Université de Montréal

Traque-moi si je le veux

À la recherche d'un cadre juridique entourant la publicité comportementale

par Virginie Jetté

Centre de recherche en droit public
Faculté de Droit de l'Université de Montréal

Mémoire présenté
en vue de l'obtention du grade de LL.M
en Maîtrise en droit des technologies de l'information

Août 2017

Université de Montréal

Traque-moi si je le veux

À la recherche d'un cadre juridique entourant la publicité comportementale

par Virginie Jetté

Centre de recherche en droit public
Faculté de Droit de l'Université de Montréal

Mémoire présenté
en vue de l'obtention du grade de LL.M
en Maîtrise en droit des technologies de l'information

A été évalué par un jury composé des personnes suivantes :

Pierre Trudel, président-rapporteur
Vincent Gautrais, directeur de recherche
Nicolas Vermeys, membre du jury

Résumé

L'arrivée de la publicité sur internet a permis aux publicitaires d'accroitre leur visibilité et d'étendre leur contrôle sur les décisions les plus simples que nous effectuons tous les jours, allant de l'achat d'une boîte de céréales, au choix de médias que nous consommons. Pour mieux comprendre le consommateur et le rejoindre avec une simplicité inégalée, les technologies de l'information ont évolué et permettent à présent la traque en ligne des internautes grâce à l'utilisation de « cookies » traceurs. Les agrégateurs de données collectent une multitude de renseignements sur tout un chacun qu'ils utilisent pour diffuser des publicités ciblées, reflétant les informations emmagasinées quant aux intérêts et préférences de l'individu qui les reçoit. Cette traque, généralement réalisée à l'insu et en l'absence de consentement de la part des utilisateurs effrayent souvent ceux qui découvrent son existence. Les pratiques commerciales qui entourent la publicité comportementale sont en effet peu connues et l'industrie semble souhaiter poursuivre ses activités à l'ombre des regards. En conséquence, elle peut plus aisément contourner ses obligations juridiques en matière de droit de la consommation et de vie privée. Ce mémoire cherche donc à mettre en lumière les pratiques d'entreprise en matière de publicité comportementale, les technologies qui la supportent et le cadre juridique qui la régit.

Mots-clés : Publicité comportementale en ligne, publicité ciblée, vie privée, protection du consommateur, renseignements personnels, collecte de données, profilage, témoins.

Abstract

The emergence of online advertising has allowed advertisers to increase their visibility and to extend their control over the simplest decisions we make every day, ranging from the purchase of a cereal box to the media we consume. To better understand the consumers and to reach them with an unparalleled simplicity, technology has evolved and now allows online tracking of Internet users through the use of tracking cookies. Data aggregators collect unprecedented amount of information about each and everyone, which they use to deliver targeted ads, reflecting the interests and preferences of the individual who receives them. This tracking, generally carried out without the knowledge and consent of the users, often frighten those who discover its existence. The commercial practices surrounding behavioural advertising are little known and the industry seems to want to pursue its activities in the shadows. As a result, it can more easily circumvent its legal obligations with respect to consumer and privacy law. This thesis aims to shed light on corporate practices regarding behavioural advertising, the technologies that support it and the legal framework that governs it.

Keywords : Online behavioural advertising, targeted advertising, privacy, consumer protection, personal information, data collection, tracking, profiling, cookies.

Table des matières

Liste des sigles

CCDL : *Charte canadienne des droits et libertés*, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11.

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

CQDL : *Chartre des droits et libertés de la personne*, RLRQ c C-12.

LC : *Loi sur la concurrence*, LRC 1985, c C-34.

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, ch 23.

LCCJTI : *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-11.

LPC : *Loi sur la protection du consommateur*, RLRQ c P-401.

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

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

PIPAA : *Personal Information Protection Act* (Alberta), SA 2003, c P-65.

PIPABC : *Personal Information Protection Act* (British Columbia), SBC 2003, c 63.

PIPEDA : *Personal Information Protection and Electronic Documents Act*, LC 2000, c 5.

Liste des abréviations

CRTC : Conseil de la radiodiffusion et des télécommunications canadiennes

DPI : Deep packet inspection

FAI : Fournisseur d'accès Internet

FTC: Federal Trade Commission

HTML : Hypertext Markup Language

HTTP : Hypertext Transfer Protocol

IAP : Inspection approfondie des paquets

PCL : Publicité comportementale en ligne

ROI : Retour sur investissement

À tous ceux qui résistent.

Remerciements

Je tiens à remercier sincèrement mon directeur de mémoire, Monsieur Vincent Gautrais, pour ses précieux et généreux conseils, ainsi que sa disponibilité qui m'a été d'une aide précieuse au moment de la rédaction de ce mémoire.

Je remercie également quelqu'un qui est devenu un bon ami lors de mes études à l'Université de Montréal, le professeur Florian Martin-Bariteau qui a su me motiver et m'aider à organiser mes idées dans le cadre de la rédaction de mon mémoire.

Je remercie aussi mes parents et ma sœur Marie-Aude pour leur amour inconditionnel et leurs encouragements, tout au long de cette aventure.

Finalement, je tiens à remercier chaleureusement mon amoureuse, pour son appui, son soutien, ses encouragements et sa patience sans lesquels je n'aurais jamais été en mesure de terminer ce défi.

Introduction

« Have you ever clicked your mouse right here? You will »[1].

À notre époque, la publicité est un phénomène établi, apparaissant à tous comme ayant toujours existée. S'il y a une part de vérité dans cette affirmation, ce n'est qu'à partir du XVIII^e^ siècle qu'elle s'est faite plus présente et plus sentie. C'est enfin, au XX^e^ siècle, sous l'impulsion des nouvelles technologies, mais surtout en réponse à l'essor incroyable des médias de masse qu'elle a elle véritablement pris son envol[2], s'imposant au quotidien de tout un chacun.

Les technologies, ayant tendance à bouleverser le monde qui nous entoure, l'arrivée d'Internet, en tant que *réseau des réseaux*[3], n'y a pas fait exception. La *première* publicité en ligne est arrivée le 27 octobre 1994, le jour du lancement de *HotWired.com*[4]. Plusieurs

---

[1] Craig KANARICK et Otto TIMMONS, « The "First" Banner Ad » (2014), en ligne : The First Banner Ad <http://thefirstbannerad.com/> (consulté le 23 janvier 2017); Rebecca GREENFIELD, « The Trailblazing, Candy-Colored History Of The Online Banner Ad », *Fast Company* (27 octobre 2014), en ligne : Fast Company <https://www.fastcompany.com/3037484/most-creative-people/the-trailblazing-candy-colored-history-of-the-online-banner-ad> (consulté le 23 janvier 2017).

[2] Aleecia M MCDONALD et Lorrie Faith CRANOR, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, Arlington, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), 16 août 2010 à la p 1.

[3] « Internet is a global network of computers » Paul LAMBERT, *Gringras, the Laws of the Internet*, 4^e^ éd, Haywards Heath, West Sussex, Bloomsbury Professional, 2015 à la p 1; « Inter is from the Latin root meaning between or among, while net is short for network » Andrew MURRAY, *Information Technology Law: The Law and Society*, 2^e^ éd, Oxford, United Kingdom, Oxford University Press, 2013 à la p 15.

[4] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 38.

annonceurs avaient signé un contrat publicitaire avec le site en question, mais l'image qui marquera l'histoire est sans contredit celle d'une bannière d'AT&T[5] qui dès lors, sera consacrée comme la première publicité en ligne.

Depuis, c'est toute une industrie du « digital advertising » qui s'est développée. Les revenus estimés à la publicité en ligne[6] à l'échelle mondiale s'élevaient à 161 milliards de dollars américains en 2015[7]. Selon différentes sources, ils pourraient s'élever à près de 252 milliards de dollars américains d'ici 2018[8]. Au Canada, les revenus de cette industrie sont à l'image planétaire, étant passés de plus de 3,8 milliards de dollars en 2014 à 4,6 milliards de dollars en 2015[9]. Les annonceurs, comme l'industrie, profitent grandement de ce monde de

---

[5] Craig KANARICK et Otto TIMMONS, « The "First" Banner Ad » (2014), en ligne : The First Banner Ad <http://thefirstbannerad.com/> (consulté le 23 janvier 2017); Rebecca GREENFIELD, « The Trailblazing, Candy-Colored History Of The Online Banner Ad », *Fast Company* (27 octobre 2014), en ligne : Fast Company <https://www.fastcompany.com/3037484/most-creative-people/the-trailblazing-candy-colored-history-of-the-online-banner-ad> (consulté le 23 janvier 2017).

[6] Ces chiffres incluent tant les annonces parues sur les ordinateurs de bureau, les ordinateurs portables que les téléphone cellulaire et les tablettes, eMarketers et Cindy LIU, *Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 2015–2020*, 2016 à la p 21, en ligne : <https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketers-Updated-Estimates-Forecast-20152020/2001916> (consulté le 10 mars 2017); Interactive Advertising Bureau of Canada, *2015 Actual + 2016 Estimated Canadian Internet Advertising Revenue Survey*, Annual Internet Advertising Revenue Reports, 2016 à la p 4, en ligne : <http://iabcanada.com/research/annual-internet-advertising-revenue-reports/> (consulté le 10 mars 2017).

[7] eMarketers et Cindy LIU, *Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 2015–2020*, 2016 à la p 21, en ligne : <https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketers-Updated-Estimates-Forecast-20152020/2001916> (consulté le 10 mars 2017); Les revenus ne cessent leur croissance puisqu'on rapportait en 2013 qu'ils s'élevaient à environ 117 milliards de dollars américains, voir Kate MATHEWS-HUNT, « CookieConsumer: Tracking online behavioural advertising in Australia » (2016) 32:1 CLSR 55 à la p 58.

[8] Kate MATHEWS-HUNT, « CookieConsumer: Tracking online behavioural advertising in Australia » (2016) 32:1 CLSR 55 à la p 58; PricewaterhouseCoopers, « Internet advertising - Key insights at a glance », en ligne : PwC.com <http://www.pwc.com/gx/en/industries/entertainment-media/outlook/segment-insights/internet-advertising.html> (consulté le 17 janvier 2017).

[9] Interactive Advertising Bureau of Canada, *2015 Actual + 2016 Estimated Canadian Internet Advertising Revenue Survey*, Annual Internet Advertising Revenue Reports, 2016 à la p 6, en ligne : <http://iabcanada.com/research/annual-internet-advertising-revenue-reports/> (consulté le 10 mars 2017).

possibilité qu'offre la publicité en ligne, puisque celle-ci permet de mesurer beaucoup plus rapidement et plus efficacement le retour sur investissement (ci-après « ROI »). Ainsi, le domaine de la publicité en ligne est un domaine si lucratif qu'il apparaît à présent être incontournable.

La publicité en ligne offre un avantage remarquable à qui sait l'exploiter. Si elle permet de rejoindre chacun en tout temps et en tout lieu[10], elle permet surtout d'en connaître beaucoup plus sur les internautes[11] que toute autre forme de publicité. À l'aide des récentes technologies mises à la disposition des publicitaires, une quantité considérable d'information peut être recueillie par une traque constante, permettant ainsi la création de profils utilisateurs remarquablement complets.

Lorsque les publicitaires ont compris comment recueillir des informations à l'aide des « *cookies* »[12], ils ont pu se lancer dans ce qu'il fut convenu d'appeler la publicité ciblée en

---

[10] « By the end of 2016, close to half of the world's population will be using the Internet [...] Although « home » remains the place where people most frequently use the Internet, in particular in developed countries, « in mobility » is the second most important access location, followed by access at work » International Telecommunication Union, *Measuring the Information Society Report 2016*, ITU MIS Report, 2016 aux pp 181‑182, en ligne : <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf> (consulté le 12 février 2017).

[11] Tout au long de ce mémoire, il est possible que nous alternions entre les termes *internaute*, *consommateur*, *client* et *citoyen*. Si certains termes révèlent un rôle précis, comme celui de consommateur ou de client qui réfèrent surtout à la relation contractuelle ou d'achat, d'autres agirons ici à titre de générique sans distinction, puisque nous reconnaissons que la publicité n'a pas toujours un caractère commercial et peut être politique, sociale, etc.

[12] Les « cookies » ou témoins traceurs sont en fait de petits fichiers textes généralement constitués d'une série de caractères permettant d'identifier un ordinateur à la manière d'un identifiant personnel. Nous aborderons plus en détails, dans la partie préliminaire, le fonctionnement des cookies. À cet égard, voir Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 276.

ligne (ci-après « PCL »). Qualifié par certains de Saint Graal[13] de la publicité, le ciblage permet de joindre l'utilisateur d'une manière unique et forgée à son image. Dès lors, il est possible de cibler avec une plus grande acuité le type de contenu susceptible de retenir l'attention d'un utilisateur et ainsi ouvrir la porte à la publicité comportementale, soit celle basée sur les habitudes et comportements d'un utilisateur donné[14]. Ce type de publicité s'effectue donc en fonction des données recueillies lors de multiples visites, sur différents sites Internet, que ces derniers aient ou non un lien entre eux. Le témoin traceur « suit » l'utilisateur, même lorsque celui-ci n'est plus sur le site visité. Dans une perspective purement économique, la PCL offre le plus haut ROI par dollar dépensé[15].

