées en au moins trois (3) catégories différentes, soit :

- Les données produites par la personne (ex : nom, mot de passe, numéro de téléphone, adresse courriel, moyen de paiement, contenus créés, importés ou reçus (écrits, photos, vidéos));
- Les données générées par son activité (ex : adresse IP, identifiants uniques de l'utilisateur, données de réseau mobile ou liées aux réseaux sans fil et appareils *Bluetooth*, horodatage des actions effectuées, données de géolocalisation, relatives aux données techniques des appareils et capteurs, vidéos vues, recherches effectuées, historique de navigation, achats, applications utilisées); et
- Les données dérivées ou inférées à partir des données des deux premières catégories ci-dessus (ex : personnalisation des annonces, fourniture de contenus, recherches et recommandations personnalisées).[472]

En somme, au terme de cette analyse factuelle et contextuelle, la Formation restreinte conclut que le très grand nombre de données traitées, leur nature qui permet de révéler avec précision « de nombreux aspects parmi les plus intimes de la vie des personnes, dont leurs habitudes de vie, leurs goûts, leurs contacts, leurs opinions ou encore leurs déplacements »[473] et le fait qu'elles

[470] *Id.*, p. 8.
[471] *Id.*, p. 9.
[472] *Id.*, p. 9.
[473] *Id.*, p. 9.

soient combinées entre elles, a pour effet de « renfor[cir] considérablement le caractère massif et intrusif des traitements dont il est question »[474].

Remarquons ici que la même approche contextuelle et axée sur les finalités a été appliquée au Canada par le CPVP et les commissariats provinciaux dans l'affaire *Tim Hortons* en 2022[475].

Concernant la description des finalités poursuivies et des données collectées : La Formation restreinte a jugé que les finalités énoncées dans les documents accessibles aux utilisateurs étaient énoncées de manière « trop générique au regard de la portée des traitements mis en œuvre et de leurs conséquences »[476]. Ainsi, ont été jugées trop vagues les formulations suivantes :

- « Les informations que nous collectons servent à améliorer les services proposés à tous nos utilisateurs »;
- « Les informations que nous collectons et l'usage que nous en faisons dépendent de la manière dont vous utilisez nos services et dont vous gérez vos paramètres de confidentialité »[477].

En outre, la description des données collectées a été considérée comme étant « imprécise et incomplète »[478]. En conséquence, ces imprécisions empêchaient les « utilisateurs de mesurer l'ampleur des traitements et le degré d'intrusion dans leur vie privée qu'ils sont susceptibles d'emporter »[479]. [Mon soulignement]

Afin de corriger la situation, la Formation restreinte a recommandé que dès le premier niveau d'information fournie aux utilisateurs, c'est-à-dire les Règles de confidentialité et conditions d'utilisation, ces dernières devraient « contenir des termes de nature à objectiver le nombre et la portée des traitements mis en œuvre »[480] et inclure « une vision d'ensemble des caractéristiques de cette combinaison en fonction des finalités poursuivies ».[481] [Mes soulignements]

[474] *Id.*, p. 9.
[475] Supra, 4.1.1., 5.1.1., 5.2.2., et Infra 6.2.1.4.
[476] *Id.*, p. 9.
[477] *Id.*, p. 9. Il s'agit donc exemples à ne pas reproduire.
[478] *Id.*, p. 9.
[479] *Id.*, p. 9.
[480] *Id.*, p. 9.
[481] *Id.*, p. 9.

Concernant la mention de la base juridique du traitement : Rappelons d'abord que ces bases selon le RGPD, sont l'intérêt légitime et le consentement. En l'espèce, dans ses Règles de confidentialité, *Google* demandait le consentement des utilisateurs et précisait la possibilité de retirer ce consentement par la suite, afin de justifier le traitement des données de ses utilisateurs à des fins de livraison de publicité personnalisée. De plus, *Google* invoquait l'intérêt légitime pour procéder à d'autres traitements notamment « pour mener des actions de marketing en vue de faire connaitre nos services auprès des utilisateurs et surtout avoir recours à la publicité afin de rendre un grand nombre de nos services disponibles gratuitement pour les utilisateurs »[482].

Toutefois, la Formation restreinte a plutôt jugé que la façon dont *Google* a formulé ces précisions dans ces documents d'information ne permettait pas réellement aux utilisateurs de faire la distinction entre la finalité de publicité ciblée basée sur le consentement de l'utilisateur et les « autres formes de ciblage utilisant par exemple le contexte de navigation, fondées sur l'intérêt légitime »[483].

Concernant la précision quant à la durée de conservation des données : La Formation restreinte a également examiné la conformité à l'article 13(2)a) du RGPD, a rappelé que pour rencontrer cette partie de l'obligation de transparence, il n'est pas suffisant de fournir « des explications très générales sur la finalité de cette conservation et [sans] aucune durée précise ni les critères utilisés pour déterminer cette durée »[484]. En conséquence, *Google* ne se conformait pas à cette exigence.

Finalement, concernant le moment de la divulgation des informations : La Formation restreinte a rappelé que conformément à 13(2) du RGPD et aux lignes directrices du CEPD sur la transparence, l'ensemble des informations à divulguer doit l'être au moment de la collecte des données, et ce même si des données sont collectées postérieurement à la création d'un compte.[485] Ainsi, dès la phase de commencement du cycle de traitement, soit dès la création du compte, toutes les informations doivent être divulguées[486]; Elles ne peuvent l'être *a posteriori*, par exemple en ayant recours à des fenêtres *pop-up* ou encore des outils de vérification de confidentialité ou des

[482] *Id.*, p. 10.
[483] *Id.*, p. 10.
[484] *Id.*, p. 10.
[485] *Id.*, p. 10.
[486] *Id.*, p. 10.

tableaux de bord, a plus forte raison puisque ces moyens employés par *Google* « suppo[saient] une démarche active et d'initiative » donc une certaine proactivité de la part de l'utilisateur qui devait aller chercher l'information additionnelle.[487] En conséquence, *Google* ne se conformait pas non plus à cette exigence.

Ainsi, ce résumé de cette décision nous permet de mieux comprendre les critères factuels et contextuels utilisés par la Formation restreinte en application des exigences du RGPD en matière de transparence. Il m'apparait effectivement qu'il est justifié et nécessaire d'exiger de ce type d'entreprise une divulgation accrue et des efforts raisonnables supérieurs pour y arriver, considérant qu'elle monétise un fort volume de données à des fins de livraison de PCL notamment.

5.3. Mise en place de mesures de sécurité : Vers une culture de cybersécurité et de cybervigilance

Les « cyber incidents » et les cyberattaques sont un des principaux enjeux auxquels nous faisons face, individuellement et collectivement, considérant que dans les cas les plus graves, ils peuvent paralyser les opérations des organisations et/ou mener au vol d'identité de personnes. Pensons aux récents incidents vécus par le Mouvement Desjardins, Industrielle Alliance, *Capital One*, BMO, *Simplii Financial* (CIBC), l'Agence du revenu du Canada, *Target* et *Equifax*.

Les lois en matière de PRP requièrent que les données collectées à des fins légitimes soient être adéquatement protégées, de manière à prévenir les incidents de sécurité et à diminuer leurs effets préjudiciables lorsqu'ils surviennent. Les entreprises sont donc responsables de prendre les mesures nécessaires pour assurer la sécurité et le caractère confidentiel des renseignements personnels qu'elles collectent, utilisent, communiquent et conservent. D'où l'importance d'inclure une stratégie de « *data minimisation* »[488], pour réduire les conséquences préjudiciables d'un éventuel incident de sécurité et/ou de confidentialité, et également de mettre en place les

[487] *Id*., p. 10.
[488] Supra, 4.2.

mesures technologiques, contractuelles et humaines nécessaires pour opérationnaliser cette obligation de sécurité.

De surcroit, ce que l'on entend aujourd'hui par « force majeure » est remis en question puisque « (…) dans le contexte où 20 % des entreprises sont victimes d'une cyberattaque chaque année, on ne peut plus plaider qu'on ne le savait pas, que c'était imprévisible ». [489] L'implantation d'une culture de cybersécurité et de cybervigilance, assurée par une gouvernance technologique appropriée, devient alors primordiale dans le contexte actuel où les organisations collectent, détiennent, transfèrent et/ou conservent un nombre important de renseignements personnels, provenant de sources variées incluant des objets connectés, par des individus (employés/bénévoles/sous-traitant) ayant une connaissance, une rigueur et des moyens variables dans l'application des principes de sécurité et de protection des renseignements personnels.

5.3.1. Évolution en cours au Canada

Le 7e principe de l'Annexe I de la LPRPDE prévoit que « [l]es renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité ». Ils doivent l'être « contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. »[490] Ainsi, il ne s'agit pas seulement d'une protection contre les attaques externes, mais également contre les transferts non autorisés à l'interne. L'article 4.7.3 précise ensuite que les mesures de protection devraient comprendre des moyens matériels, des mesures administratives et des mesures techniques, et 4.7.4 ajoute que les organisations doivent sensibiliser leur personnel à la protection des RP.

Le 1er novembre 2018, le Règlement sur les atteintes aux mesures de sécurité[491] entrait en vigueur, complétant les paragraphes 10.1(2), (3), et (5), et 10.3(1) et (3) de la LPRPDE, ayant pour effet d'augmenter significativement le cadre de protection des renseignements personnels au

[489] Selena LU (Lavery) citée par : Jean-Benoît NADEAU, « Le Québec aux avant-postes en matière de protection des données personnelles », LeDevoir (2 avril 2022), en ligne : <https://www.ledevoir.com/societe/693318/protection-des-donnees-le-quebec-aux-avant-postes>
[490] LPRPDE, principe 7, art. 4.7.1.
[491] *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64, en ligne : <https://canlii.ca/t/6b62r> (consulté le 2 avril 2023)

Canada, et provoquant des changements organisationnels et opérationnels importants pour les organisations.[492] En effet, s'alignant notamment avec le RGPD, le règlement est venu prévoir des obligations plus spécifiques et nécessaires en matière de tenu de registre d'incident et de notification des atteintes aux mesures de sécurité.

Ainsi, en premier lieu, toutes les atteintes à la PRP doivent être consignées dans le registre prévu à cet effet de l'organisation, et ce pendant 24 mois.[493] En parallèle, l'organisation doit procéder à une évaluation du risque réel de préjudice grave à l'endroit d'un individu, ce qui

> « comprend la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles »[494],

tout en tenant compte du degré de sensibilité des renseignements personnels en cause et de la probabilité qu'ils aient été mal utilisés ou soient train ou sur le point de l'être.[495] La formule applicable est donc : Risque = Impact x Probabilité[496].

De plus, si l'évaluation mène à la conclusion qu'« il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à son endroit »[497], un avis devra être transmis directement aux personnes touchées par l'incident (le règlement parlant

---

[492] Vincent BUREAU, « Atteintes à la vie privée au Québec : obligations le 1er novembre. Règlement concernant les atteintes aux mesures de sécurité » *Association des agences de communication créative - Accès membres* (2018), p. 5, par. 1.

[493] *Règlement sur les atteintes aux mesures de sécurité*, art. 6.

[494] CPVP, *Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité*, octobre 2018, révisé le 13 août 2021, par. 1 de la section « Que signifie l'expression risque réel de préjudice grave (RRPG) ? », en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/ > (consulté le 2 avril 2023)

Les mêmes exemples sont cités au niveau du gouvernement du Québec dans le contexte de l'évaluation du préjudice découlant d'un incident de confidentialité aux termes des articles 63.8 à 63.11 de la Loi sur l'accès modifiés par la Loi 25 : GOUVERNEMENT DU QUÉBEC, « Incident de confidentialité » (dernière mise à jour le 23 février 2023), section « Procédure advenant un incident de confidentialité », en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite > (consulté le 2 avril 2023)

[495] CPVP, *Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité*, *op. cit*., note 494, par. 2 de la section « Que signifie l'expression risque réel de préjudice grave (RRPG) ? »

[496] Vincent BUREAU, « Atteintes à la vie privée au Québec : obligations le 1er novembre. Règlement concernant les atteintes aux mesures de sécurité », *op. cit,* note 492, p. 3.

[497] LPRPDE, art. 10.1(3).

plutôt que personnes « intéressées »), détaillant plusieurs éléments d'information, soit les circonstances et la date ou la période (peut être approximative) de l'atteinte, la nature des renseignements personnels visés si connue, les mesures mises en place pour atténuer le risque de préjudice, les mesures que les personnes touchées peuvent prendre pour réduire le risque de préjudice ou atténuer le préjudice, et les coordonnées d'une personne à contacter pour obtenir davantage de renseignements concernant l'atteinte.[498] Le règlement prévoit toutefois certaines situations où l'avis peut être envoyé indirectement, c'est-à-dire par une communication publique, c'est-à-dire : 1) si l'avis direct pouvait causer un préjudice accru à la personne touchée par l'incident; 2) si l'avis direct pouvait représenter une difficulté excessive pour l'organisation; ou 3) si l'organisation n'a pas les coordonnées des personnes touchées.[499]

De plus, une déclaration d'atteinte devra être transmise par écrit par moyen sécurisé[500] au CPVP[501] contenant les informations listées à l'article 2(1) du règlement, c'est-à-dire essentiellement les mêmes informations transmises aux personnes touchées en ajoutant le nombre de personnes touchées et les mesures de communication entreprises auprès de ces personnes. Finalement, si l'analyse révélait un risque élevé de préjudice grave, alors « l'entreprise responsable du traitement des données avisera les organisations ou institutions gouvernementales qui pourraient réduire le risque ou le préjudice éventuellement sans le consentement des personnes concernées. »[502]

La LPRPDE prévoit que ces obligations incombent à l'entreprise qui a la gestion des renseignements personnels. Toutefois, ce principe avait été interprété plus largement dans l'affaire *AggregateIQ*, où le CPVP a confirmé que l'entreprise de données

[498] *Règlement sur les atteintes aux mesures de sécurité*, art. 3 et 4.
[499] *Id.,* art. 4 et 5.
[500] *Id.*, art. 2(1) et (3).
[501] LPRPDE, art. 10.1(1).
[502] Vincent BUREAU, « Atteintes à la vie privée au Québec : obligations le 1er novembre. Règlement concernant les atteintes aux mesures de sécurité », *op. cit,* note 492, p. 3.

> « [devait] mettre en place et maintenir des mesures de sécurité raisonnables pour s'assurer que les renseignements personnels sous sa garde ou sous son contrôle sont protégés contre l'accès ou la communication non autorisés ».[503] [Mon soulignement]

Cela dit, en pratique il est primordial, pour que ces articles produisent leurs effets, que les entreprises à qui sont transférés des renseignements personnels comme les entreprises fournisseurs de services ou les entreprises tiers à qui des renseignements personnels sont communiqués, mettent en place des mécanismes de communication de ces incidents et de collaboration dans l'analyse et dans l'atténuation des risques de préjudices. Ce mécanisme de communication devra être prévu contractuellement.

Les précisions et nouveautés apportées par le Projet de loi C-27

Dans ce même ordre d'idée, le Projet de loi C-27 à son article 61, est d'ailleurs venu préciser les obligations spécifiques incombant aux fournisseurs de services en matière de sécurité. Ainsi,

> « [l]a seule nouvelle exigence [concernant les exigences de notification et de déclaration s'appliquant aux mesures de sécurité en cas d'atteinte] est que les fournisseurs de services seront obligés, en vertu de la LPVPC, est de notifier leurs clients dès que possible après avoir " déterminé qu'une atteinte aux mesures de sécurité s'est produite " (art. 61). Ce changement établit un seuil légal minimum pour la notification des prestataires de services, question généralement régie dans les contrats de fourniture de services. Le seuil de déclenchement choisi pour la notification – une " détermination " – donnera aux fournisseurs le temps d'enquêter sur les incidents de sécurité avant de notifier. »[504]

Pour le reste, la section portant sur les mesures de sécurité (art. 57 à 60) intègre l'ensemble des dispositions actuelles de la LPRPDE et du règlement sur les atteintes aux mesures de sécurité.

Il a été constaté en outre que l'obligation générale de sécurité demeure très semblable à celle actuellement formulée sous la LPRPDE[505], c'est-à-dire de protéger les renseignements personnels au moyen de mesures de sécurité physiques, organisationnelles et technologiques

---

[503] 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 d'AggregateIQ Date Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, op. cit., note 72, par. 107 de la section « Constatations et recommandations ».

[504] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 30, par. 4.

[505] *Id.*, p. 30, par. 2

proportionnelles au degré de sensibilité des renseignements personnels[506]. Ainsi, « la sensibilité deviendra le nouveau facteur principal régissant le caractère adéquat des mesures de sécurité, bien que « la quantité, […] la répartition, [le] format et […] la méthode de stockage des renseignements » continueront d'être pertinents (art. 57(2)). »[507] Je reviendrai sur la définition de sensibilité[508], mais rappelle ici qu'il s'agit d'un concept difficile à saisir avec certitude puisqu'il varie selon les circonstances.

Autre élément important à noter, le Projet de loi C-27 vient préciser l'exigence de vérifier l'authentification des individus à l'article 57(3) traitant de la portée des mesures de sécurité[509].

Les enseignements de l'affaire Desjardins

À titre d'illustration récente et marquante au Québec, examinons les leçons à tirer de l'affaire Desjardins, où le CPVP, au terme de son enquête, a conclu aux manquements de Desjardins à ses obligations de sécurité en vertu du principe 4.7 de la LPRPDE.[510] Il a jugé insuffisantes les mesures de protection en place entre 2017 et 2019, tant au niveau de ses politiques et procédures, de la formation et de la sensibilisation des employés, des contrôles d'accès et de la séparation logique, que de la surveillance et du contrôle.[511]

Au niveau des politiques et procédures : Le CPVP a considéré que les enquêtes de sécurité menées auprès des employés étaient nécessaires, mais insuffisantes en l'espèce, et qu'elles devaient être complétées par des politiques, des formations et des mesures de contrôle[512] permettant de

[506] Projet de loi C-27, art. 57(1).
[507] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 30, par. 2.
[508] Infra, 6.2.1.4.
[509] Projet de loi C-27, art. 57(3) : « Les mesures de sécurité protègent les renseignements personnels contre, notamment, la perte ou le vol ainsi que l'accès, la communication, la copie, l'utilisation ou la modification non autorisés et elles comprennent notamment des mesures raisonnables d'authentification de l'identité de l'individu auquel ces renseignements se rapportent. »
[510] 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,* Conclusions en vertu de la LPRPDE n°2020-005, op. cit., note 71, par. 84.
[511] *Id*., par. 83.
[512] *Id*., par. 46.

vérifier si ces politiques et procédures de sécurité étaient bien suivies par les employés.[513] En effet,

> « [a]u moment de l'atteinte, Desjardins disposait d'une diversité de directives, politiques et procédures liées à la protection des renseignements personnels. Toutefois, dans plusieurs instances, Desjardins n'avait pas assuré la mise en œuvre de certaines directives, politiques ou procédures qu'elle avait adoptées. »[514][Mon soulignement]

Au niveau de la formation et de la sensibilisation des employés : Le CPVP a constaté des lacunes importantes dans l'obligation de sensibilisation et de formation des employés quant aux politiques et procédures pourtant en place :

> « (…) des employés avec des droits d'accès légitimes ont déposé des fichiers dans des sous-dossiers du répertoire partagé accessible à l'ensemble des employés de l'équipe marketing. Ces actions constituaient des traitements non conformes aux politiques et procédures de Desjardins et n'observaient pas les meilleures pratiques de travail. Ceci soulève la question de savoir si la formation offerte les a suffisamment sensibilisés quant à l'importance de préserver la confidentialité des renseignements personnels ainsi qu'à la gravité des conséquences de les rendre accessibles à des tiers non autorisés. »[515]

Or, soulignons ici que la communication aux employés des différentes politiques d'entreprise, non seulement en matière de sécurité et de confidentialité, mais également en matière de prévention du harcèlement et de diversité, équité, inclusion par exemples, est un défi que je constate chez bon nombre d'entreprises de toute taille, non pas par mauvaise foi, mais bien souvent par manque de temps et de ressources surtout dans un contexte de pénurie de main d'œuvre. La communication de ces politiques est centrale et l'intégration de cette communication dans les entrevues d'intégration lors d'une embauche, d'évaluation périodique, de formation continue et d'entrevue de fin d'emploi sont des exemples de moments clés selon moi où ces politiques devraient être communiquées et rappelées.

Au niveau du contrôle des accès et de la séparation logique : Le CPVP a constaté des accès non-autorisés qui auraient pu être empêchés si la technique de *tokenisation* recommandée par l'organisation avait été mise en place :

---

[513] *Id.*, par. 49.
[514] *Id.*, par. 56.
[515] *Id.*, par. 62.

> « (…) le système d'information de Desjardins permettait aux utilisateurs autorisés de déplacer des données à accès restreint vers des répertoires et des supports de stockage non protégés, et ce sans aucun contrôle (voir paragraphes 10 et 11). [Or] Desjardins aurait pu réduire l'exposition des données si ces dernières avaient été substituées par des données non confidentielles (masquées). Par exemple, en utilisant la technique de segmentation en unités (*tokenization*) tel que recommandé par le standard de sécurité sur la protection des données de Desjardins. »[516] [Mes soulignements]

Ainsi, le CPVP conclut que « Desjardins ne gérait pas efficacement les droits d'accès et les habilitations, qui sont des mesures de sécurité importantes, enfreignant ainsi le principe 4.7 de la LPRPDE. »[517] [Mes soulignements]

Au niveau de la surveillance et du contrôle : L'enquête du CPVP a révélé que la surveillance et le contrôle que devaient exercer Desjardins proportionnellement à la nature des données traitées étaient insuffisants. Bien que Desjardins eût été avisée en mai 2018 via un rapport d'une firme externe des failles de son système en matière de sécurité informatique et du risque élevé de faille telle qu'elle est finalement survenue, sa solution DLP (*data loss prevention* / prévention de la perte de données) n'est demeurée que partiellement déployée.[518]

De surcroit, le CPVP a remarqué que Desjardins aurait dû adopter des mesures de surveillance techniques actives et que les mesures passives n'étaient pas suffisantes considérant la nature des renseignements en question :

> « En plus de la DLP, plusieurs approches techniques [comme le système de gestion de l'information et des événements de sécurité (SIEM) et l'analyse des comportements des utilisateurs et entités (*user and entity behaviour analytics* ou UEBA)][519] peuvent être utilisées pour assurer la surveillance active des systèmes électroniques d'information. Cette approche proactive génère des alertes si l'analyse des journaux des événements révèle des comportements anormaux. [Or] Desjardins se contentait de mesures passives telles que l'analyse des journaux des événements après que des incidents aient été rapportés. Nous sommes d'avis que Desjardins aurait pu prévenir ou minimiser la fuite de données si elle avait optimisé l'utilisation de ces outils [SIEM et UEBA]. »[520] [Mon soulignement]

[516] *Id.*, par. 68.
[517] *Id.*, par. 70.
[518] *Id.*, par. 75-76.
[519] *Id.*, par. 77-78.
[520] *Id.*, par. 76.

Le CPVP conclut à une infraction à 4.7 de la LPRPDE en raison de la faiblesse et de l'insuffisance des mesures en place pour protéger un haut volume de renseignements sensibles :

> « (…) les faiblesses particulières décrites ci-dessus, individuellement et collectivement, constituent des manquements à la mise en œuvre de mesures de sécurité appropriées compte tenu du volume et de la sensibilité des renseignements personnels détenus par Desjardins. Par conséquent, Desjardins a enfreint le principe 4.7 de la LPRPDE. »[521]

Il émet ensuite une série de recommandations à Desjardins, dont la plus importante, pour les fins de la présente section, est de fournir un rapport décrivant notamment :

- Les mesures de protection organisationnelles, contractuelles et techniques[522], incluant « (…) [l]es protections additionnelles pour prévenir que la présence de renseignements personnels sur les ordinateurs des employés, suite à des transferts autorisés, ne soit à l'origine d'autres atteintes »[523], ainsi que leur fréquence de révision;[524]
- « Les indicateurs et les outils de surveillance et de contrôle permettant de vérifier l'efficience des mesures déployées »;[525]
- Les risques résiduels et la manière de les gérer;[526]
- Finaliser son calendrier de conservation des données et sa procédure de destruction, et d'y préciser les motifs à l'appui des durées de conservation établies par Desjardins
- Démontrer la surveillance des demandes d'accès et des transferts;[527]
- Dépersonnaliser ou supprimer les RP une fois arrivés à la fin de leur période de conservation déterminée;[528]
- Engager une firme de vérification externe afin d'auditer le programme de sécurité de Desjardins et de produire un rapport détaillé au CPVP.[529]

[521] *Id.*, par. 84.
[522] *Id.*, par. 124 a) ii).
[523] *Id.*, par. 124 e).
[524] *Id.*, par. 124 a) v).
[525] *Id.*, par. 124 a) iv).
[526] *Id.*, par. 124 a) vi).
[527] *Id.*, par. 124 d).
[528] *Id.*, par. 124 b) et c).
[529] *Id.*, par. 125.

Ainsi, ce que met en lumière cette affaire est l'importance de ne pas sous-estimer les menaces internes, intentionnelles ou non. Bon nombre d'entreprises investissent temps et argent pour protéger les renseignements personnels sous leur contrôle contre les attaques externes, alors que des failles internes peuvent aussi menacer les données conservées.

Cette affaire nous rappelle également qu'une entreprise ne peut se contenter de produire des politiques et se fier aveuglément au professionnalisme, à la compétence et à la bonne foi de ses employés. Elle doit être active dans la vigie du respect de ses politiques, tant par l'éducation de ses employés (formation, sensibilisation) que par l'implantation d'outils informatiques permettant la gestion de la conservation des données et de leur accès (durée de la conservation, modalités de transfert et de destruction, gestion des accès, vigie et signalement des bris de sécurité, etc.).

En outre, soulignons qu'un autre élément intéressant dans cette affaire est que les besoins marketing de l'entreprise ont, d'une certaine façon, participé à cet incident de confidentialité.

Ce cas ne traite pas spécifiquement de PCL, mais les enseignements demeurent applicables à toutes entreprises. Toute entreprise qui participe à un système de PCL devra s'assurer de respecter toutes ces obligations. Le défi toutefois sera de cartographier le cycle de vie des renseignements personnels, c'est-à-dire en faire l'inventaire, identifier leur « trajectoire » à travers les différents systèmes, fournisseurs de services et entreprises tiers, puis de veiller à ce que les mesures appropriées soient mises en place, tant dans la documentation (politiques et contrats) qu'en pratique. En outre, différentes approches peuvent être envisagées pour réduire les risques d'incidents et leurs conséquences préjudiciables, notamment la *data minimization*[530] et la segmentation des données ainsi que leur dépersonnalisation, voire leur anonymisation dans la mesure du possible[531], afin de rendre les personnes visées moins vulnérables à un vol d'identité par exemple.

[530] Supra, 4.2. et 4.3. ; TRENDMICRO, « Data Minimization », en ligne : <https://www.trendmicro.com/vinfo/us/security/definition/Data-Minimization> (consulté le 29 avril 2023)
[531] Supra, 3.2.

5.3.2. Rehaussement plus strict au Québec

Au Québec, les organisations sont tenues à des exigences similaires sur le fond à celles prévues par le régime fédéral actuel et bonifié par le Projet de loi C-27. Ainsi, le principe d'assurer la sécurité des RP traités est énoncé à l'article 10 de la Loi sur le privé, qui n'a pas été modifié par la Loi 25, et qui prévoit que

> « [t]oute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. » [Mes soulignements]

Nouveau régime de notification des atteintes

Le nouvel article 3.6 de la Loi 25 est venu mettre un place un régime de notification des atteintes aux mesures de sécurité, complété en 2022 par un règlement, similaire au règlement fédéral, dans le but de préciser les informations qui doivent être transmises dans les avis à la CAI et aux personnes concernées en cas d'incident, et incluses dans le registre des incidents de confidentialité requis par la loi.[532]

Définition large d'incident : Soulignons que l'article 3.6 de la Loi 25 prévoit une définition d'incident de confidentialité plus large que celle prévue dans le Projet de loi C-27, étant décrite comme « l'accès non autorisé par la loi à un renseignement personnel », « l'utilisation non autorisée par la loi d'un renseignement personnel », « la communication non autorisée par la loi d'un renseignement personnel » et « la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement »[533], ce qui a pour conséquence d'inclure « l'hameçonnage, le déploiement de logiciels malveillants, les attaques par rançongiciel, les botnets, les attaques par force brute, l'envoi de renseignements personnels à une mauvaise

[532] *Règlement sur les incidents de confidentialité*, (2022) 154 G.O., II, 6819, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2022F/78638.pdf>

[533] Loi 25, art. 3.6.

adresse courriel, etc. ».[534] Une telle définition pourrait avoir pour effet d'inclure les utilisations marketing non-autorisée sans être toutefois effectuée à des fins malveillantes, ce qui constituera un défi supplémentaire pour les organisations :

> « Il est intéressant de souligner que le Québec est la seule juridiction au Canada à inclure l'utilisation non autorisée de renseignements personnels dans sa définition d'incident de confidentialité. Cette inclusion pourrait engendrer des difficultés d'interprétation, à savoir si une utilisation sans consentement à des fins marketing, par exemple, puisse être considérée comme un « incident de confidentialité ». Bien qu'une telle interprétation puisse conduire à une surabondance de notifications des incidents à la CAI et aux individus concernés, les entreprises devront faire preuve de jugement dans leur évaluation du risque de préjudice […]. »[535]

Avis d'incident à CAI : De plus, remarquons que l'avis d'incident à la CAI prévu à l'article 3 du règlement est plus détaillé et complexe que celui sous le régime fédéral, devant contenir une liste complète d'information concernant l'incident, soit : 1) le nom de l'organisation (et son NEQ le cas échéant); 2) le nom et les coordonnées de la personne à contacter au sein de l'organisation; 3) une description des renseignements personnels visés par l'incident ou la raison expliquant l'impossibilité de la fournir; 4) une description des circonstances entourant l'incident ainsi que sa cause si connue; 5) la date ou période ou approximation de cette période pendant laquelle l'incident est survenu; 6) la date ou période au courant de laquelle l'organisation a pris connaissance de l'incident; 7) le nombre de personnes concernées par l'incident et le nombre (ou approximation) de résidents québécois parmi elles; 8) une description des éléments ayant mené l'organisation à conclure qu'il existe un risque de préjudice sérieux (par exemples, la sensibilité des renseignements, les utilisations malveillantes possibles, les conséquences appréhendées et la probabilité d'une utilisation à des fins préjudiciables); 9) les mesures mises en place ou qui le seront par l'organisation, ainsi que la date où les personnes ont été avisées ou le délai d'exécution envisagé; 10) les mesures prises ou qui seront prises suite à l'incident dans le but de diminuer les risques qu'un préjudice soit causé ou à atténuer ce préjudice, et les mesures visant à éviter de

[534] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit*., note 421, p. 46.
[535] *Id*., p. 46, dernier paragraphe.

tels préjudices dans le futur ainsi que les délais d'exécution de ces mesures; 11) une mention à l'effet qu'une personne ou organisme hors Québec ayant des responsabilités semblables à celles de la CAI a été avisé de l'incident le cas échéant.

Avis aux personnes concernées : L'avis aux personnes concernées par un incident quant à lui dont contenir une version allégée de l'avis à la CAI, très semblable à l'avis requis sous le régime fédéral, soit : 1) une description des renseignements touchés; 2) une description des circonstances de l'incident; 3) la date ou période de l'incident, ou une approximation; 4) une description des mesures prises ou qui seront prises pour diminuer le risque d'un préjudice ou l'atténuer; 6) les coordonnées permettant à la personne concernée de se renseigner davantage sur l'incident.[536] En outre, de manière similaire au régime fédéral, cet avis devra plutôt être donné au moyen d'un avis public lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée, ou encore de représenter une difficulté excessive pour l'organisation, ou si l'organisation n'a pas les coordonnées de la personne concernée.[537] Les mêmes éléments que l'avis privé à la personne concernée devront être inclus dans cet avis public puisque le règlement n'apporte pas de nuance dans ce cas. Le règlement ne précise pas un moyen de transmission en particulier, mais indique plutôt que l'avis public « peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée. »[538] Cette rédaction large m'apparait souhaitable puisque susceptible de mieux évoluer dans le temps avec l'évolution rapide des médias et des technologies, en plus de permettre à chaque organisation de déterminer le ou les meilleurs moyens et médias eu égard aux circonstances.