---

[13] Cette nouvelle approche de marketing où les annonceurs, plutôt que de cibler les masses, procèdent sur une base individuelle « one-to-one » constitue une révolution. Les compagnies approchent des individus spécifiques « based on information collected about the particular characteristics, preferences, and behavior of this person », Paul SCHWARTZ et Daniel SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814 à la p 1849; Voir aussi Jianqing CHEN et Jan STALLAERT, « An Economic Analysis of Online Advertising Using Behavioral Targeting » (2014) 38:2 MIS Quaterly 429 à la p 429; Hotaling soutient également, que la PCL offre le plus grand retour sur investissement pour chaque dollar publicitaire dépensé, Andrew HOTALING, « Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting » (2008) 16:2 CommLaw Conspectus 529 à la p 536.

[14] « [It] is possible for online entities to gather data on what people have done online, including their previous searches, what websites they have browsed, and perhaps even what they have purchased online. Those data, together with other information, can be used to target advertisements to people based on their behavior. », David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 50.

[15] Business News Daily, « Has Online Targeted Advertising Gone Too Far? » (7 avril 2011), en ligne : <http://www.businessnewsdaily.com/841-online-targeted-advertising.html> (consulté le 11 avril 2017); Charles CURRAN, « Study finds behaviorally targeted ads more than twice as valuable and effective as non-targeted online ads » (24 mars 2010), en ligne : NAI : Network Advertising Initiative <https://www.networkadvertising.org/blog/study-finds-behaviorally-targeted-ads-more-twice-valuable-and-effective-non-targeted-online-ads> (consulté le 11 avril 2017).

Si, au départ, Internet était perçu comme un outil de communication démocratique[16], la PCL, par le suivi des préférences, navigations et habitudes des utilisateurs, semble constituer une intrusion dans la vie privée de ces derniers, en plus de favoriser la discrimination de prix fondée sur les habitudes des consommateurs par la mise en place de prix comportementaux (de l'anglais « *behavioural pricing* »). Armés de ces nouveaux outils, les publicitaires et compagnies de ce monde envahissent nos demeures et nos vies, scrutant les moindres gestes des utilisateurs en ligne à la recherche d'une certaine *tendance* dans leurs habitudes, afin de leur offrir de la publicité à leur image. Cette nouvelle tendance, sous forme de surveillance, effraye et entraîne son lot d'inconforts et de problèmes, notamment en matière de protection des renseignements personnels, de droit de la consommation et de droit de la concurrence.

Si l'industrie numérique de la publicité permet de chiffrer l'importance du marché, d'autres domaines sont également affectés par la publicité comportementale d'une manière plus subtile. L'année 2016 a été le théâtre de débats portant sur l'intrusion de la publicité ciblée en matière de politique. À la suite de différents incidents s'étant produit sur cette scène, Tim Berners-Lee, le père du web, a fait une sortie médiatique enjoignant les gouvernements à mieux encadrer la publicité ciblée politique. Il soulignait que le « *[targeted] advertising allows a campaign to say completely different, possibly conflicting things to different groups. Is that democratic?* »[17].

---

[16] En 1989, la proposition initiale de Tim Berners-Lee de ce qui devait devenir le World Wide Web prévoyait que « The aim would be to allow a place to be found for any information or reference which one felt was important, and a way of finding it afterwards. The result should be sufficiently attractive to use that it information contained would grow past a critical threshold, so that the usefulness of the scheme would in turn encourage its increased use. » Simone BORSCI et al, *Computer Systems Experiences of Users with and Without Disabilities: An Evaluation Guide for Professionals*, Boca Raton, FL, USA, CRC Press, 2013 à la p 81.

[17] Olivia SOLON, « Tim Berners-Lee calls for tighter regulation of online political advertising », *The Guardian* (12 mars 2017), en ligne : The Guardian <https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-online-political-advertising-regulation> (consulté le 25 mars 2017).

C’est donc dans cette perspective que cet écrit se veut d’abord et avant tout une réflexion sur le phénomène moderne qu’est la publicité comportementale en ligne au regard du droit. La PCL — principale source de revenus pour les fournisseurs de contenu sur Internet — est devenue caractéristique du commerce en ligne et est un moyen en vertu duquel les annonceurs obtiennent des informations sur les clients afin de mieux cibler la publicité leur étant destinée.

Nous débuterons, tout d’abord, par décrire et circonscrire l’environnement global de la publicité comportementale en ligne et des différents mécanismes qui l’entourent dans la partie préliminaire. Par la suite, dans la première partie, nous dresserons un portrait de l’encadrement juridique de la publicité au Canada avant de procéder à une analyse concrète du cadre juridique applicable à la publicité comportementale. Dans la deuxième partie, nous aborderons les questions relatives à protection de la vie privée face aux défis posés par la PCL.

Nous soutiendrons que le suivi des préférences des utilisateurs, ainsi que la vaste quantité d’informations recueillies constituent un problème juridique d’importance. Après avoir établi les problématiques inhérentes, nous tenterons, si nécessaire, de proposer des pistes de réflexion quant à une possible réforme, le tout dans la perspective de permettre la poursuite des activités commerciales de cette pratique, tout en améliorant la protection des utilisateurs.

Chapitre préliminaire — Environnement de la publicité comportementale en ligne

« Big Data is coming, like it or not »[18].

Avant de procéder à une analyse juridique des impacts de la publicité comportementale en ligne, il nous apparaît nécessaire de s'adonner à une explication concrète du fonctionnement de la publicité comportementale et de ses différentes facettes. Cet aperçu des mécanismes entourant la PCL devrait permettre au lecteur de mieux saisir les enjeux qui en découlent.

Avec le lancement en 1994 du navigateur *Mosaic*[19], qui permettait d'afficher texte et image sur une seule page, Internet a vu ses premières publicités affichées sous forme de bannières. Le modèle d'affaires de l'époque reposait sur les fondements traditionnels de la publicité et le prix était fixé à partir du nombre d'*impressions*, soit le nombre d'internautes ayant été exposé à la publicité[20]. Le modèle s'est ensuite raffiné et s'est principalement fondé sur le « coût par mille », soit le coût par mille utilisateurs ayant visionné la publicité[21]. En raison des avancements technologiques, un nouveau modèle s'est développé, parallèlement, celui du « coût par clic », permettant entre autres une meilleure évaluation de la performance

---

[18] Paul OHM, « The Underwhelming Benefits of Big Data » (2013) 161:1 U Pa L Rev 339 à la p 346.

[19] *Mosaic* est éventuellement devenu le célèbre *Netscape*, Steven C BENNETT, « Regulating Online Behavioral Advertising » (2010) 44 John Marshall L Rev 899 à la p 900.

[20] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 38.

[21] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 39.

d'une publicité[22]. Cette pratique s'est répandue à partir du moment où *Procter & Gamble* a conclu une entente avec *Yahoo*!, stipulant que *Yahoo!* ne serait payé qu'au moment où l'internaute cliquait sur la publicité[23]. En gardant en tête ce standard de rémunération, il apparaît donc nécessaire, voire même essentiel, qu'une publicité parvienne à atteindre sa cible, sans quoi il n'y aurait pas de conversion et le *clic* recherché ne surviendrait pas.

Les mécanismes initiaux de publicité en ligne nécessitaient que les publicistes déterminent *quelle* publicité devait être affichée sur *quelle* page. On visait alors les masses avec plus ou moins de précisions, tentant, lorsque possible, de contextualiser les publicités selon le contenu de la page visitée. Cette opération avait cependant ses limites :

> On Web sites that dealt with limited industries or topics of interest, the answer was simple: serve advertisements from companies whose products and services correspond to those industries or interests. However, on more complex sites, the answer was frequently less clear-cut, pushing e-advertising firms to seek out user information as a means of more effectively targeting Web advertisements[24].

---

[22] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 39; Jianqing CHEN et Jan STALLAERT, « An Economic Analysis of Online Advertising Using Behavioral Targeting » (2014) 38:2 MIS Quaterly 429 à la p 429.

[23] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 38.

[24] Andrew HOTALING, « Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting » (2008) 16:2 CommLaw Conspectus 529 à la p 534.

C'est alors qu'est entrée en jeu la pratique du ciblage publicitaire. Dans son ensemble, celle-ci pourrait être définie comme étant « une méthode qui consiste à choisir la bonne population sur laquelle concentrer ses efforts marketing »[25]. Il s'agit donc essentiellement d'afficher *la bonne publicité au bon consommateur*. L'idée de la publicité comportementale, réduite sous sa plus simple forme, est qu'Internet nous montre ce que nous avons envie de voir. Ainsi les consommateurs « *[are] more likely to find interest in advertising tailored to their own preferences* »[26] menant inévitablement à une plus grande efficacité du marché[27]. Aux États-Unis, le *Federal Trade Commission* (ci-après « FTC ») décrit la publicité comportementale comme étant « *[the] practice of tracking an individual's online activities in order to deliver advertising tailored to his or her interests* »[28]. Cette affirmation supporte également l'idée qu'un contenu plus adapté engendre une réduction des publicités sans importance[29].

Dans ce chapitre préliminaire, nous aborderons les différentes facettes du ciblage, à savoir : (Section 1) comprendre sa topographie (Section 2), cerner l'industrie du ciblage et (Section 3) aborder les aspects techniques du ciblage.

---

[25] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 159; Voir aussi Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 9 « from a business perspective, is a marketing concept aimed at addressing a specific target group ».

[26] Ari JUELS, *Targeted Advertising ... And Privacy Too*, *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*, coll CT-RSA 2001, London, UK, Springer-Verlag, 2001, 408 à la p 409.

[27] Ari JUELS, *Targeted Advertising ... And Privacy Too*, *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*, coll CT-RSA 2001, London, UK, Springer-Verlag, 2001, 408 à la p 409.

[28] Federal Trade Commission, *FTC Staff Revises Online Behavioral Advertising Principles*, 2009, en ligne : <https://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles> (consulté le 2 avril 2016).

[29] Aleecia M MCDONALD et Lorrie Faith CRANOR, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, Arlington, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), 16 août 2010 à la p 2.

Section 1 — Topographie du ciblage

Le ciblage revêt différentes facettes. Il peut être géographique[30], démographique[31], temporel[32] — reposant sur des données d'espace-temps —, contextuel[33] — lorsqu'il repose sur la visite *actuelle* de l'utilisateur —, et finalement comportemental[34], renvoyant alors au suivi de l'utilisateur à travers les différents sites Internet qu'il a préalablement parcourus. D'autres

---

[30] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 14; Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 160.

[31] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 14; Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 160.

[32] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 14; Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161.

[33] Commissariat à la protection de la vie privée du Canada, *Position de principe sur la publicité comportementale en ligne*, 2015, 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 20 février 2017); Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161; Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 12; Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161.

[34] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161; Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 15 « Behavioral targeting works by tracking the actions (e.g. Web browsing behavior, channel switching in IPTV) of users. Data mining methods help to detect patterns in the past user behavior that are aggregated to user interest profiles which become the basis of targeting ».

types de ciblage existe également, comme le reciblage[35] — forme avancée de ciblage comportemental —, ou encore le ciblage technique, qui renvoie à la technologie particulière employée par l'utilisateur (tant logicielle que matérielle)[36]. Ce type de ciblage, plutôt que de viser l'utilisateur, cible essentiellement la machine (au sens large), s'adaptant à celle-ci. Dans la présente section, nous aborderons davantage les principaux types de ciblages.

A. Ciblage géographique

Il existe différents moyens de parvenir à la localisation d'un utilisateur. Celui-ci peut avoir volontairement fourni cette information lors de son arrivée sur une page web, par exemple par la sélection de sa région en page d'accueil ou par la création d'un profil sur le site. Cette donnée peut également être divulguée à l'insu de l'internaute, grâce à une inspection de son adresse IP — qui permet de le localiser dans l'univers physique[37] avec une exceptionnelle précision[38]. Le ciblage géographique peut également avoir lieu directement dans le monde physique, par exemple à travers l'utilisation des coordonnées GPS d'un

---

[35] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 162; Joanna PENN, « Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet » (2011) 64:3 Fed Comm LJ 599 à la p 600.

[36] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 13.

[37] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 42, à noter que l'adresse IP est attachée à l'appareil utilisé pour se connecter à Internet et non pas à l'utilisateur directement.

[38] Il faudra toutefois prendre cette affirmation avec prudence puisqu'il fut récemment démontrer que beaucoup de services de localisation par IP étaient fondés sur un modèle défectueux, voir à cet effet Kashmir HILL, « How A Strange Internet Glitch Turned This Kansas Farm Into A Digital Hell », en ligne : Fusion <http://fusion.net/story/287592/internet-mapping-glitch-kansas-farm/> (consulté le 13 novembre 2016).

appareil mobile[39] ou d'une puce RFID[40]. La capacité d'adaptation des publicitaires est sans égale, parvenant à créer des liens entre les activités d'un utilisateur et sa localisation, afin de lui offrir des publicités taillées sur mesure :

> We look at the context of what you're doing in the application and your location, and we match those two up and send you ads based on that. We pull relevant advertisers and try to target them to the right audience[41].