Avis public : Par ailleurs, le règlement précise également qu'un avis public peut être fait en sus d'un avis privé à la personne concernée, si l'organisation juge approprié de le faire pour rapidement diminuer le risque qu'un préjudice sérieux soit causé ou pour pouvoir l'atténuer.[539]

Registre des incidents : Concernant le registre des incidents de confidentialité, le règlement prévoit à son article 7, qu'il doit contenir : 1) une description des renseignements personnels visés

[536] *Id*., art. 5.
[537] *Id*., art. 6, al. 2.
[538] *Id*., art. 6, al. 4.
[539] *Id*., art. 6, al. 3.

par l'incident ; 2) une description des circonstances; 3) la date ou période de l'incident ; 4) la date ou période de prise de connaissance de l'incident par l'organisation ; 5) le nombre de personnes concernées; 6) une description des éléments menant l'organisation à conclure qu'il existe ou non un risque de préjudice sérieux aux personnes concernées; 7) si l'incident présente un risque de préjudice sérieux : les dates de transmission des avis à la CAI et aux personnes concernées et une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été le cas échéant; 8) une description des mesures prises par l'organisation suite à l'incident pour diminuer les risques de préjudice.[540] Finalement, il précise que ces renseignements doivent être tenus à jour et conservés pendant au moins cinq (5) ans suivant la connaissance de l'incident par l'organisation[541], soit trois ans de plus qu'au fédéral.

Ainsi, ce règlement apporte des précisions importantes pour orienter les organisations dans leurs efforts non seulement de documentation, mais plus profondément dans leurs efforts d'opérationnalisation de leurs obligations et d'implantation de nouveaux processus internes et de culture de cybervigilance et de cybersécurité. Comme je l'expliquais plus haut dans le contexte du régime fédéral, une structure claire et une procédure rigoureuse, constante et minutieuse permettront aux organisations de diminuer les risques d'incidents et d'atténuer les préjudices en cas d'incidents touchant tant les renseignements personnels sous leur contrôle.

Cette première phase d'entrée en vigueur de la Loi 25 en septembre 2022 complété par l'entrée en vigueur du règlement en décembre 2022, intégrant la mise en place de ce registre des incidents, un régime de notification des incidents et la nomination d'un responsable à la protection des renseignements personnels, est une première étape logique vers un changement de culture et de pratiques majeur, mais nécessaire. Elle s'attaque à deux des principaux enjeux en matière de vie privée auxquels il est urgent de s'attaquer : le vol d'identité et la fraude.

Une des causes est que trop d'organisations conservent – encore – trop de renseignements, et ce trop longtemps. Les erreurs humaines créées par la rapidité des échanges et des transactions, le manque de personnel au sein des organisations, le manque d'éducation tant des employés que

[540] *Id.*, art. 7.
[541] *Id.*, art. 8.

des individus, et parfois le manque de volonté de ces mêmes acteurs, augmentent assurément les risques et les conséquences (préjudices) liés à un incident.

Il est vrai que les attaques et les tentatives d'hameçonnage – de plus en plus raffinées et subtiles – peuvent provenir de l'externe et que les systèmes doivent être adéquatement surveillés et protégés. Toutefois, l'affaire Desjardins nous a montré qu'une mauvaise application d'un processus interne pourtant clair et documenté peut mener à des situations dommageables et extrêmement fâcheuses tant pour les individus que pour les organisations qui doivent maintenir la confiance de leurs clients et de leurs partenaires commerciaux.

Obligations dans le cadre d'un contrat de fourniture de services : comparaison entre le Projet de loi C-27 et la Loi 25

La deuxième phase d'entrée en vigueur de la Loi 25 le 22 septembre 2023 sur les mesures de sécurité comporte également son lot de défis.

À l'instar des articles 11(2), 57, 61 et 68 du Projet de loi C-27, le nouvel article 18.3 de la Loi 25 intègre des dispositions spécifiques précisant les obligations des fournisseurs de service et conséquemment des clauses contractuelles qui doivent être incluses dans les contrats entre une organisation et un fournisseur si un transfert de renseignements personnels est nécessaire dans le cadre du mandat ou du contrat avec ce fournisseur. C'est obligation était de mettre en place les mesures de sécurité nécessaires et la seconde étant de notifier l'organisation en cas d'atteinte. Toutefois, loi québécoise est non seulement plus précise, mais également plus exigeante dans la mesure où 18.3(1)2°) prévoit :

> « Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service ou d'entreprise visé au premier alinéa doit aviser sans délai le responsable de la protection des renseignements personnels de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et il doit également permettre au responsable de la

protection des renseignements personnels d'effectuer toute vérification relative à cette confidentialité.»[542]

En conséquence, il ne s'agit pas seulement d'aviser l'organisation-cliente lorsqu'il y a un incident aux mesures de sécurité, mais également lorsqu'il y a eu violation ou tentative de violation à la confidentialité des renseignements, ce qui a le potentiel de couvrir de nombreuses situations. De plus, le responsable à la protection des renseignements personnels de l'organisation-cliente devra personnellement être avisé afin qu'il puisse procéder aux vérifications nécessaires. Sur ces deux éléments, il a été soulevé à juste titre qu'il n'est pas clair si l'organisation-cliente et son fournisseur de services pourront aménager dans leur contrat les conditions auxquelles ces obligations seront soumises, par exemple de limiter l'obligation de notification aux incidents de confidentialité, ou de préciser la fréquence et les conditions des vérifications par le responsable à la protection des renseignements personnels de l'organisation-cliente.[543]

Arrimer les articles 18.3 de la Loi 25 avec les articles 57 et 61 du Projet de loi C-27 et concilier leurs différences dans des clauses contractuelles demandera une réflexion de la part des entreprises. Ceci constitue malheureusement un exemple parmi tant d'autres du défi que représente la compréhension et l'opérationnalisation des obligations pour les entreprises qui font affaires au Québec et au Canada.

5.4. Obligation en matière de transferts transfrontaliers hors Québec et hors Canada

Passons maintenant à la question des transferts transfrontaliers, sujet inévitable dans un contexte de PCL en contexte nord-américain[544]. Je propose maintenant d'examiner la question de l'application territoriale de la LPRPDE et de la Loi 25, puis d'en analyser les exigences pertinentes.

[542] Notons que 18.3(3) prévoit que lorsque le mandataire est un organisme public ou un membre d'un ordre professionnel, les exigences de 18.3(2) ne sont pas applicables.
[543] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit*., note 421, p. 40.
[544] Infra, chapitre 1 et 2.5.

5.4.1. Zone grise quant au champ d'application territorial de la LPRPDE et de la Loi 25 aux flux transfrontaliers hors du Canada

La LPRPDE « s'applique aux organisations qui exercent des activités commerciales au Canada dans les provinces qui n'ont pas édicté une loi "essentiellement similaire" sur la protection des renseignements personnels dans le secteur privé, et dans toutes les provinces et tous les territoires dans le cas des organisations qui sont de compétence fédérale ».[545]

Les trois provinces qui détiennent actuellement un décret d'exclusion à la LPRPDE sont le Québec[546], l'Alberta[547] et la Colombie-Britannique[548], ayant toutes trois adopté des lois en matière de protection des renseignements personnels qui ont été reconnues comment étant essentiellement similaires à la partie 1 de la LPRPDE. En conséquence, en vertu de l'article 1 de ces trois décrets, toute organisation, autre qu'une entreprise fédérale, qui est assujettie à la *Personal Information Protection Act* (Alberta)[549], à la *Personal Information Protection Act* (Colombie-Britannique)[550] ou à la *Loi sur la protection des renseignements personnels dans le secteur privé* (Québec)[551] et qui exploite une entreprise au sens de l'article 1525 CCQ, est exclue de l'application de la partie 1 de la LPRPDE à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels qui s'effectuent à l'intérieur de ces provinces.

À titre d'illustration, dans une affaire récente, le CPVP a confirmé :

> « (…) il devient de plus en plus impératif que les activités des entreprises technologiques qui sont actives au-delà des frontières respectent les obligations en matière de protection des renseignements personnels dans tous les territoires de compétence où elles exercent

[545] Miguel BERNAL-CASTILLERO et Nancy HOLMES*, Les lois fédérales du Canada sur la protection de la vie privée*, *op. cit*., note 124, par. 4.
[546] *Décret d'exclusion visant des organisations de la province de Québec*, DORS/2003-374, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://laws-lois.justice.gc.ca/fra/reglements/DORS-2003-374/page-1.html > (consulté le 15 janvier 2023)
[547] *Décret d'exclusion visant des organisations de la province d'Alberta*, DORS/2004-219, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : < https://laws-lois.justice.gc.ca/fra/reglements/DORS-2004-219/page-1.html > (consulté le 15 janvier 2023)
[548] *Décret d'exclusion visant des organisations de la Colombie-Britannique,* DORS/2004-220, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : < https://laws-lois.justice.gc.ca/fra/reglements/DORS-2004-220/page-1.html > (consulté le 15 janvier 2023)
[549] *Personal Information Protection Act*, S.A. 2003, ch. P-6.5
[550] *Personal Information Protection Act*, S.B.C. 2003, ch. 63
[551] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1

> leurs activités. »[552] Ainsi, « [m]ême si les renseignements ont été recueillis dans un autre territoire de compétence, que ce soit au Royaume-Uni ou aux États-Unis, AIQ est toujours tenue de s'acquitter de ses obligations liées au traitement de ces renseignements au Canada, en vertu des lois canadiennes. »[553] [Mes soulignements]

Bien que le champ d'application territorial respectif de la loi fédérale canadienne et des lois provinciales essentiellement similaires puisse sembler clair, force est de constater que le sujet n'est pas sans ambigüité concernant la loi québécoise. En effet, un débat subsiste à savoir si c'est la loi québécoise ou la loi fédérale qui trouve application par rapport aux transferts à l'extérieur du Canada. Cette ambigüité a d'ailleurs été soulevée par le Groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel en 2014[554], qui résumait ainsi, en 2014, le débat juridique :

> « En ce qui concerne le champ d'application territorial, la décision de la Commission européenne constatant le niveau de protection adéquat de la protection accordée par la LPRPDE indique notamment qu'"[à] chaque fois qu'une province adoptera une loi essentiellement similaire, les organisations, catégories d'organisations ou activités couvertes seront exclues de l'application du droit fédéral pour les transactions intraprovinciales; la loi fédérale continuera de s'appliquer à toutes les collectes, utilisations et communications interprovinciales et internationales de renseignements personnels ainsi qu'à tous les cas où les provinces n'ont pas adopté, en tout ou en partie, de loi essentiellement similaire ". Cette position est semblable à celle adoptée par le Commissariat à la protection de la vie privée du Canada.
>
> Toutefois, la CAI considère que dans le cas de transactions interprovinciales et internationales, tant la LPRPDE que la loi québécoise s'appliquent. La CAI explique en effet qu'au Canada, la loi constitutionnelle de 1867 organise le partage des compétences entre

---

[552] 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 d'AggregateIQ Data Services Ltd*., Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, *op. cit.,* note 72, par. 2.

[553] *Id*., par. 6.

Il s'agit d'une enquête conjointe avec le CPVP menée avec le Commissariat de la Colombie-Britannique concernant *AggregateIQ Data Services Ltd*. Dans cette affaire, il s'agissait d'une entreprise de Colombie-Britannique qui utilisait et communiquait des renseignements personnels de citoyens canadiens, américains et britanniques, notamment des renseignements de profils psychographiques tirés des données de *Facebook* obtenues par *Cambridge Analytica* et *SCL Elections*, au moyen d'une application tierce, afin de fournir des services liés aux données dans le cadre de campagnes politiques pour le compte de clients situés dans le monde entier.

[554] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, 4 juin 2014, en ligne : <https://www.dataprotection.ro/servlet/ViewDocument?id=1290 > (consulté le 15 janvier 2023)

Note : « Le groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. » : *Id*., p. 1.

les gouvernements fédéral et provinciaux et que l'article 92, paragraphe 13, dispose que "[d]ans chaque province, la législature pourra exclusivement faire des lois relatives aux matières tombant dans […] la propriété et les droits civils dans la province ". La CAI considère en outre que la notion de " propriété et droits civils dans la province " renvoie à toute relation entre personnes physiques et inclut le droit à la protection de la vie privée, qui comprend le droit à la protection des données à caractère personnel. En effet, l'article 3 et les articles 35 à 41 du Code civil québécois prévoient des dispositions sur la protection de la vie privée et des données.

En outre, la loi québécoise a pour objet d'établir " des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil " (article 1er).

En conclusion, les positions prônées par l'État fédéral et la province sur le champ d'application de la loi québécoise divergent. Si le Commissariat à la protection de la vie privée du Canada considère que la législation fédérale s'applique aux transferts tant interprovinciaux qu'internationaux des renseignements personnels, la CAI considère que la loi québécoise s'applique toujours aux situations internationales. Cette divergence d'interprétation entre le Commissariat à la protection de la vie privée du Canada et la CAI n'est pas nouvelle étant donné qu'en 2003, à la suite de l'adoption de la LPRPDE, la Cour d'appel du Québec a été saisie de la question de savoir si la compétence exclusive de la LPRPDE pour les entreprises fédérales était anticonstitutionnelle. À ce jour, la Cour d'appel du Québec n'a toujours pas statué.

[…]

Le groupe de travail considère dès lors qu'il est nécessaire de clarifier le champ d'application territorial de la loi québécoise avant que la Commission européenne n'apprécie si ce texte assure un niveau de protection adéquat. »[555]

[Références omises, mes soulignements]

Depuis cette publication, la Cour d'appel du Québec n'a toujours pas statué sur cette question, et la Commission ne semble pas s'être prononcée sur le statut d'adéquation du Québec. Dans l'intervalle, certains praticiens appliquent l'interprétation fédérale voulant que la LPRPDE « (…) s'applique aux organisations du secteur privé au niveau fédéral, mais aussi lorsque les renseignements personnels sont divulgués au-delà des frontières provinciales ou internationales »[556], alors que d'autres préfèreront appliquer les deux.

[555] *Id.*, p. 4 et 5.

[556] Par exemple : Caroline JONNAERT et Élisabeth LESAGE-BIGRAS, « Cookies et vie privée : ce que toute organisation devrait savoir », *op. cit.*, note 15, par. 3.

5.4.2. Au Canada

Voyons maintenant les principales exigences énoncées par la LPRPDE, les exigences proposées par le CPVP, puis les dispositions clés du Projet de loi C-27 en matière de transferts transfrontaliers.

En résumé, la LPRPDE prévoit que les organisations au Canada peuvent transférer des renseignements personnels à des tierces parties à des fins de traitement, mais elles demeurent responsables de la protection de ces renseignements, et doivent assurer un degré de protection comparable, par voie contractuelle ou autre.[557]

Les lignes directrices toujours en vigueur à ce jour, et ce depuis 2009, sur le transfert transfrontalier des renseignements personnels[558] (ci-après les « lignes directrices de 2009 ») sont venues préciser comment la LPRPDE s'applique à ces transferts, tant à des tierces parties au Canada qu'à des tierces parties hors du Canada. Ainsi, le principe 1 des lignes directrices de 2009 prévoit :

> « 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. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. »[559] [Nos soulignements]

Notons que le CPVP parle de prendre les moyens raisonnables[560] donc d'une obligation de moyens et non de résultats.

Le CPVP précise ensuite que les renseignements ainsi transférés « ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été recueillis à l'origine »[561], par exemple dans le contexte où une organisation impartit certains de ses processus à une tierce partie[562]. Il précise également que le terme « traitement » est interprété comme signifiant toute « utilisation » desdits renseignements

---

[557] LPRPDE, annexe 1, principe 4.1.3.
[558] CPVP, *Transfert frontalier de renseignements personnels*, 27 janvier 2009, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/> (consulté le 2 avril 2023)
[559] *Id*.
[560] *Id*.
[561] *Id*., par. 10.
[562] *Id*.

et non toute « communication »,[563] ce qui signifie que « [s]i les renseignements sont utilisés aux fins auxquelles ils ont été recueillis, aucun consentement supplémentaire n'est requis pour procéder au transfert. »[564] Un exemple éloquent de cette distinction est le cas de l'affaire *Home Depot*[565].

Quant au degré de protection comparable, il s'agit d'avoir l'assurance[566] d'un degré de protection équivalent -donc sans être nécessairement le même- à celui dont aurait bénéficié les renseignements s'ils n'avaient pas été transférés à une tierce partie.[567] Le meilleur moyen selon le CPVP pour s'en assurer est par voie contractuelle,[568] en y incluant par exemple différentes certifications ou normes techniques, et des obligations réciproques comme la mise en place d'un processus immédiat de collaboration visant à réduire les conséquences en cas d'atteinte aux mesures de sécurité comme nous l'avons vu plus haut.

Pour rencontrer ces obligations, le CPVP recommande aux organisations du Canada d'évaluer au préalable les risques d'atteinte à l'intégrité, à la sécurité et à la confidentialité des renseignements personnels de leurs clients suite au transfert.[569] Cela requière donc de s'informer correctement tant sur l'organisation tierce que sur le pays où se trouve cette organisation avant de procéder à un accord pour l'utilisation ou la communication de de renseignements personnels afin de s'assurer principalement que les processus, politiques et mesures de sécurité nécessaires sont bien en place, que le personnel est correctement formé, pouvant aller jusqu'à la vérification et à l'inspection de ces mesures si les circonstances le justifient. Le pays et/ou l'État où se trouve l'organisation tierce devrait également faire partie des considérations de l'organisation du Canada et du Québec, dans la mesure où une organisation située dans un régime étranger instable représente un risque supplémentaire à considérer.[570] Ajoutons également à cette liste

[563] *Id*., par. 28
[564] *Id*., par. 12
[565] Supra, 5.1.1, 5.2.1 et 5.2.2.
[566] CPVP, *Transfert frontalier de renseignements personnels*, *op. cit*., note 558.
[567] *Id*., par. 12
[568] *Id*., par. 28
[569] *Id*., par. 28
[570] *Id*., par. 22

les états totalitaires comme la Russie et la Chine, et pensons à l'exemple récent de l'interdiction aux fonctionnaires américains et canadiens d'utiliser *TikTok*[571].

Finalement, en 2009, le CPVP recommandait que les organisations soient transparentes envers leurs consommateurs au sujet de leurs pratiques de transfert.[572] Ainsi,

> « [l]es organisations doivent aviser leurs consommateurs de façon claire et compréhensible que leurs renseignements personnels pourraient être traités dans un pays étranger, et que les organismes d'application de la loi et de sécurité nationale de ce pays pourraient y accéder. Idéalement, cela devrait être fait au moment de la collecte des renseignements. Une fois que des consommateurs avertis décident de faire affaire avec une entreprise, ils ne peuvent s'opposer à ce que leurs renseignements personnels soient transférés. »[573]

Par la suite, à l'issue des dernières consultations menées par le CPVP concernant le transfert transfrontalier des renseignements personnels aux fins de traitement, ce dernier avait annoncé maintenir les lignes directrices actuelles. Bien qu'il jugeât que « les mesures de protection de la vie privée actuelles sont clairement insuffisantes »[574], il préférait plutôt attendre la révision de la LPRPDE pour renforcer ces mesures. En effet, dans son annonce du 23 septembre 2019, le CPVP rappelait la conclusion de la Cour d'appel fédérale dans la décision de 2004 *Englander* c. *Telus Communications Inc*. :

> « [E]n raison du " caractère non législatif " de la rédaction de la LPRPDE et du fait que cette loi " est un compromis sous le rapport aussi bien de la forme que du fond ", qu'une règle spéciale d'interprétation s'applique à cet égard. La Cour a précisé ce qui suit : " L'annexe 1 ne se prête pas à l'interprétation rigoureuse habituellement possible. Cela étant, la meilleure solution pour la Cour est de se confier aux critères de la souplesse, du sens commun et du pragmatisme. "»[575]

---

[571] LA PRESSE CANADIENNE, « Le gouvernement canadien interdit l'application TikTok sur ses cellulaires », *Les affaires* (27 février 2023), en ligne : <https://www.lesaffaires.com/techno/internet/le-gouvernement-canadien-interdit-l-application-tiktok-sur-ses-cellulaires/639468> (consulté le 28 avril 2023)

[572] CPVP, *Transfert frontalier de renseignements personnels*, *op. cit*., note 558, par. 28.

[573] *Id*., par. 27.

[574] CPVP, « Annonce. Le Commissariat tire ses conclusions suite à la consultation sur les transferts aux fins de traitement » (23 septembre 2019), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2019/an_190923/> (consulté le 2 avril 2023)

[575] *Id*., citant *Englander* c. *Telus Communications Inc.*, 2004 CAF 387, en ligne : <https://decisions.fca-caf.gc.ca/fca-caf/decisions/fr/item/31309/index.do>

Il convient effectivement probablement mieux que ce soit le législateur qui se penche sur cette question dans le cadre d'une révision des dispositions de la LPRPDE dans son ensemble, notamment pour s'assurer du maintien des objectifs de la loi et de produire une loi révisée dont les dispositions s'harmoniseront entre elles et formeront un tout susceptible d'être plus cohérent et applicable, ce que le Projet de loi C-11, puis C-27 ont tenté de faire.

Ainsi, le Projet de loi C-27 prévoit maintenant, sous l'obligation de transparence, l'exigence de rendre accessible

> « le fait [que l'organisation] effectue ou non des transferts ou des communications de renseignements personnels interprovinciaux ou internationaux pouvant avoir des répercussions raisonnablement prévisibles sur la vie privée. »[576]

Il s'agit de la seule obligation spécifique aux transferts internationaux et interprovinciaux dans le Projet de loi.[577]

Pour compléter cette exigence de transparence, il faut plutôt se référer aux articles concernant la communication aux fournisseurs de services pour prendre connaissance des exigences incombant à l'organisation si elle fait affaire avec un tel tiers situé hors Canada. L'article 11(1) du Projet de loi prévoit que l'organisation doit veiller contractuellement ou autrement à ce que le fournisseur de services étranger offre une protection aux renseignements personnels équivalente à celle du régime fédéral canadien. Quant à lui, le fournisseur de services, étranger ou local, a l'obligation de protéger les renseignements personnels qui lui sont transférés au moyen de mesures de sécurité matérielles, organisationnelles et techniques[578] et d'aviser dès que possible l'organisation en cas d'atteinte aux mesures de sécurité[579]. Ces deux obligations spécifiques sont prévues à l'article 11(2) qui prévoit que « [l]es obligations prévues à la présente partie, à l'exception de celles prévues aux articles 57 et 61, ne s'appliquent pas au fournisseur de services relativement aux renseignements personnels qui lui sont transférés. Il est toutefois assujetti à

---

[576] Projet de loi C-27, art. 62(2)d).
[577] Elisa HENRY et Anthony HÉMOND, *Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises,* Borden Ladner Gervais – Perspectives, 6 décembre 2022, par. 3 de la section « Distinction avec le régime fédéral », en ligne : <https://www.blg.com/fr/insights/2022/12/cross-border-transfers-of-personal-information-outside-quebec > (consulté le 4 avril 2023)
[578] Projet de loi C-27, art. 57.
[579] *Id*., art. 61.

l'ensemble de ces obligations s'il les recueille, les utilise ou les communique à toutes autres fins que celles pour lesquelles ils lui ont été transférés. » Ces dispositions clarifient bien les obligations du fournisseur de services par rapport à celles de l'organisation. Elles sont un ajout important et utile pour les organisations canadiennes.

Il sera donc intéressant de voir comment le CPVP modifiera ses lignes directrices, si le Projet de loi C-27 est adopté sans plus d'exigences spécifiques concernant les transferts transfrontaliers.

5.4.3. Au Québec

La Loi 25 est venue renforcir considérablement le régime applicable en matière de transferts de renseignements personnels hors Québec, et de manière plus exigeante que la LPRPDE et le Projet de loi C-27, étant alignée avec le RGPD sur ce point. Ces dispositions entreront en vigueur à compter du 22 septembre 2023.

La Loi 25 ajoute d'abord l'exigence d'informer la personne concernée « du nom du tiers pour qui la collecte est faite, du nom du tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins visées au paragraphe 1° du premier alinéa et de la possibilité que les renseignements soient communiqués à l'extérieur du Québec. »[580] [Mes soulignements] Il ne suffit donc pas d'être transparent, mais également que la communication au tiers soit nécessaire aux fins prédéterminées.

En outre, la Loi 25 ajoute à son article 17, la nouvelle exigence de procéder avant le transfert à l'évaluation des facteurs relatifs à la vie privée (EFVP) afin de s'assurer que les renseignements bénéficient des mesures de protection adéquates.[581] Cette évaluation n'était pas obligatoire, mais recommandée sous l'actuelle Loi sur le privé.

Pour obtenir des exemples de projets qui peuvent être visés par ce type d'évaluation, notons que la CAI en 2021, dans le contexte d'application de la loi sur le privé (pré-Loi 25) a fourni des exemples de projets pour lesquels elle recommandait de procéder à l'EFVP, notamment « la mise en place ou modification d'un programme ou d'un service, recours à une technologie particulière,

[580] Loi 25, art. 8 al.2
[581] Elisa HENRY et Anthony HÉMOND, *Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises*, *op. cit.,* note 577, par. 6.

initiative publique, etc. »[582] pouvant, d'une part, impliquer le traitement de renseignements personnels, ou d'autre part, risquant d'avoir une incidence sur le respect de la vie privée des personnes[583], tels :

> « - Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service;
>
> - Chercher une nouvelle clientèle, explorer de nouveaux marchés;
> - Faire appel à un système d'algorithme ou d'intelligence artificielle;
> - Installer un système de vidéosurveillance;
> - Comparer différentes versions de bases de données ou de fichiers;
> - Acquérir ou fusionner des organisations;
> - Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc. »[584]

Concernant la norme de l'adéquation, Me Henry et Me Hémond remarquaient que cette norme a été adoptée lors de l'étude du Projet de loi article par article pour remplacer la norme plus stricte de l'équivalence proposée dans le Projet de loi 64.[585] Ainsi, l'évaluation devra se faire en tenant compte des éléments listés à l'article 17 qui se lira comme suit :

> « 17. Avant de communiquer à l'extérieur du Québec un renseignement personnel, la personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée. Elle doit notamment tenir compte des éléments suivants :
>
> 1° la sensibilité du renseignement;
>
> 2° la finalité de son utilisation;
>
> 3° les mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait;
>
> 4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.

---

[582] CAI, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, *op. cit*., note 331, p. 13.
[583] *Id*., p. 4 par. 1.
[584] *Id*., p. 4 par. 2.
[585] Elisa HENRY et Anthony HÉMOND, *Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises*, *op. cit.*, note 577, par. 5.

> La communication peut s'effectuer si l'évaluation démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus. Elle doit faire l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.
>
> Il en est de même lorsque la personne qui exploite une entreprise confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement.
>
> Le présent article ne s'applique pas à une communication prévue au paragraphe 7° du premier alinéa de l'article 18. » [Mes soulignements]

Ainsi, une organisation ne sera pas autorisée, à compter de septembre 2023, à procéder à tout transfert hors Québec sans avoir procéder à cette EFVP et sans que cette EFPV ait permis de conclure que les renseignements personnels seront adéquatement protégés.

L'article 17 inclut plusieurs éléments à analyser, constituant chacun un possible défi pour organisations qui auront à l'appliquer.

Concernant l'exigence d'évaluer le régime juridique du pays destinataire : Force est d'admettre que cela pourrait ne pas être simple. Premièrement, comme le soulignaient Me Henry et Me Hémond, cela comprend de tenir compte du caractère exécutoire des mesures contractuelles de protection, par exemple

> « si les lois d'ordre public / lois de police de l'État de réception ne permettent pas de mettre en œuvre les mesures de protection contractuelles par l'entreprise (par exemple si le régime étranger en matière de surveillance revient à nier la protection requise par les Principes de l'OCDE[586]) ou conduiraient à refuser l'exé[cution] [d']un jugement québécois enjoignant l'exécution du contrat, alors la protection offerte dans l'État de réception ne pourra vraisemblablement pas être qualifiée d'adéquate. »[587]

[586] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, 1980 (révisées en 2013), en ligne : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188 > (consulté le 23 avril 2023), ci-après « les Principes de l'OCDE »)

[587] *Id.*, par. 10.

Deuxièmement, cela pourrait impliquer de « procé[der] à une veille législative régulière des juridictions vers lesquelles les renseignements seront transférés afin, le cas échéant, de mettre à jour leurs EFVP transfert à l'instar de ce que recommande le Comité européen sur la protection des données dans ses recommandations 01/2020 » [588] et à l'instar des recommandations 2021 de la CAI[589].

Malheureusement, l'ancien projet d'article 17.1 a été aboli du Projet de loi 64, lequel chargeait le gouvernement de procéder à cette analyse :

> « 17.1. Le ministre publie à la *Gazette officielle du Québec* une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec. ».[590] [Mon soulignement]

Comme le faisait remarquer Me Gratton concernant le Projet de loi 64 :

> « L'article 17.1 du projet de loi prévoit que le gouvernement publiera une liste des États dont le régime juridique encadrant les renseignements personnels équivaut à celui du Québec. Il s'agit là d'un travail colossal. Le gouvernement a peut-être sous-estimé les efforts qui lui seraient nécessaires pour publier une telle liste exhaustive. En vertu de la législation européenne, un tel exercice d'évaluation des États étrangers est effectué par la Commission européenne après un processus long et très détaillé impliquant le Comité européen de la protection des données et les représentants des États membres. Le fait que la Commission européenne ait déclaré la LPRPDE adéquate en 2001, et la Loi sur le secteur privé inadéquate en 2014 alors qu'elle est plus contraignante que la LPRPDE à plusieurs égards illustre d'autant plus les défis posés par toute méthodologie de comparaison des lois. »[591] [Références omises]

---

[588] *Id.*, par. 11, référant à : COMITÉ EUROPÉEN SUR LA PROTECTION DES DONNÉES, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE*, version 1.0 adoptée le 10 novembre 2020 et version 2.0 adoptée le 18 juin 2021, en ligne : <https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fr.pdf > (consulté le 23 avril 2023)

[589] CAI, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, *op. cit*, note 331, p. 6.

[590] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 1re sess, 42e lég, Québec (présenté le 12 juin 2020), Art. 103 modifiant l'article 17 et 17.1, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html > (consulté le 5 avril 2023)

[591] Éloïse GRATTON, *Nos réflexions sur le projet de loi no 64 (protection sur la vie privée dans le secteur privé au Québec*, 22 septembre 2020, par. 2 de la section « II – Transferts de renseignements à l'extérieur du Québec », en ligne : <https://www.eloisegratton.com/blog/2020/09/22/nos-reflexions-sur-le-projet-de-loi-no-64-quebec-et-protection-de-la-vie-privee-dans-le-secteur-prive/ > (consulté le 5 avril 2023)

Ainsi, elle soulignait à juste titre que l'analyse de l'équivalence des différentes lois étrangères que le gouvernement s'était engagé à faire aurait été colossale et le résultat incertain, vu la complexité et l'ampleur de la tâche.[592]

Or, 17.1 ayant été retiré du Projet de loi 64, ce fardeau reposera plutôt désormais sur les organisations. Cela représentera une tâche ardue surtout pour les petites et moyennes organisations qui bénéficient de ressources et d'expertises internes plus limitées pour faire cette évaluation et l'exercice comparatif des régimes juridiques en cause, et ont des moyens financiers restreints pour payer un conseiller externe pour le faire.

Toutefois, avec le temps, nous pouvons nous attendre à ce que cette analyse se fasse éventuellement de plus en plus rapidement considérant qu'une liste des États avec un régime comparable au régime juridique québécois finira par être dressée et partagée d'une façon ou d'une autre part le secteur privé, mais fort possiblement aussi par le gouvernement lui-même puisque le secteur public est aussi soumis à cette obligation.

Ainsi, les organisations québécoises devront identifier toutes les juridictions vers lesquelles il y aura transfert de renseignements personnels[593], évaluer si ces régimes juridiques enfreignent ou non les Principes de l'OCDE[594] et

> « [p]our chacune [des juridictions] évaluer si des mesures contractuelles, organisationnelles et techniques permettraient de réduire ce risque à un niveau acceptable, permettant d'assurer une protection adéquate aux renseignements transférés »[595].

Dans un contexte de PCL, les fournisseurs de services avec qui les organisations collaborent sont principalement canadiens, américaine et de l'Union européenne. Ainsi, le RGPD et la LPRPDE (et le Projet de loi C-27) ne poseront évidemment pas problème, mais la situation américaine est plus

---

[592] *Id*., par 15

[593] Elisa HENRY et Anthony HÉMOND*, Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises*, *op. cit.*, note 577, par. 1 de la section « Piste de conformité »

[594] *Id*.; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, *op. cit*., note 586.