Comme le souligne Sol Tanguay[42], ce type de ciblage permet aux annonceurs de concentrer leurs efforts sur une zone où ils parviendront à atteindre le public désiré.

B. Ciblage démographique/sociodémographique

Le ciblage démographique vise un public en fonction de ses caractéristiques sociodémographiques. Ce type de ciblage implique une catégorisation fondée notamment sur l'âge, le sexe ou le revenu. Cette pratique n'est pas nouvelle ni unique au ciblage en ligne. Le

---

[39] Bette MARSTON, « Where in the world? (Core Concepts: Geotargeting) » (2010) 44:12 Marketing News 6; « Obtaining someone's location at any given point in time is fairly easy, by the way. A typical smartphone has four ways that it can be physically tracked: triangulation from cell towers, GPS, Bluetooth, and Wi-Fi signal—each of which are individually identifiable with serial codes that are globally unique to each phone's hardware. » Gregory MAUS, « How data brokers sell your life, and why it matters » (24 août 2015), en ligne : The Stack <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/> (consulté le 11 avril 2017); En outre, il semblerait que les algorithmes soient à présent suffisamment développés pour parvenir à prévoir les déplacements des utilisateurs, en recoupant avec l'information provenant de leurs amis David TALBOT, « A Phone that Knows Where You're Going », en ligne : MIT Technology Review <https://www.technologyreview.com/s/428441/a-phone-that-knows-where-youre-going/> (consulté le 10 avril 2017).

[40] Nancy KING, « When Mobile Phones are RFID-Equipped - Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce » (2008) 15:1 Mich Telecomm & Tech L Rev 107.

[41] Bette MARSTON, « Where in the world? (Core Concepts: Geotargeting) » (2010) 44:12 Marketing News 6.

[42] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161.

ciblage démographique découlerait de l'ère des premières bases de données, dans les années 1970, et proviendrait en général de données publiques et gouvernementales[43]. Outillés de telles données, il est alors possible de créer des publicités basées sur ces caractéristiques, et de rejoindre un public cible, par exemple un groupe d'hommes âgé de 35-40 ans. Il est également possible qu'il y ait recoupement entre données démographiques et données géographiques[44] permettant alors de circonscrire d'autant plus la cible.

C. Ciblage temporel

Le ciblage temporel s'inscrit dans le temps et cherche à livrer des messages en fonction de l'heure, du jour de la semaine et des activités ayant normalement cours durant cette période de temps. À l'instar de la publicité traditionnelle télévisuelle ou radiophonique, où certaines publicités surviennent à des moments précis, selon les besoins des annonceurs et les messages qu'ils cherchent à véhiculer. Une publicité annonçant par exemple un nouveau petit déjeuner à un restaurant rapide aura certainement plus de succès le matin qu'en fin d'après-midi. Dans une perspective quelque peu différente, un annonceur pourrait avoir intérêt à promouvoir ses publicités lors de ses heures d'ouverture[45], ou durant une période où il souhaite acquérir une nouvelle clientèle. Comme les autres modes de ciblage, le ciblage temporel peut survenir de concert avec d'autres méthodes et ainsi considérer des caractéristiques particulières, tenant compte non seulement du temps, mais aussi de l'utilisateur, du contexte et de d'autres caractéristiques. Une publicité annoncée sur un site de plein air risque de ne pas faire mouche un samedi après-midi entre treize et seize heures.

---

[43] Paul SCHWARTZ et Daniel SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814 à la p 18.

[44] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 14.

[45] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161.

D. Ciblage contextuel

Il existe essentiellement deux formes de ciblage contextuel. La première repose sur le contenu de ce que l'internaute regarde. Dans ce contexte, sur une page dédiée aux sports de plein air, il serait possible que l'utilisateur soit exposé à des publicités reliées au contenu, par exemple des articles de plein air ou des escapades.

Le deuxième concerne ce que l'utilisateur recherche, par exemple par l'utilisation d'un moteur de recherche[46]. On pourrait considérer l'exemple du bottin téléphonique comme étant représentatif du ciblage contextuel. Un utilisateur recherchant un plombier se trouverait exposé à une multitude d'annonces selon le contexte, soit la recherche d'un plombier.

E. Ciblage comportemental

Comme nous l'avons mentionné, le ciblage comportemental renvoie au suivi de l'utilisateur à travers les différents sites Internet qu'il parcourt. On présume des champs d'intérêt d'un internaute, en raison de son historique de navigation, de son profil utilisateur et de toutes autres données à la disposition de l'annonceur[47]. Les publicités sont alors affichées indépendamment du support et du contenu du site web[48]. Par exemple, on retrouvera des

---

[46] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161.

[47] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 15.

[48] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 161, citant ; Alan OUAKRAT, « Le ciblage comportemental, une perte de contrôle des éditeurs sur les données de l'audience » (2012) 6:1 Tic&société, en ligne : Tic&société <http://ticetsociete.revues.org/1251>.

publicités d'articles de plein air sur un site de nouvelles, bien que ce site ne soit pas spécifiquement dévolu aux activités de plein air.

> The essential purpose of online profiling, from its inception, was to record online behavior for the purpose of producing targeted advertising. Such targeted advertising could take into account prior online behavior in order to present consumers with goods and services they were most likely to buy[49].

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[50], par l'inspection de paquets profonds[51], 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[52]. 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

---

[49] Steven C BENNETT, « Regulating Online Behavioral Advertising » (2010) 44 John Marshall L Rev 899 à la p 900.

[50] Voir section 3, ci-dessous.

[51] Sophie STALLA-BOURDILLON, Evangelia PAPADAKI et Tim CHOWN, « From Porn to Cybersecurity Passing by Copyright: How mass Surveillance Technologies are Gaining Legitimacy... The Case of Deep Packet Inspection Technologies » (2014) 30:6 CLSR 670; Andreas KUEHN et Milton MUELLER, *Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States*, Syracuse NY, Syracuse University, School of Information Studies, 2012, en ligne : <https://papers.ssrn.com/abstract=2014181> (consulté le 27 mars 2017); Aaron K MASSEY et Annie I ANTÓN, « Behavioral Advertising Ethics » dans Melissa Jane Dark, dir, *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*, IGI Global, 2011, 162.

[52] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 275.

donc ciblé à travers un profil bâti à son image menant alors à une personnalisation au plan individuel[53].

F. Reciblage

Le reciblage, ou « *retargeting* » est l'ultime personnalisation de la publicité comportementale puisqu'elle n'est plus bâtie sur un profil abstrait, mais est bien propre à chaque individu[54]. Ce type de ciblage est la conséquence directe des actions de l'utilisateur puisqu'il est déterminé en fonction de l'intérêt démontré envers un produit ou un service sur une page donnée. Le meilleur exemple de reciblage est lorsqu'un utilisateur ajoute des biens dans son panier virtuel, sans conclure la transaction, et que plus tard, sur un site différent, il verra les produits de son panier apparaître en publicité. Cette publicité pourrait en outre, être assortie d'un rabais afin d'inciter l'internaute à compléter son achat. Ainsi, seuls les internautes qui ont visité la page en question et démontré un intérêt envers le produit sont visés par un tel ciblage[55].

Afin d'illustrer ce qu'est le reciblage, imaginons la situation suivante : Camille se rend sur le site de son magasin de meuble préféré, elle y voit une magnifique commode *rétro* et

---

[53] Christian SCHLEE, *Targeted advertising technologies in the ICT space: a use case driven analysis*, Wiesbaden, Springer Vieweg, 2013 à la p 11« targeting addresses users anonymously via a target group they belong to (e.g. women, age 20-49) ». Mike SMITH, *Targeted: how technology is revolutionizing advertising and the way companies reach consumers*, New York, American Management Association, 2015 à la p 114 « Suppose you wanted advertise only to males over age 65 who are left-handed, wear trifocals, are tax-reform advocates, are vegan, and pack lunches for themselves but won't pack their sandwiches in plastic bags. […] Marketers create profiles for their presumed ideal customers. These profiles tend to become more and more detailed and elaborate as marketers try to home in on the right candidates for their products ».

[54] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 162.

[55] Joanna PENN, « Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet » (2011) 64:3 Fed Comm LJ 599 à la p 603.

l'ajoute à son panier. Après quelques minutes de réflexion, elle choisit de ne pas poursuivre sa transaction et quitte le site. Le lendemain en lisant les nouvelles en ligne, elle aperçoit une publicité de son magasin de meubles préféré, annonçant la commode en rabais. Nul doute que cette initiative a pour but de poursuivre les clients comme Camille à conclure la transaction.

Section 2 — Industrie du ciblage

En raison de l'importante quantité de sites web, l'industrie de la publicité en ligne doit faire affaire avec une variété d'acteurs qui ont chacun un rôle à jouer dans la chaîne publicitaire. Nous traiterons, dans la présente section, les différents rôles et objectifs de ces acteurs.

A. Les annonceurs

Tout d'abord, l'annonceur serait le premier élément de la chaîne publicitaire. Il s'agit essentiellement de celui qui souhaite annoncer son produit, service ou message. Comme ceux-ci ne possèdent généralement pas de moyens particuliers pour joindre l'internaute, ils doivent faire affaire avec une agence publicitaire. Cette agence aura généralement pour responsabilité de créer une publicité de concert avec l'annonceur. Tous les annonceurs n'emploient pas nécessairement une agence et procèdent alors en interne, notamment grâce à la relative simplicité de l'affichage sur Internet.

Ainsi, l'annonceur peut agir seul, ou de concert avec une agence publicitaire qui pourrait le guider dans son processus de réalisation d'une publicité. Comme il s'agit de « convertir les utilisateurs exposés à leur publicité en clients […], ils doivent communiquer le

bon produit ou service, au bon moment, au bon endroit et à la bonne personne »[56]. Dans cette perspective, l'annonceur pourra faire affaire avec d'autres entités lui permettant de joindre cette « bonne personne », comme notamment des prestataires de solutions analytiques (« *analytics providers* »), chercheurs en marketing[57].

B. Les consommateurs

Les consommateurs sont le dernier maillon de la chaîne. L'objectif final pour un annonceur est de convertir en clients les internautes ayant été exposés à la publicité ou, à tout le moins, de les amener à poser une action (comme visiter une page web, s'inscrire à une liste de diffusion, etc.).

C. Les éditeurs

Les éditeurs de contenu (de l'anglais *publishers*) réfèrent aux différents « lieux » où l'internaute sera exposé à une publicité. Il peut s'agir de portails d'information comme MSN ou Yahoo! ; des sites de nouvelles comme ledevoir.com ou lapresse.ca ; des moteurs de recherches comme *Google* ou *Bing* ; des sites de médias sociaux comme *Facebook* ou *LinkedIn* ; ou tout autre site[58]. Les éditeurs développent du contenu et vendent ensuite des espaces publicitaires. Inévitablement, plus un site sera riche en contenu et en visites, plus ses

---

[56] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 163.

[57] Omer TENE et Jules POLONETSKY, « To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising » (2012) 13:1 Minn J L Sci & Tech 281 à la p 282.

[58] Mike SMITH, *Targeted: how technology is revolutionizing advertising and the way companies reach consumers*, New York, American Management Association, 2015 à la p 19.

espaces publicitaires prendront de la valeur[59] (de la même manière qu'une publicité de 30 secondes durant le *Super Bowl* s'est vendue en 2016 à un prix aussi élevé que 5 millions de dollars US[60]).

Ils représentent le dernier lien (et peut-être le seul) entre l'annonceur et le consommateur. Il est en effet possible que l'annonceur ait directement acheté un espace publicitaire sur la plateforme de l'éditeur ou qu'il ait fait affaire avec un intermédiaire ou plusieurs intermédiaires pour acheter un tel espace. Certains éditeurs de contenu ont la capacité de vendre directement leurs espaces publicitaires aux annonceurs et procèdent alors en interne sans intermédiaires. D'autres choisissent de faire affaire avec des intermédiaires via des sociétés publicitaires. Il est également possible qu'un éditeur procède indépendamment et vende ses surplus à un intermédiaire.

Dans tous les cas, c'est en navigant sur les sites d'éditeurs que sont déposés les *témoins* qui serviront à la traque des utilisateurs[61].

D. Les sociétés publicitaires

Le marché des sociétés publicitaires se divise essentiellement entre les réseaux (« *ad networks* ») et les plateformes d'enchères (« *ad exchanges* »)[62]. Pour l'éditeur de contenu, il

---

[59] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 164.

[60] « Cost of Super Bowl Advertising Breakdown by Year », en ligne : Superbowl-ads.com <http://superbowl-ads.com/cost-of-super-bowl-advertising-breakdown-by-year/> (consulté le 4 avril 2017).

[61] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 164.

n'existe que peu de différences entre le réseau et la plateforme d'enchères. Pour afficher la publicité sur son site, il lui suffit généralement de placer quelques balises HTML fournies par la société publicitaire et le code saura faire le lien entre l'internaute, la page, le serveur et l'annonceur[63]. Les sociétés publicitaires, qu'il s'agisse d'« *ad networks* » ou d'« *ad exchanges* » mettent en relation les annonceurs avec les consommateurs par l'entremise des éditeurs[64]. Une large partie du web offre un contenu gratuit aux internautes et vit des revenus de la publicité. Un des arguments les plus souvent mis de l'avant par les supporteurs de la PCL est que celle-ci « *supports the economic vitality of digital publishers, content providers, and other ad-supported Internet businesses* »[65]. Ainsi, la mise en place de sociétés publicitaires a permis aux éditeurs de petite et moyenne taille de poursuivre leurs opérations en générant des revenus[66].

Avec l'explosion du nombre de sites web, les agences publicitaires traditionnelles n'étaient plus en mesure de rejoindre toutes les plateformes afin d'acheter des espaces pour leurs clients. C'est donc ainsi que sont nés les réseaux publicitaires. Le seul rôle des réseaux est de rendre disponible des espaces publicitaires aux annonceurs à faible coût. Pour ce faire,

---

[62] Julia ZUKINA, « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation within the Internet Behavioral Advertising Industry » (2012) 7:1 Brooklyn Journal of Corporate, Financial Commercial Law 277 à la p 280.

[63] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 46.

[64] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 693.

[65] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 289.

[66] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 aux pp 693‑694.

ils achètent des lots auprès des annonceurs et les regroupent en réseaux[67]. Leur objectif est de parvenir à agréger la plus grande audience possible afin de maximiser leurs revenus. Il importe donc d'avoir, parmi leur catalogue, une diversité d'éditeurs.

Les plateformes d'enchères, quant à elles, regroupent également des espaces publicitaires à la manière de réseaux, mais procèdent à la vente d'une manière un peu différente. Plutôt que d'acheter eux-mêmes les espaces, ils bâtissent des plateformes où les annonceurs peuvent enchérir sur un inventaire d'espaces publicitaires disponibles. Ces échanges permettent aux « *buyers and sellers to value inventory on an impression by impression basis in real time* »[68].

Lorsqu'un consommateur visite le site d'un éditeur, plusieurs opérations techniques ont lieu instantanément. Le serveur de l'éditeur envoie au navigateur de l'utilisateur un « ad tag » contenant de l'information relative à la localisation du serveur publicitaire (« *ad server* ») de l'éditeur. Ce serveur prend alors la décision de *quelle* publicité affichée par l'entremise du programme *Ad Selector*[69]. Concrètement, les firmes chargées de la collecte de données cherchent à optimiser l'expérience et procèdent à la segmentation des utilisateurs en fonction

---

[67] Mike SMITH, *Targeted: how technology is revolutionizing advertising and the way companies reach consumers*, New York, American Management Association, 2015 à la p 20; Azam KHAN, « The Inner Workings of Ad Networks and Ad Exchanges » (11 octobre 2011), en ligne : <http://www.adweek.com/digital/the-inner-workings-of-ad-networks-and-ad-exchanges/> (consulté le 5 avril 2017).

[68] Azam KHAN, « The Inner Workings of Ad Networks and Ad Exchanges » (11 octobre 2011), en ligne : <http://www.adweek.com/digital/the-inner-workings-of-ad-networks-and-ad-exchanges/> (consulté le 5 avril 2017); Julia ZUKINA, « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation within the Internet Behavioral Advertising Industry » (2012) 7:1 Brooklyn Journal of Corporate, Financial Commercial Law 277 à la p 280; Mike SMITH, *Targeted: how technology is revolutionizing advertising and the way companies reach consumers*, New York, American Management Association, 2015 à la p 20.

[69] Azam KHAN, « The Inner Workings of Ad Networks and Ad Exchanges » (11 octobre 2011), en ligne : <http://www.adweek.com/digital/the-inner-workings-of-ad-networks-and-ad-exchanges/> (consulté le 5 avril 2017).

des caractéristiques qui leur sont propres[70]. Cette opération implique enfin de combiner le profil de l'utilisateur avec de l'information comme le type de site sur lequel il se trouve[71]. Cette opération regroupe alors deux types de ciblage, soit un ciblage contextuel[72] et un ciblage comportemental fondé sur le profil.

> [When] a buyer visits a website, an advertising exchange combines the buyer's profile with information about his or her current website activity in order to more precisely target advertisements. The exchange then conducts an auction in which businesses bid for the opportunity to present their targeted advertisements (the whole process takes milliseconds)[73].

Lorsqu'un utilisateur visite une page Internet, c'est donc une véritable course aux enchères qui s'ensuit. Les traqueurs fournissent alors l'information au plus offrant et en quelques millisecondes, l'utilisateur voit apparaître une publicité taillée sur mesure, le tout sans que le site ou l'utilisateur soit conscient du processus ayant lieu en arrière-plan.

Puisque les réseaux publicitaires affichent de la publicité sur des milliers de sites Internet[74], ils ont également la possibilité de suivre un utilisateur sur l'ensemble des sites de leurs réseaux grâce aux *témoins* qui seront déposés par les agrégateurs de données, lors de la

---

[70] Richard WARNER et Robert H SLOAN, « Behavioral advertising: From one-sided chicken to informational norms » [2012] 15 Vand J Ent & Tech L 49 à la p 57.

[71] Richard WARNER et Robert H SLOAN, « Behavioral advertising: From one-sided chicken to informational norms » [2012] 15 Vand J Ent & Tech L 49 à la p 58.

[72] Julia ZUKINA, « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation within the Internet Behavioral Advertising Industry » (2012) 7:1 Brooklyn Journal of Corporate, Financial Commercial Law 277 à la p 280.

[73] Richard WARNER et Robert H SLOAN, « Behavioral advertising: From one-sided chicken to informational norms » [2012] 15 Vand J Ent & Tech L 49 à la p 58.

[74] En parlant d'un des plus grands réseau de la fin du 20e siècle, DoubleClick Daniel J Solove disait : « Numerous websites subscribe to DoubleClick. This means that if I click on the same website as you at the very same time, we will receive different advertisements calculated by DoubleClick to match our interests. People may not know it, but DoubleClick cookies probably reside on their computer. As of the end of 1999, DoubleClick had amassed 80 million customer profiles. » Daniel J SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, Fredericksburg, NYU Press, 2006 à la p 25.

visite d'un membre du réseau[75]. En plus de partager la publicité, les annonceurs étant impliqués dans les réseaux partagent également de l'information à travers ces *témoins*[76].

> Network advertisers use cookies in a sophisticated way to track consumer behavior. First, they solicit websites to become part of their advertising networks. Then, when a consumer first visits a website that is a member of an advertising network, the member website sends a cookie with a unique tracking number to the web browser. This cookie is configured to be included with all requests for content sent to any of the network advertiser's member websites. Thus, each time the consumer visits any of the member websites, the network advertiser can associate the consumer with the web content that the consumer accessed.
>
> This behavior is hidden from the consumer; the consumer does not normally know anything about the cookies, which websites are members of which advertisers' networks, or what information a member website might share with the network advertiser[77].

Ainsi, les plateformes d'enchères et réseaux mettent à disposition des annonceurs des plateformes permettant d'acquérir « *the right to reach anonymous individuals nearly instantaneously* »[78]. En d'autres termes, il s'agit d'acheter le droit de présenter leur publicité à un utilisateur individuellement en se permettant d'être aussi sélectifs qu'ils le souhaitent[79]. Pour être en mesure de procéder à ce choix, il est nécessaire d'avoir des profils précis pouvant être notamment recueillis auprès d'agrégateurs de données avant qu'entre en jeu le mécanisme des témoins nécessaire afin de procéder à cette traque.

---

[75] Frederik J Zuiderveen BORGESIUS, « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation » (2016) 32:2 CLSR 256 à la p 257.

[76] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 688.

[77] Dustin BERGER, « Balancing Consumer Privacy with Behavioral Targeting » (2010) 27:1 Santa Clara Computer & High Tech LJ 3 aux pp 9‑10.

[78] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 690.

[79] Mike SMITH, *Targeted: how technology is revolutionizing advertising and the way companies reach consumers*, New York, American Management Association, 2015 aux pp 60‑61.

E. Les courtiers de données

Les courtiers de données (de l'anglais « *data brokers* ») sont des entités définies par le FTC comme étant des compagnies qui :

> [collect] information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud[80].

Leur existence est généralement méconnue du public, ces derniers opérant dans l'ombre[81], à un point tel qu'il est difficile de déterminer le nombre d'agrégateurs qui procèdent à la traque, au partage et à la vente de données personnelles[82]. La force des courtiers — et c'est ce qui inquiète particulièrement — est leur capacité à acquérir des données tant dans le monde *réel* que le monde virtuel « *[these] private companies, called data brokers, buy and sell data about individuals obtained from myriad sources including government records, financial transactions/purchases, online activities, some medical records, phone records,*

---

[80] US Senate, Committee on Commerce, Science and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes.*, 2013 à la p 1, en ligne : <https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf> (consulté le 9 janvier 2017); Samuel GROGAN et Aleecia M MCDONALD, *Access Denied! Contrasting Data Access in the United States and Ireland*, Proceedings on Privacy Enhancing Technologies, 3, avril 2016, 191 à la p 192, en ligne : <http://www.degruyter.com/view/j/popets.2016.2016.issue-3/popets-2016-0023/popets-2016-0023.xml>.

[81] US Senate, Committee on Commerce, Science and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes.*, 2013 à la p 36, en ligne : <https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf> (consulté le 9 janvier 2017).

[82] Steve KROFT, « The Data Brokers: Selling your personal information » (9 mars 2014), en ligne : <http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/> (consulté le 10 avril 2017).

etc. »[83]. Certaines firmes de courtage de données en font d'ailleurs une spécialisation[84]. Plus inquiétante serait leur implication dans les sphères publiques.

> A request by Senator Edward Markey for more specifics on the brokers' clients was met with a general reply from Acxiom noting that though they would not divulge their clients' identities (valuing their privacy very highly) their clients include "47 Fortune 100 clients", "5 of the 13 largest U.S. federal government agencies" and "Both major national political parties"[85].

Ces courtiers n'évoluent pas nécessairement dans le milieu de la publicité, mais bien dans celui de la donnée. Leur principale préoccupation, voire leur unique préoccupation, est de posséder une vaste quantité de données et il arrive parfois que celles-ci proviennent des réseaux publicitaires mêmes[86].

Section 3 — Technologies du ciblage

Bien que l'aspect technique puisse à la fois ennuyer et effrayer le juriste, il semble important dans la compréhension des mécanismes d'acquérir une certaine base en la matière.

---

[83] Gregory MAUS, « How data brokers sell your life, and why it matters » (24 août 2015), en ligne : The Stack <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/> (consulté le 11 avril 2017).

[84] « Getting to know you » (13 septembre 2014), en ligne : The Economist <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party> (consulté le 18 avril 2016).

[85] Gregory MAUS, « How data brokers sell your life, and why it matters » (24 août 2015), en ligne : The Stack <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/> (consulté le 11 avril 2017).

[86] « Getting to know you » (13 septembre 2014), en ligne : The Economist <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party> (consulté le 18 avril 2016); Steve KROFT, « The Data Brokers: Selling your personal information » (9 mars 2014), en ligne : <http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/> (consulté le 10 avril 2017).

Comme le rappelle Massey, une compréhension des technologiques est absolument essentielle pour le juriste spécialisé en vie privée[87].

Cette section sera donc consacrée aux technicités nécessaires à la compréhension de la PCL, par l'analyse des mécanismes qui la sous-tendent. Nous sommes persuadés que la compréhension technique permet un meilleur dialogue entre les techniciens et les juristes, entraînant ainsi un meilleur encadrement de la PCL. Nous débuterons ainsi, par quelques informations techniques avant d'entrer dans le vif du sujet, celui des controversés *témoins*.

A. Réseaux, langages et protocoles

Distinguons l'Internet du World Wide Web (le web). Le premier réfère à une technologie englobant le second. Le web est essentiellement une partie d'Internet, un langage commun qui permet aux ordinateurs de communiquer entre eux sur Internet[88].

Le langage formant l'expression visuelle commune aux ordinateurs connectés sur le web est principalement le *Hypertext Markup Language* (« HTML »)[89] et le protocole permettant aux ordinateurs du réseau de communiquer entre eux est le *Hypertext Transfer Protocol* (« HTTP »)[90]. La force de l'*hypertexte* réside dans la création de liens (d'où le terme

---

[87] Aaron MASSEY, « Getting to October: Why Understanding Technology Is Essential for Privacy Law » (2014) 51 Idaho L Rev 695.

[88] Paul LAMBERT, *Gringras, the Laws of the Internet*, 4e éd, Haywards Heath, West Sussex, Bloomsbury Professional, 2015 à la p 9; Andrew MURRAY, *Information Technology Law: The Law and Society*, 2e éd, Oxford, United Kingdom, Oxford University Press, 2013 à la p 33.

[89] Paul LAMBERT, *Gringras, the Laws of the Internet*, 4e éd, Haywards Heath, West Sussex, Bloomsbury Professional, 2015 à la p 9; Andrew MURRAY, *Information Technology Law: The Law and Society*, 2e éd, Oxford, United Kingdom, Oxford University Press, 2013 à la p 33.