[595] Elisa HENRY et Anthony HÉMOND, *Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises*, *op. cit.*, note 577.

compliquée. Son analyse demeure incontournable considérant l'importance des GAFAM et à leurs outils omniprésents dans l'écosystème publicitaire et marketing numériques en général. Or, comme nous l'avons vu plus haut[596], l'arrêt *Schrems II* est venu invalider le régime de transferts de données entre l'Union européenne et les États-Unis dans le cadre du *Privacy Shield*[597], en raison de l'absence de limitation adéquate quant à l'accès par les autorités américaines aux données personnelles en vertu des programmes de surveillance, et de l'absence de recours suffisants et effectifs pour les individus concernés. En conséquence comme expliqué plus haut, pour palier à cette absence d'adéquation, la CNIL recommandait donc de mettre en place des règles d'entreprise contraignantes et des clauses contractuelles types de la Commission européenne. Dans une perspective Nord-Américaine, les entreprises canadiennes pourraient avoir à négocier les clauses contractuelles nécessaires avec les entreprises fournisseurs américaines afin de tenter de pallier, dans la mesure du possible, aux écarts entre la Loi 25 et la loi de l'état américain applicable.

Soulignons ici que cette possibilité de palier à ces écarts par le biais des clauses contractuelles n'était pas possible lors de la première version du Projet de loi 64 déposé. En effet, l'article 17(1)3° parlait seulement des « mesures de protection dont le renseignement bénéficierait ». L'ajout « y compris celles qui sont contractuelles » a été fait suite aux consultations, pendant lesquelles des juristes comme Me Gratton avaient soulevé qu'il était hautement problématique que le projet de loi ne permette pas de mécanismes alternatifs comme les clauses contractuelles types pourtant reconnues dans le régime européen[598], et rappelant que cela « (…) pourrait empêcher un bon nombre d'entreprises de transférer des renseignements personnels en dehors de la province, et ce, au détriment de l'innovation et du maintien de l'économie numérique du Québec ».[599]

Concernant le contrat avec le destinataire : Toutefois, sur ce point également, les organisations peuvent vivre certaines difficultés dans la pratique. En effet, certaines plateformes ne

[596] Infra, 2.5.3.
[597] CNIL, *Invalidation du Privacy Shield : les suites de l'arrêt de la CJUE*, en ligne : <https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue > (consulté le 16 août 2022)
[598] Éloïse GRATTON, *Nos réflexions sur le projet de loi no 64 (protection sur la vie privée dans le secteur privé au Québec*, *op. cit*., note 591, par. 2 de la section « II – Transferts de renseignements à l'extérieur du Québec »
[599] *Id.*, par. 3 de la section « II – Transferts de renseignements à l'extérieur du Québec »

fonctionnent pas avec un contrat, mais par la création d'un compte, auquel est applicable la politique de vie privée de la plateforme. La possibilité de négocier ou d'ajouter quoi que ce soit d'adapté au régime québécois, par exemple la destruction des données une fois accomplies les finalités visées, peut être complexe, voire impossible à garantir. L'organisation devra donc prendre ce facteur en considération dans son évaluation.

Concernant les « principes de protection des renseignements personnels généralement reconnus » : Me Henry et Me Hémond soulignaient que ces principes réfèrent aux principes énoncés dans les lignes directrices de 1980 et mises à jour en 2013 de l'OCDE[600], c'est-à-dire :

> « (i) limitation en matière de collecte, (ii) qualité des renseignements, (iii) spécification des finalités, (iv) limitation de l'utilisation, (v) garanties de sécurité, (vi) transparence, (vii) participation individuelle, et (viii) responsabilité. En l'absence de directive règlementaire sur l'article 17, il apparait raisonnable d'utiliser cette grille d'analyse dans le cadre d'une EFVP transfert en vertu de la Loi amendée. »[601]

Soulignons que la CAI, dans son Guide de 2021, listait l'ensemble des principes de la Loi sur le privé, soit : la détermination des fins de la collecte, la limitation, l'information aux personnes concernées, la mise en place des mesures de sécurité appropriées, la limitation de l'accès aux renseignements personnels, la limitation de leur utilisation, l'obtention du consentement à les communiquer à autrui, l'obtention du consentement à la collecte (sauf exception prévue par la loi) et assurer la qualité des renseignements (à jour et exacts au moment de leur utilisation pour une prise de décision).[602] Il faudra donc attendre les précisions règlementaires ou des lignes directrices modifiées de la CAI pour obtenir un éclaircissement plus précis applicable au Québec le cas échéant, surtout concernant l'obligation de consentement et l'obligation de l'EFVP.

---

[600] Elisa HENRY et Anthony HÉMOND, *Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises*, *op. cit*., note 577, par. 8 premier boulet; ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, *op. cit*., note 586.

[601] *Id.*, par. 8 premier boulet.

[602] CAI, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, *op. cit*., note 331, p. 13.

5.5. Documentation des pratiques et les moyens de mise en application des différentes obligations

Comme nous l'avons vu tout au long de ce mémoire, l'ensemble des obligations sont fortement liées à l'obligation de documenter, que ce soit le programme de conformité de l'organisation, la formation aux employés, les finalités prédéterminées et les finalités nouvelles et leurs acceptabilité, les renseignements personnels nécessaires et traités, leur cycle de vie (collecte, utilisation, communication, durée de conservation, destruction ou anonymisation), la technique d'anonymisation employée, l'EFVP, l'élaboration de politique de confidentialité et de protection des renseignements personnels et de pratiques et lignes directrices internes connexes, l'inclusion de clauses contractuelles avec les fournisseurs de services, les mesures de sécurité mises en place et le registre des incidents, le registre des consentements obtenus[603] et le registre des consentements retirés, etc. Cette documentation est également nécessaire à l'exercice des différents droits donné aux utilisateurs/consommateurs en vertu des lois en matière de vie privée, soit le droit à la portabilité des données, le droit à l'oubli / désindexation, le droit à l'accès, le droit à la rectification, les droits relatifs à la prise de décision automatisée[604], et le droit au retrait du consentement[605].

Cette documentation sert non seulement d'outils à l'organisation pour structurer ses efforts et incidemment correctement s'acquitter de ses obligations, mais également à démontrer cette conformité et cette responsabilisation,[606] ce fardeau lui incombant, lors d'une demande ou d'une enquête déposée auprès d'une autorité de contrôle ou d'un organisme d'autoréglementation, ou

[603] Voire des consentements réobtenus suite à un retrait de consentement, ce qui s'est observé selon le récent rapport des Normes de la publicité concernant le programme Choix de pub de la DAAC, où l'une des personnes qui avait déposé une plainte a finalement demandé conseil sur la façon d'accepter à nouveau la PCL :
LES NORMES CANADIENNES DE LA PUBLICITÉ, *Programme de responsabilité Choix de* pub, *Rapport de conformité 2022*, avril 2023, p. 9, dernier paragraphe, en ligne : <https://adstandards.ca/wp-content/uploads/Programme-de-responsabilite-Choix-de-pub-Rapport-2022.pdf > (consulté le 15 avril 2023)
[604] Supra, 5.2.2. et 5.2.3.
[605] Infra, 6.1.3.2. et 6.2.1.3.
[606] Comme le rappelaient entre autres le CPVP et les commissariats à la protection de la vie privée de l'Alberta et de la Colombie-Britannique dans : CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit.*, note 212, Principe directeur no. 7 « Être responsable : Se tenir prêt à démontrer en tout temps sa conformité ».

encore d'une poursuite judiciaire. Elle peut également permettre de démontrer un niveau de responsabilisation et de diligence susceptible de réduire les sanctions applicables.

Ainsi, l'obligation de documentation se retrouve énoncée à plusieurs reprises tant dans l'annexe I de la LPRPDE, dans le Projet de loi C-27, dans la Loi 25 et dans la loi sur le privé qui la précède, que dans le RGPD notamment. Il s'agit d'un incontournable.

PARTIE III – Perspective utilisateur

Ayant adopté, dans les parties I et II de ce mémoire, un angle descriptif et analytique axé sur la perspective des organisations, je propose maintenant d'étudier la perspective utilisateur, plus précisément son exercice de contrôle par le biais de son consentement.

Chapitre 6 – L'exercice de contrôle de l'utilisateur : analyse de l'obligation de consentement

Je propose maintenant, dans cette troisième et dernière partie, d'examiner la question du consentement. Comme nous l'avons vu plus haut, l'utilisateur bénéficie d'autres droits et mécanismes leur permettant d'exercer un certain contrôle sur leurs renseignements personnels, c'est-à-dire ceux en lien avec l'exercice des droits d'accès et de rectification, du droit d'être informé de l'existence des systèmes décisionnels automatisés[607] et du droit à la portabilité des données, de même que le droit de porter plainte auprès du responsable de la protection des renseignements personnels de l'organisation ou auprès des autorités de contrôle, et du droit privé d'action.

Faute d'espace, je ne les ai qu'effleuré dans ce mémoire. Toutefois, concernant le droit à la portabilité des données, je soulignerais le commentaire du cabinet BLG sur ce point touchant les activités publicitaires :

> « Afin de protéger les intérêts commerciaux des entreprises, y compris les algorithmes utilisés pour générer des données inférées, le droit à la portabilité des données exclut expressément de son champ d'application les renseignements personnels qui ont été créés ou inférés à partir des renseignements recueillis auprès de l'individu. Les données inférées peuvent par exemple prendre la forme de déductions sur la probabilité qu'un client achète certains produits ou services ou encore la probabilité qu'il soit intéressé à recevoir du contenu publicitaire particulier. »[608]

[607] Concernant l'implication en matière de PCL, voir Supra 5.2.2.

[608] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit.*, note 421, p. 35, par. 1

Ainsi, je me concentrai ici plutôt sur le mécanisme de contrôle en lien avec l'obligation d'obtenir un consentement valable et de permettre son retrait. Je propose de me pencher sur les paramètres légaux de l'obligation de consentement ainsi que sur ses limites dans la pratique.

6.1. Obligation d'obtenir un consentement valable : fondements et principes généraux

Le consentement est un principe pilier en droit de la vie privée et de la protection des renseignements personnels. L'obligation des organisations d'obtenir un consentement valable vise à rendre possible cet exercice de choix et de contrôle par les utilisateurs sur leurs renseignements personnels, lequel est central d'une perspective utilisateur[609], et permet d'équilibrer les différents besoins et intérêts en présence. En effet :

> « Interprétée traditionnellement comme le droit d'être laissé en paix, la notion de protection de la vie privée a pris nombre de nouvelles dimensions dans le monde actuel des technologies de pointe. Les experts l'assimilent au droit de jouir d'un espace privé, d'avoir des communications privées, de ne pas être surveillé et de voir respecté le caractère sacré de son corps. Pour la plupart des gens, il s'agit avant tout de pouvoir contrôler ce que l'on sait à leur sujet et qui a accès à ces renseignements. »[610]
>
> [Mes soulignements]

Dans son jugement de juin 2022 sur demande d'autorisation d'Option Consommateurs d'exercer une action collective contre *Google*, l'honorable juge Bisson rappelait les trois facettes du droit à la vie privée ainsi que les fondements du contrôle repris par la Cour suprême du Canada :

---

[609] Comme le rapportait Option Consommateurs en 2015 dans son rapport sur la PCL : les « (…) principales réticences [des consommateurs] ne tiennent pas nécessaire dans le fait d'être suivis ou non sur Internet; c'est plutôt l'impression que la pratique s'effectue subrepticement, sans leur autorisation, qui suscite chez eux les réactions les plus vives. »
OPTION CONSOMMATEURS, *Le prix de la gratuité. Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne ?*, Rapport de recherche réalisé par Option Consommateurs et présenté au Bureau de la consommation d'Industrie Canada, juin 201, p. 29, par. 2, en ligne : <https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf> (consulté le 22 avril 2023)

[610] Miguel BERNAL-CASTILLERO et Nancy HOLMES, *Les loi fédérales du Canada sur la protection de la vie privée*, *op. cit*., note 124, par. 1.

« [109] Même si le droit à la vie privée est une notion difficile à circonscrire, la Cour suprême du Canada, dans l'arrêt *R*. c. *Spencer*[611], a eu l'occasion de se prononcer sur les dimensions du droit à la vie privée et a indiqué que le droit à la vie privée englobe au moins trois facettes qui se chevauchent, mais qui se distinguent sur le plan conceptuel : la confidentialité, le contrôle et l'anonymat [par. 38 de *R*. c. *Spencer*]. Au sujet du contrôle, la Cour suprême du Canada rappelle ceci :

> [40] Or, le droit à la vie privée comprend également, en matière informationnelle, la notion connexe, mais plus large, de contrôle, d'accès et d'utilisation, c'est-à-dire [TRADUCTION] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes à quel moment les renseignements les concernant sont communiqués, de quelle manière et dans quelle mesure » : A. F. Westin, *Privacy and Freedom* (1970), p. 7, cité dans *Tessling*, par. 23[2]. Le juge La Forest a d'ailleurs souligné ce point dans l'arrêt *Dyment* en affirmant que la facette du droit à la vie privée en ce qui a trait aux renseignements personnels qui porte sur le contrôle « découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend » (*Dyment*, p. 429, citant *L'ordinateur et la vie privée*, le Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice (1972), p. 13). […]
>
> [...]
>
> [47] À mon avis, il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de téléphone qui figurent parmi les renseignements relatifs à l'abonné. […] [Soulignement du Tribunal] »[612]

Voyons maintenant comme les législateurs canadiens et québécois ont articulé ce contrôle autour du consentement.

6.1.1. Le principe général de consentement

La LPRPDE, le Projet de loi C-27, la Loi 25 et la Loi sur le privé qui l'a précédée, ainsi que le RGPD notamment prévoient que les organisations doivent obtenir un consentement valide de la part des individus afin d'être autorisées à collecter, utiliser ou communiquer leurs renseignements personnels. Toutefois, le degré de flexibilité par rapport aux exceptions à ce principe, permettant

[611] *R*. c. *Spencer*, 2014 CSC 43, par. 37 à 47.
[612] *Option Consommateurs* c. *Google*, 2022 QCCS 2308 (CanLII), par. 3, en ligne : <https://canlii.ca/t/jq114> (consulté le 12 février 2023)

un consentement implicite ou l'absence de consentement, varie d'une juridiction à l'autre. Je les mettrai en lumière dans le texte ci-dessous.

Tout d'abord, au niveau de la LPRPDE, l'obligation de consentement est énoncée au principe 4.3 de l'annexe I, lequel est complété par les articles 6.1, 7 et 10.2(3) de la LPRPDE, ainsi que par 4.4.2 de son annexe I. Le principe 4.3(1) de l'annexe I se lit comme suit :

> « Toute 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. » [Mes soulignements]

Dans le Projet de loi C-27, l'article 15(1) propose une formulation plus claire et concise, mais qui reprend le même principe : « Sauf disposition contraire de la présente loi, l'organisation qui recueille, utilise ou communique des renseignements personnels doit d'abord obtenir le consentement valide de l'individu concerné. »

Au Québec, l'article 14 de la Loi sur le privé - qui sera modifié à partir du 22 septembre 2023 par le nouvel article 14 de la Loi 25 - énonçait de manière claire que le principe de consentement s'appliquait à la collecte, à la communication et à l'utilisation d'un renseignement personnel :

> « 14. Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.
>
> Un consentement qui n'est pas donné conformément au premier alinéa est sans effet. »

Or, la première phrase du nouvel article 14 ne précise plus cela :

> « 14. Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.
>
> Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus est donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur.

> Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.
>
> Un consentement qui n'est pas donné conformément à la présente loi est sans effet. ».

En conséquence, il faut lire cet article avec tous les autres articles de la Loi 25 parlant du consentement, et pour ainsi constater l'absence d'article mentionnant que le consentement est requis pour une telle collecte. Ainsi, bien que l'obligation de consentement dans la Loi 25 soit omniprésente, elle est formulée à la négative et de manière indirecte. Elle se retrouve ainsi enchâssée dans l'obligation de transparence des articles 8, 8.1 et 12.1[613] et aux différents articles dressant la liste des situations où il n'est pas parmi de collecter, d'utiliser (art. 4.1, 12(1)), de transférer à des fournisseurs de services (18.3) ou de communiquer à des tiers (art. 13(1)) des renseignements personnels sans consentement, ainsi qu'aux articles listant les quelques exceptions prévues à l'obligation d'obtention du consentement (art. 3.5 (2), 12(2), 18.4, 21).

Les exigences concernant « un consentement valable », sans être nommé ainsi dans la Loi 25, sont regroupées sous l'article 14, complété par les articles 18.1, 12(1), et 13(2) sur la question de la forme de consentement requise (implicite ou expresse).

Bref, la Loi 25 aurait assurément été plus facile à analyser et à comprendre, tant pour les juristes que pour les organisations qui auront à l'appliquer, si elle avait été structurée d'une manière similaire au Projet de loi C-27. Cela aurait peut-être également permis au législateur de constater les contradictions et ambigüités qui s'y sont glissées notamment concernant la forme de consentement requise.

6.1.2. Les exceptions à l'obligation d'obtenir un consentement

La LPRPDE, le Projet de loi C-27 et la Loi sur le privé et la Loi 25 prévoient des exceptions à l'obligation de consentement, ces obligations étant plus nombreuses sous le régime fédéral.

[613] L'article 12(1) de la Loi 25 prévoit qu'« [u]n renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée ».

Les exceptions prévues par la LPRPDE

La LPRPDE prévoit plusieurs cas de figure où une organisation est autorisée à traiter des renseignements personnels à l'insu ou sans le consentement de la personne, principalement pour des questions d'ordre public ou d'administration de la justice. Ainsi, la note contenue sous 4.3 de l'annexe I de la LPRPDE prévoit de manière générale :

> « Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins du contrôle d'application de la loi, de la détection d'une fraude ou de sa prévention, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels. »

Ensuite, les alinéas 1, 2 et 3 de l'article 7 de la LPRPDE dressent une liste exhaustive d'exceptions où il est permis de collecter, d'utiliser ou de communiquer, respectivement, des renseignements personnels à l'insu de l'intéressé ou sans son consentement. D'autres exceptions s'ajoutent, notamment sous 7.2, dans un contexte de transaction commerciale, sous 7.3 dans le cadre d'une relation d'emploi ou encore sous 10.2 (3) visant une communication à une autre organisation ou à une institution gouvernementale dans le but de réduire le risque de préjudice ou de réduire le préjudice en cas d'atteinte aux mesures de sécurité.

Les exceptions plus nombreuses sous le Projet loi C-27

Le Projet de loi C-27 quant à lui vient ajouter une série d'exceptions importantes à l'obtention d'un consentement, offrant une plus grande flexibilité aux organisations, tel le transfert

(utilisation) à des fournisseurs de services,[614] l'utilisation de renseignements dépersonnalisés à des fins de recherche, analyse et développement,[615] la communication entre l'organisation avec son avocat ou son notaire,[616] entre une institution gouvernementale et un proche parent ou représentant autorisé d'une personne blessée, malade ou décédée,[617] la communication à des fins de statistiques, études ou recherches dans les paramètres précisés,[618] la collecte à des fins journalistiques, artistiques ou littéraires,[619] et la communication à des fins socialement bénéfiques.[620]

Exception des activités d'affaires : Y ont également été ajoutées les exceptions concernant certaines activités d'affaires et certaines activités légitimes. Ainsi, le Projet de loi prévoit une exception à l'obtention du consentement pour la collecte et l'utilisation en vue de réaliser une activité d'affaires auxquelles s'attendrait une personne raisonnable[621]. Il précise toutefois que cela exclut spécifiquement l'activité visant à influencer le comportement ou la décision de l'individu[622], donc la PCL et les autres types de publicités ciblées notamment, mais inclut « les activités nécessaires à la fourniture d'un produit ou à la prestation d'un service demandé par l'individu à l'organisation », « les activités nécessaires à la sécurité de l'information, des systèmes ou des réseaux de l'organisation », « les activités nécessaires pour assurer la sécurité d'un produit ou d'un service que l'organisation fournit », et « toute autre activité règlementaire », le tout « sous réserve des règlements »[623]. Comme le faisait remarquer le cabinet BLG, ces activités d'affaires n'incluent toutefois plus « les activités menées à des fins de diligence raisonnable pour réduire ou prévenir les risques commerciaux de l'organisation » qui avaient été incluses dans le Projet de loi C-11.[624]

---

[614] Projet de loi C-27, art. 19.
[615] *Id*., art. 21.
[616] *Id*., art. 25.
[617] *Id*., art. 33 et 34.
[618] *Id*., art. 35.
[619] *Id*., art. 38.
[620] *Id*., art. 39.
[621] *Id*., art. 18(1).
[622] *Id*., art. 18(2).
[623] *Id*., art. 18(2)a), b), c) et d).
[624] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p.12, par. 3.

Exception de l'intérêt légitime : Une deuxième exception introduite dans le Projet de loi C-27 permet la collecte et l'utilisation en vue de réaliser « une activité dans laquelle [l'organisation] a un intérêt légitime qui l'emporte sur tout effet négatif que la collecte ou l'utilisation peut avoir pour l'individu », mais à plusieurs conditions : 1) une personne raisonnable s'attendrait à cette collecte ou l'utilisation en vue de cette activité, mais excluant l'activité d'influencer le comportement ou les décisions d'un individu;[625] 2) l'organisation doit avoir au préalable avoir « décel[é] tout effet négatif potentiel que la collecte ou l'utilisation est susceptible d'avoir pour l'individu »[626]; 3) l'organisation doit avoir « trouv[é] et [pris] des moyens raisonnables pour réduire la probabilité que ces effets se produisent ou pour les atténuer ou les éliminer »[627]; et 4) l'organisation doit « se conformer à toute autre exigence règlementaire ».[628]

Ainsi, les exigences concernant l'exception de l'intérêt légitime ne peuvent s'appliquer simplement et ne peuvent être prises à la légère. En outre, soulignons que les exceptions des activités d'affaires et de l'intérêt légitime sont sujettes à des règlements à venir, ce qui ajoute assurément une incertitude quant aux cas précis qui pourront se qualifier.

Les exceptions limitées sous la Loi 25

La Loi 25 prévoit quelques exceptions « de base », similaires à celles présentes dans le Projet de loi C-27, à l'obligation d'obtention d'un consentement, en commençant par l'article 3.5 (2) permettant la communication d'un renseignement personnel à toute personne ou organisme dans le but de réduire le risque sérieux de préjudice grave suivant un incident de confidentialité. Ensuite, le nouvel article 12(2) exempte les organisations d'obtenir un consentement dans cinq cas précis, c'est-à-dire pour 1°) l'utilisation à une autre fin compatible avec la fin initiale, si cette fin secondaire a un lien pertinent et direct avec les fins initiales, excluant les fins secondaires de prospection commerciale ou philanthropique[629], et donc la PCL; 2°) l'utilisation manifestement au bénéfice de la personne concernée; 3°) l' « utilisation nécessaire à des fins de prévention de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité »; 4°)

[625] Projet de loi C-27, art. 18(3).
[626] *Id*., art.18(4)a).
[627] *Id*., art. 18(4)b).
[628] *Id*., art. 18(4)c).
[629] Loi 25, art. 12(3).

l'utilisation « nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée », sous réserve des limites que j'aborderai à 6.2.2.; et 5°) l'utilisation nécessaire « à des fins d'étude, de recherche ou de production de statistiques » à condition que les renseignements aient été dépersonnalisés.

En outre, sont également prévues les exceptions visant la communication en vue de conclure une transaction commerciale (art. 18.4 Loi 25) ou à des fins d'étude, de recherche ou de production de statistiques (art. 21 Loi 25), également présentes dans le Projet de loi C-27.

Comme le résumait le CPVP lors des consultations dans le cadre du Projet de loi 64, ce dernier (et la Loi 25 qui en a découlé)

> « introduit plusieurs nouvelles exceptions au consentement. Bien que le Projet de loi du Québec semble suivre l'exemple du RGPD à plusieurs égards, tel n'est pas le cas pour toutes les nouvelles exceptions au consentement. […] Le projet de loi ajoute un certain nombre d'exceptions au consentement à celles présentement en vigueur, mais n'introduit pas de bases légales de traitement des données comme celles que l'on retrouve dans le RGPD, ni semble viser à refléter les bases légales du RGPD [le consentement, le contrat, l'obligation légale, la mission d'intérêt public, l'intérêt légitime et la sauvegarde des intérêts vitaux[630]] ».[631]

Ainsi, la Loi 25 se retrouve à être une loi plus restrictive que le RGPD sur ce point, en voulant être plus protectrice des droits des utilisateurs, mais en étant moins flexible pour les organisations. Cela constitue un lourd fardeau, tant pour les organisations que pour les utilisateurs, sur qui repose en conséquence une pression accrue.

6.1.3. Les éléments principaux constituant un consentement valable

Du côté de la LPRPDE, les sous-principes 4.3.1 à 4.3.8 de l'annexe I de la LPRPDE détaillent l'exercice de cette obligation de manière à constituer un consentement valable. Ces exigences ont été précisées en 2018 par les lignes directrices sur le consentement valable publiées conjointement par le CPVP et les commissariats à la vie privée de l'Alberta et de la Colombie-

[630] CNIL, *La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD*, 2 décembre 2019, en ligne : <https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales> (consulté le 15 avril 2023)
[631] CPVP, « Questions et réponses – projet de loi no 64, Comparution du commissaire à la protection de la vie privée du Canada devant l'Assemblée nationale du Québec », (24 septembre 2020), section « Compatibilité avec le RGPD », en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/qa_20200924/#fn49-rf> (consulté le 15 avril 2023)

Britannique (ci-après « les commissariats »), visant à refléter les principes sous-jacents de la LPRPDE et des lois sur la protection des RP dans le secteur privé de l'Alberta, de la Colombie-Britannique et du Québec essentiellement similaires.[632] Je propose ici d'en résumer les composantes les plus importantes, c'est-à-dire la forme de consentement, le droit de retrait et la demande de consentement en soi complétée par les informations à divulguer, en ajoutant les modifications proposées par le Projet de loi C-27 et en présentant les différences et similarités avec la loi québécoise.

Cela dit, rappelons au préalable qu'un consentement ne peut être donné si les fins ne sont pas acceptables et si les renseignements personnels traités ne sont pas nécessaires.[633] Ces principes de base sont les mêmes au niveau québécois. Ainsi, le consentement ne saurait constituer une « solution miracle » pouvant libérer l'organisation de ses autres obligations en matière de PRP, telle la limitation à la collecte et prendre les mesures nécessaires pour assurer la sécurité des renseignements personnels.[634]

6.1.3.1. La détermination de la forme requise du consentement (explicite ou implicite) : facteurs à évaluer

La détermination de la forme de consentement explicite ou implicite est un point central, dont la compréhension et l'application sont malheureusement complexifiées par des dispositions législatives manquant de clarté et étant différentes d'une juridiction à une autre.

Au Canada

Au niveau fédéral, 4.3.4 de l'annexe I de la LPRPDE prévoit actuellement que la forme requise variera selon les circonstances et la nature des renseignements, c'est-à-dire en tenant compte de la sensibilité des renseignements. Ainsi, un consentement explicite est généralement requis du moment où « les renseignements sont susceptibles d'être considérés comme sensibles »[635]. Au

[632] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, section « Aperçu » par. 3
[633] *Id*., section « Fins acceptables ». Supra 4.1 et 4.2.
[634] *Id*., section « Le consentement n'est pas une solution miracle »
[635] LPRPDE, annexe I, art. 4.3.6.

contraire, en présence de renseignements « moins sensibles, un consentement implicite serait normalement jugé suffisant »[636].

Le deuxième critère pour déterminer la forme requise de consentement est les attentes raisonnables de la personne[637]. Ainsi, comme le rappelaient le CPVP, le CPVP-Alberta et le CPVP-Colombie-Britannique dans leurs lignes directrices de 2018 sur le consentement valable, ces deux critères avaient été confirmés par la Cour suprême du Canada en 2016[638].

En outre, dans ces lignes directrices, les commissariats ont ajouté un troisième critère qui est l'absence de risque résiduel important de préjudice grave, afin de pouvoir conclure qu'un consentement implicite peut être suffisant dans les circonstances.[639]

J'approfondirai la question du degré de sensibilité et la question des attentes raisonnables à la section 6.2. Quant à l'évaluation de la présence ou de l'absence de risque résiduel important de préjudice grave, cet élément a été résumé au point 5.3 de ce mémoire portant sur les mesures de sécurité.

Pour revenir sur la question de la forme du consentement, le Projet de loi C-27, à son l'article 15(5), s'inscrit dans la continuité de la LPRPDE et maintient que le consentement explicite demeure la forme de consentement par défaut, et reprend les deux critères actuels de la LPRPDE pour évaluer si un consentement implicite est approprié, c'est-à-dire la sensibilité des renseignements personnels traités et les attentes raisonnables de la personne[640] sans mention toutefois du troisième critère de l'absence de risque résiduel important de préjudice grave qui a été ajouté par les commissariats dans leurs lignes directrices de 2018 sur le consentement valable. Ainsi l'article 15(5) du Projet de loi se lit comme suit :

---

[636] *Id*.
[637] *Id.*, annexe I, art. 4.3.5.
[638] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, note de bas de page 14 : « *Banque Royale du Canada* c. *Trang*, 2016 CSC 50, par. 23. Voir également les paragraphes 8(2), 8(2.2) et 8(4) de la PIPA de l'Alberta. »
[639] *Id.*, « Déterminer la forme de consentement appropriée » par. 1.
[640] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p. 13, par. 2.

> « Le consentement doit être obtenu expressément, sauf si, sous réserve du paragraphe (6), il est approprié de présumer le consentement implicite de l'individu compte tenu de la nature sensible des renseignements personnels à recueillir, à utiliser ou à communiquer et des attentes raisonnables de cet individu. » [Mes soulignements]

Notons toutefois qu'aucune de ces deux notions n'a été définie explicitement dans le Projet de loi.[641] Les organisations devront donc s'appuyer sur les interprétations du CPVP et de la CAI et de la définition de la Loi 25 pour évaluer ces deux concepts[642].

Concernant le caractère approprié ou non approprié, le paragraphe 15(6) du Projet de loi C-27 prévoit qu'« [i]l n'est pas approprié pour l'organisation de présumer le consentement implicite d'un individu lorsqu'elle recueille ou utilise ses renseignements personnels en vue d'une activité mentionnée aux paragraphes 18(2) ou (3) » [mes soulignements], c'est-à-dire les cas d'exception à l'obtention du consentement prévus par le Projet de loi, principalement :

1. « les activités nécessaires en lien avec la fourniture d'un produit ou la prestation d'un service demandé par l'individu à l'organisation »[643], donc notamment dans le cadre d'un contrat ou d'un avant-contrat
2. « les activités nécessaires à la sécurité de l'information, des systèmes ou des réseaux de l'organisation »[644]
3. « les activités nécessaires pour assurer la sécurité d'un produit ou d'un service que l'organisation fournit »[645]
4. les activités dans lesquelles l'organisation a un intérêt légitime qui l'emporte sur tout effet négatif pour l'individu, à condition qu'« une personne raisonnable s'[attende] à la collecte ou à l'utilisation en vue d'une telle activité »[646] et que « les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu »[647].

La forme de consentement requise dans ces cas n'est donc pas claire à première vue. Le fait d'écrire que le consentement implicite est inapproprié dans ces circonstances porte à confusion. Constatant également ce manque de clarté, le cabinet BLG proposait l'analyse et la conclusion suivantes :

---

[641] *Id*.
[642] Infra, 6.2.
[643] Projet de loi C-27, al. 18(2)a).
[644] *Id*., al. 18(2)b).
[645] *Id*., al. 18(2)c).
[646] *Id.*, al. 18(3)a).
[647] *Id.*, al. 18(3)b).

> « Contrairement au projet de loi C-11 (2020), la LPVPC introduit une limite potentiellement importante à la notion de consentement implicite lorsque le traitement est effectué conformément à l'une des nouvelles exceptions au consentement pour des activités d'affaires déterminées ou légitimes en vertu de l'article 18 de la LPVPC. En particulier, l'article 15(6) de la LPVPC semble créer une règle selon laquelle le consentement implicite est jugé inapproprié si la collecte ou l'utilisation de renseignements personnels est effectuée pour une activité relevant de la nouvelle exception au consentement pour des activités d'affaires déterminées (art. 18(2)) ou pour des activités dans lesquelles l'organisation a un intérêt légitime (art. 18(3)). »[648] [Mes soulignements]
>
> Ainsi, « [u]ne organisation ne peut pas présumer le consentement implicite pour recueillir ou utiliser des renseignements dans le contexte d'une " activité d'affaires " - elles ne peuvent que se fier sur un consentement exprès ou satisfaire les critères prévus par l'exception des activités d'affaires (art. 15(6)). »[649]
>
> En conclusion, « [l]'intention semble être de renforcer la notion de consentement en exigeant des organisations qu'elles se fondent sur l'une des exceptions au consentement mentionnées ci-dessus ou qu'elles obtiennent un consentement explicite pour une ou plusieurs des activités décrites dans ces dispositions. Toutefois, compte tenu de l'ampleur des activités potentiellement couvertes par l'exception relative à l'intérêt légitime, il n'est pas clair dans quelle mesure une organisation peut s'appuyer sur le consentement implicite sans procéder au préalable à une évaluation de l'intérêt légitime conformément à l'article 18(4) de la LPVPC […]. Nous pouvons nous attendre à ce que la portée et l'application de l'article 15(6) de la LPVPC soient clarifiées à mesure que le projet de loi C-27 progresse dans le processus législatif. »[650] [Mes soulignements]

Ainsi, une modification dans la rédaction de cet article serait effectivement souhaitable afin d'assurer sa compréhension et son application conforme par les organisations, mais également par les utilisateurs, joueurs clés sur qui repose une responsabilité accrue de comprendre et consentir au traitement de leurs renseignements personnels. Il sera également pertinent de voir si le CPVP jugera bon par la suite de modifier ses lignes directrices sur le consentement valable.

[648] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p.13, par. 4.
[649] *Id*., p. 13, par. 3.
[650] *Id.,* p. 13, par. 5.

Au Québec

L'article 14 de la Loi sur le privé et l'article de la Loi 25 qui le modifie ne précisent étonnamment pas quelle est la forme de consentement requise par défaut, bien qu'il précise les éléments requis pour constituer un consentement valable. Ainsi, la nouvelle mouture de l'article 14 utilise encore le terme « manifeste » sans toutefois préciser davantage :

> « 14. Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.
>
> Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus est donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur.
>
> Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.
>
> Un consentement qui n'est pas donné conformément à la présente loi est sans effet. »
>
> [Mes soulignements]

Les seuls articles où une forme de consentement est précisée sont les articles 12(1) et 13(2) où il est spécifié que les renseignements sensibles doivent faire l'objet d'un consentement « manifesté de façon expresse ». À ces deux articles s'ajoute le nouvel article 8.1 qui a pour effet d'introduire l'exigence d'un consentement explicite préalable à l'activation de fonctions permettant d'identifier, de localiser ou d'effectuer un profilage. Je reviendrai sur cet ajout majeur[651].

[651] Infra, 6.2.

6.1.3.2. Permettre l'exercice du droit de retrait du consentement

Les lois fédérales et les lois provinciales essentiellement similaires au Canada[652] prévoient le droit de retrait du consentement, sous réserve des restrictions légales ou règlementaires (par exemple dans le secteur financier) ou contractuelles.[653]

L'effet d'un tel retrait est essentiellement le même au fédéral et au Québec. En effet, alors que la LPRPDE n'offrait pas de précision, les commissariats sont venus spécifier qu'une demande de retrait « devrait être respectée et mettre fin à toute collecte ou utilisation ultérieure des renseignements personnels de l'individu »[654]. De plus, dans certaines circonstances, ils sont d'avis que ce retrait pourrait entraîner la suppression des renseignements personnels (par exemple lors de la suppression d'un compte utilisateur sur un réseau social)[655]. Toutefois, l'article 17(2) du Projet de loi C-27 s'arrête à préciser que l'exercice du droit de retrait a pour effet de faire cesser dès que possible la collecte, l'utilisation et la communication des renseignements personnels visés, ce qui semble plus réaliste que la suppression, bien que le défi demeure de taille considérant le nombre important de parties prenantes dans la « chaîne de la PCL ». Du côté québécois, les articles 8(1) et 22(2) de la Loi 25 combinés prévoient qu'une demande de retrait a pour conséquence de faire cesser l'utilisation et la communication des renseignements personnels collectés[656], le terme « collecte » étant absent. En conséquence, on peut se questionner à savoir si une demande de retrait en vertu de la loi québécoise entraînerait aussi un arrêt de la collecte, puisque cela n'est pas précisé.

---

[652] LPRPDE, Annexe I, art. 4.3.8; Projet de loi C-27, art. 17; Loi 25, art. 8(1)4°), 22 ce dernier étant spécifique à la prospection commerciale et philanthropique.
[653] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, « Retrait du consentement »
[654] *Id*., section « Retrait du consentement »
[655] *Id.*
[656] Loi 25, art. 22(2).

6.1.3.3. Concernant l'obligation de transparence, la demande de consentement et son objectif de « compréhension » par l'utilisateur

Au Canada

L'article 4.3.2 de l'annexe I de la LPRPDE[657] prévoit l'obligation d'informer la personne de la collecte et de déployer « un effort raisonnable pour s'assurer que les personnes sont informées des fins auxquelles les renseignements sont utilisés. » Il précise également qu'un consentement est valable si les fins ont été « énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués. » En outre, l'article 6.1 de la LPRPDE ajoute que « le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti. » Dans le même ordre d'idée, 4.4.2 de l'annexe I précise que le consentement ne peut évidemment pas avoir été obtenu au moyen d'un subterfuge.

Les lignes directrices sur le consentement valable de 2018 sont venues apporter plusieurs précisions et un grand nombre de recommandations de mise en application de cette obligation.

Demande de consentement : Dans un premier temps, considérant que « l'information fournie (…) doit être facilement accessible dans son intégralité – mais, pour éviter une surabondance d'information et faciliter la compréhension par les individus, il faut mettre de l'avant certains éléments afin d'obtenir un consentement éclairé ».[658] Ainsi, en ce qui concerne la demande de consentement en soi, « les organisations doivent permettre aux individus d'examiner rapidement les éléments clés qui auront une incidence sur leur décision en matière de protection des renseignements personnels au départ lorsqu'ils envisagent d'utiliser le produit ou le service

[657] Supra, 5.2.
[658] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 1.

offert, de faire un achat, de télécharger une application, etc. À cette fin, les organisations doivent de façon générale mettre davantage l'accent sur certains éléments clés »[659], en :

- Indiquant le plus précisément possible les renseignements recueillis ou susceptibles de l'être;
- Identifiant les tiers ou catégorie de tiers à qui les renseignements personnels seront communiqués;
- Énonçant de manière détaillée et en langage clair toutes les fins de traitement, incluant les fins essentielles et les fins non essentielles à la prestation d'un service, en « soulign[ant] toute fin qui ne serait pas évidente pour la personne ou à laquelle elle pourrait raisonnablement ne pas s'attendre dans le contexte »;[660]
- Les conséquences du traitement, incluant les risques résiduels importants de préjudice grave le cas échéant[661]. Cela dit, si de tels risques probables subsistaient malgré les efforts d'atténuation de l'organisation, le CPVP rappelle que le traitement « serait généralement considér[é] inappropri[é] en vertu du paragraphe 5(3) de la LPRPDE et ne devrait donc pas faire l'objet d'un consentement. »[662] Rappelons effectivement au passage que toute fin inappropriée ne peut faire l'objet d'un consentement valide[663].

À cette fin, des avis « juste-à-temps », des « outils interactifs » (par exemple des vidéos explicatifs et des outils infographiques[664]) et des « interfaces mobiles personnalisées » sont des exemples d'outils que les commissariats ont recommandé de mettre en place, et par le fait même de tirer parti des possibilités qu'offre l'environnement numérique.[665]

[659] *Id.*, Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 3.
[660] *Id.*, Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 3, 3e boulet.
[661] *Id.,* Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 3, 4e boulet; Supra, 5.3.
[662] *Id.,* Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 3, 4e boulet.
[663] Supra, 4.1.
[664] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, Principe directeur no. 4 « Faire preuve d'innovation et de créativité », par. « Outils interactifs »
[665] *Id.,* Principe directeur no. 4 « Faire preuve d'innovation et de créativité », par. 2.

Mises à jour : Dans le même ordre d'idée, les commissariats ajoutent que le « consentement éclairé est un processus continu qui évolue selon les circonstances »[666] et qu'en conséquence, les organisations ne pouvaient se contenter d'un consentement obtenu « à un moment statique dans le temps, mais elles devraient plutôt traiter le consentement comme un processus dynamique et interactif »[667]. Pour y arriver ils recommandent de « rédiger une foire aux questions et [de] la mettre à jour régulièrement, [d']utiliser de nouvelles technologies intelligentes ou [de] faire appel à un assistant virtuel »[668] pour bonifier ou faire des changements mineurs. Les changements majeurs aux pratiques quant à eux, comme l'ajout d'une nouvelle fin ou la nouvelle communication à un tiers à des fins autres que celles du traitement initialement prévu, devant plutôt faire l'objet d'un nouvel avis, voire d'un nouveau consentement le cas échéant auprès des utilisateurs.[669] Ils recommandent également de faire des rappels périodiques aux utilisateurs de leurs options en matière de vie privée, allant jusqu'à les inviter à revoir celles qu'ils avaient choisies.[670]

Informations disponibles en tout temps : En outre, ces lignes directrices sur le consentement valable recommandent de rendre l'intégralité de l'information concernant ces pratiques de gestion des renseignements personnels de l'organisation (par exemple la politique et les avis de confidentialité[671]) disponible facilement et en tout temps aux personnes intéressées.[672] Cette présentation peut se faire « par couches ou par un autre moyen appuyant le contrôle de l'utilisateur sur le degré de détail fourni, aid[ant] à comprendre les textes longs et complexes grâce à un résumé des principaux points figurant au début »[673] et permettant aux utilisateurs d'approfondir leurs recherches selon leurs besoins pour être en mesure d'exercer leur choix. Cette information doit préférablement être « facilement accessible à partir de tous les appareils

[666] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 1.
[667] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 1.
[668] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 2.
[669] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 3.
[670] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 4.
[671] *Id.,* Principe directeur no. 5 « Prendre en compte la perspective du consommateur », par. 3.
[672] *Id.*, Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 2.
[673] *Id.*, Principe directeur no. 2 « Permettre aux individus de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée » par. 3.

que les membres de leur(s) auditoire(s) cible(s) pourraient utiliser ».[674] En outre, afin de tenir compte de la perspective du consommateur, les commissariats insistent pour que le « processus de consentement [soit] facile à comprendre, convivial et adapté à la nature du produit ou du service que [les entreprises] offrent ainsi qu'à leur auditoire cible »[675]. Or, tout en recommandant cela, soulignons que dès le paragraphe qui suit cette recommandation, les commissariats parlent plutôt « d'utiliser un niveau de langue adapté à un auditoire diversifié »[676]. Sur ce point, il m'apparait y avoir contradiction.

Pour se faire, les commissariats mettent de l'avant différentes mesures, telles la consultation des utilisateurs et la création de groupes de consultation, le recours à des designers UX et à des spécialistes en protection de la vie privée, en passant par le suivi des meilleures pratiques en la matière, le tout en précisant que ces suggestions « sont censées être adaptables en fonction de la taille de l'organisation ainsi que de la quantité et du type de renseignements personnels [traités] »[677]. Finalement, les commissariats rappellent que les pratiques exemplaires suggèrent une vérification périodique des pratiques de gestion afin que l'information fournie aux utilisateurs soit toujours exacte et véridique eu égard au traitement qui est fait par l'organisation des renseignements personnels.[678]

En somme, force est de constater que ces recommandations ne pourront pas toutes être suivies à la lettre par toutes les organisations, considérant l'ampleur des ressources qu'elles requièrent. Toutefois, plusieurs suggestions d'ordre pratique sont assurément très intéressantes et implantables. Le défi sera plus grand, mais nécessaire pour les organisations – surtout les plus petites - traitant de grandes quantités de renseignements personnels, de nature variée, avec des degrés différents de sensibilité.

De plus, un des éléments importants qui se dégage de ces lignes directrices, mais qui n'est pas nommé comme tel, est l'attente des commissariats à l'égard des organisations de participer à

[674] *Id.,* Principe directeur no. 5 « Prendre en compte la perspective du consommateur », par. 3.
[675] *Id.,* Principe directeur no. 5 « Prendre en compte la perspective du consommateur », par. 2.
[676] *Id.,* Principe directeur no. 5 « Prendre en compte la perspective du consommateur », par. 3.
[677] *Id.,* Principe directeur no. 5 « Prendre en compte la perspective du consommateur », par. 4 et 5.
[678] *Id.,* Principe directeur no. 6 « Faire du consentement un processus dynamique et continu », par. 5.

l'éducation des utilisateurs et de contribuer à la littératie numérique. Dans l'industrie de la PCL, ce rôle est notamment occupé par les différentes associations, principalement la DAAC dont j'ai notamment parlé dans la partie I de ce mémoire.

L'arrivée du Projet de loi C-27 intègre un certain nombre de ces recommandations, tel l'emploi d'un langage clair et adapté dans les avis. Ainsi, un consentement sera considéré comme valide si les informations utiles et nécessaires à la formulation de ce consentement sont communiquées, c'est-à-dire les fins, la manière et les conséquences raisonnablement prévisibles de la collecte/utilisation/communication à l'individu, le type précis de renseignements personnels collectés/utilisés/communiqués, ainsi que le nom des tiers ou catégories de tiers à qui ils seront communiqués,[679] le tout en « langage clair et raisonnablement compréhensible pour un individu visé par les activités de l'organisation ».[680] Il devra être obtenu au plus tard au moment de la collecte, ou avant l'utilisation ou la communication à un tiers.[681] Toutefois, le Projet de loi C-27 n'apporte pas de précision concernant la manière et le format dans lequel les avis devront être transmis aux utilisateurs[682]. On peut donc s'attendre à ce que les lignes directrices des commissariats sur le sujet, priorisant notamment les avis « juste à temps » et des avis « par couches » soient maintenues, d'autant plus que ce sont des pratiques exemplaires recommandées notamment par la DAAC et les Normes canadiennes de la publicité[683] et déjà implantées ou en voie de l'être chez bon nombre d'organisations au Canada. Certains qualifient cette absence de précision dans la loi de problématique, mais il faut également reconnaître que l'absence de précision dans la loi sur ce point peut permettre une certaine latitude et flexibilité et aux meilleures pratiques de se développer et d'évoluer plus librement.

[679] Projet de loi C-27, par. 15(3).
[680] *Id*., par. 15(4).
[681] *Id*., par. 15(2).
[682] Sepideh ALAVI et al., *Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises*, *op. cit*., note 74, p.14, par. 3.
[683] LES NORMES CANADIENNES DE LA PUBLICITÉ*, Programme de responsabilité Choix de pub, Rapport de conformité 2022*, *op. cit*., note 603, p. 14

Au Québec

Les articles 7, 8, 8.1, 8.2 et 14 de la Loi 25 prévoient également une obligation d'information lors de la collecte et par la suite sur demande qui sous-tend et permet l'exercice du consentement et/ou de son retrait. Contrairement au Projet de loi C-27, elle ne précise pas l'objectif de compréhension, bien qu'il soit sous-entendu, mais prévoit des divulgations additionnelles concernant notamment les transferts hors Québec,[684] comme nous l'avons vu plus haut, et l'utilisation de technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer un profilage d'une personne à l'article 8.1 et 8.2. La Loi 25 fait également référence à l'utilisation du langage simple et clair.[685]

6.2. Application dans un contexte de PCL

La deuxième grande question préoccupant les organisations qui participent à la PCL, avec la question de l'anonymisation et de la dépersonnalisation dont j'ai traité plus haut, est la question à savoir si la forme du consentement passera d'un régime de consentement implicite/négatif/par retrait (opt-out), vers un régime de consentement explicite/positif (opt-in) avec l'entrée en vigueur de la Loi 25 et du Projet de loi C-27.

Je traiterai également de deux autres questions concernant le consentement, soit la question du consentement à l'utilisation par un fournisseur de services de l'organisation et à la communication à un tiers, ainsi que de l'illégalité du consentement comme condition de services.

6.2.1. Analyse de la forme de consentement valide dans un contexte de PCL : d'un régime de consentement « opt-out » vers un régime de consentement « *opt-in* » ?

Afin d'analyser cette question, je résumerai la position de principe sur la publicité comportementale en ligne du CPVP sur laquelle s'est alignée la DAAC et bon nombre

[684] Loi 25, art. 8(2).
[685] *Id*., art. 8(4) et 8.2.

d'organisations canadiennes depuis leur parution, puis j'approfondirai la question de la sensibilité des renseignements personnels et des attentes raisonnables, et proposerai une conclusion.

6.2.1.1. Canada : Position de principe actuelle du CPVP sur la PCL

En 2011, le CPVP publiait des lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne[686] se voulant une orientation générale concernant l'application de la LPRPDE à la publicité comportementale en ligne. Il publiait ensuite en 2015 sa position de principe sur la publicité comportementale en ligne[687] dans laquelle le CPVP conclu, dans un premier temps et comme nous l'avons vu dans la section 4.1.1, que la PCL peut constituer une fin acceptable. En outre, il conclut qu'un consentement est requis, mais qu'il peut prendre une forme implicite qui est valable dans certaines circonstances. Parmi les facteurs menant à sa position que nous pourrions qualifier « de compromis », le CPVP reconnait le rôle de la publicité comportementale dans l'écosystème numérique ainsi que les attentes des utilisateurs vis-à-vis d'un certain niveau d'accès à du contenu et au risque de lassitude ou de réaction négative que pourraient vivre à la longue les utilisateurs. Ainsi :

> « Dans cette optique, nous avons adapté ce cadre pour le consentement négatif à la PCL, en tenant compte du fait que la PCL peut être acceptable dans certaines conditions. Les entreprises présentes sur le Web ont besoin de générer des recettes et les publicités comportementales semblent être plus lucratives que les publicités contextuelles. D'autres modèles d'affaires sont moins populaires dans l'environnement en ligne, où les utilisateurs s'attendent à de l'information et à des services gratuits (ces modèles reposent néanmoins aussi sur l'obtention de certains renseignements personnels par une organisation). Les utilisateurs s'attendent également à un accès instantané. L'affichage constant d'avis aux utilisateurs sur les témoins et l'accès bloqué à des sites financés par la publicité finiront par frustrer les utilisateurs et pourraient susciter chez eux une lassitude ou une réaction négative à l'égard des efforts visant à protéger leurs renseignements personnels.

[686] CPVP, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, *op. cit*., note 210.

[687] Note : « La position de principe énoncée (…) porte sur l'application de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) à la collecte et à l'utilisation de données concernant les activités sur le Web des personnes, à des fins de publicité comportementale en ligne (PCL) uniquement, au moyen de technologies comme les témoins, les pixels invisibles, les supertémoins, les témoins soi-disant « zombie » et les données des appareils. »
CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit*., note 11, par. 1.

Position : Le consentement négatif pourrait être acceptable sous certaines conditions, énoncées ci-dessous, dans le cadre des deux restrictions proposées ci-après. »[688]

Au terme de son analyse des pratiques et des consultations qu'il avait menées en 2010, le CPVP traçait le cadre suivant :

> « La PCL nécessite un consentement valable. Le consentement implicite ou négatif au suivi et au ciblage de personnes à des fins de publicité comportementale peut être acceptable si les paramètres suivants sont en place:
>
> - Les utilisateurs sont avisés des objectifs de la pratique de façon claire et compréhensible — ces objectifs doivent être manifestes et ne peuvent être enfouis dans une politique de protection de la vie privée. Il faut que les organisations soient transparentes quant à leurs pratiques et se demandent comment elles peuvent informer efficacement les utilisateurs de leurs pratiques en matière de publicité comportementale en ligne à l'aide de divers moyens de communication, comme l'utilisation de bannières en ligne, de technologies multicouches et d'outils interactifs.
> - Les utilisateurs sont informés de ces fins au moment de la collecte ou avant et reçoivent de l'information sur les diverses parties qui participent au processus de publicité comportementale en ligne.
> - Les utilisateurs peuvent facilement renoncer à la pratique, idéalement au moment de la collecte ou avant.
> - La renonciation est immédiate et durable.
> - Les renseignements recueillis et utilisés se limitent, dans la mesure du possible, aux renseignements non sensibles (éviter les renseignements qui sont généralement considérés comme sensibles, par exemple les renseignements sur la condition médicale ou la santé, les finances, les origines ethniques et raciales, les opinions politiques, la vie sexuelle ou l'orientation sexuelle et les croyances religieuses ou philosophiques, ainsi que les données génétiques et biométriques).
> - Les renseignements recueillis et utilisés sont détruits dès que possible ou anonymisés efficacement. »[689] [Mes soulignements, référence omise]

Toutefois, comme le notait le CPVP dans sa position sur la PCL[690], cette position a été publiée puis révisée alors que l'article 6.1 de la LPRPDE, ajoutant le critère des attentes raisonnables à l'évaluation de l'article 4.3 de l'annexe I de la LPRPDE.

---

[688] *Id*., section « Consentement valable : consentement négatif ou consentement positif ? », par. 3 et 4.
[689] *Id*., section « Sommaire » par. 4.
[690] « La LPRPDE a été modifiée après l'élaboration de la présente position de principe. En vertu de l'article 6.1, qui a alors été ajouté, pour l'application de l'article 4.3 de l'annexe 1, le consentement de l'intéressé n'est valable que

Or l'intégration de ce critère déterminant dans l'analyse contextuelle de la forme requise de consentement semble avoir pour effet de venir limiter les situations dans lesquelles un consentement négatif pourrait être considéré valable, tel que l'illustre la récente décision du CPVP dans l'affaire *Home Depot*[691]. En effet,

> « [p]our conclure qu'un consentement explicite (*opt-in*) aurait dû être obtenu, le CPVP s'appuie sur sa détermination que la transmission des données à la plateforme de réseautage social ne répondait pas aux attentes raisonnables des clients qui avaient donné leur adresse courriel pour recevoir des reçus électroniques. Le CPVP en est venu à cette conclusion même si la pratique consistant à transmettre des données ne concernant pas des renseignements personnels sensibles ni ne créait un risque résiduel important de préjudice grave pour les clients. »[692]

Toutefois, le niveau d'analyse de ce critère des attentes raisonnables par le CPVP dans cette affaire a été critiqué puisqu'elle ne tenait pas compte de tous les factuels contextuels pertinents entourant la pratique en cause qui doivent être évalués dans leur ensemble.[693]

Ainsi, cette décision met en lumière l'importance de tenter de gérer les attentes raisonnables des utilisateurs concernant les fins principales et les fins secondaires en fournissant des avis préalables et mettant en place un outil de retrait de consentement fonctionnel. Toutefois :

> « Si la décision n'empêche pas les organisations de compter sur un consentement tacite pour toutes les formes de marketing et d'analytique, elle met en lumière l'importance de fournir des avis préalables sur le recours auxdites pratiques, de fixer des limites claires quant à l'usage que les partenaires peuvent faire des informations, et de permettre aux clients de retirer facilement leur consentement à l'utilisation de leurs informations à des fins secondaires. Cela dit, en l'absence de lignes directrices claires sur ces questions, les organisations qui comptent sur le retrait du consentement pour traiter des informations

---

s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti. » CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit.,* note 11, note de bas de page 15

[691] Supra, 5.1.1., 5.2.1., 5.2.2 et 5.4.2.

[692] Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée*, *op. cit.,* note 446, « Contexte », par. 2

[693] La critique a été formulée par Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée*, *op. cit.,* note 446, rappelant l'interprétation large préconisée par la Cour suprême du Canada dans *Banque Royale du Canada* c. *Trang,* [2016] 2 RCS 412

> aux fins de marketing et d'analyse des données seront toujours à risque de contrevenir à la loi, surtout s'il est question de pratiques nouvelles susceptibles de ne pas répondre aux attentes raisonnables des clients. »[694] [Mes soulignements]

À la lumière de cette application du critère des attentes raisonnables du CPVP, des nouvelles dispositions proposées par le Projet de loi C-27[695], de sous la possible influence de la Loi 25 et de l'interprétation plus stricte que semblent adopter la CAI, est-ce que le CPVP pourrait être amené à réviser sa position concernant la PCL et à remettre en question la forme de consentement implicite qui pouvait jusqu'ici est considérée comme valide si les renseignements en question ne sont pas sensibles et si un mécanisme de retrait est en place ? De plus, est-ce que le législateur canadien souhaitera préciser ces dispositions et s'aligner avec le RGPD comme le Québec semble l'avoir fait ?

Dans tous les cas, espérons que les consultations à venir permettront de nourrir les réflexions du législateur et de clarifier la situation pour l'avenir, afin que les entreprises qui participent à la PCL bénéficient du temps nécessaire à la modification de leur pratique vers une forme de consentement explicite le cas échéant, considérant que des lacunes au niveau de la prévisibilité et de la certitude des exigences applicables peuvent représenter un risque considérable pour la santé financière et la compétitivité des organisations d'ici. Comme cela a été souligné par plusieurs :

> « Il est crucial que le secteur privé ne soit pas pris au dépourvu par l'interprétation de concepts clés comme la notion du consentement, en particulier dans les domaines du marketing et de l'analyse de données, qui sont au cœur du modèle d'affaires de nombreuses entreprises. Les entreprises ont besoin d'orientations concrètes et d'outils de conformité leur apportant certitude et prévisibilité dans l'application de ces exigences de la loi. La non-conformité peut poser des risques importants, notamment nuire à la réputation des entreprises et engager leur responsabilité financière, en particulier dans le contexte de réformes des lois fédérales et provinciales sur la protection de la vie privée.

[694] Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée*, *op. cit.,* note 446, « Contexte », par. 6.
[695] Supra 6.1.3.1.

Une approche collaborative plus proactive est donc essentielle pour protéger les clients tout en tenant compte des besoins des entreprises. »[696]

6.2.1.2. Québec : Vers un régime de consentement express (« *opt-in* »)

Au Québec, le flou quant à la forme de consentement requise persiste depuis des années, mais les nouvelles dispositions de la Loi 25 et l'interprétation que la CAI en fait semblent nous diriger vers une forme de consentement explicite à compter du 22 septembre 2023. Regardons l'évolution de la situation dans le temps.

En 2013, la CAI, dans son document sur le profilage et la publicité ciblée, ne précisait pas la forme de consentement requise, mais se contentait plutôt de regrouper les dispositions de la Loi sur le privé :

> « Ainsi, si une entreprise constitue un dossier sur vous afin de vous offrir des biens ou des services (ex : achat en ligne d'un billet de concert), elle doit vous informer des renseignements personnels qu'elle entend collecter et obtenir votre consentement. Elle peut, dès lors, recueillir les renseignements vous concernant nécessaires à l'exécution de ce contrat (par exemple, pour un billet de concert : nom et prénom, numéro de carte de crédit, adresse). L'entreprise ne doit collecter que les renseignements nécessaires à l'objet du contrat, elle ne peut donc recueillir d'autres renseignements, et ce, même avec votre consentement. Et, si l'entreprise veut utiliser vos renseignements à d'autres fins, non pertinents à l'objet du dossier, ou si elle veut les communiquer à des tiers, elle doit vous demander votre consentement. Pour être valide, le consentement doit être manifeste[697], libre, éclairé, donné à des fins spécifiques et il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. »[698] [Mes soulignements]

Par la suite, dans son rapport quinquennal de 2016, elle précisait qu'

> « [e]n vertu de la Loi sur le privé, le consentement doit être " manifeste ", ce qui signifie qu'il ne doit laisser aucun doute quant à la volonté qui y est exprimée, et ce, quel que soit

---

[696] Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée*, *op. cit.,* note 446, dernier paragraphe.

[697] L'expression « consentement manifeste » employée dans la Loi sur le privé et reprise dans la Loi 25, ne trouve aucune occurrence dans le dictionnaire de droit québécois et canadien du CAIJ, mais le terme « manifeste » est définit comme étant ce « [q]ui est très apparent, que l'on peut déceler à la seules vue ou lecture d'un document, d'un dossier, d'un jugement », par exemple une « erreur manifeste » : *Dictionnaire de droit québécois et canadien*, CAIJ, édition révisée 2016, en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=Manifeste%20(adj.)&t=edictionnaire&sort=relevancy&m=search > (consulté le 17 avril 2023)

[698] CAI, *Le profilage et la publicité ciblée, op. cit.,* note 218, p. 2.

le moyen utilisé pour l'exprimer. Il peut donc être explicite ou implicite. »[699] [Mon soulignement]

La CAI proposait donc

> « que la loi [sur le privé] soit modifiée afin que la communication de renseignements sensibles ou leur utilisation à d'autres fins que celles de leur collecte ne soit possible qu'avec le consentement explicite de la personne concernée ou l'autorisation de la loi. »[700]

Ce qui a été fait dans la Loi 25. En outre, les termes employés par la CAI en 2016 exprimaient sa désapprobation concernant l'utilisation des données des consommateurs à leur insu afin de cibler leurs intérêts et plaidait en conséquence pour l'actualisation des concepts en matière de PRP sans toutefois préciser la forme de consentement requise pour les renseignements non sensibles.[701] Ce que le Projet de loi 64 n'avait pas non plus précisé initialement.

Ainsi, l'ambiguïté - ou flexibilité - quant à la forme de consentement requise dans un contexte de PCL persistait dans le Projet de loi 64 dans sa version initiale. En effet, l'article 99 qui introduisait le nouvel article 8.1 exigeait à l'alinéa 2 de divulguer les « moyens offerts pour désactiver les fonctions permettant de localiser ou d'effectuer du profilage ».[702] C'est par la suite que 8.1 a été modifié pour exiger que soient divulgués les moyens offerts pour les activer [703] :

> « 8.1. En plus des informations devant être fournies suivant l'article 8, la personne qui recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci doit, au préalable, l'informer :
>
> 1° du recours à une telle technologie;
>
> 2° des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.
>
> Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des

[699] CAI, *Rétablir l'équilibre, Rapport quinquennal 2016*, *op. cit*., note 219, p. 89, par. 3.
[700] *Id*., p. 89, par. 4.
[701] *Id*., p. 78.
[702] Projet de loi 64 version initiale présentée en 2020 : *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 1ère session, 42e législature, art. 99, en ligne : <https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html?appelant=MC>
[703] Loi 25, art. 107.

préférences personnelles, des intérêts ou du comportement de cette personne. » [Mes soulignements]

Précisons que le nouvel article 8.3 prévoit une présomption de consentement à l'utilisation et à la communication des renseignements personnels lorsqu'une personne a fourni ses renseignements suite à une divulgation des informations listées à l'article 8, pour les fins qui lui avaient été énoncées. Ainsi, le législateur a omis d'inclure 8.1 à l'article 8.3, évitant une contradiction avec 8.1(1)2°), et nous renforçant l'interprétation que le consentement positif sera dorénavant la forme requise dans un contexte de PCL.