[90] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 à la p 152.

hyperliens) vers d'autres documents[91]. Les liens forment alors la troisième et dernière composante de l'architecture initiale (et la plus répandue) du web (HTTP, HTML et les URL)[92]. Le navigateur, pour sa part, est un logiciel installé sur l'ordinateur d'un utilisateur et sert d'interprète en affichant à l'utilisateur le contenu de la page.

> When a user clicks on a (hypertext) link in a Web browser, the browser (sometimes referred to as "client" or "user agent") typically connects to the Web server identified by the uniform resource locator (URL) embedded in the link and sends it a request message, to which the server sends a response message. Then, after receiving the response, the browser disconnects from the server. Because the client makes a new connection for each request, the server treats each request as though it were the first one it had received from that client. We therefore consider the request to be "stateless": each request is treated completely independently of any previous one[93].

Le procédé HTTP est synchrone, c'est-à-dire qu'il ne peut y avoir de réponse tant que la requête n'est pas parvenue au serveur. Son fonctionnement est donc aussi simple qu'une requête du navigateur au serveur et d'une réponse du serveur vers le navigateur[94]. On dit du web qu'il est « amnésique » en raison de son incapacité innée de retenir de l'information une fois le canal de communication refermé. C'est donc dans cet esprit que sont nés les *témoins*,

---

[91] Paul LAMBERT, *Gringras, the Laws of the Internet*, 4e éd, Haywards Heath, West Sussex, Bloomsbury Professional, 2015 à la p 10; Erik WILDE, *Wilde's WWW: technical foundations of the World Wide Web*, Berlin ; New York, Springer, 1999 à la p 53.

[92] Erik WILDE, *Wilde's WWW: technical foundations of the World Wide Web*, Berlin ; New York, Springer, 1999 à la p 54.

[93] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 à la p 152.

[94] Erik WILDE, *Wilde's WWW: technical foundations of the World Wide Web*, Berlin ; New York, Springer, 1999 à la p 61.

permettant alors de contourner cette limitation technique[95]. Si le HTTP agit comme fondement du web, les témoins se sont développés comme complément à celui-ci[96].

B. Témoins

Les *témoins* permettent la personnalisation, retenant les préférences des utilisateurs, comme la langue ou la localisation de l'utilisateur, afin de lui présenter, par exemple, des nouvelles locales ou la météo[97]. Du point de vue commercial, le développement de services de vente en ligne aurait été difficile sans les *témoins*, puisque ceux-ci facilitent le commerce, permettant d'ajouter des items dans un panier virtuel et d'y revenir plus tard en constatant que les items y sont toujours.

Les « *cookies* » ou témoins de connexion sont de petits fichiers texte contenant de l'information qui circule entre le serveur et le navigateur permettant d'identifier un internaute, afin de pallier à la nature amnésique du web[98]. Ils sont déposés par le serveur dans le

---

[95] « Basically, a cookie is a piece of information which is exchanged between a client and a server and is used to maintain the state information which is not part of HTTP » Erik WILDE, *Wilde's WWW: technical foundations of the World Wide Web*, Berlin ; New York, Springer, 1999 à la p 123; « The cookie mechanism allows a web server to store a small amount of data on the computers of visiting users, which is then sent back to the web server upon subsequent requests. Using this mechanism, a website can build and maintain state over the otherwise stateless HTTP protocol ». Nick NIKIFORAKIS et al, *Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting*, *Proceeding SP '13 Proceedings of the 2013 IEEE Symposium on Security and Privacy*, IEEE, 2013, 541 à la p 541.

[96] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 à la p 152.

[97] Steven C BENNETT, « Regulating Online Behavioral Advertising » (2010) 44 John Marshall L Rev 899 à la p 905.

[98] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 à la p 154.

navigateur d'un utilisateur et enregistrent de l'information qui pourra être accessible lorsque l'utilisateur retournera de nouveau sur le serveur activant alors le témoin[99].

Autrement dit, les *témoins* sont une pièce de technologie qui permet de suivre l'utilisateur et de dresser son portrait numérique, de déterminer le temps passé sur un site, s'il a cliqué sur une publicité, les recherches qu'il aura effectuées, son adresse IP et bien d'autres informations[100], mais surtout, il possède un identificateur unique[101]. Le témoin contient également d'autres informations techniques comme un nom, le domaine visé par le *témoin*, une date d'expiration et des indications concernant son mode de transmission (à savoir si elle doit être faite sur un canal sécurisé ou non)[102].

Il existe en outre plusieurs types de témoins de connexion. Ils peuvent être de sessions ou persistants. Les *témoins* de sessions ne posent généralement pas de problème en ce qu'ils

---

[99] Commissariat à la protection de la vie privée du Canada, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, 2011, en ligne : <https://www.priv.gc.ca/media/1964/report_201105_f.pdf> (consulté le 5 février 2017); Arnold ROOSENDAAL, *Facebook Tracks and Traces Everyone: Like This!*, coll Tilburg Law School Legal Studies Research Paper Series No 03/2011, 2010 à la p 4, en ligne : <https://papers.ssrn.com/abstract=1717563> (consulté le 29 novembre 2016); En outre, il fût démontré que certains services, dont Facebook, « suivent » les internautes, même lorsque ceux-ci ne sont pas membre du site social, « Facebook tracks users, even those who don't use it, says privacy report » (3 avril 2015), en ligne : HackRead <https://www.hackread.com/facebook-tracks-users-even-those-who-dont-use-it-report/> (consulté le 10 avril 2017); Author: Robert McMillan Robert McMillan BUSINESS, « Not on a Social Network? You've Still Got a Privacy Problem », en ligne : WIRED <https://www.wired.com/2014/10/privacy-friendster/> (consulté le 10 avril 2017).

[100] Commissariat à la protection de la vie privée du Canada, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, 2011 à la p 14, en ligne : <https://www.priv.gc.ca/media/1964/report_201105_f.pdf> (consulté le 5 février 2017).

[101] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 276. À titre d'exemple un utilisateur pourrait avoir l'identifiant suivant 26360352454e72bd||t=1490661908|et=730|cs=002213fd4830bf600d40732163 attribué par DoubleClick, service publicitaire propriété du réseau Google.

[102] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 aux pp 173‑174.

sont automatiquement supprimés lorsque la page est quittée[103]. Ceux-ci ne suivent donc l'utilisateur que lors de sa visite sur un site donné. Les témoins persistants ou témoins traceurs sont quant à eux présents dans le temps, au-delà de la simple navigation[104].

Outre les *témoins*, il existe également d'autres modes de traque en ligne que nous aborderons ultérieurement.

(i) Témoins primaires

Le premier type de témoin est celui des témoins primaires ou «*first-party cookie*»[105]. Celui-ci réfère à un témoin de connexion qui ne vise que la communication avec l'appareil utilisé par l'utilisateur et un site donné[106]. Il s'agit essentiellement d'un modèle de communication fermée où l'information ne circule qu'à l'intérieur du circuit, entre l'appareil et le site et vice-versa[107]. À cet égard, il ne pose généralement aucun problème et est perçu

---

[103] Frederik J Zuiderveen BORGESIUS, « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation » (2016) 32:2 CLSR 256 à la p 257; Adam LEGGE, « Online behavioural advertising: A comparative study of regulation between the EU and Hong Kong » (2015) 31:3 CLSR 422 à la p 423.

[104] Adam LEGGE, « Online behavioural advertising: A comparative study of regulation between the EU and Hong Kong » (2015) 31:3 CLSR 422 à la p 423.

[105] Sophie DESCHÊNES-HÉBERT, « La publicité comportementale en ligne, une nouvelle ère de la publicité : les internautes doivent-ils s'inquiéter de leur vie privée ? », en ligne : Legault Joly Thiffault <http://www.ljt.ca/fr/publications/publication_123.sn> (consulté le 3 avril 2016).

[106] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 688; Angelica NIZIO, « Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a Do Not Track Mechanism » (2014) 2014:1 U Ill JL Tech & Pol'y 283 à la p 286.

[107] Mike LESINSKI, « Understanding the Difference Between Third-Party and First-Party Data », en ligne : Allant <http://www.allantgroup.com/blog/understanding-the-difference-between-third-party-and-first-party-data> (consulté le 10 août 2016).

comme étant utile aux utilisateurs[108], puisque les informations qu'il communique concernent les préférences de navigation entre l'utilisateur et le site. Cette communication suppose une relation directe.

Bien que ces *témoins* soient généralement utilisés pour améliorer l'expérience utilisateur (en se rappelant de la langue de choix par exemple), ils peuvent également servir à générer des revenus publicitaires lorsqu'un annonceur fait directement affaire avec l'éditeur. Le profilage n'est donc pas l'apanage unique des témoins tiers traités ci-après[109].

Les témoins primaires, tout comme les autres types de témoins, sont enregistrés et liés au navigateur. Un utilisateur a toujours l'option de les supprimer, bien qu'ils puissent être difficiles à trouver pour l'utilisateur néophyte. Cette opération prend place à l'intérieur du navigateur. Comme les témoins sont liés au navigateur, un utilisateur averti pourrait choisir d'alterner entre différentes options afin d'éviter une traque.

(ii) Témoins tiers

Le second type de *témoin*, le *témoin* tiers ou « *third-party* »[110] est celui qui est utilisé dans le modèle de la publicité comportementale puisqu'il permet de « suivre » un utilisateur lors de ses visites sur différents sites[111]. Les témoins tiers sont presque toujours liés à la

---

[108] Sophie DESCHÊNES-HÉBERT, « La publicité comportementale en ligne, une nouvelle ère de la publicité : les internautes doivent-ils s'inquiéter de leur vie privée ? », en ligne : Legault Joly Thiffault <http://www.ljt.ca/fr/publications/publication_123.sn> (consulté le 3 avril 2016).

[109] David M KRISTOL, « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151 à la p 164.

[110] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 688.

[111] Steven C BENNETT, « Regulating Online Behavioral Advertising » (2010) 44 John Marshall L Rev 899 à la p 901.

recherche de profit[112]. Ce qui dérange particulièrement dans le *témoin* tiers est son côté invasif[113].

Le profilage est effectué par des compagnies qui n'ont pas nécessairement de lien avec l'utilisateur[114] et qui font partie d'un réseau publicitaire[115]. Ces témoins tiers sont ainsi déposés dans les appareils par des firmes spécialisées, qui collectent les renseignements et qui sont en mesure de procéder instantanément à l'analyse de ces données. Ainsi, aucune information n'est transmise au site sur lequel l'utilisateur se trouve, celui-ci n'agissant que comme un des nombreux intermédiaires sur lesquels s'affiche la publicité destinée à l'utilisateur. Dans cette perspective, le site ignore tout de l'utilisateur, jusqu'à ce que celui-ci lui livre délibérément ses informations, par exemple en s'enregistrant ou en effectuant une commande.

Pris individuellement, les renseignements fournis par les témoins de connexion peuvent sembler banals et tout à fait anonymes. Or, comme le souligne Hoofnagle[116], le problème avec le modèle des témoins tiers réside dans l'agrégation d'informations permettant l'identification de l'utilisateur hors-ligne. Warner et Sloan soutiennent à cet effet que :

---

[112] Adam LEGGE, « Online behavioural advertising: A comparative study of regulation between the EU and Hong Kong » (2015) 31:3 CLSR 422 à la p 423.

[113] Angelica NIZIO, « Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a Do Not Track Mechanism » (2014) 2014:1 U Ill JL Tech & Pol'y 283 aux pp 286‑287.

[114] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 276.

[115] Marvin AMMORI et Luke PELICAN, « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665 à la p 688.

[116] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 276.

> [It] merges our digital footprints into pictures of surprising intrusiveness and accuracy. Advertisers can determine where you work, how and with whom you spend your time, and "[w] ith 87% certainty … where you'll be next Thursday at 5:35 p.m.".[117]

Ainsi, une telle traque peut conduire assez aisément à l'identification des conditions médicales, opinions politiques ou préférences sexuelles d'un utilisateur[118].

(iii) Témoins Flash

Ce type de témoin (appelés formellement « *Local Shared Objects* »[119]) ne repose pas sur la technologie HTTP, mais plutôt sur le logiciel *Flash* d'*Adobe*[120], et se distingue du témoin traditionnel, car il est enregistré à même le disque dur de l'internaute. Ils peuvent contenir jusqu'à 100 kb d'information alors que les témoins HTTP ne peuvent en contenir que 4 kb. De plus, alors qu'un témoin standard expire par défaut à la fin d'une session, à moins d'avoir spécifié une date d'expiration, un *témoin Flash* ne possède pas d'expiration par défaut[121]. Cette technologie en fait donc un traceur beaucoup plus résilient, puisqu'il ne peut être supprimé en même temps que les témoins traditionnels, son emplacement dans l'ordinateur étant différent. Le *Commissariat à la vie privée du Canada* notait dans son rapport, en 2010, que le contrôle sur les témoins *Flash* était irréaliste, car les options le

---

[117] Richard WARNER et Robert H SLOAN, « Behavioral advertising: From one-sided chicken to informational norms » [2012] 15 Vand J Ent & Tech L 49 à la p 52.

[118] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 276.