Ainsi, l'article 8.1(1)2° de la Loi 25, située sous l'obligation de transparence, est devenue une disposition clé semblant introduire la forme de consentement explicite préalable lorsqu'il y a emploi d'une technologie permettant d'identifier, de localiser ou d'effectuer un profilage et des moyens offerts pour activer ces fonctions, et ce peu importe que le renseignement soit sensible ou non. Cette exigence s'appliquerait donc « à diverses technologies ainsi que dans différents contextes (par exemple, certains outils de surveillance des employés, les témoins de connexion et les technologies similaires utilisées pour la publicité ciblée, etc.). »[704]

En outre, si nous considérons l'intention du législateur exprimée en commission parlementaire, conjuguée à l'interprétation sommaire publiée par la CAI à ce jour, il devient encore plus clair que 8.1(1)2° introduit une ère de consentement positif. Toutefois, le fait que cette disposition ait été intégrée sous l'article concernant l'obligation de transparence contribue à alimenter une certaine ambiguïté :

> « L'interprétation de l'article 8.1 soulève des difficultés puisqu'il n'est pas clair si cette disposition constitue le simple prolongement de l'obligation de transparence prévue à l'article 8 LPRPSP ou s'il s'agit d'une restriction concrète à l'utilisation de technologies de localisation, d'identification et de profilage. S'exprimant au sujet de cette nouvelle disposition en commission parlementaire, Éric Caire, ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, a indiqué que celle-ci avait pour conséquence d'introduire un consentement explicite (opt-in) pour la collecte de renseignements personnels au moyen de technologies ayant des fonctions d'identification, de localisation ou de profilage. De plus, la CAI sur son site Web mentionne

[704] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit.*, note 421, p. 16, par. 1.

que " ces technologies ne pourront être activées par défaut; ce sera à la personne concernée de les activer si elle le souhaite "[705]. En d'autres termes, l'individu doit poser un geste positif pour signifier son intention d'activer une fonction spécifique. Or, le libellé de l'article 8.1 se limite plutôt à une obligation d'« informer » les individus des moyens disponibles pour activer ces fonctions, sans toutefois préciser que ces moyens doivent exister dans les faits ou que les fonctions elles-mêmes doivent être systématiquement désactivées. Dans tous les cas, à la lumière des commentaires de la CAI, il est prudent d'envisager de revoir l'utilisation de certaines technologies pour profiler, localiser ou identifier des individus et, si nécessaire, de mettre en œuvre de nouveaux processus pour demander à l'utilisateur d'activer certaines fonctions. […] » [Mes soulignements]

Cela étant dit, le doute subsiste néanmoins au sujet des fichiers témoins en raison de la présence de l'article 9.1 prévoyant l'exigence de protection de la vie privée dès la conception, où « le législateur a pris soin d'exclure expressément les témoins de connexion » de son champ d'application.[706] En effet, sur ce point il semble y avoir contradiction. Il conviendrait donc que soit précisé le type de témoins visés par 9.1 afin d'harmoniser cette disposition avec 8.1, par exemple les témoins de mesure d'audience, tel qu'ils ont été exclus de l'obligation de consentement dans le projet de règlement *ePrivacy*[707]. Rappelons aussi, comme nous l'avons survolé plus haut, que plusieurs technologies, autres que les témoins, sont utilisées en PCL comme les identifiants uniques et les pixels. En conséquence, lorsque ces technologies sont utilisées, il n'y aurait pas de contradiction apparente entre 9.1 et 8.1.

En conséquence, des clarifications officielles seraient appréciées afin de dissiper tout doute concernant l'interprétation de ces dispositions. Ainsi, si un consentement tacite ne peut plus être considéré comme suffisant, cela représentera un changement majeur non seulement pour les organisations québécoises, mais également pour les organisations canadiennes ayant des opérations à travers le Canada incluant le Québec et qu'elles appliquent actuellement le

[705] En effet, la CAI a publié sur son Espace évolutif la ligne suivante : « En d'autres mots, ces technologies ne pourront être activées par défaut; ce sera à la personne concernée de les activer si elle le souhaite. »
CAI, « Technologie d'identification, de localisation ou de profilage », en ligne : <https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/technologie-identification-localisation-profilage/> (consulté le 8 mars 2023)
[706] Éloïse GRATTON, Elisa HENRY et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *op. cit.*, note 421, p. 13 par. 3.
[707] Infra, 6.2.3.

consentement implicite dans les paramètres jugés acceptables par le CPVP dans sa position de principe sur la PCL. Elles devront donc modifier tous leurs processus, systèmes, politiques et contrats avec le standard québécois.

Néanmoins, si finalement l'interprétation de la CAI sur le sujet concluait plutôt à la possibilité qu'un consentement implicite soit valide, outre que dans le contexte de 8.3 où la personne a fourni ses renseignements personnels, il se pourrait tout de même que la forme de consentement requise soit le consentement exprès, considérant l'élargissement de la définition de renseignements sensibles qui s'observe[708] et l'évaluation plutôt stricte des attentes raisonnables des utilisateurs par les autorités de contrôle québécoise et fédérale.

Soulignons également qu'une divergence au niveau des lignes directrices québécoises et fédérales le cas échéant, serait très complexe à gérer pour les entreprises d'ici. Un encadrement harmonisé à travers le Canada serait idéal.

6.2.1.3. L'importance du droit de retrait du consentement dans un contexte de PCL

D'une perspective utilisateur, il s'agit d'un des éléments de conformité les plus importants, sur lequel insistent les autorités de contrôle et sur lequel les utilisateurs s'appuient, comme dans le contexte de la loi canadienne antipourriel.

Comme nous l'avons vu plus haut[709], le droit de retrait est prévu aux articles 8(1)4°) et 22 - spécifique à la prospection commerciale et philanthropique - de la Loi 25, à l'article 4.3.8 de l'annexe I de la LPRPDE et à l'article 17 du Projet de loi C-27.

Le CPVP, dans sa position de principe concernant la PCL, réaffirmait le rôle important et incontournable de ce mécanisme de contrôle dans un contexte de PCL :

> « Une personne doit être informée de toute collecte ou utilisation des activités de navigation sur Internet et y consentir. Par conséquent, si une personne ne peut refuser le suivi et le ciblage, par un mécanisme de consentement négatif, ou parce qu'il n'existe aucun moyen viable de contrôler la technologie utilisée, ou parce qu'un refus rendrait le

[708] Infra, 6.2.1.4.
[709] Supra, 6.1.3.2.

> service inutilisable, les organisations ne doivent pas faire appel à ce type de technologie à des fins de publicité comportementale en ligne. À l'heure actuelle, cela pourrait inclure, par exemple, des témoins soi-disant « zombie », des supertémoins et l'empreinte de l'appareil. D'autres renseignements sur les technologies de suivi en ligne figurent dans notre fiche d'information *Les témoins et le suivi sur le Web*. »[710] [Mon soulignement]

Il y confirmait ainsi que le fait de mettre en place un mécanisme fonctionnel de retrait était une des conditions essentielles afin de considérer qu'un consentement implicite pouvait être considéré comme valable dans un contexte de PCL.

En effet, cette importance est notable et se manifeste clairement chez les utilisateurs dans l'industrie. En effet, selon le rapport 2022 des Normes canadiennes de la publicité concernant le programme Choix de pub de la DAAC, 50% des plaintes reçues en 2022 par cet organisme portaient sur la difficulté de refuser la PCL.[711] Il existe différents outils gestion de consentement (collecte et retrait) vers lesquels les entreprises peuvent et pourront se tourner. Spécifiques à la PCL, il existe actuellement des outils de retrait du consentement proposés par la DAAC (Canada), la DAA (US) et la EDAA (Europe) utilisés par les entreprises participantes à ces programmes dont j'ai traité dans la partie I de ce mémoire. Ainsi, l'icône permet d'informer les utilisateurs de l'identité des entreprises participantes qui participent à la PCL, mais également permet à ces utilisateurs de retirer leur consentement afin de ne plus recevoir de PCL provenant d'une, plusieurs ou toutes les entreprises participantes au programme.

Rappelons également que pour que ce genre d'outil demeure conforme à la loi fédérale et à la loi québécoise, il conviendra de s'assurer que l'outil de retrait de consentement continue de permettre non seulement de faire cesser la livraison de PCL à la personne concernée, mais également toute la collecte, utilisation et communication[712] faites par les entreprises auprès de qui cette personne aura choisi de retirer son consentement à recevoir de la PCL. Cela constituera un défi important, considérant la complexité des flux de données et la multitude des intervenants « dans la chaîne de la PCL ». Toutefois, un outil permettant de notifier plusieurs entreprises en

[710] CPVP, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, *op. cit*., note 210, paragraphe « Restrictions »
[711] LES NORMES CANADIENNES DE LA PUBLICITÉ, *Programme de responsabilité Choix de pub, Rapport de conformité 2022*, *op. cit.*, note 603, p. 9, par. 1.
[712] Projet de loi C-27, art. 17(2); Loi 25, art. 22(2).

même temps, comme celui du programme d'autoréglementation Choix de pub, dont font notamment partie *Google* et *Amazon*, constitue une solution assurément des plus pratiques, tant pour les organisations, leurs fournisseurs, les tiers, que les utilisateurs.

En outre, avec le virage possible vers un régime de type *opt-in* au Québec applicable d'emblée dans un contexte de ciblage et de profilage, et du resserrement à venir au Canada également, ce genre d'outil et de programme d'autoréglementation demeureront utiles et pertinents, tout en étant appelés à être complémentaires aux autres outils d'obtention et de gestion des consentements des organisations, tel que cela est devenu le cas en Europe lors de l'entrée en vigueur du RGPD. L'outil de retrait de la DAAC ne sera plus suffisant considérant que le régime de consentement implicite ne sera plus celui en vigueur au Canada et au Québec, ou le sera, mais pour des cas très limités, comme nous l'avons vu plus haut.

Il convient également de souligner que ce retrait de consentement devra se faire de manière précise pour éviter qu'un retrait soit trop précis ou trop large par rapport à ce que souhaite vraiment la personne qui exerce son choix, ce que le Projet de loi C-27 permet explicitement en précisant que la demande de retrait peut s'exercer en tout ou en partie,[713] en voyant un avis à l'organisation.[714]

Il conviendra également de réfléchir à la possibilité que cette personne change d'idée par la suite et choisisse finalement de redonner son consentement afin de recommencer à recevoir de la PCL de la part de certaines organisations. Il s'avère en effet que ce phénomène commence à s'observer dans l'industrie[715], d'où l'importance de tenir un registre des consentements et des retraits assez précis, pour être en mesure de réactiver le processus de PCL sur demande de la personne le cas échéant. Il pourrait être encore plus pertinent de permettre de sélectionner non seulement les organisations de confiance qu'une personne pourra choisir, mais également les

[713] Projet de loi C-27, par. 17(1).
[714] *Id*., par. 17(2).
[715] Selon le récent rapport des Normes de la publicité concernant le programme Choix de pub de la DAAC, l'une des personnes qui avaient déposé une plainte a finalement demandé conseil sur la façon d'accepter à nouveau la PCL, jugeant finalement préférable dans son cas de recevoir de la PCL plutôt que des publicités de nature générale : LES NORMES CANADIENNES DE LA PUBLICITÉ, *Programme de responsabilité Choix de pub, Rapport de conformité 2022*, *op. cit.*, note 603, p. 9, dernier paragraphe.

catégories d'intérêts pour lesquelles cette personne accordera son consentement, par exemple pour certains types de produits ou de services.

En somme, beaucoup de travail et de réflexion reste à venir, non seulement dans une perspective de conformité aux lois, règlements et programmes d'autoréglementation, mais surtout afin de saisir l'opportunité de revoir, d'assainir et d'améliorer les pratiques des organisations et d'accroître le niveau de littéracie numérique des utilisateurs, et ce au bénéfice de tous.

6.2.1.4. Évaluation du degré de sensibilité d'un renseignement personnel : approche contextuelle

Attardons-nous maintenant à l'évaluation du degré de sensibilité des renseignements personnels. Il s'agit d'un concept qui est récurrent dans la LPRPDE, le Projet de loi C-27 et dans la Loi 25, afin d'évaluer non seulement la forme de consentement requise, mais également la détermination des fins acceptables, l'intensité du programme de gestion des renseignements personnels, les mesures de sécurité à mettre en place, la durée de conservation, l'évaluation du risque réel de préjudice grave, la proportionnalité des procédés techniques et administratifs de la dépersonnalisation.[716]

La LPRPDE contient une définition et une liste d'exemples non exhaustive à son article 4.3.4 de son annexe I sur la forme de consentement, prévoyant que

> « [s]i certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être. » [Mes soulignements]

Or, cet article n'a pas été repris par le Projet de loi C-27 actuel qui n'inclut pas de définition de renseignements personnels sensibles. Les deux seuls endroits où un renseignement est qualifié de sensible sont aux paragraphes 2(2), c'est-à-dire les renseignements de personnes mineures, et au paragraphe 66(3) traitant des renseignements médicaux de nature sensible. Au contraire,

[716] Au niveau du Projet de loi C-27 par exemple, l'ensemble des articles faisant référence au degré de sensibilité sont les suivants : art. 9(2), 12(2)a), 15(5), 22(1)b)ii), 22(3)a)ii), 53(2), 57(1), 58(8), 62(2)e), 66(3) et 74.

le législateur québécois a plutôt choisi de définir ce qu'est un renseignement personnel sensible, soit

> « lorsque, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée. »[717]

Ainsi, il conviendra donc de continuer à appliquer une approche contextuelle basée sur le l'expectative de vie privée / attentes raisonnables de la personne.

Pour plus de précision, il faut se tourner vers les lignes directrices sur le consentement valable et sa position en matière de PCL, où CPVP considère que cette catégorie de renseignements comprend les renseignements relatifs à la santé ou aux finances d'un individu ou encore à certains choix de vie plus personnels. En outre, en mai 2022, il publiait un bulletin d'interprétation concernant les renseignements sensibles dans lequel il rappelait que certains renseignements sont presque toujours considérés comme sensibles, tels les renseignements médicaux et les renseignements financiers comme le revenu, mais que tout renseignement a également le potentiel de devenir sensible selon le contexte, ou s'il est combiné avec d'autres renseignements, ou encore s'il a une incidence sur la réputation de la personne.[718]

Dans les dernières années, le CPVP a procédé à plusieurs enquêtes lors desquelles ont été confirmé et précisé la définition de renseignements personnels. Je propose ici de regarder les exemples les plus importants.

Dans son enquête de 2014 visant les pratiques de publicités ciblées de *Google*, le CPVP concluait que les activités en ligne et l'historique des sites Web liés à la santé qui avaient été visités dans le cadre de recherche d'information sur un appareil médical pour traiter l'apnée du sommeil

[717] Loi 25, art. 12.
[718] CPVP, *Bulletin d'interprétation : Renseignements sensibles*, mai 2022, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_10_sensible/> (consulté le 16 avril 2023)

constituaient des renseignements personnels sensibles sur l'état de santé, et qu'en conséquence un consentement explicite aurait dû être obtenu :

> « Le plaignant cherchait de l'information sur un appareil médical utilisé pour traiter l'apnée du sommeil. Étant donné que sa plainte concerne des renseignements personnels sur son état de santé (c.-à-d. activités en ligne et historique des sites Web liés à la santé qui ont été visités), le Commissariat estime que cette information est sensible. Par conséquent, pour la collecte ou l'utilisation des renseignements personnels sensibles du plaignant sur son état de santé en vue de lui présenter des annonces personnalisées en fonction de son comportement en ligne, le consentement implicite n'est pas suffisant; il faut obtenir son consentement explicite. »[719] [Mes soulignements]

L'affaire *Ashley Madison* de 2016, quant à elle, illustre bien comme des renseignements a priori non sensibles peuvent devenir sensibles s'ils sont utilisés à des fins révélant les choix de vie d'une personne. En résumé, *Avid Life Media Inc*. (ALM) exploitait plusieurs sites Web de rencontres, principalement Ashley Madison, qui s'adressaient aux adultes à la recherche d'une aventure en toute confidentialité.[720] Au terme de son enquête, le CPVP a conclu que

> « [*Avid Life Media Inc*. (ALM)] offre des services de rencontres pour adultes en ligne. À cette fin, elle recueille, détient et utilise des renseignements sensibles concernant ses utilisateurs, y compris des renseignements qui révèlent leurs pratiques, leurs préférences et leurs fantasmes sexuels. De surcroît, Ashley Madison est un site Web conçu pour les gens à la recherche d'une aventure, activité où la discrétion est attendue et primordiale. Ainsi, même des renseignements qui pourraient sembler anodins pris isolément dans un autre contexte (p. ex. le nom et l'adresse de courriel) peuvent devenir sensibles lorsqu'ils sont associés au site Web Ashley Madison. »[721] [Mon soulignement, références omises]

En outre, dans son rapport de 2019 concernant les pratiques de *AggregateIQ*, le CPVP confirmait que les renseignements personnels sensibles comprennent également les renseignements qui

---

[719] CPVP, *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE n° 2014-001**,** 14 janvier 2014, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-001/ >

[720] CPVP, *Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie, Rapport de conclusions d'enquête en vertu de la LPRPDE n°2016-005*, 22 août 2016, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2016/lprpde-2016-005/>

[720] *Id*., par. 1.

[721] *Id*.

« pourraient révéler des opinions politiques et des croyances personnelles »[722] et ajoutait que l'origine ethnique est considérée comme un renseignement « potentiellement sensible »[723].

De manière plus récente, le CPVP concluait en 2022 dans l'affaire *Tim Hortons*[724], que les données de géolocalisation détaillées et collectées en continu à des fins publicitaires qui outrepassaient les besoins légitimes de l'entreprise se qualifiaient de renseignements personnels très sensibles :

> « Il convient de noter que les données de localisation détaillées recueillies par l'application peuvent être des renseignements personnels de nature très sensible. Tout comme Radar, au nom de Tim Hortons, a déduit le domicile ou le lieu de travail d'une personne à l'aide de données recueillies par l'application, une entreprise pourrait utiliser l'information sur les déplacements d'une personne pour générer des connaissances intimes à son sujet. Par exemple, sur son état de santé et les traitements médicaux qui lui sont prodigués, ou encore ses croyances religieuses, ses préférences sexuelles, ses affiliations sociales et politiques, et plus encore. Même si la preuve indique que Tim Hortons n'a pas utilisé les données de localisation Radar pour générer de telles inférences, la possibilité réelle que les renseignements de localisation soient utilisés de cette façon les rend particulièrement sensibles. »[725] [Mes soulignements]

Ainsi, la notion de sensibilité demeure un concept large et appelé à varier selon le contexte et évolutive en fonction de l'évolution des pratiques, des technologies et des attentes raisonnables des utilisateurs. Il est raisonnable de constater, à la lumière de l'évolution des modifications législatives et des décisions du CPVP, que la définition de renseignement sensible tend à s'élargir. Considérant que cette qualification détermine notamment la forme de consentement requise, un examen minutieux par les organisations est requis. Ainsi, l'exercice pourrait s'avérer complexe considérant de plus que « (…) ce qui constitue pour quelqu'un une ingérence intolérable dans sa vie privée peut être jugé acceptable par quelqu'un d'autre. »[726]

---

[722] 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 d'AggregateIQ Data Services Ltd., op. cit*., note 72, par. 47.
[723] *Id*., « Conclusion » par. 4.
[724] Supra, 4.1.1., 5.1.1., 5.2.2. et 5.2.3.
[725] CPVP, *Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons,* Conclusions en vertu de la LPRPDE n°2022-001, *op. cit*., note 371, par. 43.
[726] Miguel BERNAL-CASTILLERO et Nancy HOLMES, *Les lois fédérales du Canada sur la protection de la vie privée*, *op. cit*., note 124, par. 2.

6.2.2. La distinction importante entre l'utilisation par des entreprises fournisseurs de services et la communication à un tiers

Deux types de transferts sont centraux et omniprésents dans un contexte de PCL. Le premier est l'envoi ou l'accès à des renseignements personnels collectés par l'organisation à un fournisseur de services dans le cadre d'un contrat ou d'un mandat. Le second est la communication à une entreprise tiers, hors d'un contrat de services ou mandat.[727] Cette distinction importante est faite dans les lois fédérale et québécoise en matière de vie privée. Toutefois, nous verrons que le premier type de transfert peut rapidement basculer vers le deuxième type de transfert. Les organisations devront porter une attention particulière à cette situation.

Utilisation par des fournisseurs de services de l'organisation

Introduction d'une définition : Le Projet de loi C-27 vient ajouter d'importantes précisions concernant les fournisseurs de services actuellement absentes dans la LPRPDE. Ainsi, il intègre une définition de fournisseur de services, étant « [t]oute organisation, notamment une société mère, une filiale, une société affiliée, un entrepreneur ou un sous-traitant, qui fournit un service au nom ou pour le compte d'une autre organisation pour lui permettre de réaliser ses fins. (*service provider*). »[728]

Régime applicable aux fournisseurs de services : Toute organisation se qualifiant comme tel tombe sous le régime applicable aux fournisseurs de services sous lequel un transfert de renseignements personnels peut leur être fait à l'insu ou sans le consentement de l'individu.[729]

---

[727] Notons que ces deux types de transferts font l'objet de termes différents dans la LPRPDE, le Projet de loi C-27 et la Loi 25, mais que pour les fins de la présente analyse, je propose d'utiliser les expressions utilisées dans le Projet de loi C-27 soit « utilisation par un fournisseur de services » et « communication à un tiers », les jugeant plus claires. Cette distinction conceptuelle entre « utilisation » et « communication » a été soulignée dans le contexte des conclusions 2023 de l'enquête du CPVP concernant *Home Depot* dans :
Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée*, *op. cit*., note 446, par. 2 de la section « 1. La distinction entre " utilisation " et " communication " de renseignements personnels quand des informations sont transmises à un partenaire pour l'analyse des données »

[728] Projet de loi C-27, art. 2(1).

[729] *Id*., art. 19.

Néanmoins, si le transfert se fait d'une province canadienne à une autre ou hors Canada, l'organisation doit veiller à rendre accessible « le fait qu'elle effectue ou non des transferts ou des communications de renseignements personnels interprovinciaux ou internationaux pouvant avoir des répercussions raisonnablement prévisibles sur la vie privée. »[730]

Il incombera à l'organisation qui procède au transfert, étant responsable des renseignements personnels qu'elle a décidé de recueillir et dont elle a établi les fins de traitement,[731] de « veille[r], contractuellement ou autrement, à ce que [son fournisseur de services] offre à leur égard une protection équivalente à celle qu'elle est tenue d'offrir sous le régime de la présente loi. »[732]

Ainsi, le fournisseur de services qui agit dans les limites de son mandat et qui utilise les renseignements personnels aux fins déterminées par l'organisation et pour lesquelles elle a obtenu les consentements valables requis n'est pas soumis à l'ensemble des obligations prévues au Projet de loi, sauf quant à celles des articles 57 et 61.[733] Toutefois, se fiant sur les enseignements de l'affaire *AggregateIQ*, le fournisseur aurait avantage à vérifier la validité des consentements obtenus par l'organisation pour procéder à la PCL, mais devrait assurément demander des garanties suffisantes à cet effet dans son contrat à l'organisation mandante qui lui a transféré les renseignements personnels. En effet, dans son rapport, le CPVP précisait :

> « Toutefois, dans des cas antérieurs, le CPVP a admis qu'en vertu de la LPRPDE, une organisation peut compter sur le consentement obtenu par une autre partie pour recueillir et utiliser des renseignements personnels. Ce faisant, cependant, le CPVP estime et conclut que l'organisation doit prendre des mesures raisonnables pour s'assurer que l'obligation de consentement est remplie, en s'assurant que l'utilisation et la communication des renseignements se font conformément au consentement des personnes concernées. »[734] [Mes soulignements]

Les engagements et représentations nécessaires devront être faits dans le contrat entre l'organisation et son fournisseur, et un mécanisme de communication des plus efficaces devra

[730] *Id*., art. 62(2)d). et Supra 5.4.2.
[731] *Id*., art. 7(1) et (2).
[732] *Id*., art. 11(1).
[733] *Id*., art. 11(2). Et Supra 5.3.1.
[734] 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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, *op., cit*., note 72, par. 20.

être mis en place afin de permettre l'accomplissement des différentes obligations qui incombent à l'organisation et au fournisseur de services en vertu de la loi, principalement celles de l'article 55(4) concernant une demande de retrait des renseignements personnels,[735]et de l'article 61 concernant la notification d'une atteinte de sécurité. En outre, le contrat devra prévoir des représentations et garanties de la part de l'organisation responsable en matière d'obtention des consentements valables et de non-responsabilité du fournisseur en cas de traitement de renseignements personnels pour les fins déclarées par l'organisation sans consentement valable.

Du côté du Québec, la Loi 25 prévoit également une exception au consentement pour un transfert à un fournisseur, mais exige un contrat écrit entre l'organisation et son fournisseur de services, et réitère le critère de nécessité. Ainsi, l'article 18.3 prévoit :

> « Une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elle confie à cette personne ou à cet organisme.
>
> Dans ce cas, la personne qui exploite une entreprise doit :
>
> 1° confier le mandat ou le contrat par écrit;
>
> […] » [Mes soulignements]

L'article 8(2) ajoute l'obligation d'informer la personne concernée « du nom du tiers pour qui la collecte est faite, du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins visées au paragraphe 1° du premier alinéa et de la possibilité que les renseignements soient communiqués à l'extérieur du Québec. » Le mot « tiers » devant raisonnablement se comprendre ici au sens de « fournisseurs de services » puisque la communication doit être nécessaire aux fins visées par l'organisation.

[735] « L'organisation qui procède au retrait des renseignements personnels d'un individu informe, dès que possible, tout fournisseur de services à qui elle a transféré les renseignements et veille à ce que celui-ci procède à leur retrait. » Projet de loi C-27, art. 55(4)

Communication à des tiers

Le fournisseur de services est toutefois susceptible de basculer dans la catégorie du tiers à qui ont été communiqués des renseignements personnels, et ainsi devenir assujetti à l'ensemble des obligations prévues par la loi, du moment où « il les recueille, les utilise ou les communique à toutes autres fins que celles pour lesquelles ils lui ont été transférés »[736] comme le précise le Projet de loi C-27. Je propose d'en résumer ci-dessous le régime applicable puis certains exemples récents jugés les plus pertinents.

Rappel du régime applicable : La LPRPDE, ne faisait pas de distinction claire entre une utilisation par un fournisseur de services et une communication à un tiers, au sens où le Projet de loi C-27 l'entend maintenant. Ainsi, sous l'article 4.3.7.b) de son annexe, la LPRPDE prévoit un régime de consentement négatif à la communication de renseignements personnels à des tiers, en spécifiant qu'une case à cocher pourrait permettre à une personne de refuser que ses renseignements personnels soient communiqués à d'autres organisations, mais que si la case demeure non cochée, alors l'organisation peut présumer que la personne consent à la communication de ses renseignements personnels.

Dans les lignes directrices sur le consentement valable, le CPVP, le CPVP-Alberta et le CPVP-Colombie-Britannique, se fondant sur le concept d'attentes raisonnables, ajoutaient toutefois que les organisations devraient être le plus précises possible quant aux tiers ou catégories de tiers si ces derniers sont trop nombreux ou changeant, à qui pourront être communiqués les renseignements personnels, considérant que « [l]es individus s'attendent à ce qu'une organisation ne communiquer pas à un tiers, à leur insu et sans leur consentement, les renseignements personnels qu'ils lui fournissent. »[737] En outre, ils ajoutaient que les organisations devraient « accorder une attention particulière à toute communication à des tiers susceptibles d'utiliser les renseignements à leurs propres fins plutôt que pour simplement leur

[736] *Id*., par. 11(2) *in fine*. Le tiers devient dès lors responsable des renseignements personnels qui « relèvent » dès lors de lui au sens de 7(1) et (2) du Projet de loi C-27.
[737] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, Principe directeur no. 1 « Mettre l'accent sur les éléments clés », par. 3, 2e boulet.

fournir des services de la part de l'organisation ayant originalement recueilli les renseignements ».[738]

Suivant cette ligne de pensée, le Projet de loi C-27 est venu préciser que pour obtenir un consentement valide, doit être révélé aux utilisateurs le nom des tiers ou catégories de tiers auxquels les renseignements personnels pourraient être communiqués[739] et a intégré l'obligation de fournir sur demande de l'individu le nom des tiers ou catégories de tiers à qui ses renseignements personnels ont été communiqués.[740]

Au Québec toutefois, l'article 13 de la Loi 25 prévoit que « [n]ul de peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie. »

Illustration du changement de statut « fournisseur de services » vers « tiers » : Voyons maintenant des exemples récents où une entreprise a été considérée comme un tiers plutôt qu'un fournisseur de services.

Dans la récente affaire *Home Depot*[741], le CPVP a considéré que le transfert de renseignements personnels vers Meta pour un outil de conversion en ligne, faisait de Meta un tiers à qui les renseignements avaient été communiqués sans consentement valide puisqu'elle utilisait ensuite les renseignements à ses propres fins. Selon le CPVP, ce transfert constituait une « communication » plutôt qu'une « utilisation » des renseignements personnels puisque les informations ont ensuite été traitées par Meta à ses propres fins commerciales incluant des fins publicitaires, ce qui aurait donc nécessité l'obtention d'un consentement supplémentaire puisqu'il s'agissait de fins secondaires.[742]

---

[738] *Id*.
[739] Projet de loi C-27, art. 15(3)e).
[740] *Id*., art. 63(2).
[741] CPVP, *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, Conclusions en vertu de la LPRPDE n°2023-001, *op. cit,* note 425. Supra 5.2.1.
[742] Éloïse GRATTON, Andy NAGY et François JOLI-CŒUR, *Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du*

Ainsi, il est possible de conclure que

> « [c]ela signifie qu'une organisation qui a obtenu un consentement valide pour recueillir et utiliser des renseignements personnels à des fins précises peut transmettre ces renseignements à un fournisseur de services tiers sans obtenir de consentement supplémentaire, pourvu que le fournisseur ne les traite qu'aux fins en question. Tant le fournisseur que l'organisation qui retient ses services pour traiter les renseignements personnels en son nom sont alors tenus par la LPRPDE de protéger les renseignements recueillis et de veiller à ce qu'ils soient traités exclusivement aux fins pour lesquelles le consentement a été donné[2]. »[743] [Référence omise]

Un autre exemple pertinent est celui de l'affaire *AggregateIQ* où les commissariats fédéral, de l'Alberta et de la Colombie-Britannique soulignaient que la LPRPDE ne contient pas d'exceptions relatives au consentement équivalentes à celles de la *Personal Information Protection Act* de la Colombie-Britannique[744], c'est-à-dire des paragraphes 12(2), 15(2) et 18(2) qui permettent à une entreprise qui agit pour le compte d'une autre organisation de traiter des renseignements personnels sans avoir directement obtenu le consentement des individus[745] :

> «12 Collection of personal information without consent
>
> (2)An organization may collect personal information from or on behalf of another organization without consent of the individual to whom the information relates, if
>
> (a)the individual previously consented to the collection of the personal information by the other organization, and
>
> (b)the personal information is disclosed to or collected by the organization solely
>
> (i)for the purposes for which the information was previously collected, and

---

Commissariat à la protection de la vie privée, *op. cit.*, note 446, par. 2 de la section « 1. La distinction entre " utilisation " et " communication " de renseignements personnels quand des informations sont transmises à un partenaire pour l'analyse des données »

[743] *Id.*, par. 1 de la section « 1. La distinction entre « utilisation » et « communication » de renseignements personnels quand des informations sont transmises à un partenaire pour l'analyse des données »

[744] *Personal Information Protection Act*, [SBC 2003] Chapter 63, en ligne : <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01 >

[745] 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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, *op., cit*., note 72, Consentement, par. 16-20.

(ii)to assist that organization to carry out work on behalf of the other organization. »[746]

Ainsi, le CPVP a conclu que *AggregateIQ* avait outrepassé les limites dans lesquelles avaient été donnés les consentements obtenus :

> « Dans le cadre de son travail pour des campagnes canadiennes, AIQ était souvent au fait du consentement obtenu par ces clients, qu'elle invoquait à ses fins, mais ce consentement ne s'étendait pas toujours aux travaux qu'elle effectuait pour ces campagnes. Par exemple, des gens ont souvent saisi leurs renseignements personnels sur des sites Web pour montrer leur soutien à un candidat ou à des campagnes. Ce faisant, ils auraient consenti à recevoir des nouvelles et des renseignements sur la campagne en question. Toutefois, ce consentement n'allait pas jusqu'à permettre que ces renseignements soient communiqués à Facebook ou à d'autres plateformes de médias sociaux aux fins de diffusion de publicités ciblées ou pour trouver et cibler des personnes similaires au moyen de l'analytique. »[747] [Mes soulignements]

Le CPVP recommandait donc que 1) *AggregateIQ* prenne les mesures raisonnables pour s'assurer que le consentement qu'elle invoque est bel et bien conforme à la loi de la Colombie-Britannique et à celle du Canada; 2) Que ces mesures devraient comprendre notamment des mesures contractuelles et l'examen du libellé du consentement utilisé par son client; 3) Que si les renseignements personnels s'avèrent être des renseignements sensibles, ou si le traitement des données dépasse les attentes raisonnables de l'individu, *AggregateIQ* doit alors s'assurer que le consentement licite a été obtenu pour ses fins. [748] *AggregateIQ* ne pouvait invoquer un consentement dont elle n'avait pas vérifié la validité et ne pouvait se dégager de cette responsabilité et s'en remettre uniquement aux dires de son client. Il lui incombait d'inclure les garanties et les obligations suffisantes au contrat avec son client et procéder à une réelle vérification de la licéité du traitement et de la validité des consentements.

---

[746] *Personal Information Protection Act*, [SBC 2003] Chapter 63, art. 12(2), en ligne: <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01 >

[747] 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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, *op., cit*., note 72, Conclusion, par. 5.

[748] *Id*., Constatations et recommandations, par. 94.