[119] Mika D AYENSON et al, *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning*, SSRN, 2011 à la p 2, en ligne : <https://papers.ssrn.com/abstract=1898390> (consulté le 5 mars 2017).

[120] Ashkan SOLTANI et al, *Flash Cookies and Privacy*, SSRN, 2009 à la p 1, en ligne : <https://papers.ssrn.com/abstract=1446862> (consulté le 5 avril 2017).

[121] Ashkan SOLTANI et al, *Flash Cookies and Privacy*, SSRN, 2009 à la p 158, en ligne : <https://papers.ssrn.com/abstract=1446862> (consulté le 5 avril 2017).

concernant étaient difficiles d'accès, voire inexistantes[122], restreignant fortement l'autonomie de l'utilisateur.

En plus des difficultés inhérentes à la suppression des témoins *Flash*, ceux-ci sont souvent utilisés dans la résurrection (« *respawning* ») de témoins traditionnels[123].

> Using Flash cookie respawning, advertisers can continue to track individuals uniquely even if the user deliberately tries to avoid web tracking. Thus the new user 987,654,321 can be matched with the older user 123,456,789[124].

Finalement, cette résurrection de témoins est faite en l'absence de tout avis à l'attention de l'utilisateur qui aurait délibérément choisi de supprimer ses témoins[125].

C. Empreinte numérique

Les *témoins* laissent des miettes, des morceaux de code. On les supprime à l'occasion. Certains se réinstallent et d'autres disparaissent, mais ils sont accessibles, même lorsque cette opération paraît être difficile. Une chose est cependant (presque) toujours unique, il s'agit de l'empreinte *digitale* d'un ordinateur. Lorsque les chercheurs ont découvert qu'il était possible

---

[122] Commissariat à la protection de la vie privée du Canada, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, 2011 à la p 31, en ligne : <https://www.priv.gc.ca/media/1964/report_201105_f.pdf> (consulté le 5 février 2017).

[123] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 279; Commissariat à la protection de la vie privée du Canada, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, 2011 aux pp 13, 31, en ligne : <https://www.priv.gc.ca/media/1964/report_201105_f.pdf> (consulté le 5 février 2017).

[124] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 279.

[125] Sarah Cathryn BRANDON, « What's Mine is Yours: Targeting Privacy Issues and Determining the Best Solutions for Behavioral Advertising » (2011) 29 Marshall J Computer Info L 637 à la p 642.

d'identifier un ordinateur sans avoir recours aux témoins, une nouvelle porte s'est ouverte pour une traque discrète[126].

L'identification à partir de l'empreinte numérique d'un appareil (« *device fingerprinting* ») se fait à partir de données, notamment comme le système d'exploitation de l'utilisateur, le type de navigateur, la version de celui-ci, ses préférences, les polices d'écritures installées, la langue, le fuseau horaire et la taille de l'écran[127]. Comme il existe des millions de combinaisons possibles, celles-ci forment une image à peu près unique et se révèlent être un outil formidable pour la publicité comportementale, en plus d'être difficile à empêcher[128]. En effet, il n'existe pas de véritable méthode de retrait[129] et le tout se fait entièrement à l'insu de l'utilisateur[130].

---

[126] Adam TANNER, « The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next », *Forbes*, en ligne : Forbes <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/> (consulté le 10 avril 2017); Julia ANGWIN, « Meet the Online Tracking Device That is Virtually Impossible to Block » (21 juillet 2014), en ligne : ProPublica <http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block> (consulté le 10 avril 2017).

[127] Frederik J Zuiderveen BORGESIUS, « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation » (2016) 32:2 CLSR 256 aux pp 257‑258; Adam TANNER, « The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next », *Forbes*, en ligne : Forbes <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/> (consulté le 10 avril 2017).

[128] BORGESIUS, *supra* note 74 aux pp 257‑258.

[129] Nick NIKIFORAKIS et al, *Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting*, *Proceeding SP '13 Proceedings of the 2013 IEEE Symposium on Security and Privacy*, IEEE, 2013, 541.

[130] Omer TENE et Jules POLONETSKY, « To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising » (2012) 13:1 Minn J L Sci & Tech 281 à la p 295.

D. Inspection approfondie des paquets

L'inspection approfondie des paquets (« IAP ») ou « *Deep Packet Inspection* » (« DPI ») est définie par le CRTC comme étant une :

> [technologie] permettant aux fournisseurs de réseau d'examiner le contenu des paquets de données qui forment un message ou une transmission sur un réseau. L'IAP sert à préserver l'intégrité et la sécurité des réseaux. Cette technologie permet aux fournisseurs de services Internet et à d'autres organisations l'accès généralisé aux renseignements expédiés par Internet[131].

Cette technologie fut initialement développée dans une optique de sécurité, permettant l'interception et l'analyse de *paquets* sur Internet[132]. Les fournisseurs d'accès à Internet (« FAI ») avaient donc accès à un outil qui théoriquement pouvait permettre de contrer les virus et infractions au droit d'auteur[133]. Or, depuis, les FAI et leurs partenaires utilisent cette technologie dans une perspective de surveillance gouvernementale et à des fins de publicité

---

[131] Gouvernement du Canada, Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), *Glossaire concernant la télécommunication*, 2009, *sub verbo* « Inspection approfondie des paquets », en ligne : Glossaire concernant la télécommunication <http://www.crtc.gc.ca/multites/mtwdk.exe?k=glossaire-glossary&l=60&w=262&n=1&s=5&t=2> (consulté le 21 février 2017).

[132] Milton L MUELLER et Hadi ASGHARI, « Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States » (2012) 36:6 Telecomm Pol'y 462 à la p 462.

[133] Milton L MUELLER et Hadi ASGHARI, « Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States » (2012) 36:6 Telecomm Pol'y 462 à la p 462; Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 3, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).

ciblée[134]. Cette méthode de surveillance ne requiert aucun logiciel et il s'avère impossible de détecter une telle activité[135].

L'inspection approfondie des paquets génère des informations extrêmement détaillées sur l'ensemble des habitudes des internautes. En outre, l'information peut aller du simple historique de navigation jusqu'au détail de contenu courriel, conversations vocales, transfert de fichiers de type « *peer-to-peer* » ou de jeu en ligne[136]. Là où d'autres moyens de traque ont rencontré des réponses techniques complexes, la DPI permet une surveillance complète et totale des habitudes (et même plus) d'utilisation des internautes[137]. Ainsi, les FAI ont accès à l'intégralité des actions posées sur le web par leurs utilisateurs[138]. Dès lors, ils peuvent contribuer à la PCL en créant des banques de données des profils utilisateurs qui pourront être accessibles aux compagnies publicitaires[139].

---

[134] Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 4, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).

[135] Dustin BERGER, « Balancing Consumer Privacy with Behavioral Targeting » (2010) 27:1 Santa Clara Computer & High Tech LJ 3 aux pp 12‑13.

[136] Andrea PERSON, « Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience » (2010) 62:2 Fed Comm LJ 435 à la p 438.

[137] Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 6, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).

[138] Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 6, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017); Andrea PERSON, « Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience » (2010) 62:2 Fed Comm LJ 435 à la p 442.

[139] Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 6, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).

> [An] ISP has access to all of a consumer's Web activity and, because of this, has the ability to gather a more complete picture of the consumer's preferences. Accordingly, the advertisements that an ISP has the ability to create are more exceptionally relevant—"[a] nd the more relevant the ad, the higher the price a provider can charge an advertiser." While the information on exactly which ISPs are using the technology is unclear, marketing information available on a number of DPI Web sites has indicated that the technology is being used by ISPs[140].

En outre, en raison de la consolidation des entreprises de publicité sur Internet, les annonceurs peuvent avoir accès à la publicité sur des centaines de sites et ainsi être en mesure de « suivre les gens à travers ces domaines » sans qu'aucune divulgation ne soit faite[141].

---

[140] Andrea PERSON, « Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience » (2010) 62:2 Fed Comm LJ 435 à la p 442.

[141] Monroe Edwin PRICE, Stefaan VERHULST et Libby MORGAN, *Routledge Handbook of Media Law*, Abingdon, Oxon ; New York, Routledge, 2013.

Partie 1 — Cadre juridique en matière de publicité comportementale

« If you're not paying for it, you're not the customer; you're the product »[142].

L'industrie entourant la publicité comportementale en ligne est loin d'être transparente. Il est difficile de percer cette industrie et les technologies qui se développent pour la nourrir le font à un rythme incroyable. Plusieurs initiatives[143] ont été mises sur pied pour éduquer la population sur les risques de la publicité comportementale et surtout de la traque massive qui la soutient. En matière d'encadrement, de telles initiatives permettraient idéalement aux décideurs publics de mieux comprendre les préoccupations des utilisateurs.

La panoplie d'outils déployés par l'industrie pour procéder aux suivis des préférences et habitudes des utilisateurs contribue ainsi à déterminer ce que le consommateur veut, et du même coup, à une offre publicitaire adaptée. Plusieurs soutiennent que tous y sont gagnants, tant les annonceurs et les éditeurs, que les consommateurs. D'une part, les annonceurs

---

[142] Omer TENE et Jules POLONETSKY, « Big Data for All: Privacy and User Control in the Age of Analytics » (2013) 11:5 NW J Tech & IP 239 à la p 255 citant : ; Jonathan ZITTRAIN, « Meme patrol: "When something online is free, you're not the customer, you're the product." » (21 mars 2012), en ligne : Future of the Internet - And how to stop it. <http://blogs.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/> (consulté le 28 mars 2017).

[143] Brett GAYLOR, « Do Not Track Documentary », en ligne : Do Not Track <https://donottrack-doc.com/> (consulté le 23 février 2017); Future of Privacy Forum, « All About DNT », en ligne : All About DNT <https://allaboutdnt.com/> (consulté le 23 février 2017); Electronic Frontier Foundation, « Do Not Track », en ligne : <https://www.eff.org/issues/do-not-track> (consulté le 13 janvier 2017); « Do Not Track - Universal Web Tracking Opt Out », en ligne : <http://donottrack.us/> (consulté le 28 février 2017).

parviennent à rejoindre plus aisément et à moindre coût les utilisateurs. Selon différentes études, ils obtiennent aussi le meilleur retour sur investissement que tout autre type de publicité en ligne[144]. D'autre part, les éditeurs de contenu bénéficient largement de cette industrie puisqu'ils sont les vitrines dans lesquelles sont exposées les publicités, formant alors leur principal, voire unique, revenu. Finalement, si les consommateurs bénéficient de publicités moins envahissantes, car plus pertinents, ils tirent principalement avantage d'un contenu — généralement gratuit — de la part des éditeurs, car financés à même la publicité. Malgré tout, les consommateurs ne sont pas convaincus des bienfaits de la publicité comportementale et surtout, ils la craignent.

Il nous apparaît à présent nécessaire de présenter un état du droit, puis de déterminer dans quelle mesure la PCL nuit à l'autonomie des consommateurs et à quel degré elle peut constituer une pratique commerciale trompeuse justifiant une réforme juridique. Bien qu'il y ait des preuves indiquant que la capacité des consommateurs à prendre des décisions indépendantes soit menacée par l'extraction de données de plus en plus sophistiquées grâce à la PCL, il est nécessaire de prendre en considération les lois existantes avant de proposer une réforme permettant de remédier à cette situation.

En outre, nous reconnaissons qu'il existe une solide base d'intérêts commerciaux au cœur de la publicité sur Internet en général et spécifiquement lorsqu'il est question de PCL, ce qui peut empêcher toute réforme significative. La diffusion sur Internet est née d'un désir de rendre l'information libre et accessible, un axiome qui a longtemps dominé les esprits des internautes. Ces utilisateurs ont depuis longtemps refusé de payer directement pour le contenu

---

[144] Tel que discuté au chapitre préliminaire. Voir à ce sujet : Business News Daily, « Has Online Targeted Advertising Gone Too Far? » (7 avril 2011), en ligne : <http://www.businessnewsdaily.com/841-online-targeted-advertising.html> (consulté le 11 avril 2017); Charles CURRAN, « Study finds behaviorally targeted ads more than twice as valuable and effective as non-targeted online ads » (24 mars 2010), en ligne : NAI : Network Advertising Initiative <https://www.networkadvertising.org/blog/study-finds-behaviorally-targeted-ads-more-twice-valuable-and-effective-non-targeted-online-ads> (consulté le 11 avril 2017); Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 165.

qui était jadis acheté, comme les journaux, les magazines et la musique pour n'en nommer que quelques-uns. En conséquence, ces services sont « achetés » sous la forme de droits publicitaires, les tarifs applicables à cette publicité étant fonction de la capacité des fournisseurs de contenu à rassembler des informations sur les préférences de leurs utilisateurs. Alors que le système actuellement utilisé a évolué de manière itérative, ceci ne constitue pas une excuse pour que les techniques publicitaires menacent l'autonomie des consommateurs. Cependant, la base actuelle d'une réforme possible reste entre les mains des éditeurs de contenu (à qui les utilisateurs fournissent consciemment ou non, des informations comportementales) et des annonceurs (qui sont à la recherche de telles informations).

Nous allons donc à présent tenter de définir le cadre juridique applicable en matière de PCL tant au Québec qu'au Canada. Nous procéderons tout d'abord (chapitre 1) par une analyse des lois applicables à la publicité en ligne, puis (chapitre 2) nous aborderons les questions spécifiques de protection du consommateur.