Ainsi, du moment où le transfert est considéré comme une communication en raison du changement de finalité contrairement aux attentes raisonnables des utilisateurs, ce tiers devient responsable de s'assurer que le consentement valable a été obtenu auprès de l'organisation qui lui a transféré les renseignements personnels.

Un autre exemple est celui dont traite le rapport d'enquête de 2018 du CPVP concernant la communication de renseignements détenus par Facebook sur ses utilisateurs par l'entreprise *Profile Techonology Ltd*. Dans cette affaire, des plaintes de Canadiens avaient été déposées auprès du CPVP contre cette entreprise de Nouvelle-Zélande[749] qui avait collecté à leur insu leurs renseignements de profil Facebook (nom, prénom, date de naissance, nom d'utilisateur, photo, situation amoureuse, politique, situation concernant les communications, lieu, écoles, groupes et clubs, noms des amis, choix musicaux, QI estimatif, influence sociale, allégations concernant les comportements sociaux) pour leur créer des profils individuels ou de groupe sur la plateforme de rencontre www.profileengine.com de l'entreprise *Profile Technology*.[750] Cette dernière avait alors affirmé que, suite à un contrat exécuté pour le compte de Facebook (pour la fourniture d'un puissant moteur de recherche), Facebook aurait accepté que Profile Technologie ait accès aux renseignements que les utilisateurs Facebook avaient consenti à rendre publics et accessibles sur les moteurs de recherche.[751] *Profile Technology* affirmait également qu'il n'était qu'un moteur de recherche comme *Google*, et non une plateforme de rencontre en soi. Le CPVP a refusé l'ensemble de ces arguments à l'effet que les renseignements étaient des renseignements publics et qu'ils pouvaient être validement utilisés par l'entreprise en vertu de son contrat avec *Facebook*. Le CPVP avait plutôt conclut :

> « À notre avis, basé sur l'examen du Résumé de l'étude d'impact de la règlementation associé au *Règlement* [Gazette du Canada, Partie II, vol. 135., no 1, SOR/DORS/2001-7], la justification qui sous-tend l'exception pour les renseignements accessibles au public dans le *Règlement* prévoie que les renseignements accessibles au public décrits sont d'un certain type ou d'une certaine qualité, de sorte que le consentement des personnes à les

[749] CPVP, *La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée, Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002*, *op. cit*., note 349.
[750] *Id*., par. 1 et 13.
[751] *Id*., par. 15.

> rendre publics peut être déduit par le simple fait que la personne les a fournis ou ne s'est pas opposée à leur accès, ou encore que leur publication sert un objectif public plus large. Dans le cas des profils Facebook, nous estimons qu'il n'est pas [clair] que des individus auraient eu l'intention de rendre leurs renseignements publics, particulièrement en l'espèce, puisque les profils Facebook en question ont été créés à un moment où Facebook était relativement nouveau et où ses politiques étaient en évolution. De plus, à l'époque, les profils Facebook permettaient par défaut l'indexation par les moteurs de recherche. Toutefois, tel que nous l'avons indiqué dans notre rapport de conclusions en vertu de la LPRPDE n° 2009-008, le Commissariat a analysé ce paramètre par défaut et soutenu qu'il n'était pas conforme aux attentes raisonnables des utilisateurs et qu'il n'avait pas été bien expliqué aux utilisateurs. De plus, les gens peuvent afficher de l'information sur Facebook pour diverses raisons (par exemple, pour être retrouvé et contacté par des amis), et pas nécessairement pour diffuser de l'information au grand public. »[752] [Mes soulignements]

Le CPVP a aussi adopté la même position à l'égard de *Facebook* dans son enquête de 2018 visant la communication de renseignements personnels à l'application tierce *thisisyourdigitallife* (TYDL), cette dernière les ayant ensuite transmises à la firme de recherche *Cambridge Analytica* et à sa filiale *SCL Elections*, qui avait malheureusement fait scandale aux États-Unis[753]. Au terme de son enquête, le CPVP avait conclu que Facebook aurait dû s'assurer que le consentement obtenu par un tiers était valable en s'assurant que les utilisateurs comprenaient raisonnablement les fins pour lesquelles leurs renseignements seraient utilisés et qu'en conséquence Facebook n'avait pas obtenu le consentement valable en contravention de la LPRPDE[754]. Fait important à noter ici, ces conclusions ont été rejetées par la Cour qui a conclu que « le [CPVP n'est pas parvenu à s'acquitter de la charge qui lui incombait de prouver que Facebook a enfreint la LPRPDE pour avoir omis d'obtenir des consentements valables. »[755]

Commentons ici le fait qu'effectivement, considérant le fait que *Facebook* monétise de manière très lucrative une quantité massive de renseignements personnels et dispose de moyens et ressources importants, il est raisonnable d'exiger de l'entreprise un degré de responsabilité supérieur et des mesures plus importantes par rapport à d'autres entreprises dont la mission

[752] *Id.*, par. 92.
[753] *Canada (Commissaire à la protection de la vie privée)* c. *Facebook, Inc.*, 2023 CF 533 (CanLII), par. 1, en ligne : <https://canlii.ca/t/jwq5l> (consulté le 24 avril 2023)
[754] *Id.,* par. 65.

[755] *Id*., par. 78.

première n'est pas le commerce de la donnée. En outre, cette attente plus grande s'explique et se justifie d'autant plus considérant les conséquences d'une communication non-autorisée à des tiers à des fins autres et à haut potentiel préjudiciable comme la désinformation nuisant à l'exercice démocratique (comme dans le cas du scandale *Cambridge Analytica*) ou encore de discrimination algorithmique intégrant des biais conscients ou inconscients (comme dans le cas de *Beaulieu* c. *Facebook*)[756].

D'ailleurs, les Normes canadiennes de la publicité en 2023 rappelaient, dans leur plus récent rapport sur le programme Choix de pub (2022), que les participants qui sont considérés comme des tiers par le programme et qui agissent aussi comme propriétaires, devraient porter une faire preuve d'une transparence accrue et s'assurer de mettre en place le mécanisme de retrait efficace malgré le nombre d'intervenants en place :

> « (…) en plus de fournir un avis sur la façon dont leur plateforme technologique utilise des données à des fins de publicité ciblée par centres d'intérêt et un mécanisme de retrait pour cette plateforme, ces tiers doivent également fournir :
>
> • Un avis portant sur les pratiques de publicité ciblée par centres d'intérêt sur le site Web, qui consistent à informer les utilisateurs de la divulgation de données à d'autres tiers à des fins de publicité ciblée par centres d'intérêt.
>
> • Un avis renforcé sur le site Web : un hyperlien situé au-dessus de la ligne de flottaison, sous la forme de l'icône et du texte Choix de pub ou dans un bandeau de consentement aux témoins et qui informe sur-le-champ le consommateur d'activités de publicité ciblée par centres d'intérêt et qui le dirige vers une mention complète des pratiques de publicité ciblée par centres d'intérêt sur le site Web.
>
> • Un mécanisme de retrait pour tous les tiers qui recueillent et qui utilisent des données sur le site Web à des fins de publicité ciblée par centres d'intérêt (plutôt qu'un mécanisme de retrait qui s'applique uniquement à la plateforme technologique du participant), en développant un outil à l'interne, en faisant appel à un prestataire approuvé ou en incluant un hyperlien vers l'outil *WebChoices* de la DAAC. »[757] [Mes soulignements]

[756] Supra, 1.2.2.

[757] LES NORMES CANADIENNES DE LA PUBLICITÉ*, Programme de responsabilité Choix de pub, Rapport de conformité 2022*, *op. cit.*, note 603, p. 7.

Ainsi, les organisations devront porter une attention particulière au type de transfert qui est fait et au régime applicable. Cela impliquera une analyse accrue et l'implantation d'une transparence et d'une communication considérable entre les différents intervenants afin que l'ensemble des obligations soient opérationnalisées.

6.2.3. Le consentement à la PCL comme condition de service

Comme vu plus haut[758], sauf dans les cas d'exception prévus par les lois en matière de vie privée, un réel choix doit être donné aux utilisateurs et, comme le rappelaient les commissariats, les utilisateurs doivent conserver la possibilité de choisir « oui » ou « non » au traitement de leurs renseignements personnels.[759] En conséquence, « [u]ne organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées. »[760]

Le CPVP, le CPVP-Alberta et le CPVP Colombie-Britannique dans leurs lignes directrices sur le consentement valable, permettaient exceptionnellement que le traitement de renseignements personnels puisse être une condition de services s'il est essentiel et nécessaire pour réaliser les fins légitimes divulguées par l'organisation :

> « La collecte, l'utilisation et la communication de renseignements personnels sur lesquels un individu ne peut exercer aucun contrôle (si ce n'est de renoncer à utiliser un produit ou un service) sont appelées « conditions de service ». 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. Les organisations devraient faire preuve de transparence et être préparées à expliquer les raisons pour lesquelles une collecte, une utilisation ou une communication en particulier est une condition de service, surtout si les raisons ne sont pas évidentes.

[758] Supra 6.1.2.
[759] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, Principe directeur no. 3 « Donner clairement aux individus la possibilité de choisir « oui » ou « non », par. 1.
[760] LPRPDE, Annexe I, art. 4.3.3.

> 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). »[761] [Mes soulignements]

Toutefois, concernant la PCL spécifiquement, le CPVP précisait qu'elle ne devrait pas être une condition pour utiliser un site Internet, bien qu'elle puisse être considérée comme une fin légitime. Ainsi, le CPVP considère qu'il existe des alternatives publicitaires à la PCL et donc que la PCL spécifiquement ne devrait pas constituer une condition de services[762] :

> « **Position :** Étant donné que certains utilisateurs peuvent être mal à l'aise à l'idée d'être "suivis" sur le Web, tout en jugeant utiles les publicités adaptées à leurs intérêts, et compte tenu du fait que les services sont généralement gratuits et que les utilisateurs doivent s'attendre à ce que certains renseignements personnels soient nécessaires pour accéder aux services et à l'information, la PCL peut être considérée comme une fin acceptable pour la collecte, l'utilisation ou la communication de renseignements personnels, du point de vue d'une personne raisonnable. Toutefois, la publicité comportementale en ligne ne devrait pas être considérée comme une condition permettant aux personnes d'utiliser Internet en général. Les sites Web peuvent compter sur d'autres formes de publicité. Un consentement valable et des limites sur les types de renseignements recueillis et utilisés à des fins de profilage sont nécessaires. La protection de l'information est également cruciale, tout comme l'est la limitation de la durée de conservation des données. »[763] [Mon soulignement]

Cette position a toutefois été critiquée en 2015 par Option Consommateurs au Québec, rapprochant au CPVP d'être resté trop vague sur le critère de nécessité :

> « Si ces nuances apportées par le CPVP évoquent la limitation des types de renseignements recueillis et utilisés, notons que le critère de nécessité y demeure encore là bien peu exploré. D'un côté, notre analyse des politiques de confidentialité révèle que les services en ligne recueillent, à toutes fins pratiques, toute bribe d'information pouvant être captée sur leurs utilisateurs. De l'autre, pourtant, les conclusions du CPVP à l'égard de la PCL effectuée dans le cadre de la fourniture d'un service sans frais semblent occulter le fait que, même si les fins de la collecte d'un renseignement sont acceptables, une

[761] CPVP, *Lignes directrices pour l'obtention d'un consentement valable*, *op. cit*., note 212, Principe directeur no. 3 « Donner clairement aux individus la possibilité de choisir " oui " ou " non " », par. 1, 2 et 3.

[762] Il est raisonnable de penser que le CPVP pourrait avoir la même position à l'égard d'autre type de publicité s'appuyant sur une forme de ciblage, tel le reciblage publicitaire puisqu'il implique également un "suivi" de l'utilisateur.

[763] CPVP, *Position de principe sur la publicité comportementale en ligne*, *op. cit*., note 11, section **«** L'offre de publicités ciblées en fonction des comportements est-elle une fin acceptable aux termes du paragraphe 5(3) de la LPRPDE et constitue-t-elle une condition de service? », dernier paragraphe.

entreprise " ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées ".

On peut ici se demander si le critère de nécessité, aussi légitimes les fins soient-elles, n'a pas été trop expéditivement gommé. Est-il vraiment nécessaire de colliger toutes les informations générées par un internaute pour atteindre la rentabilité commerciale? En pratique, force est d'admettre que, sous [le] couvert d'une fin acceptable, on semble imposer aux consommateurs un prix sans aucun plafond pour obtenir des services en ligne.

Dans un tel contexte, il n'est peut-être pas déraisonnable d'espérer que le principe de limitation de la collecte dans le cadre de la PCL soit revisité. L'exercice, bien entendu, s'avèrerait fastidieux et dépasserait largement le cadre de la présente recherche. Cela exigerait non seulement l'accès aux algorithmes des entreprises en ligne, mais aussi le déploiement de ressources technologiques et juridiques importantes afin d'analyser ceux-ci. Cependant, les autorités gouvernementales devront peut-être envisager sérieusement de s'y astreindre si elles souhaitent évaluer plus qu'approximativement la conformité des entreprises à la loi. »[764]

Notons que par la suite, le Projet de loi C-27 est venu préciser qu'une organisation qui fournit un bien ou service à un individu ne peut exiger que cet individu consente à la collecte/utilisation/communication de renseignements non nécessaires à la fourniture du bien ou la prestation du service, en raison du fait qu'elle lui fournit un bien ou un service.[765] La pierre angulaire de cette analyse sera donc le critère de nécessité.[766]

Décision majeure à venir au Québec

Cela dit, Option Consommateurs n'aura pas attendu l'action espérée de la part des autorités gouvernementales pour prendre action.

En effet, une décision importante était rendue par la Cour supérieure à l'été 2022 autorisant l'action collective intentée par Option Consommateurs contre *Google*[767] dans laquelle il est reproché à *Google* « de recueillir sans autorisation préalable des renseignements de ses

[764] OPTION CONSOMMATEURS, *Le prix de la gratuité. Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne ?*, *op. cit*., note 609, p. 43-44.
[765] Projet de loi C-27, par. 15(7).
[766] Supra, 4.2.
[767] Supra, 2.1.6.

utilisateurs lorsqu'ils utilisent les Services *Google* ou les Outils *Google* et de les partager avec des tiers »[768] dans un contexte de création de profils à des fins de profilage et ciblage publicitaire, et ce malgré le mode de navigation privée employée par les plaignants. Ainsi :

> « [3] Selon la demanderesse, *Google* n'obtiendrait pas le consentement suffisant des membres du groupe afin de collecter leurs renseignements personnels lorsqu'ils utilisent ses services ne nécessitant pas la création d'un compte *Google* (les « Services *Google* ») ou lorsqu'ils naviguent sur des sites Internet utilisant l'un des outils publicitaires ou d'analyse offerts par elle (les « Outils *Google* »). Plus spécifiquement, la demanderesse allègue que *Google* refuse et/ou néglige d'obtenir le consentement suffisant des membres du groupe :
>
> • En ne recherchant pas un tel consentement dans le cadre de ses conditions d'utilisation et/ou en n'obtenant pas un tel consentement dans le cadre d'une politique de confidentialité inutilement longue, complexe et sinueuse;
>
> •En ignorant sciemment les demandes expresses des membres du groupe envisagé qui lui signifient refuser cette collecte par l'entremise de la fonction « interdire le suivi » de leur navigateur; et
>
> • En représentant faussement aux membres du groupe envisagé qu'ils peuvent contrôler les renseignements personnels qu'elle collecte sur eux, notamment en affirmant que le mode de navigation privée permet de parcourir l'Internet confidentiellement. »[769] [Mes soulignements]

Le Tribunal a conclu qu'il y avait bel et bien eu violation du droit à la vie privée en vertu de la LPRPDE et de la Loi sur le privé constituant une faute civile au sens du CCQ, mais également qu'il y avait eu démonstration de la cause en dommages en vertu de la Charte québécoise des droits et libertés :

> « [110] Ainsi, il y a donc violation du droit à la vie privée, ce qui constitue une faute civile. Le Tribunal conclut qu'il y a également démonstration par la demanderesse de dommages compensatoires et de causalité en vertu de l'article 49 alinéa 1 de la Charte, pour les mêmes motifs que ceux indiqués précédemment quant à l'article 1457 CcQ. En effet, un recours en vertu de la Charte suit la même logique qu'un recours en vertu du CcQ : dans la mesure où un manquement à un droit protégé par la Charte est établi, il y faute civile, et ensuite dommage et lien de causalité doivent être établis. »[770] [Références omises]

---

[768] Joannie LANGLOIS, « Action collective autorisée contre Google », SOQUIJ | Blogue (20 juillet 2022), par. 1, en ligne : < https://blogue.soquij.qc.ca/2022/07/20/action-collective-autorisee-contre-google/ > (consulté le 12 février 2023)

[769] *Option Consommateurs* c. *Google*, 2022 QCCS 2308 (CanLII), *op. cit.*, note 196, par. 3.

[770] *Id.*, par. 110.

Concernant les violations alléguées à la LPC, le « Tribunal [a conclu] que la demanderesse a démontré sa cause d'action en dommages compensatoires et punitifs en vertu de l'article 41 LPC pour la navigation privée seulement. Toutes les autres allégations relatives à la LPC sont rejetées, car elles n'ont pas été démontrées. »[771] Et concernant les violations alléguées à la Loi sur la concurrence, le Tribunal a conclu que la demanderesse a démontré sa cause d'action en dommages compensatoires pour la navigation privée seulement et autorise la conclusion permettant à la demanderesse de réclamer les honoraires d'avocats, les déboursés et les frais d'expert, en vertu de l'article 36(1) de cette loi.[772] Le Tribunal a donc rejeté toutes les autres allégations relatives à cette loi, car elles n'ont pas été démontrées.[773]

Ainsi, outre les questions de consentement dans un contexte de services gratuits, un débat fort intéressant aura lieu concernant l'existence de préjudice, la nature et l'évaluation des dommages, ainsi que sur la valeur des renseignements personnels. En effet, à l'étape de l'autorisation du recours collectif, il a été reproché à *Google* de monétiser les renseignements personnels de ses membres, et le Tribunal a conclu à l'existence d'un dommage et a accepté l'analogie de la demanderesse avec le droit à l'image et l'application des principes dégagés par les arrêts célèbres *Laoun* c. *Malo*[774] et *Aubry* c. *Éditions Vice-Versa inc.*[775]

Je propose d'en reproduire ici les principaux passages pertinents afin de saisir l'ampleur de l'intégration du concept « d'appropriation » employé par le Tribunal, du parallèle proposé avec le droit à l'image et de la conclusion concernant l'évaluation des dommages qui devraient correspondre à une somme égale à la valeur des renseignements personnels recueillis par *Google*:

> « [98] Donc, selon ce que la demanderesse allègue et qui est avéré, *Google* s'approprie sans droit les renseignements personnels des membres du groupe, qu'elle utilise afin de créer des profils d'utilisateurs qui lui permettent d'être le leader mondial en matière de publicité ciblée et de générer, en 2019, des revenus de 134 811 milliards de dollars américains attribuables à la publicité en ligne.

[771] *Id.*, par. 137.
[772] *Id.*, par. 142.
[773] *Id.*, par. 143.
[774] *Laoun* c. *Malo*, 2003 CanLII 24556 (QC CA), en ligne : <https://canlii.ca/t/1c1zb> (consulté le 19 février 2023)
[775] *Aubry* c. *Éditions Vice-Versa inc.*, 1998 CanLII 817 (CSC), [1998] 1 RCS 591, en ligne : <https://canlii.ca/t/1fqt6> (consulté le 19 février 2023)

[99] Dans ces circonstances, le Tribunal accepte l'analogie que présente la demanderesse quant aux dommages. En effet, il existe en jurisprudence peu d'exemples de cas dans lesquels le fait qu'un bien soit dérobé par une personne ne prive pas nécessairement son possesseur original de la possibilité d'en jouir. Le Tribunal accepte ainsi la suggestion de la demanderesse selon laquelle le parallèle le plus utile est celui du droit à l'image. En effet, lorsqu'une personne voit son image utilisée à des fins commerciales sans son autorisation, elle n'est pas nécessairement privée de la possibilité de faire elle-même une utilisation commerciale de cette image. Les tribunaux reconnaissent cependant que la personne qui usurpe l'image est responsable d'indemniser sa victime du gain manqué en raison de sa faute, le tout en vertu de l'article 1611 CcQ. Ce courant jurisprudentiel reconnaît donc l'existence d'un dommage dans ce cas.

[100] Dans l'arrêt *Laoun* c. *Malo*, la Cour d'appel a reconnu qu'une comédienne était en droit de recevoir l'équivalent du cachet qu'elle avait reçu à l'origine pour associer son image à une marque de lunettes après que les photos promotionnelles ont été réutilisées sans droit : […]

[101] S'il est vrai que cette évaluation se fait relativement aisément lorsque la victime a l'habitude d'utiliser son image commerciale et qu'un marché connu existe pour en déterminer la valeur, la méthode demeure la même lorsque la victime est anonyme aux yeux du public comme en témoigne cet extrait de l'arrêt *Aubry* c. *Éditions Vice-Versa inc*. de la Cour suprême du Canada :

> [74] En ce qui a trait à l'aspect patrimonial de l'atteinte à la vie privée, nous sommes d'avis que l'exploitation commerciale ou publicitaire de l'image, qu'elle soit d'une personne connue ou d'un simple particulier, est susceptible de causer à la victime un préjudice matériel. L'indemnité doit alors être calculée en fonction de la perte effectivement subie et du gain manqué (art. 1073 *C.c.B.C.*). […] Ni le juge de première instance, ni les juges de la Cour d'appel, n'ont traité de la question de l'aspect patrimonial du dommage. Or, l'intimée était en droit d'exiger une somme en échange de l'utilisation de son image. L'intimée a allégué qu'il y a eu exploitation commerciale et elle a présenté une preuve à l'appui de la demande de dommages et intérêts à ce titre. Le témoignage de M. Gilbert Duclos révèle que celui-ci doit habituellement payer entre 30 $ et 40 $ l'heure pour les services d'un mannequin, généralement pour une période de deux à quatre heures. L'intimée aurait donc normalement eu droit à une somme d'argent. Notons qu'en l'espèce, c'est la seule preuve dont nous disposions pour calculer ces dommages. Dans d'autres circonstances, suivant la preuve offerte, il n'est pas impossible que les dommages patrimoniaux soient compensés par une participation aux profits, suivant les principes du gain manqué et de la perte subie.
>
> […]

[102] De l'avis du Tribunal, au présent stade, ces arrêts démontrent : 1) l'existence de dommages ici; et 2) une méthode simple et claire pour évaluer le préjudice matériel associé à l'utilisation commerciale sans droit des renseignements personnels des membres du groupe.

> [103] Dans ces circonstances, le Tribunal est d'avis qu'« il n'est pas déraisonnable de conclure » que les membres ont subi un dommage d'une somme égale à la valeur des renseignements personnels recueillis par *Google* lorsqu'ils utilisent les Services *Google* ou parcourent la Toile. Le montant ou le quantum n'a pas à être précisé au présent stade.
>
> [104] Finalement, quant à la causalité entre la faute et les dommages, le Tribunal est d'avis qu'elle doit être ici présumée, à titre de présomption de fait provenant des allégations factuelles de la Demande modifiée. On peut présumer que le dommage équivalent à la valeur des renseignements personnels recueillis par *Google* est causé par la collecte illégale des renseignements personnels par *Google*.
>
> [105] Le Tribunal conclut donc que la demanderesse a établi tous les éléments requis pour démontrer la présence de responsabilité extracontractuelle de *Google* en vertu de l'article 1457 CcQ. Passons à la *Charte des droits et libertés de la personne*. »[776]
>
> [Mes soulignements, Référence omise]

Ainsi, il est vrai que le droit à la vie privée dont découle la protection des renseignements personnels est un droit de la personnalité. Il est également évident que l'expectative de vie privée des utilisateurs naviguant en mode privé n'a pas été respectée et que *Google* ne pourra justifier une telle contravention.

Toutefois, le parallèle quant à la nature du dommage et à son évaluation me semble plus difficile à appliquer tel quel dans un contexte de PCL. En effet, dans les deux arrêts auxquels font référence la demanderesse et le Tribunal, les plaignantes étaient des personnes reconnaissables dans les publications non autorisées. Ainsi, l'utilisation ou la réutilisation de leur image sans leur consentement leur portait préjudice d'une façon différente de celles des personnes dont les renseignements personnels ont utilisé sans leur consentement.[777]

Dans le cas de *Google*, les circonstances sont différentes dans la mesure où le ciblage ne se fait pas sur une base individuelle, mais sur la base du groupe d'intérêts dans lequel se retrouve le profil de l'utilisateur. En outre, bien que ces services ne nécessitent pas la création d'un compte *Google*, il y a tout de même une utilisation des services et outils fournis par *Google* en

[776] *Option Consommateurs* c. *Google*, *op. cit*., note 196, par. 98 à 105.
[777] Dans le cas de Mme Malo, il s'agissait de compenser le manque à gagner. Dans le cas de Mme Aubry, il s'agissait aussi d'un manque à gagner, mais également d'une atteinte à sa réputation lui ayant causé un préjudice moral.

contrepartie de renseignements que pourra utiliser *Google* pour fournir ses services publicitaires et ainsi financer ces services.

Il sera donc fort intéressant de suivre cette affaire, dont les conclusions auront un impact important sur l'écosystème numérique au Québec.

UE : projet de règlement ePrivacy et Cookie Wall

La question du consentement continue de faire l'objet de nombreux débats et questionnements, tant sur sa forme et sur sa gestion, que sur sa répercussion sur le financement de nombreuses plateformes éditrices et incidemment sur l'accès au contenu en ligne. Les mêmes débats et recherche de compromis s'observent en Europe où les discussions se poursuivent concernant l'encadrement juridique du *Cookie Wall* au sein du règlement *ePrivacy* et où l'industrie publicitaire y poursuit ses démarches dans le but de faire reconnaître le véritable *Cookie Wall*, c'est-à-dire de pouvoir bloquer complètement l'accès à un site sans être obligé de proposer une alternative directement sur le site.[778]

Ainsi, en date de février 2022, le Considérant 20 aaaa du projet de règlement *ePrivacy*, proposait que les éditeurs puissent rendre disponible une version de base de leur plateforme aux utilisateurs refusant de consentir à l'utilisation des cookies à des fins marketing, et une version complète de cette plateforme aux utilisateurs qui accepteraient ces cookies :

> « In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would

[778] GESTE, « EPrivacy : La phase de trilogue peut enfin commencer ! » (26 février 2022) en ligne : <https://geste.fr/eprivacy-la-phase-de-trilogue-peut-enfin-commencer/> (consulté le 7 janvier 2023)

> normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position. »[779]

Le fait d'interdire aux éditeurs européens de refuser l'accès à leur site à un utilisateur qui n'aurait pas accepté les *cookies* impliqués pose évidemment problème. C'est pourquoi ce Considérant a été jugé encourageant par les éditeurs.[780] Notons que sont exclus de la demande de consentement les cookies/traceurs de mesure d'audience pour le compte de l'éditeur du site ou du service expressément demandé par l'utilisateur.[781] En deuxième lieu, dans leur critique de ce projet de règlement, les éditeurs mettent l'accent sur le fait qu'« [e]n dehors des problématiques publicitaires, une rédaction trop stricte pourrait avoir des conséquences importantes pour les éditeurs et notamment de potentiels impacts sur les certificateurs d'audience, la rémunération des ayants droit, les relations commerciales (mesure de la performance publicitaire y compris contextuelle) …».[782] En effet, il est important de considérer l'écosystème numérique dans son ensemble ainsi que le rôle de la publicité dans son financement, sans toutefois négliger de trouver un encadrement juridique nécessaire, mais équilibré.

6.3. Les limites du consentement : défis et réflexions

Rendre possible l'exercice d'un certain contrôle est l'un des éléments permettant de contribuer à la mise en équilibre, voire à la conciliation entre les besoins et les intérêts des utilisateurs par rapport à ceux des autres parties prenantes participants à la PCL. Toutefois, il convient d'en reconnaître les limites afin d'améliorer les pratiques.

[779] *Id*.
[780] *Id*.
[781] *Id*.
[782] *Id*.

6.3.1. Le consentement individuel n'est pas la solution à tous les enjeux individuels et collectifs vécus dans l'univers numérique

À l'époque de la conception du Projet de loi 64, le Professeur Pierre Trudel critiquait un régime qui jusque-là avait été trop axé sur le consentement et donc affaibli par les limites inhérentes au consentement, au détriment d'autres obligations qui protègeraient davantage les utilisateurs, soit la transparence, la responsabilité / l'imputabilité des organisations et la sécurité. Ainsi, il expliquait que

> « [l]es lois ne peuvent plus reposer sur la fiction que c'est l'individu qui aurait le "contrôle" de ses données. Une telle conception a donné lieu à un cadre juridique dysfonctionnel qui, dans le monde hyperconnecté, ne protège personne. »[783]

Il soutenait au contraire qu'elles « ont surtout facilité l'accaparement par les géants du Web de la valeur des données produites dans le monde connecté »[784], alors que les « enjeux réels associés à la valorisation des informations produites dans le monde connecté » sont plutôt d'assurer la sécurité et la confidentialité des données et d'éviter les pratiques discriminatoires auxquelles le consentement individuel ne peut pallier, telle la discrimination algorithmique dont nous avons vu un exemple récent ci-dessus[785] qui pourrait être amplifiée par l'utilisation de l'intelligence artificielle intégrant les divers biais, ainsi que la détermination dynamique des prix[786] (*dynamic pricing*) dont je n'ai pas traité spécifiquement dans ce mémoire faute d'espace. Sur ce sujet précis, je soulignerais rapidement que cette pratique soulève de nombreuses questions éthiques et légales, à plus forte raison si elle est faite de manière occulte et à mauvais escient de manière à créer une forme de discrimination non justifiable. En effet, comme le soulignait Virginie Jetté au sujet la tarification comportementale :

> « (…) la tarification comportementale réfère aux changements de prix qui peuvent résulter de données qui indiquent si les consommateurs sont plus susceptibles de payer des prix plus élevés pour un bien. Cette forme de manipulation du marché représente, selon certains, une violation manifeste de la confiance envers les entreprises et constituerait

[783] Pierre TRUDEL, « Renseignements personnels : les vraies urgences », Le Devoir (18 février 2020), par. 4, en ligne : <https://www.ledevoir.com/opinion/chroniques/573151/renseignements-personnels-les-vraies-urgences> (consulté le 22 avril 2023)
[784] *Id.*, par. 1.
[785] Supra 1.2.2.
[786] *Id.*, par. 6. Et Supra, p. 124.

> une pratique trompeuse soutenue par la collecte d'information sur le comportement des consommateurs. »[787]

Ainsi, comme elle le constatait :

> « Une tarification comportementale ciblée est actuellement en place dans les industries hôtelières et aériennes, où toutes les informations disponibles sur les consommateurs sont prises en compte lors de la tarification de ce type d'actifs tangibles et physiques, mais temporaires[788]. Certains soutiennent que l'échange de renseignements sur les consommateurs au sujet de la préférence et de la viabilité d'une chambre d'hôtel ou d'un siège d'avion couplé avec les prix ciblés par l'analyse comportementale des consommateurs a un effet positif[789]. Or, les perceptions d'illégalité augmentent lorsque les entreprises utilisent le marketing comportemental non seulement pour cibler les marchandises vers les consommateurs, pratique qui, bien que « désagréable », n'annule pas la liberté d'action du consommateur, mais modifient les prix des biens en fonction de ce qu'ils savent payer. Essentiellement, il s'agit d'une forme de discrimination de prix où " [the] goal of price discrimination is to maximize profits by adjusting the price that different customers pay based on data about the consumer "[790]. »[791]

Dans un contexte de PCL, force est de constater qu'une grande attention a été et est encore portée sur le consentement comme moyen de contrôle individuel des actions de ciblage et de profilage publicitaire qui inspire un sentiment naturel d'inconfort, alors que les actions réellement préjudiciables pour les utilisateurs sont plutôt au niveau des dérives possibles d'une utilisation à mauvais escient, tels les exemples cités par Trudel soit l'incident de sécurité engendrant un vol d'identité ainsi que les pratiques discriminatoires. Comme le soulignait Trudel, il s'agit d'enjeux non seulement individuels[792], mais collectifs et en ce sens, que le contrôle individuel ne serait réglé à lui seul.

Dans le même ordre d'idée, et toujours dans le contexte du Projet de loi 64 au Québec, d'autres juristes avaient soulevé la problématique que la réforme mettait en place une nouvelle loi qui

---

[787] Virginie JETTÉ, *op. cit*, note 19, p. 63

[788] Nicola JENTZSCH, Geza SAPI et Irina SULEYMANOVA, « Targeted pricing and customer data sharing among rivals » (2013) 31:2 International Journal of Industrial Organization 131.