Chapitre 1 — Définir le cadre juridique en matière de publicité

Même si on la retrouve sur Internet, la cyberpublicité ou publicité en ligne est régie par les mêmes règles que les autres modes de transmission classiques de messages publicitaires que sont notamment la radio et la télévision. Afin d'approfondir notre compréhension, nous devons donc effectuer un survol de la législation applicable en matière de publicité au Québec et au Canada.

Au Canada, la publicité est d'une part régie par la *Loi sur la concurrence*[145] (ci-après « LC ») au niveau fédéral, puis d'autre part, où elles ont été promulguées, par des législations

[145] *Loi sur la concurrence*, LRC 1985, c C-34 [LC].

provinciales. Au Québec, la publicité est donc régie à la fois par la LC et par la *Loi sur la protection du consommateur*[146] (ci-après « LPC »). Dans les deux cas, en matière de publicité, l'objectif principal vise à protéger les consommateurs contre les publicités fausses ou trompeuses[147].

Section 1 — Publicité comportement et Loi sur la concurrence

La *Loi sur la concurrence* est une loi fédérale dans laquelle se trouvent des dispositions civiles et criminelles. Son but général est de

> [préserver] et de favoriser la concurrence au Canada dans le but de stimuler l'adaptabilité et l'efficience de l'économie canadienne, d'améliorer les chances de participation canadienne aux marchés mondiaux tout en tenant simultanément compte du rôle de la concurrence étrangère au Canada, d'assurer à la petite et à la moyenne entreprise une chance honnête de participer à l'économie canadienne, de même que dans le but d'assurer aux consommateurs des prix compétitifs et un choix dans les produits[148].

La LC est sous la responsabilité d'*Innovation, Sciences et Développement économique Canada*[149], ministère du Gouvernement du Canada, anciennement appelé *Industrie Canada*, responsable de la politique économique. Le *Bureau de la concurrence* est responsable de son

---

[146] *Loi sur la protection du consommateur*, RLRQ c P-401 [LPC].

[147] Sur ce point : « Nul 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 ». *Loi sur la concurrence*, LRC 1985, c C-34, art 52(1) [LC]; « Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur » *Loi sur la protection du consommateur*, RLRQ c P-401, art 219 [LPC].

[148] *Loi sur la concurrence*, LRC 1985, c C-34, art 1.1 [LC].

[149] Bureau de la concurrence, « Bureau de la concurrence » (24 mai 2017), en ligne : Gouvernement du Canada <https://www.canada.ca/fr/bureau-concurrence.html> (consulté le 29 mai 2017).

administration et de son application[150] sous la gouverne du *Commissaire de la concurrence*[151]. Le principal mandat du Bureau est de faire « la promotion de l'éthique publicitaire dans les marchés en décourageant les pratiques commerciales trompeuses et en encourageant l'offre d'une information valable, afin de permettre aux consommateurs de faire des choix éclairés »[152].

A. Publicité fausse et trompeuse

Le *Commissaire de la concurrence* dispose d'importants pouvoirs d'enquête[153] lui permettant de déceler les cas d'infraction potentiels, tant en matière civile que criminelle. Les deux régimes sont prévus par la LC et laissés au choix du demandeur[154]. Ainsi, la disposition législative criminelle se trouve en l'article 52 (1) qui criminalise les indications fausses et trompeuses en matière de publicité :

> Nul 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**.

---

[150] Bureau de la concurrence, « Notre organisme » (31 mars 2005), en ligne : Gouvernement du Canada <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/h_00125.html> (consulté le 29 mai 2017).

[151] *Loi sur la concurrence*, LRC 1985, c C-34, art 7(1)(a) [LC].

[152] Bureau de la concurrence, « Promotion de l'éthique publicitaire » (20 avril 2005), en ligne : Gouvernement du Canada <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/h_00529.html> (consulté le 29 mai 2017).

[153] *Loi sur la concurrence*, LRC 1985, c C-34, art 10(1) [LC].

[154] *Loi sur la concurrence*, LRC 1985, c C-34, art 9 [LC].

Le législateur fédéral a ainsi voulu s'attaquer au problème de la fausse représentation, la rendant passible d'une poursuite au criminel. En conséquence, en matière de publicité, les « *indications* [qui sont] *fausses ou trompeuses sur un point important* », c'est-à-dire celles qui, de par les pratiques délibérées et/ou insouciantes de l'annonceur, risquent de porter atteinte à l'intérêt public peuvent exposer le responsable à des poursuites criminelles[155].

En matière civile, l'article 74.01 de la LC prévoit une procédure civile d'examen à laquelle la loi réfère comme étant le « comportement susceptible d'examen » :

> Est susceptible d'examen le comportement de quiconque donne au public, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques :
>
> **a)** ou bien des indications fausses ou trompeuses sur un point important[156].

Notons immédiatement que bien qu'il existe deux régimes (criminel et civil), en vertu de l'article 74.16 LC, ceux-ci sont mutuellement exclusifs, les mêmes actes ne pouvant à la fois faire l'objet d'une poursuite au criminel et de la procédure civile :

> Aucune demande ne peut être présentée à l'endroit d'une personne au titre de la présente partie si les faits au soutien de la demande sont les mêmes ou essentiellement les mêmes que ceux allégués au soutien d'une procédure engagée à l'endroit de cette personne en vertu des articles 52 ou 52.01[157].

Sur la définition à accorder à « fausses ou trompeuses » la Cour supérieure de l'Ontario s'est à cet effet prononcée, statuant que :

> A representation is "misleading in a material respect" where an "ordinary citizen would likely be influenced by that impression in deciding whether or not he would purchase the product being offered." A misleading representation is material where it

---

[155] Henry LUE et Sangeetha PUNNIYAMOORTHY, *Canadian marketing law handbook*, 2e éd, Toronto, Carswell, 2012 à la p 101.

[156] *Loi sur la concurrence*, LRC 1985, c C-34, art 74.01(1) [LC].

[157] *Loi sur la concurrence*, LRC 1985, c C-34, art 74.16 [LC].

is of "much consequence or [is] important or pertinent or germane or essential to the matter."[158]

De plus, soulignons que la notion de *point important* est rattachée « à l'importance que l'acheteur peut accorder à l'indication pour prendre la décision d'acheter ou non le produit »[159]. En d'autres mots « est fausse ou trompeuse sur un point important toute indication qui incite une personne à adopter une conduite qui, sur la foi de cette indication, lui semble avantageuse »[160]. Est-ce qu'en d'autres circonstances, le consommateur aurait été tenté d'acheter le produit, n'eût été de cette déclaration ?

En termes de procédure, le Bureau mène d'abord son enquête et renvoie ensuite le dossier au procureur général en vue d'une poursuite suivant l'article 23 de la LC. Sur déclaration de culpabilité, le coupable est passible d'une amende et/ou d'un séjour en prison qui peut aller jusqu'à quatorze ans.

Malgré le caractère civil et non criminel de cette procédure d'examen, les conséquences peuvent tout de même s'avérer très graves pour le contrevenant, à qui il peut être ordonné de modifier ses pratiques ou de payer une amende[161]. Il est important de mentionner que tant l'article 52 (1) que 74.01 LC visent à la fois des personnes physiques et morales, du moment où elles tentent de « promouvoir directement ou indirectement soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques »[162]. Dans les

---

[158] *Commissioner of Competition v Yellow Page Marketing*, 2012 ONSC 927 au para 34.

[159] BLG, *Cibler le consommateur Canadien — Un important exposé sur le droit de la publicité et du marketing au Canada*, 2014 à la p 6, en ligne : <http://blg.com/fr/Nouvelles-Et-Publications/Documents/Cibler_le_consommateur_Canadien_-_SEP2016.pdf> (consulté le 29 mars 2017).

[160] Bureau de la concurrence, *Lignes directrices. Application de la Loi sur la concurrence aux indications dans Internet*, Gatineau, 2009 à la p 3, en ligne : <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet-2009-10-16-f.pdf/$FILE/RepresentationsInternet-2009-10-16-f.pdf> (consulté le 28 mai 2017).

[161] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 392.

[162] *Loi sur la concurrence*, LRC 1985, c C-34, art 52(1), 74.01(1) [LC].

deux cas, pour déterminer respectivement « si les indications sont fausses ou trompeuses sur un point important » (art. 52 (4) LC) ou « si le comportement est susceptible d'examen » (art.74.011 (4) LC), le critère dont il faut tenir compte est celui de l'impression générale[163].

Dans un jugement rendu en 2012, la Cour suprême du Canada a évalué le caractère faux et trompeur en vertu de la LPC en établissant un test en deux étapes dans son analyse. Bien que le jugement repose principalement sur la LPC et particulièrement sur l'analyse de son article 218, disposant que « [pour] déterminer si une représentation constitue une pratique interdite, il faut tenir compte de l'impression générale qu'elle donne et, s'il y a lieu, du sens littéral des termes qui y sont employés », la Cour suprême a exprimé que :

> Nous sommes d'avis que la notion du consommateur crédule et inexpérimenté, comme l'a employée la jurisprudence prédominante au Québec avant le jugement dont appel, respecte mieux les objectifs de protection contre la publicité fausse ou trompeuse […] les tribunaux appelés à évaluer la véracité d'une représentation commerciale devraient procéder, selon l'art. 218 L.p.c., à une analyse en deux étapes, en tenant compte, si la nature de la représentation se prête à une telle analyse, du sens littéral des mots employés par le commerçant : (1) décrire d'abord l'impression générale que la représentation est susceptible de donner chez le consommateur crédule et inexpérimenté ; (2) déterminer ensuite si cette impression générale est conforme à la réalité. Dans la mesure où la réponse à cette dernière question est négative, le commerçant aura commis une pratique interdite[164].

Ainsi, en matière de publicité, la LC interdit les *indications fausses* ou *trompeuses* sur un point important. Nous devons donc nous demander ce qui pourrait constituer des *indications fausses* ou *trompeuses.* Toutefois, la LC ne fournit aucune définition relativement à celles-ci. Selon Pritchard et Vogt, l'information véhiculée par la publicité devrait être

---

[163] Pour les deux articles la rédaction est identique : « dans toute poursuite intentée en vertu du présent article, pour déterminer si les indications sont fausses ou trompeuses sur un point important il faut tenir compte de l'impression générale qu'elles donnent ainsi que de leur sens littéral. » *Loi sur la concurrence*, LRC 1985, c C-34, art 52(4), 74.011(4) [LC].

[164] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 78.

« *accurate and complete* »[165] afin d'éviter notamment que la confiance du public n'en souffre ou que les compétiteurs ne se nuisent les uns les autres en se dépréciant mutuellement. Ainsi, il ne s'agit pas d'empêcher l'exubérance dans la mise en valeur du produit, mais bien la fausse représentation[166]. D'après le critère établi de l'impression générale, on sait d'ores et déjà que les indications susceptibles d'être considérées comme fausses ou trompeuses doivent être interprétées eu égard à l'impression générale qu'elles suscitent[167]. À cet égard, Goldman et Bodrug[168] avancent que le « *context in which the words are used may affect the impression they convey* »[169].

Le jugement *R c Impérial Tobacco Products Ltd*[170] rendu par la Cour d'appel de l'Alberta peut aussi être éclairant. Citant respectivement les jugements américains *Aronberg et al v. FTC*[171] et *FTC v. Sterling Drug Inc,*[172]*,* le juge Clement indiqua que :

> The law is not made for experts but to protect the public—that vast multitude which includes the ignorant, the unthinking and the credulous, who, in making purchases, do not stop to analyze but too often are governed by appearances and general impressions. Advertisements must be considered in their entirety and as they would be read by those to whom they appeal.
>
> […]
>
> It is necessary in these cases to consider the advertisement in its entirety and not to engage in disputatious dissection. The entire mosaic should be viewed rather than each tile separately. "The buying public does not ordinarily carefully study or weigh each

---

[165] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 45.

[166] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 45.

[167] Voir *Loi sur la concurrence*, LRC 1985, c C-34, art 54(4), 74.011(4) [LC].

[168] Calvin S GOLDMAN et J D BODRUG, *Competition Law of Canada*, Juris Publishing, Inc, 2013.

[169] Calvin S GOLDMAN et J D BODRUG, *Competition Law of Canada*, Juris Publishing, Inc, 2013.

[170] *R v Imperial Tobacco Products Limited*, 1971 1971 ALTASCAD 44 (CanLII), [1971] 5 WWR 409.

[171] *Aronberg v Federal Trade Commission*, 132 F.2d 165 (7th Cir. 1942).

[172] *FTC v Sterling Drug, inc*, 215 F.Supp. 327 (1963).

word in an advertisement. The ultimate impression upon the mind of the reader arises from the sum total not only of what is said but also of all that is reasonably implied"[173].

L'appréciation se fait donc eu égard au contexte en vertu d'un test, du consommateur moyen soit donc capable de faire la part des choses entre la réalité et la fiction[174]. En outre, en matière de publicité comportementale, le critère à retenir est le même, à savoir la publicité ne doit pas être fausse, ni trompeuse et l'ont doit s'appuyer sur l'impression générale qu'elle renvoie pour en déterminer le caractère.