[789] *Id*.

[790] Allen GANNETT, « Behavioral Pricing: A Consumer's Worst Nightmare » (21 janvier 2012), en ligne : The Next Web (consulté le 6 décembre 2016).

[791] Virginie JETTÉ, *op. cit*, note 19, p. 64.

[792] Pierre TRUDEL, « Renseignements personnels : les vraies urgences », *op. cit*., note 783, par. 2.

avait pour seule base légale le consentement, et craignant que la multiplication des avis et des demandes de consentement qui en découlerait ait un effet négatif sur l'expérience de navigation et d'utilisation, mais rendant banal et dénué de sens l'exercice du consentement des utilisateurs pourtant central et primordial.

Parmi ceux-ci, Me Gratton était d'avis, dans ses commentaires soumis à la commission de révision de la Loi sur le privé, que le consentement ne devait être réservé qu'aux décisions réellement importantes et sur lesquelles les individus avaient un réel choix :

> « Un recours excessif au consentement ne fournit qu'un faux sentiment de protection et vide le concept même de consentement de toute utilité ou de sens. Le consentement doit être une mesure de dernier recours, qui signale aux personnes concernées l'importance de l'activité à laquelle elles consentent. L'importance du consentement est perdue lorsqu'il est sollicité pour une activité banale. L'utilisation du consentement devrait idéalement être limitée aux situations où la personne concernée se voit offrir un choix réel, par opposition à un choix purement illusoire, ou inexistant. »[793] [Mes soulignements]

C'est pourquoi, elle proposait plutôt d'inclure d'autres bases légales de traitement, comme sous le RGPD :

> « (…) le renforcement du consentement, qui a déjà été amorcé dans le projet de loi [64], devrait être poursuivi avec une approche plus novatrice, en introduisant des bases juridiques autres que le consentement, comme c'est le cas en en Europe […] [où] le RGPD reconnaît cinq autres bases légales de traitement, dont les intérêts légitimes d'une entreprise ou la nécessité d'exécuter un contrat (on peut penser ici aux contrats de service ou aux contrats de travail). Cette approche a été défendue avec succès en Europe et n'a pas entraîné une perte de contrôle des renseignements personnels par les individus, et ce, en partie grâce aux protections offertes par la loi. ».[794] [Références omises, Mes soulignements]

Comme nous l'avons vu plus haut, d'autres bases légales de traitement ont été intégrées dans la Loi 25 et sont proposées dans le Projet de loi C-27. Toutefois, dans un contexte de PCL, puisque la forme de consentement requise semble se diriger vers un consentement positif, et ce de manière distincte pour toutes les finalités, l'avenir nous dira si effectivement cela aura pour effet de diluer cet exercice et de le banaliser. Peut-être y aurait-il plutôt lieu de limiter les demandes

[793] Éloïse GRATTON, *Nos réflexions sur le projet de loi no 64 (protection de la vie privée dans le secteur privé au Québec*, *op. cit*., note 591, section « I – La notion de " consentement "», par. 3.
[794] *Id*., section « I – La notion de " consentement "», par. 4.

de consentement explicite aux traitements de renseignements sensibles, tout en maintenant toutes les autres obligations en place et en s'assurant que les utilisations avec un potentiel préjudiciable, discriminatoire ou de désinformation, puissent être mieux détectées par les autorités de contrôle et par les individus.

6.3.2. Les limites au consentement éclairé

Il est raisonnable de questionner la possibilité que ce consentement soit bien libre et éclairé dans un environnement numérique complexe. De surcroît, comment y parvenir « dans un contexte où tout se passe à une vitesse impressionnante ? »[795]

En effet, l'effectivité d'un régime basé sur le consentement, sous sa forme explicite de surcroit, repose sur la capacité des utilisateurs de comprendre non seulement les nombreux avis et politiques nécessaires à l'exercice de leurs choix, mais également le fonctionnement de l'écosystème numérique en général, les flux de données, les types de renseignements traités, les types d'utilisation et finalités, le niveau de confiance à allouer à telle ou telle organisation en matière de sécurité et de PRP, et les conséquences de donner ou de refuser un consentement, etc. Or, en 2003, 22 % de la population québécoise de plus de 16 ans n'avait qu'un niveau 1 de littéracie, c'est-à-dire un niveau « très faible » en compréhension de textes,[796] influençant leur capacité à « prendre des décisions éclairées, atteindre [leurs] objectifs personnels et bien évoluer en société »[797].

En outre, nous pouvons aussi questionner le niveau d'intérêt, de disponibilité (temps) et de volonté des utilisateurs à lire et analyser l'information fournie et à exercer un choix, et ce de manière répétée, au fil des sites et applications consultés, et des ajouts ou modifications de finalités. De surcroit, pour que ce choix soit complet, il peut devoir impliquer le paramétrage de tous les navigateurs utilisés -dont la configuration est différente- sur tous les appareils utilisés

[795] Virginie JETTÉ, *op. cit*., note 19, p. 108.
[796] *Enquête internationale sur l'alphabétisation et les compétences des adultes (EIACA)*, 2003, dans LE CENTRE DE DOCUMENTATION SUR L'ÉDUCATION DES ADULTES ET LA CONDITION FÉMININE (CDÉACF), « Situation de l'alphabétisation au Québec », par. 6, en ligne : <http://cdeacf.ca/ace/a_propos/situation > (consulté le 22 avril 2023)
[797] FONDATION POUR L'ALPHABÉTISATION, « La littératie : mieux la comprendre », en ligne : <https://fondationalphabetisation.org/lanalphabetisme/tout-sur-lanalphabetisme/la-litteratie/ > (consulté le 22 avril 2023)

(tablette, cellulaire, ordinateur), en plus de tenir compte des modules d'opposition d'éditeurs (ex : désactivation des *cookies Google Analytics*).[798]

Corolairement, l'exercice du droit de retrait du consentement comporte également son lot de défis, tant techniques, technologiques, qu'humains[799]. Il s'agit d'ailleurs d'une des limites importantes soulevées à juste titre par Option Consommateurs dans son rapport de 2015 sur la PCL, où il y dénonçait notamment « la portée inégale » des options de retrait d'un service à l'autre[800] ainsi que la formule de retrait « à la pièce » c'est-à-dire pour chaque entreprise participant à la PCL[801]. Option Consommateurs y reconnaissait d'ailleurs le mécanisme de retrait de la DAAC « parmi toutes les options offertes par les entreprises [comme] le moyen paraissant le plus simple et efficace pour refuser la PCL (…) laquelle permet de se désinscrire en bloc du suivi des nombreuses entreprises participantes »[802]. Toutefois, l'effectivité du programme demeure encore limitée à son niveau de notoriété dans la population et du nombre d'organisations participantes qui y adhèrent, bien que ce nombre soit en croissance, comme le remarquait notamment Virginie Jetté :

> « Si certaines solutions apportées semblent bonnes, elles comportent également leurs lots de failles. D'une part, comme il s'agit d'autorégulation, celle-ci se fait sur une base volontaire. D'autre part, les utilisateurs ne connaissent pas nécessairement les bienfaits de tels programmes et ne cherchent pas non plus à les découvrir puisqu'ils ne sont pas nécessairement conscients du risque posé par les témoins.
>
> Or, l'ultime problème des programmes d'autorégulation semble émerger dans le confort qu'ils produisent. Un utilisateur serait tenté de croire qu'il met fin à la collecte de

[798] Exemples tirés de la politique de la plateforme française « vousfinancer » : VOUS FINANCER, « Données personnelles et gestion des cookies », en ligne : <https://www.vousfinancer.com/donnees-personnelles > (consulté le 19 avril 2023)
[799] Supra, 6.2.1.3.
[800] OPTION CONSOMMATEURS, *Le prix de la gratuité. Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne ?*, *op. cit*., note 609, p. 29, par. 2.
[801] *Id*., p. 28.
[802] *Id*., p. 29, par. 1.

renseignements personnels alors qu'il met plutôt fin à la publicité comportementale[803]. » [804]

6.3.3. Les limites au consentement libre

De plus, il est raisonnable de souligner les limites au caractère libre de l'exercice du consentement.

Bien que le consentement ne puisse plus être une condition de services[805], il comprend tout de même un choix de la part de l'utilisateur quant au niveau de contenu auquel il aura accès gratuitement et au prix qu'il est prêt à payer pour avoir accès au contenu. Par exemple, certaines plateformes éditrices ont déjà choisi d'offrir la possibilité à l'utilisateur d'opter pour un accès gratuit avec publicité ou un accès payant sans publicité sous forme d'abonnement, ou encore d'offrir un accès illimité par abonnement ou un accès gratuit avec un accès limité au contenu. Ainsi, ce choix implique une volonté et une capacité financière de payer pour le contenu consulté au lieu d'y avoir accès gratuitement (ex : *Spotify Premium*, Le Devoir, etc.).

De plus, l'explosion des objets connectés (Internet des objets), venant déjà complexifier la donne au niveau des critères de nécessité et de limitation considérant la collecte vaste et potentiellement infinie de données qu'elle permet[806], présente des enjeux au niveau de la transparence et du consentement. En effet, comme en faisait déjà état Alexandre Plourde dans sa critique de 2019 sur l'Internet des objets et la PRP, les pratiques de traitement de renseignements personnels qu'il a étudié n'étaient généralement accessibles qu'après l'achat de l'objet en question soit lors de l'installation. Dès lors l'acheteur ne disposait pas d'un réel choix

---

[803] The Economist, « Getting to know you » (11 septembre 2014), en ligne : <https://www.economist.com/special-report/2014/09/11/getting-to-know-you?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18798097116&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=EAIaIQobChMIhYrN4YfQ_gIVASqzAB09bwHqEAAYASAAEgI1X_D_BwE&gclsrc=aw.ds> (consulté le 18 avril 2016), cité par : Virginie JETTÉ, *op. cit*., note 19, p. 114-115.

[804] Virginie JETTÉ, *op. cit*., note 19, p. 114-115.

[805] Supra, 6.2.3.

[806] Alexandre PLOURDE, « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans Barreau du Québec, Service de la formation continue, Développements récents en droit à la vie privée (2019), vol 465, Montréal (QC), Éditions Yvon Blais, 2019, 33, par. « C. Les limites d'une collecte infinie », en ligne : <https://edoctrine.caij.qc.ca/developpements-recents/465/369051330/ > (consulté le 22 avril 2023)

par rapport au traitement de ses renseignements personnels outre que d'arrêter d'utilisation l'objet ou l'application dans certains cas.[807] En outre, il ajoutait la problématique d'une collecte par ses objets dans des lieux publics où le consentement devient illusoire :

> « [l]a présence de ces appareils dans des lieux pouvant être fréquentés par plusieurs personnes étire les limites du principe du consentement. Comment le passager d'une voiture connectée ou le visiteur d'une maison où se trouve un assistant vocal, par exemple, peuvent-ils valablement être informés et consentir à ce qu'on recueille leurs renseignements personnels ? Comment assurer la conformité à la loi lorsqu'un tel appareil se trouve dans un lieu public ?
>
> On peut trouver quelques pistes de réponse dans les décisions de la CAI concernant la vidéosurveillance, qui indiquent que, conformément au critère de nécessité, cette pratique doit être effectuée de la manière la moins intrusive possible et que l'entreprise qui s'y livre doit en informer le public, par exemple au moyen d'avis. Cependant, appliquer la même logique dans l'environnement connecté, où une multitude d'objets peuvent simultanément recueillir, en permanence, des données concernant des personnes en chaque lieu, pose des problèmes qu'on peine à résoudre avec les solutions déjà dégagées par la CAI. »[808] [Mes soulignements, référence omise]

Ainsi, la configuration des paramètres de confidentialité par défaut pourra résoudre plusieurs situations problématiques eu égard au consentement, mais ne les règlera pas toutes. En ce sens, il s'agit ici d'une autre limite au consentement.

6.3.4. Autres limites

Une autre limite concerne les utilisateurs multiples pour un même appareil, par exemple l'ordinateur familial. En effet, l'exercice pourrait s'avérer complexe pour les plateformes qui se fondent sur l'adresse IP d'un appareil alors que plusieurs utilisateurs aux intérêts et profils variés sont liés à cette même adresse IP. Cette problématique avait également été soulevée par Gratton en 2010.[809]

Ajoutons également au passage la question des enfants, en rappelant qu'au fédéral seuls les tuteurs peuvent consentir au nom d'un enfant de moins de treize ans, et ce sous une forme

[807] *Id.*, p. 55 et 56.
[808] *Id.*, p. 56, par. 3 et 4.
[809] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299, p. 300.

explicite,[810] mais qu'il est interdit de faire de la publicité destinée à ces enfants au Québec en vertu de la LPC.[811] Voici d'ailleurs un autre exemple de complexité juridique et factuelle liée à la PCL.

[810] Supra, 6.2.1.4.
[811] Supra, 2.1.4.

CONCLUSION

Résumé

Comme le constatait Michel Serres, la révolution numérique que nous vivons est une révolution concernant l'information qui a pour effet de transformer profondément nos sociétés, tant au niveau de la culture que du commerce et de la science notamment.[812] De multiples nouvelles techniques, pratiques et entreprises ont alors vu le jour dans de nombreux secteurs d'activité, telle la PCL dans les secteurs du commerce et des communications-marketing.

Constatant cette effervescence technologique et juridique ainsi que ses impacts sur les différentes organisations que je côtoie dans le cadre de ma pratique professionnelle, j'ai souhaité me pencher, dans le cadre de ce mémoire, sur le nouveau cadre juridique applicable – ou en voie de l'être – aux organisations participant à la PCL au Québec et au Canada. J'ai choisi d'adopter une approche conjuguant pratique et théorie, me permettant de soulever les éléments plus problématiques au niveau règlementaire et législatif d'une perspective entreprise (parties I et II) et d'une perspective utilisateur (partie III). Cette approche m'a également permis d'adopter un regard plus critique sur les pratiques du secteur privé et sur certains de ces joueurs en particulier, et sur des pistes de réflexion nécessaires pour mieux arrimer les divers intérêts en présence.

Ainsi, dans la partie I de ce mémoire, nous avons pu constater l'état de la complexité factuelle entourant la PCL et l'écosystème publicitaire en général, en brossant un portrait des différentes parties prenantes, de leurs intérêts et de leur rôle, ainsi que de la dynamique qui s'opère entre elles. De plus, nous avons pu constater que la pluralité et l'évolution rapide et récente des normes formelles et informelles, tant provinciales, fédérales qu'étrangères, applicables à la PCL, créent une complexité juridique.

[812] Supra, Prologue

Dans les parties II et III, je me suis attardée aux différentes obligations incombant au secteur privé en vertu de la LPRPDE, de la Loi 25 et du projet de loi C-27, en prenant soin d'identifier et d'analyser les exigences qui étaient les plus cruciales d'une perspective entreprise, soit la responsabilité, l'exercice de la transparence, les critères de finalités légitimes et de nécessité, ainsi que les obligations de minimisation à la collecte et à la conservation, de transparence, de sécurité, de consentement et de documentation qui en découlent, le tout, dans un contexte de transferts transfrontières propre à la PCL.

Cette analyse nous permet de constater un manque de clarté et d'harmonisation entre le régime québécois et fédéral concernant des dispositions pourtant clé en matière de PRP et de PCL, principalement l'anonymisation (et les difficultés créées par la délégation normative employée) et la forme de consentement requise (explicite ou implicite), amplifiées par une définition de plus en plus large de renseignements personnels et de renseignements personnels sensibles. Sur la question de la forme de consentement valable dans un contexte de PCL, tel qu'expliqué, il m'apparaitrait raisonnable que la forme implicite liée à un mécanisme de retrait efficace et à une transparence accrue continue d'être considérée comme valable au Québec et au Canada lorsque les renseignements personnels sont non ou peu sensibles.

Ce resserrement au niveau de ces obligations et cet élargissement au niveau de ces définitions clés s'observent non seulement au niveau normatif, mais également au niveau des rapports et des lignes directrices des autorités de contrôle, c'est-à-dire dans les nombreux rapports d'enquête, positions et les lignes directrices du CPVP - bien que traditionnellement plus nuancé par rapport au secteur privé - que des récentes publications de la CAI sur son Espace évolutif.

L'analyse proposée dans la partie III portant sur l'obligation de consentement valable et ses limites d'une perspective utilisateur, permet de conclure que le consentement (surtout le consentement explicite) a effectivement et malheureusement ses limites et qu'il ne peut régler toutes les problématiques et les enjeux individuels et collectifs en lien avec le traitement de renseignements personnels. Notamment, il ne peut être totalement libre et éclairé dans la

mesure où son exercice demande temps, connaissances et volonté de la part de l'utilisateur, et ce de manière répétée et renouvelée à chaque plateforme et chaque nouvelle fin, pouvant ainsi créer un désintérêt et une perte de sens pour cet exercice pourtant important. De plus, il est complexe à obtenir et à gérer dans un contexte d'objets connectés et d'appareils utilisés par plusieurs utilisateurs.

En conséquence, les entreprises devront orienter leurs efforts non seulement sur les mécanismes d'obtention et de retrait du consentement, mais aussi sur une transparence et une stratégie de responsabilisation accrues (sécurité/confidentialité, documentation), en plus de mieux prévoir et encadrer contractuellement les transferts de renseignements personnels à leurs fournisseurs de services et aux entreprises tiers.

Pistes de réflexion et d'amélioration proposées

Pour les entreprises : Ainsi, la clé pour les organisations et les individus sera d'abord de cartographier les flux de données et de prendre conscience de leur responsabilité et pouvoirs en matière de PRP. La vigilance de tous, en commençant par les organisations, sera de mise et des changements de pratiques devront en découler non seulement pour se conformer aux lois, mais également des réflexions plus profondes concernant les pratiques marketing actuelles et leur amélioration.

Ces réflexions du côté entreprise devront essentiellement porter sur la limitation de la quantité et la qualité des données nécessaires d'une perspective marketing. À cette fin, le *data minimization* et l'intégration de la vie privée par défaut seront d'une aide précieuse :

> « Après tout, la meilleure façon de protéger un renseignement reste encore de ne pas le générer – et la meilleure façon d'éviter qu'il soit compromis reste encore de ne pas le conserver. Dans le contexte d'une modernisation de la Loi sur le privé, nous sommes d'avis que de telles approches limitatives gardent leur pertinence pour minimiser la collecte de données et pour garantir que la configuration de ces appareils est, par défaut, la plus respectueuse possible de la vie privée. »[813]

[813] Alexandre PLOURDE, « Retour vers le futur : l'Internet des objets et la protection de la vie privée », *op. cit*., note 806, p. 51, par. 2.

De plus, ajoutons à ces deux éléments l'utilisation de l'anonymisation et de techniques rigoureuses de dépersonnalisation, qui seront des alliés de taille dans cette transition ayant pour but de mieux protéger la vie privée des gens tout en permettant aux organisations privées et publiques d'utiliser les renseignements personnels à bon escient.

En outre, si la tendance se maintient, le consentement sous sa forme explicite est appelé à s'implanter au Québec et les entreprises devront redoubler d'efforts pour faire preuve d'une transparence suffisante et mettre en place des mécanismes de gestion des consentements efficaces. Pour les y aider, des programmes d'autoréglementation et des outils émanant de l'industrie seront des plus utiles.

Finalement, les organisations devront porter une attention particulière à l'aspect non seulement légal, mais éthique de certaines utilisations et aux dérives possibles de l'utilisation des renseignements personnels à mauvais escient, que cela soit fait consciemment ou par négligence : discrimination, désinformation, etc.

En effet, de nombreux enjeux méritent d'être soulevés, comme le concluait Virginie Jetté en 2017 :

> « (...) les dangers relatifs à la PCL ne se limitent pas aux pratiques des entreprises. De nombreux auteurs appellent à une protection accrue des utilisateurs, martelant que les législations en matière de vie privée sont défaillantes, voire désarmées devant le phénomène de la publicité ciblée. À cet égard, nous rappelons que le père du web lui-même s'est dit préoccupé quant à l'enjeu de la publicité ciblée politique[814], allant jusqu'à questionner le caractère démocratique de cette pratique. Constatant que la publicité ciblée outrepasse sa fonction marketing utilitaire et se répand à d'autres sphères, il y a lieu de se questionner quant aux enjeux découlant d'un tel développement. Des auteurs ont signalé ses dangers liés aux questions de surveillance dans un État de droit. Certains se sont montrés préoccupés quant aux possibilités de discrimination qui pourraient survenir, suggérant notamment que la publicité ciblée était susceptible de renforcer la

[814] Liat CLARK, « Tim Berners-Lee: We need to re-decentralize the Web », Ars Technica (6 février 2014), en ligne : Ars Technica (consulté le 10 avril 2017); Olivia SOLON, « Tim Berners-Lee calls for tighter regulation of online political advertising », The Guardian (12 mars 2017), en ligne : The Guardian (consulté le 25 mars 2017), cités par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.

> discrimination raciale, de même que celle fondée sur la classe sociale[815]. En ce sens, la publicité ciblée présenterait un risque pour l'autonomie et la dignité humaine[816].
>
> Certains auteurs se concentrent plutôt sur les risques que cette pratique suppose pour l'État démocratique. Soulignant que l'État démocratique, de nature, protège les citoyens contre les abus de droit et les dérives autoritaires de leurs gouvernements[817], ils s'inquiètent du profilage qui pourrait découler de la transparence accrue que la publicité ciblée suppose pour les informations personnelles des individus en société[818]. La dispersion des informations personnelles créerait ainsi un flou entre la nature privée et publique des informations de chacun, menaçant le fondement même de l'assise démocratique[819]. S'opèrerait alors un renversement où, contrairement au principe démocratique, la transparence définirait les informations personnelles des citoyens et non les activités de l'État. Il s'agit donc d'une opportunité pour améliorer les pratiques marketing, mais également pour prendre un pas de recul sur les méthodes et les usages qui en sont faits. »[820] [Mes soulignements]

Aux utilisateurs : Les utilisateurs quant à eux devront accroitre leur niveau de littéracie (numérique, technologique, juridique et économique) de manière à mieux comprendre non seulement leurs droits, mais également l'écosystème numérique plus largement afin d'en avoir une compréhension générale suffisante permettant d'exercer les bons choix individuels propres à chacun.

Aux législateurs et autorités de contrôle : Nous avons pu constater tout au long de l'analyse des différentes obligations, que le principal obstacle à la mise en conformité des entreprises se situe à deux niveaux : la compréhension et l'opérationnalisation des obligations. Pour plusieurs, cela représentera un défi complexe et coûteux.

Malheureusement, le manque de clarté et de cohérence des dispositions clés (consentement, anonymisation, transferts transfrontières), la fluidité des concepts clés (nécessité, définition de

[815] Shaun B SPENCER, « Privacy and Predictive Analytics in E-Commerce » (2015) 49 New Eng L Rev 629, cité par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.
[816] *Id*., p. 640. Cité par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.
[817] Joel R. REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 449. Cité par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.
[818] *Id.*, p. 447. Cité par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.
[819] *Id*., p. 449. Cité par Virginie JETTÉ, *op. cit*., note 19, p. 114-115.
[820] Virginie JETTÉ, *op. cit*., note 19, p. 114-115.

renseignements sensibles), le tout conjugué au manque d'harmonisation entre les différentes lois à l'échelle nationale et internationale rendent fastidieux cet effort de conformité.

De surcroit, elles nourrissent les divergences d'interprétation nuisibles aux saines et productives relations entre les organisations entre elles, mais également entre les organisations, les organismes d'autoréglementation et les autorités de contrôle.

Cela met en lumière la pertinence d'une approche participative et collaborative entre les organismes règlementaires, les autorisés de contrôle, le milieu universitaire, les organisations, les organismes d'autoréglementation[821] et les associations de défense des droits et intérêts des consommateurs. Elle permettrait de faciliter les efforts d'élaboration des règlements prévus et des lignes directrices requises en temps utiles, en plus d'accroître leur application de manière conforme par les entreprises. Une telle approche contribuerait également à maintenir un dialogue constructif et favorable à la production de normes communautaires adéquates et pertinentes pour soutenir l'industrie dans ses efforts d'opérationnalisation des obligations légales.

Cette communication et ces efforts seront de plus en plus nécessaires afin de surmonter les défis que posent la conciliation des différents intérêts en présence et la lutte contre des menaces individuelles et collectives, telles les cyberattaques, la discrimination algorithmique et la désinformation, complexifiés par la mondialisation, l'évolution rapide des technologies (objets connectés, IA), le virage rapide vers le numérique et la transformation des stratégies marketing et média.

Dans le contexte où les flux de données franchissent plusieurs frontières, cette harmonisation des valeurs piliers et des exigences principales en matière de PRP est essentielle à leur effectivité et à la protection des droits et libertés. Ainsi, le concept d'interopérabilité de la protection de la vie

[821] L'OCDE recommandant d'ailleurs d'« encourager et soutenir l'autorégulation, sous forme de code de conduite ou de toute autre manière » : ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, *op. cit*., note 586, art. 19d).

privée (« *privacy interoperability* ») devient de plus en plus important notamment d'une perspective économique[822] :

> « L'augmentation significative des flux de données personnelles a incité les décideurs politiques à essayer de développer une approche cohérente de la gouvernance de la vie privée, tant au niveau national qu'au-delà des frontières. Dans ce contexte, le besoin d'interopérabilité des cadres de protection de la vie privée et des données ("interopérabilité de la vie privée") a pris une plus grande importance. Bien qu'il y ait un large consensus sur l'importance de l'interopérabilité de la vie privée, la façon d'y parvenir dans la pratique est moins bien comprise. Cette boite à outils "*Going Digital*" [de l'OCDE] décrit les problèmes liés à l'interopérabilité des cadres de protection de la vie privée et des données, et met en évidence les initiatives prometteuses des gouvernements et des autorités chargées de l'application de la vie privée aux niveaux national et international. Cette note vise à contribuer à une compréhension commune de l'interopérabilité de la vie privée dans le contexte de la gouvernance de la vie privée et de la protection des données et des flux transfrontaliers de données personnelles. »[823] [Mon soulignement. Traduction libre]

Prenons donc tous un pas de recul afin de regarder de manière objective et critique non seulement les dérives et les faux pas possibles afin de les corriger, mais également afin d'assumer notre responsabilité partagée comme utilisateurs, entreprises, associations, autorités de contrôle, législateurs, pour identifier les possibilités et les opportunités qu'offre l'irréversible révolution numérique.

[822] OCDE, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, *op. cit*., note 586, Partie six.
[823] L. ROBINSON, K. KIZAWA et E. RONCHI, « Interoperability of privacy and data protection frameworks », *OECD Going Digital Toolkit Notes*, *op. cit*., note 821.

Références bibliographiques

TABLE DE LA LÉGISLATION

Textes fédéraux

Code criminel, LRC 1985, c C-46, en ligne : <https://canlii.ca/t/6dzjf>

Décret d'exclusion visant des organisations de la province d'Alberta, DORS/2004-219, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://laws-lois.justice.gc.ca/fra/reglements/DORS-2004-219/page-1.html>

Décret d'exclusion visant des organisations de la Colombie-Britannique, DORS/2004-220, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://laws-lois.justice.gc.ca/fra/reglements/DORS-2004-220/page-1.html>

Décret d'exclusion visant des organisations de la province de Québec, DORS/2003-374, Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://laws-lois.justice.gc.ca/fra/reglements/DORS-2003-374/page-1.html>

Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois, Projet de loi C-11 (Première lecture), 2e session, 43e législature (Can.), en ligne : <https://parl.ca/DocumentViewer/fr/43-2/projet-loi/C-11/premiere-lecture>

Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, Projet de loi C-27 (1re lecture), 1re session, 44e législature (Can.), en ligne : <https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>

Loi sur la concurrence, LRC 1985, c C-34, en ligne : <https://canlii.ca/t/6dj9g>

Loi sur la protection des renseignements personnels, LRC 1985, c P-21, <http://canlii.ca/t/6c2m5>

Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5, <http://canlii.ca/t/6c2fl>

Loi sur le droit d'auteur, LRC 1985, c C-42, en ligne : <https://canlii.ca/t/6cdt9>

Loi sur les banques, LC 1991, c 46, en ligne : <https://canlii.ca/t/6dj9l>

Loi sur les marques de commerce, LRC 1985, c T-13, en ligne : <https://canlii.ca/t/6d5fr>

Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la loi sur la concurrence, la loi sur la protection des renseignements personnels et les documents électroniques et la loi sur les télécommunications, LC 2010, c 23, en ligne : <https://canlii.ca/t/6b07x>

Protocole d'entente sur la coopération, la coordination et l'échange d'information entre le Commissaire à la concurrence, le Conseil de la radiodiffusion et des télécommunications canadiennes et la Commissaire à la protection de la vie privée du Canada dans le cadre de l'exécution de leur mandat au titre de la loi canadienne antipourriel, 23 janvier 2014, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/loi-canadienne-anti-pourriel/mou_casl_2014/>

Règlement sur la protection du commerce électronique (CRTC), DORS/2012-36, en ligne : <https://canlii.ca/t/69fmr>

Règlement sur les atteintes aux mesures de sécurité, DORS/2018-64, en ligne : <https://canlii.ca/t/6b62r>

Textes québécois

Charte des droits et libertés de la personne, RLRQ c C-12, en ligne : <https://canlii.ca/t/6dmsf> (consulté le 24 février 2023)

Code civil du Québec, RLRQ c CCQ-1991, en ligne : <https://canlii.ca/t/6dzcm> (consulté le 12 février 2023), art. 35 à 41

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, Projet de loi 64, 1ère session, 42e législature, en ligne : <https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html?appelant=MC>

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25, en ligne : <https://canlii.ca/t/6d6s0>

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ C A-2.1, en ligne : <https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-

2.1/derniere/rlrq-c-a-2.1.html?autocompleteStr=loi%20sur%20l%27acc%C3%A8s&autocompletePos=1>

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q. 1993, c. P-39.1.

Loi sur la protection du consommateur, RLRQ c P-40.1, art. 215 à 253, en ligne : <https://canlii.ca/t/6dr0n> (consulté le 12 février 2023)

Règlement d'application de la Loi sur la protection du consommateur, RLRQ c P-40.1, r 3, en ligne : <https://canlii.ca/t/6dq40> (consulté le 12 février 2023), Section II (art. 87 à 91).

Règlement sur les incidents de confidentialité, (2022) 154 G.O., II, 6819, en ligne : <https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2022F/78638.pdf>

Textes autres provinces canadiennes et étrangers

California Consumer Privacy Act, Ch.55, 2018, Sec.3., en ligne : <*https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5*>

Declaration for the Future of Internet, 2022, en ligne : <https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet>

Délibération n°2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n°2019-093 du 4 juillet 2019), 2019, en ligne : <*https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179*>

Personal Information Protection Act, S.A. 2003, ch. P-6.5

Personal Information Protection Act, S.B.C. 2003, ch. 63

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 (général sur la protection des données), 2016, en ligne : <https://www.cnil.fr/fr/reglement-europeen-protection-

donnees#:~:text=R%C3%A8glement%20(UE)%202016%2F679,sur%20la%20protection%20des%20donn%C3%A9es>

TABLE DES JUGEMENTS

Jurisprudence canadienne

Jurisprudence québécoise

Jurisprudence étrangère

Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC., en ligne : <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038032552> (consulté en juillet 2022)

Data Protection Commissioner c. *Facebook Ireland Ltd et Maximillian Schrems*, Cour de justice de l'Union européenne, 16 juillet 2020, en ligne : <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=4594815>

RAPPORTS ET PUBLICATIONS OFFICIELS

Rapports et publications officiels fédéraux

BUREAU DE LA CONCURRENCE, *Archivé – Le Bureau de la concurrence conclut une entente avec Bell Canada exigeant que Bell paie 10 millions de dollars pour publicité trompeuse*, 28 juin 2011, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03388.html>

———. *Guide des modifications apportées en 2022 à la Loi sur la concurrence*, 24 juin 2022, en ligne : <https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/comment-nous-favorisons-concurrence/education-sensibilisation/publications/guide-modifications-apportees-2022-loi-concurrence#sec04> (consulté le 22 janvier 2023)

———. *Recueil des pratiques commerciales trompeuses*, Volume 1, 10 juin 2015, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03946.html>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Aperçu des lois sur la protection des renseignements personnels au Canada*, novembre 2017, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/#heading-0-0-3-1> (consulté le 12 février 2023)

———. « Annonce. Le Commissariat tire ses conclusions suite à la consultation sur les transferts aux fins de traitement » (23 septembre 2019), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2019/an_190923/> (consulté le 2 avril 2023)

———. *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE n° 2013-017, 20 novembre 2013, en ligne :

<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-017/> (consulté le 7 avril 2021)

———. *À propos du Commissariat*, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/> (consulté le 4 janvier 2023)

———. *Bulletin d'interprétation : Renseignements sensibles*, mai 2022, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_10_sensible/> (consulté le 16 avril 2023)

———. *Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité*, octobre 2018, révisé le 13 août 2021, par. 1 de la section « Que signifie l'expression risque réel de préjudice grave (RRPG) ? », en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/> (consulté le 2 avril 2023)

———. *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 d'AggregateIQ Data Services Ltd.,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2019-004, 26 novembre 2019, en ligne : <https://priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-004/> (consulté le 5 janvier 2023)

———. *Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2016-005, 22 août 2016, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2016/lprpde-2016-005/>

———. *Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons*, Conclusions en vertu de la LPRPDE n°2022-001, 1er juin 2022, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2022/lprpde-2022-001/> (consulté le 1er avril 2023)

———. *Enquête sur la conformité à la LPRPDE de Desjardins suite à l'atteinte aux mesures de sécurité des renseignements personnels entre 2017 et 2019*, Conclusions en vertu de la LPRPDE n°2020-005, 14 décembre 2020, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-

prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2020/lprpde-2020-005/> (consulté le 5 janvier 2023)

———. *Enquête sur la conformité de Home Depot du Canada Inc. à la LPRPDE*, Conclusions en vertu de la LPRPDE n°2023-001, 26 janvier 2023, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2023/lprpde-2023-001/#fn4> (consulté le 31 mars 2023)

———. *Enquête visant les entreprises*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/?q%5B0%5D=28&Page=1> (consulté le 1er mars 2023)

———. *Examen des répercussions sur la vie privée de l'application Alerte COVID*, 31 juillet 2020, 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/urgences-sanitaires/rev_covid-app/> (consulté le 19 mars 2023)

———. *La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée,* Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002, 12 juin 2018, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-002/> (consulté le 26 mars 2023)

———. *Les priorités stratégiques liées à la vie privée*, 14 décembre 2018, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/priorites-strategiques-liees-a-la-vie-privee-du-commissariat/les-priorites-strategiques-liees-a-la-vie-privee/> (consulté le 4 janvier 2023)

———. *Lignes directrices pour l'obtention d'un consentement valable*, mai 2018, révisé le 13 août 2021, 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 1er mars 2023)

———. *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, décembre 2011, révisé le 13 août 2021, en ligne : <https://www.priv.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 1er mars 2023)

———. *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2014-001, 14 janvier 2014, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-001/>

———. *Position de principe sur la publicité comportementale en* ligne, décembre 2015, révisé le 13 août 2022, en ligne : < https://www.priv.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/bg_ba_1206/ > (consulté le 1er mars 2023)

———. *Questions et réponses – projet de loi no 64, Comparution du commissaire à la protection de la vie privée du Canada devant l'Assemblée nationale du Québec*, 24 septembre 2020, en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/qa_20200924/#fn49-rf

———. *Transfert frontalier de renseignements personnels*, 27 janvier 2009, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/> (consulté le 2 avril 2023)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, DIRECTION DE L'ANALYSE DES TECHNOLOGIES, *Publicité comportementale en ligne (PCL),* Projet de recherche de suivi, juin 2015, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2015/oba_201506/> (consultée le 4 décembre 2022)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA et OFFICE OF THE INFORMATION & PRIVACY COMMISIONER OF BRITISH COLUMBIA, *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, avril 2012, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/gl_acc_201204/> (consulté le 1er avril 2023)

GOUVERNEMENT DU CANADA, « Bureau de la concurrence Canada », en ligne : <https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr> (consulté le 4 janvier 2023

———. « Conseil de la radiodiffusion et des télécommunications canadiennes », en ligne : <https://crtc.gc.ca/fra/internet/anti.htm> (consulté le 4 janvier 2023)

STATISTIQUE CANADA*, Enquête internationale sur l'alphabétisation et les compétences des adultes (EIACA)*, 2003, en ligne : <https://www23.statcan.gc.ca/imdb/p2SV_f.pl?Function=getSurvey&Id=15034>

Rapports et publications officiels québécois

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, 10 mars 2021, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf > (consulté le 24 mars 2023)

----------. *La collecte de renseignements personnels*, en ligne : <https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/> (consulté le 26 mars 2023)

----------. *Le profilage et la publicité ciblée*, octobre 2013, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FI_profilage.pdf> (consulté le 30 janvier 2023)

----------. *Publicité ciblée et protection des renseignements personnels*, en ligne : <https://www.cai.gouv.qc.ca/publicite-ciblee-et-protection-des-renseignements-personnels/> (consulté le 25 mars 2023)

----------. *Rétablir l'équilibre, Rapport quinquennal 2016*, septembre 2016, p. 73, en ligne : < https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf> (consulté le 3 mars 2023)

----------. *Technologie d'identification, de localisation ou de profilage*, en ligne : <https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/technologie-identification-localisation-profilage/> (consulté le 25 mars 2023)

CONSEIL DE LA RADIODIFFUSION ET DES TÉLÉCOMMUNICATIONS CANADIENNES, *Exigences de la Loi canadienne anti-pourriel concernant l'installation de programmes informatiques*, 18 septembre 2020, en ligne : <https://crtc.gc.ca/fra/internet/install.htm> (consulté le 10 février 2023)

----------. *Lignes directrices sur le consentement tacite dans le cadre de la Loi canadienne anti-pourriel (LCAP)*, 4 septembre 2015, en ligne : <https://crtc.gc.ca/fra/com500/guide.htm> (consulté le 5 février 2023)

GOUVERNEMENT DU QUÉBEC, *Anonymisation*, 23 février 2023, en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/anonymisation> (consulté le 2 avril 2023)

----------. *Incident de confidentialité*, 23 février 2023, en ligne : <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite > (consulté le 2 avril 2023)

———. *L'anonymisation et autres mesures de protection de la vie privée*, en ligne : https://www.cipvp.ca/protection-de-la-vie-privee-organismes/lanonymisation-et-autres-mesures-de-protection-de-la-vie-privee/> (consulté le 19 mars 2023)

Rapports et publications officiels étrangers

COMITÉ EUROPÉEN SUR LA PROTECTION DES DONNÉES, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE*, version 1.0 adoptée le 10 novembre 2020 et version 2.0 adoptée le 18 juin 2021, en ligne : <https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fr.pdf > (consulté le 23 avril 2023)

COMMISSION NATIONALE DE L'INFORMATISATION ET DES LIBERTÉS, *Règlement européen sur la protection des données : ce qui change pour les professionnels*, 10 juillet 2018, en ligne : <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels> (consulté le 22 janvier 2023)

———. *Fiche n°7 : Minimiser les données collectées*, en ligne : <https://lincnil.github.io/Guide-RGPD-du-developpeur/#Fiche_n%C2%B07%C2%A0:_Minimiser_les_donn%C3%A9es_collect%C3%A9es> (consulté le 26 mars 2023)

———. *Invalidation du Privacy shield : les suites de l'arrêt de la CJUE*, en ligne : <https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue> (consulté le 16 août 2022)

———. *La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD*, 2 décembre 2019, en ligne : <https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales> (consulté le 15 avril 2023)

———. *La protection des données dans le monde*, en ligne : <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde> (consulté le 16 août 2022)

———. *Les règles d'entreprise contraignantes (BRC)*, en ligne : <https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr > (consulté le 16 août 2022)

———. *Responsable de traitement : comment identifier et traiter des transferts de données hors de UE ?,* 23 juin 2021, en ligne : <https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue> (consulté le 16 août 2022)

———. *Règlement européen : le Délégué à la protection des données, c'est obligatoire ?*, en ligne : <https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-le-delegue-la-

protection-des-donnees-cest-obligatoire#:~:text=La%20d%C3%A9signation%20d'un%20D%C3%A9l%C3%A9gu%C3%A9,des%20personnes%20%C3%A0%20grande%20%C3%A9chelle > (consulté le 29 mars 2023)

———. *Règlement européen sur la protection des données : ce qui change pour les professionnels*, 10 juillet 2018, en ligne : <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels> (consulté le 22 janvier 2023)

———. *Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne,* 21 décembre 2022, en ligne : <https://www.cnil.fr/fr/transfert-de-donnees-les-clauses-contractuelles-types-cct-de-la-commission-europeenne> (consulté le 5 mars 2023)

———. *Transférer des données hors de l'UE*, en ligne : <https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue> (consulté le 16 août 2022)

———. *Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne*, 1er mars 2023, en ligne : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation> (consulté le 12 mars 2023)

EUROPEAN DATA PROTECTION BOARD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, *Version 2.0*, adoptées le 7 juillet 2021, en ligne : <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr>

———. *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 28 février 2023, en ligne : <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_fr> (consulté le 12 mars 2023)

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 7/2014 sur la protection des données à caractère personnel au Québec*, 4 juin 2014, en ligne : <https://www.dataprotection.ro/servlet/ViewDocument?id=1290 > (consulté le 15 janvier 2023)

INFORMATION COMMISSIONER'S OFFICE (UK), *Anonymisation and pseudonymisation guidance*, en ligne : <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/> (consulté le 27 avril 2023)

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « Emerging privacy-enhancing technologies : Current regulatory and policy approaches », Documents de travail de l'OCDE sur l'économie numérique, n° 351, Éditions OCDE, 2023, Paris, en ligne : <https://doi.org/10.1787/bf121be4-en > (consulté le 23 avril 2023);

———. *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel,* 1980 (révisées en 2013), en ligne : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188> (consulté le 23 avril 2023)

———. *Recommandation du Conseil sur la coopération transfrontière dans l'application des législations protégeant la vie privée*, 2007, en ligne: <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0352> (consulté le 23 avril 2023)

PERSONAL DATA PROTECTION COMMISSION (SINGAPORE), *Guide to Basic Anonymisation*, 31 mars 2021, en ligne : <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf> (consulté le 27 avril 2023)

BIBLIOGRAPHIE

Articles et monographies

BENYEKHLEF, K., *Une possible histoire de la norme : les normativités émergentes de la mondialisation*, 2e édition, Montréal, Les Éditions Thémis, 2015

BERNAL-CASTILLERO, M. et HOLMES, N., « Les loi fédérales du Canada sur la protection de la vie privée », dans Bibliothèque du Parlement, *Publications de recherche* (1er janvier 2013, révisée le 17 novembre 2020), en ligne : <https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/200744E> (consulté le 15 janvier 2023)

BOERMAN, S.C., KRUIKEMEIER, S. & ZUIDERVEEN BORGESIUS, F.J., « Online Behavioral Advertising: A Literature Review and Research Agenda », *Journal of Advertising* (2017) 46:3, 363-376, DOI: 10.1080/00913367.2017.1339368, en ligne : <https://www.tandfonline.com/doi/full/10.1080/00913367.2017.1339368 > (consulté le 4 janvier 2023)

DÉZIEL, P.-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans Barreau du Québec, Service de la formation continue, Développements récents en droit à la vie privée (2019), vol 465, Montréal (QC), Éditions Yvon Blais, 2019, 1, en ligne : <https://edoctrine.caij.qc.ca/developpements-recents/465/369051329>

GAUTRAIS V., « Proposition de Règlement général sur la protection des données : un regard d'ailleurs », dans Nathalie MARTIAL-BRAZ (dir.), *La proposition de règlement européen relatif aux données à caractère personnel*, Collection Trans Europe Experts, Société de législation comparée,

Paris, 2014, en ligne : <https://www.gautrais.com/publications/proposition-de-reglement-general-sur-la-protection-des-donnees-un-regard-dailleurs/>

GAUTRAIS V. et LAVILLE H., « Pour une gouvernance participative des données personnelles au Québec » dans Mathilde HAUTEREAU-BOUTONNET et Cyril SINTEZ, Mélanges en l'honneur de Catherine Thibierge, 2023, (à paraître)

GRATTON, É., « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299.

LAPIERRE G. et PELLETIER M., « Les répercussions de la Loi 25 en droit des affaires » dans Barreau du Québec, Service de la formation continue, Développements récents en droit des affaires (2022), vol 519, Montréal (QC), Éditions Yvon Blais, 2022, 189, en ligne : https://edoctrine.caij.qc.ca/developpements-recents/519/c-10c7f1df-e4ab-42f8-8219-0ebaeee7d256 > (consulté le 23 avril 2023)

PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans Barreau du Québec, Service de la formation continue, Développements récents en droit à la vie privée (2019), vol 465, Montréal (QC), Éditions Yvon Blais, 2019, 33, en ligne : <https://edoctrine.caij.qc.ca/developpements-recents/465/369051330/> (consulté le 22 avril 2023)

ROBINSON L., KIZAWA K. et RONCHI E., « Interoperability of privacy and data protection frameworks », *OECD Going Digital Toolkit Notes*, n° 21, Éditions OCDE, (2021) Paris, en ligne: <https://doi.org/10.1787/64923d53-en> (consulté le 23 avril 2023)

SVANTESSON, D., « Data localisation trends and challenges : Considerations for the review of the Privacy Guidelines », *Documents de travail de l'OCDE sur l'économie numérique*, n° 301, Éditions OCDE, 2020, Paris, en ligne : <https://doi.org/10.1787/7fbaed62-en> (consulté le 23 avril 2023)

Dictionnaires et glossaires

CAIJ, Dictionnaire de droit québécois et canadien, édition révisée 2016, en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=Manifeste%20(adj.)&t=edictionnaire&sort=relevancy&m=search > (consulté le 17 avril 2023)

DÉFINITIONS MARKETING, en ligne : <https://www.definitions-marketing.com/definition/annonceur/> (consulté le 3 janvier 2023)

LAROUSSE, « Gestion », en ligne : <https://www.larousse.fr/dictionnaires/francais/gestion/36853 > (consulté le 6 juillet 2022)

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), Vitrine linguistique, Fiche terminologique, « Gestion », en ligne : <https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26543848 > (consulté le 6 juillet 2022)

WIZISHOP, en ligne : <https://www.wizishop.fr/lexique-ecommerce/reciblage-publicitaire> (consulté le 4 décembre 2022)

———. en ligne : <https://www.wizishop.fr/lexique-ecommerce/conversion> (consulté le 4 décembre 2022)

Autres : Billets de blogue, articles de journaux et sites Internet

ALAVI, S., CHARLESTON, E. S., DU PERRON, S. et al., « Loi sur la protection de la vie privée des consommateurs du Canada (Projet de loi C-27) : incidences sur les entreprises », *Borden Ladner Gervais – Perspectives* (21 juin 2022), en ligne: <https://www.blg.com/fr/insights/2022/06/canadas-consumer-privacy-protection-act-bill-c27-impact-for-businesses> (consulté le 11 mars 2023)

ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « Au sujet de la DAAC », en ligne : <https://youradchoices.ca/fr/au-sujet > (consulté le 3 mars 2023)

———. « Foire aux questions « Quels sont les avantages que m'offre la publicité ciblée par centre d'intérêt en ligne ? », en ligne : <https://youradchoices.ca/fr/faq> (consulté le 3 janvier 2023)

———. « Foire aux questions », en ligne : <https://youradchoices.ca/fr/faq> (consulté le 4 décembre 2022)

———. « Outils », en ligne : <https://youradchoices.ca/fr/outils> (consulté le 4 décembre 2022)

———. *Principe canadiens d'autorèglementation de la publicité ciblée par centre d'intérêt*, document révisé en octobre 2022, en ligne : <https://assets.youradchoices.ca/pdf/principles/DAAC-AdChoices-Principles-French.pdf > (consulté le 29 mars 2023)

———. « Réforme de la LPRPDE et propositions provinciales en matière de protection de la vie privée », (3 décembre 2020), en ligne : <https://youradchoices.ca/fr/actualites/2020/12/3/rforme-de-la-lprpde-et-propositions-provinciales>

APPLE, « iOS 16 », en ligne : <https://www.apple.com/ca/fr/ios/ios-14/> (consulté le 7 avril 2021)

————. « User Privacy and Data Use », en ligne: <https://developer.apple.com/app-store/user-privacy-and-data-use/> (consulté le 6 janvier 2023)

————. « User Privacy and Data Use », Using the AppTrackingTransparency Framework, en ligne : <https://developer.apple.com/app-store/user-privacy-and-data-use/> (consulté le 7 avril 2021)

ASSOCIATION DES AGENCES DE COMMUNICATION CRÉATIVE, *Guide de sélection d'agence*, 2023 (à paraître)

BUREAU, V., « Atteintes à la vie privée au Québec : obligations le 1er novembre. Règlement concernant les atteintes aux mesures de sécurité » *Association des agences de communication créative - Accès membres* (2018)

CHAVEZ, A., « Expanding testing for the Privacy Sandbox for the Web », *Google The Keyword* (27 juillet 2022), en ligne: <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> (consulté le 16 août 2022)

COMMISSION EUROPÉENNE, « L'UE et des partenaires internationaux ont présenté une déclaration sur l'avenir de l'internet », Communiqué de presse (28 avril 2022) en ligne : <https://france.representation.ec.europa.eu/informations/lue-et-des-partenaires-internationaux-ont-presente-une-declaration-sur-lavenir-de-linternet-2022-04-28_fr> (consulté le 22 janvier 2023)

COMMISSION EUROPÉENNE, « L'UE et des partenaires internationaux ont présenté une déclaration sur l'avenir de l'internet », Communiqué de presse (28 avril 2022) en ligne : <https://digital-strategy.ec.europa.eu/fr/news/eu-and-international-partners-put-forward-declaration-future-internet> (consulté le 22 janvier 2023)

DESCHÊNES V., « Dépersonnalisé, anonymisé, agrégé, pseudonymisé; mais de quoi parlez-vous! », *ROBIC / Publications*, (10 décembre 2020), en ligne : <https://www.robic.ca/publications/depersonnalise-anonymise-agrege-pseudonymise-mais-de-quoi-parlez-vous/> (consulté le 23 mars 2023)

EUROPEAN INTERACTIVE DIGITAL ADVERTISING ALLIANCE, « À propos de la publicité comportementale », en ligne : <https://www.youronlinechoices.com/fr/a-propos-de-la-publicite-comportementale/> (consulté le 4 janvier 2023)

FONDATION POUR L'ALPHABÉTISATION, « La littératie : mieux la comprendre », en ligne : <https://fondationalphabetisation.org/lanalphabetisme/tout-sur-lanalphabetisme/la-litteratie/ > (consulté le 22 avril 2023)

FUCHS, J., « Dynamic Pricing : The Complete Guide », HUBSPOT (7 septembre 2022), en ligne : <https://blog.hubspot.com/sales/dynamic-pricing#:~:text=Dynamic%20pricing%20%E2%80%94%20also%20known%20as,and%20time%20until%20the%20flight. > (consulté le 26 mars 2023)

INTERNATIONAL ADVERTISING BUREAU (IAB), « OpenRTB », en ligne : <https://www.iab.com/guidelines/openrtb/#:~:text=Real%2Dtime%20Bidding%20(RTB),to%20how%20financial%20markets%20operate> (consulté le 24 avril 2023)

GESTE, « EPrivacy : La phase de trilogue peut enfin commencer ! » (26 février 2022) en ligne : <https://geste.fr/eprivacy-la-phase-de-trilogue-peut-enfin-commencer/> (consulté le 7 janvier 2023)

GLOVER, D. G. C., et HANTHO E., « 2021/2022 Bilan et perspective en Cyber/Données : Modifications prévues aux lois sur la protection de la vie privée au Canada », *McCarthy Tétrault* (28 février 2022), en ligne : <https://www.mccarthy.ca/fr/references/blogues/techlex/20212022-bilan-et-perspectives-en-cyberdonnees-modifications-prevues-aux-lois-sur-la-protection-de-la-vie-privee-au-canada> (consulté le 6 mars 2023)

GRATTON, É., « Nos réflexions sur le projet de loi no 64 (protection sur la vie privée dans le secteur privé au Québec » (22 septembre 2020), *Éloïse Gratton*, en ligne : <https://www.eloisegratton.com/blog/2020/09/22/nos-reflexions-sur-le-projet-de-loi-no-64-quebec-et-protection-de-la-vie-privee-dans-le-secteur-prive/ > (consulté le 5 avril 2023)

GRATTON, É., HENRY, E. et JOLI-CŒUR, F., « Amendements proposés à la loi québécoise sur la protection des renseignements personnels : Conséquences sur les entreprises », *Borden Ladner Gervais - Perspectives* (15 juin 2020), en ligne : <https://www.blg.com/fr/insights/2020/06/proposed-amendments-to-quebec-privacy-law-impact-for-businesses> (consulté le 23 mars 2023)

GRATTON, É., HENRY, E., JOLI-CŒUR, F., DU PERRON, S. et al., *Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises*, *Borden Ladner Gervais - Perspectives*, mis à jour en octobre 2022, en ligne : <https://www.blg.com/fr/insights/2021/11/quebec-privacy-law-reform-a-compliance-guide-for-organizations> (consulté le 13 avril 2023)

GRATTON, É., NAGY, A. et JOLI-CŒUR, F., « Marketing numérique et analyse de données : les détaillants canadiens utilisant des outils de conversion hors ligne auront des leçons à tirer d'une décision du Commissariat à la protection de la vie privée », *Borden Ladner Gervais - Perspectives,* (20 février 2023), en ligne : <https://www.blg.com/fr/insights/2023/02/digital-marketing-and-analytics-lessons-for-canadian-retailers-using-offline-conversion-tools> (consulté le 31 mars 2023)

GUILMAIN A. et SENÉCAL F., « Collecte de données et éthique : des enjeux à décoder », *École des dirigeants, HEC Montréal* (octobre 2022), en ligne : <https://ethique-conformite.hec.ca/communaute/collecte-de-donnees-et-ethique-des-enjeux-a-decoder/?_ga=2.51290281.1260303918.1669831872-1693310516.1669831872&_gl=1*ss1dub*_ga*MTY5MzMxMDUxNi4xNjY5ODMxODcy*_ga_FPW0B8V0CE*MTY2OTgzMTg3Mi4xLjEuMTY2OTgzMTkzNy42MC4wLjA> (consulté le 19 mars 2023)

HENRY, E. et HÉMOND, A., « Transfert de renseignements personnels hors du Québec : nouvelles exigences pour les entreprises » *Borden Ladner Gervais – Perspectives* (6 décembre 2022), en ligne : <https://www.blg.com/fr/insights/2022/12/cross-border-transfers-of-personal-information-outside-quebec > (consulté le 4 avril 2023)

JEFFERY, E., « Advertising without Third-Party Cookies: Frequently Asked Questions », *AX INSIGHTS* (6 janvier 2023), en ligne : <https://audiencex.com/advertising-without-third-party-cookies-frequently-asked-questions/ > (consulté le 16 août 2022)

JONNAERT, C. et LESAGE-BIGRAS, É., « Cookies et vie privée : ce que toute organisation devrait savoir », *Infopresse* (22 juin 2022) en ligne : <https://www.infopresse.com/cookies-et-vie-privee-ce-que-toute-organisation-devrait-savoir/> (consulté le 24 février 2023)

KIROVSKA, G., « What is a Consent Management Platform (CMP) and Do You Need One? », *LiveRamp* (20 mars 2020) en ligne : <https://liveramp.com/blog/consent-management-platform-cmp/ > (consulté le 8 mars 2023)

KOVALENKO, I., « Digital Advertising Ecosystem: Components », Smartyads (mis à jour le 9 septembre 2021), en ligne : <https://smartyads.com/blog/digital-advertising-ecosystem-components/> (consulté le 3 janvier 2023)

KUDRYATSEV, K., « La Cour d'appel du Québec approuve un recours collectif contre Facebook », *Agence France-Presse, Le Devoir* (4 janvier 2023) en ligne : <https://www.ledevoir.com/societe/justice/776725/la-cour-d-appel-du-quebec-approuve-un-recours-collectif-contre-facebook> (consulté le 6 janvier 2023)

LA PRESSE CANADIENNE, « Le gouvernement canadien interdit l'application TikTok sur ses cellulaires », *Les affaires* (27 février 2023), en ligne : <https://www.lesaffaires.com/techno/internet/le-gouvernement-canadien-interdit-l-application-tiktok-sur-ses-cellulaires/639468> (consulté le 28 avril 2023)

LANGLOIS, J., « Action collective autorisée contre Google », *SOQUIJ BLOGUE* (20 juillet 2022) en ligne : <https://blogue.soquij.qc.ca/2022/07/20/action-collective-autorisee-contre-google/> (consulté le 6 janvier 2023)

LE CENTRE DE DOCUMENTATION SUR L'ÉDUCATION DES ADULTES ET LA CONDITION FÉMININE (CDÉACF), « Situation de l'alphabétisation au Québec », en ligne : <http://cdeacf.ca/ace/a_propos/situation > (consulté le 22 avril 2023)

LES NORMES CANADIENNES DE LA PUBLICITÉ, COMITÉ DIRECTEUR SUR LE MARKETING D'INFLUENCE, *Lignes directrices sur la divulgation*, révisé automne 2020, en ligne : <https://adstandards.ca/fr/ressources/marketing-dinfluence/>

LES NORMES CANADIENNES DE LA PUBLICITÉ, *Code canadien des normes de la publicité*, (révisé juillet 2019) en ligne : < https://adstandards.ca/fr/code-canadien/code-en-ligne/ > (consulté le 3 mars 2023)

———., « Les plaintes », en ligne : < https://adstandards.ca/fr/plaintes/ > (consulté le 3 mars 2023)

———., « Procédure en matière de différends publicitaires », en ligne : <https://adstandards.ca/fr/plaintes/differends-publicitaires/ > (consulté le 3 mars 2023)

———., *Programme de responsabilité Choix de* pub, *Rapport de conformité 2022*, avril 2023, en ligne : <https://adstandards.ca/wp-content/uploads/Programme-de-responsabilite-Choix-de-pub-Rapport-2022.pdf> (consulté le 15 avril 2023)

LÉVESQUE, F., « Données personnelles : une loi avec plus de mordant », *La Presse* (12 février 2020) en ligne : <https://www.lapresse.ca/actualites/politique/202002/11/01-5260568-donnees-personnelles-une-loi-avec-plus-de-mordant.php>

LEWIS, S., « Industry Response to Apple iOS », *Canadian Media Directors Council (CMDC)* (20 janvier 2021) en ligne : <https://www.cmdc.ca/news-mentor/apple> (consulté le 7 avril 2021)

LUBECK, A., « Disparition des cookies tiers : Soyez prêts! », *Grenier Magazine*, vol. 6, n°24 (6 avril 2021) en ligne : <https://magazines.grenier.qc.ca/magazine-parution/2021-04-06/#4/>

NADEAU, J.-B., « Le Québec aux avant-postes en matière de protection des données personnelles », *LeDevoir* (2 avril 2022), en ligne : < https://www.ledevoir.com/societe/693318/protection-des-donnees-le-quebec-aux-avant-postes>

OPTION CONSOMMATEURS, « Le prix de la gratuité. Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne ? », Rapport de recherche réalisé par Option Consommateurs et présenté au Bureau de la consommation d'Industrie Canada (juin 2015), en ligne : <https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf> (consulté le 22 avril 2023)

PACI, J., « Tout savoir sur la nouvelle directive ePrivacy pour s'y préparer au mieux », *Mailjet* (6 novembre 2022) en ligne : <https://www.mailjet.com/fr/blog/bonnes-pratiques-emailing/directive-eprivacy/#chapter-2> (consulté le 7 janvier 2023)

SANDOVAL, C., « What is the Difference Between an API and an SDK ? » *Nordic APIS* (2 juin 2016), en ligne : < https://nordicapis.com/what-is-the-difference-between-an-api-and-an-sdk/> (consulté le 6 janvier 2023)

SCASSA, T., « Anonymization and De-identification in Bill C-27 », *Teresa Scassa - Blog* (6 juillet 2022) en ligne: <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80 > (consulté le 24 mars 2023)

SCHOMER, A., « Publisher Ad Monetization After the Third-Party Cookie », *eMarketer* (8 mars 2021), en ligne : <https://www.emarketer.com/content/publisher-ad-monetization-after-third-party-cookie> (consulté le 6 janvier 2023)

SOOKMAN. B., « CPPA: identifying the inscrutable meaning and policy behind the de-identifying provisions », *Barry Sookman* (7 décembre 2020), en ligne : <https://www.barrysookman.com/2020/12/07/cppa-identifying-the-inscrutable-meaning-and-policy-behind-the-de-identifying-provisions/> (consulté le 19 mars 2023)

TEMKIN, D., « Charting a course towards a more privacy-first web », *Google Ads & Commerce Blog* (3 mars 2021), en ligne: <https://blog.google/products/ads-commerce/a-more-privacy-first-web/> (consulté le 16 août 2022)

TRENDMICRO, « Data Minimization », <https://www.trendmicro.com/vinfo/us/security/definition/Data-Minimization> (consulté le 29 avril 2023)

TRUDEL, P., « Renseignements personnels : les vraies urgences », *Le Devoir* (18 février 2020), en ligne : <https://www.ledevoir.com/opinion/chroniques/573151/renseignements-personnels-les-vraies-urgences> (consulté le 22 avril 2023)

VIE PUBLIQUE (Gouv. Français), « Le règlement européen sur les services numériques (DSA) vise une responsabilisation des plateformes » (dernière modification : 26 octobre 2022), en ligne : <https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act> (consulté le 22 janvier 2023)

Autres : Mémoire de maîtrise et thèse de doctorat

GRATTON, É., *Redefining personal information in the context of the Internet*, Thèse de doctorat, Montréal, Faculté de droit, Université de Montréal, 2012, p. 294-295, en ligne :

<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/19676/Gratton_Eloise_2012_these.pdf?sequence=4&isAllowed=y>

JETTÉ V., *Traque-moi si je le veux. À la recherche d'un cadre juridique entourant la publicité comportementale*, mémoire de maîtrise, Montréal, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, 2017, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/20384/Jette_Virginie_2017_memoire.pdf?sequence=2&isAllowed=y>

Autres : Conférences et webinaires

ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, « AdChoices in Canada », Webinaire (18 mars 2021)

————. « Programme canadien d'autoréglementation pour la publicité comportementale en ligne », Webinaire d'introduction (26 février 2015), en ligne : <https://assets.youradchoices.ca/pdf/DAAC-choixdepub-webinaire.pdf>

ALLIANCE DE LA PUBLICITÉ NUMÉRIQUE DU CANADA, ASSOCIATION CANADIENNE DES ANNONCEURS et CANADIAN MEDIA DIRECTORS' COUNCIL, Webinaire « The State of Identity in Online Advertising: A focus on Canada » (18 novembre 2021), en ligne : <https://us02web.zoom.us/webinar/register/rec/WN_eOwaoTPvQ06KD4ou2-P69g?meetingId=cTkoaRCDuJaZ3NdEJ692itXotvoaXujIkxdL-Znve5E8ANR-8X3b7cMHCaXLHgzF.fmZJTpE4HTO0w-ct&playId=&action=play&_x_zm_rtaid=rWB24S9kQzG8yRg4Cf5MWg.1640274121136.cc5166f33d54d31228dbb4a51d104a3d&_x_zm_rhtaid=743>

CAILLÉ, S., Conférence virtuelle « Quel avenir dans un monde sans cookie », *Dialekta* (30 novembre 2021), en ligne : <https://dialekta.com/fr/conferencier-quel-avenir-pour-les-annonceurs-dans-un-monde-sans-cookie/>

EUROPEAN INTERACTIVE DIGITAL ADVERSITING ALLIANCE (EDAA), « From choices to voices : Transparency in action », Conférence, Sommet international de la *European Interactive Digital Adversiting Alliance* (EDAA), 15 novembre 2021, Londres, en ligne : <https://www.edaasummit.eu/>

SCORZA, G., Garante per la protezione dei dati personali (Autorité italienne de la protection des données), Allocution, Sommet international de la *European Interactive Digital Adversiting Alliance* (EDAA), 15 novembre 2021, Londres, en ligne : < https://edaa.eu/2021-edaa-summit-talks-up-the-importance-of-transparency-and-trust-in-digital-advertising/>

SERRES, M., « Les Nouvelles technologies : révolution culturelle et cognitive », Conférence, 40e anniversaire de l'INRIA, 2007, en ligne : <https://www.youtube.com/watch?v=ZCBB0QEmT5g>