B. Communication au public

Par ailleurs, l'application de la LC suppose que les indications fausses ou trompeuses sur un point important aient été faites *au public* aux fins de promouvoir, directement ou indirectement, soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques[175]. D'après Young et Fraser, ce type de communication « *would include representations made to the community at large, even only directed at a particular section of that community* »[176]. Il en ressort que ce concept doit être interprété dans un sens assez libéral. Toutefois, nous ne pouvons nous empêcher de nous demander si la publicité comportementale, sous sa forme extrême, c'est-à-dire personnalisée au niveau individuel, pourrait être considérée comme étant adressée « au public ». Selon le dictionnaire de droit québécois et

---

[173] *R v Imperial Tobacco Products Limited*, 1971 1971 ALTASCAD 44 (CanLII), [1971] 5 WWR 409 au para 53.

[174] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 45.

[175] *Loi sur la concurrence*, LRC 1985, c C-34, art 52(1) et 74.01(1) [LC].

[176] David M W YOUNG et Brian R FRASER, *Canadian advertising & marketing law*, Toronto, Carswell, 1990 à la p 21 cité par ; Véronique ABAD, « L'effectivité des recours en matière de publicité sur Internet » (2005) 10:2 Lex Electronica à la p 20, en ligne : Lex Electronica <http://www.lex-electronica.org/articles/vol10/num2/leffectivite-des-recours-en-matiere-de-publicite-sur-internet/> (consulté le 29 juillet 2017).

canadien[177], le terme « public » est entendu au sens de « ensemble des personnes qui forment une collectivité »[178]. Reprenant alors les propos de Young et Fraser, une représentation faite à une partie d'une collectivité serait une représentation faite au public. En matière de publicité comportementale, nous soutenons que, même si la publicité ne parvient qu'à un seul individu, celle-ci pourrait et devrait être considérée comme étant effectuée au public, puisque les fondements de la PCL reposent sur la création de profils d'individus. Ainsi, bien qu'un seul individu pourrait se trouver ciblé par une combinaison de facteurs, il faudrait supposé qu'elle entendait joindre un certain nombre de consommateurs visés. Refuser de considérer une telle représentation comme ayant été faite au public nous semble particulièrement problématique, car il signifierait que la loi deviendrait inapplicable à ce type de promotion. Les annonceurs pourraient alors ajouter certains éléments automatiquement à une publicité, la rendant dès lors absolument unique et s'excluant alors du spectre de la loi.

Ayant fait le tour des dispositions pertinentes relativement à la législation fédérale, nous nous attarderons maintenant à la législation provinciale.

Section 2 — Loi sur la protection du consommateur

Définir le cadre juridique de la publicité est une tâche d'ampleur, selon les auteures Pritchard et Vogt, parce que les problématiques qu'il cherche à encadrer sont nombreuses[179]. Les auteures soulignent à cet effet que cette complexité est d'autant plus apparente au Québec,

---

[177] CAIJ, *JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien*, 2016, en ligne : JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien <https://dictionnairereid.caij.qc.ca/> (consulté le 4 août 2017).

[178] CAIJ, *JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien*, 2016, *sub verbo* « Public », en ligne : JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien <https://dictionnairereid.caij.qc.ca/recherche#q=public%20&t=edictionnaire&sort=relevancy&m=search> (consulté le 4 août 2017).

[179] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 459.

obligeant les publicitaires à maîtriser différentes lois reflétant les particularités culturelles de la société québécoise[180]. La loi provinciale la plus importante applicable à la publicité est sans aucun doute la *Loi sur la protection du consommateur*.

Avant sa création, c'était le Code civil du Québec qui s'appliquait pour encadrer les relations entre commerçants et consommateurs. Toutefois, il semblerait que cet encadrement favorisait systématiquement les commerçants au détriment des consommateurs, qui n'étaient pas suffisamment informés quant aux produits et services qui leur étaient proposés et ne pouvaient donc pas faire d'achats éclairés[181]. Après l'adoption d'une première loi visant à accroitre la protection des consommateurs québécois en 1971, la *Loi sur la protection du consommateur* fut finalement adoptée en 1978[182]. Bien qu'elle fut modifiée à quelques reprises, la LPC n'a que peu changé depuis son adoption en 1978 et reste indépendante du Code civil du Québec. En outre, elle cherche à protéger le consommateur contre « des formes d'abus liés à la qualité et à la sécurité des biens, au secteur des services professionnels, à la publicité trompeuse, etc. »[183].

Le principal objectif de la loi est « *[to] address the need for increased consumer protection, and represented an attempt to equalize the power between merchants, advertisers and the average consumer* »[184]. Ainsi, la LPC « est née de la volonté sociale d'établir des

---

[180] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 459.

[181] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 aux pp 459‑460.

[182] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 460.

[183] Myriam JÉZÉQUEL, « Historique de la Loi sur la protection du consommateur » (2003) 35:21 Journal du Barreau, en ligne : Journal du Barreau <http://www.barreau.qc.ca/pdf/journal/vol35/no21/historique.html> (consulté le 24 août 2017).

[184] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 459.

règles pour protéger les intérêts du consommateur »[185]. Compte tenu des dispositions qu'elle renferme, la Loi est généralement perçue comme étant plus contraignante que la Loi sur la concurrence ou que les autres lois provinciales[186]. En outre, on y trouve notamment une interdiction de la publicité ciblant les enfants de moins de treize ans[187], unique disposition du genre au pays, voire dans le monde.

Nous analyserons à présent dans quelle mesure la Loi sur la protection du consommateur s'applique en matière de publicité comportementale.

A. Similarités avec la Loi sur la concurrence

À l'instar de la *Loi sur la concurrence*, la LPC s'applique en matière de publicité. Elle interdit aussi certaines pratiques commerciales, qu'on retrouve au titre II. Ainsi, à l'instar des articles 52 (1) et 74.01 (1) a) de Loi (canadienne) *sur la concurrence* elle prévoit, en son article 219, qu'« [aucun] commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur »[188].

À cet égard, l'article 218 nous indique que l'appréciation doit se faire tenant compte du critère de l'impression générale : « pour déterminer si une représentation constitue une pratique interdite, il faut tenir compte de l'impression générale qu'elle donne et, s'il y a lieu, du sens littéral des termes qui y sont employés ». À cet égard, l'arrêt *Richard c. Time* indique que :

---

[185] Myriam JÉZÉQUEL, « Historique de la Loi sur la protection du consommateur » (2003) 35:21 Journal du Barreau, en ligne : Journal du Barreau <http://www.barreau.qc.ca/pdf/journal/vol35/no21/historique.html> (consulté le 24 août 2017).

[186] Brenda L PRITCHARD, Susan VOGT et Association of Canadian Advertisers, *Advertising and Marketing Law in Canada*, 5e éd, Markham, Ontario, LexisNexis, 2015 à la p 461.

[187] *Loi sur la protection du consommateur*, RLRQ c P-401, art 248 [LPC].

[188] *Loi sur la protection du consommateur*, RLRQ c P-401, art 219 [LPC].

> [47] L'expression « sens littéral des termes qui y sont employés » ne pose pas de problème d'interprétation. Elle reconnaît simplement que chaque mot contenu dans une représentation doit être interprété selon son sens ordinaire. Cette partie du texte de l'art. 218 L.p.c. vise à interdire aux commerçants de soulever une défense basée sur une signification subtile, technique ou alambiquée d'un mot utilisé dans une représentation. Le législateur a ainsi souhaité que l'on donne aux mots utilisés dans les représentations un sens conforme à celui qu'ils possèdent dans la vie quotidienne[189].

En l'espèce, la Cour suprême traite du caractère objectif de la détermination d'une pratique interdite. Elle souligne qu'il n'est pas nécessaire qu'un préjudice résulte de l'acte interdit. :

> [50] Cette approche respecte l'esprit de la L.p.c., dont l'objectif principal demeure la protection du consommateur. Les tribunaux doivent alors être en mesure de sanctionner toute représentation qui, objectivement, constitue une pratique interdite. **Le fait qu'une représentation commerciale ait causé ou non un préjudice à un ou plusieurs consommateurs n'est pas pertinent pour décider si un commerçant a commis une pratique interdite au sens du titre II** de la L.p.c.[190] (Nos soulignements).

En outre, la Cour reconnaît que le consommateur doit être perçu comme étant *crédule et inexpérimenté* et prévoit un *test* en deux étapes dans la détermination :

> [78] Nous sommes d'avis que la notion du consommateur crédule et inexpérimenté, comme l'a employée la jurisprudence prédominante au Québec avant le jugement dont appel, respecte mieux les objectifs de protection contre la publicité fausse ou trompeuse […] les tribunaux appelés à évaluer la véracité d'une représentation commerciale devraient procéder, selon l'art. 218 L.p.c., à une analyse en deux étapes, en tenant compte, si la nature de la représentation se prête à une telle analyse, du sens littéral des mots employés par le commerçant : (1) décrire d'abord l'impression générale que la représentation est susceptible de donner chez le consommateur crédule et inexpérimenté ; (2) déterminer ensuite si cette impression générale est conforme à la réalité. Dans la mesure où la réponse à cette dernière question est négative, le commerçant aura commis une pratique interdite[191].

---

[189] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 47.

[190] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 50.

[191] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 78.

Par ailleurs, l'article 217 LPC prévoit que « [la] commission d'une pratique interdite n'est pas subordonnée à la conclusion d'un contrat ». Or, si l'article 2 indique que la LPC « s'applique à tout contrat conclu entre un consommateur et un commerçant »[192], l'affaire Richard c Time a confirmé qu'elle s'applique aussi en matière de publicité, et ce malgré l'absence d'un contrat[193]. De plus, il est possible pour un consommateur d'avoir accès à un recours en dommages-intérêts en vertu de l'article 272 LPC, même en l'absence d'un contrat[194]. Ainsi, l'absence de relation contractuelle entre l'internaute et un annonceur permet d'ouvrir un recours lorsqu'il y a un manquement à une obligation de la LPC.

Il faut se référer à l'article 1 (h), pour savoir comment la LPC définit un *message publicitaire :* « un message destiné à promouvoir un bien, un service ou un organisme au Québec »[195]. Mais à qui la LPC s'applique-t-elle ? Comme elle protège le consommateur, il semble fondamental de s'interroger sur celui-ci. La loi le définit, en son article 1(e), comme étant « une personne physique, sauf un commerçant qui se procure un bien ou un service pour les fins de son commerce »[196]. Le protégeant notamment, en matière de publicité, contre le *publicitaire* faisant œuvre de fausse représentation, la loi s'applique donc aussi à ce deuxième acteur, qu'elle définit comme étant « une personne qui fait ou fait faire la préparation, la publication ou la diffusion d'un message publicitaire »[197].

Si une certaine jurisprudence prévoit qu'il est nécessaire de prouver l'intention de tromper[198], il doit être mentionné que l'affaire Richard c Time a établi qu'il n'était pas nécessaire de démontrer l'intention de tromper de l'annonceur pour que ce dernier soit

---

[192] *Loi sur la protection du consommateur*, RLRQ c P-401, art 2 [LPC].

[193] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 25.

[194] *Faucher c Costco Wholesale Canada Ltd*, 2015 QCCQ 3366 au para 36.

[195] *Loi sur la protection du consommateur*, RLRQ c P-401, art 1(h) [LPC].

[196] *Loi sur la protection du consommateur*, RLRQ c P-401, art 1(e) [LPC].

[197] *Loi sur la protection du consommateur*, RLRQ c P-401, art 1(m) [LPC].

[198] *Dumont c Sears Canada inc*, 2015 QCCQ 13883 au para 31; *Lelièvre c Magasin La clé de sol inc*, 2011 QCCQ 5774 au para 17; *Faucher c Costco Wholesale Canada Ltd*, 2015 QCCQ 3366 au para 39.

reconnu coupable de représentation fausse ou trompeuse[199]. Les juges LeBel et Cromwel s'exprimèrent ainsi :

> le recours prévu à l'art. 272 L.p.c. allège son fardeau de preuve au moyen d'une présomption absolue de préjudice découlant de toute illégalité commise par le commerçant ou le fabricant. **Cette présomption dispense le consommateur de la nécessité de prouver l'intention de tromper du commerçant**, comme l'exigerait le droit civil en matière de dol[200].

Contrairement à la Loi sur la concurrence qui établissait que la représentation devait être faite « au public », la LPC ne laisse que peu de place au doute. Le consommateur est protégé contre toute publicité fausse ou trompeuse. Dès lors, il importe peu de déterminer la nature publique de la communication publicitaire. Nous soutenons donc, que le caractère général de la Loi permet une application directe en matière de publicité comportementale et ce quel que soit le degré de personnalisation d'une publicité.

B. Office de la protection du consommateur

En son article 291, la LPC crée l'*Office de la protection du consommateur,* « organisme gouvernemental chargé de protéger le consommateur »[201], en intervenant « auprès des commerçants afin qu'ils respectent leurs obligations envers les consommateurs […] [et en aidant] les consommateurs à faire des choix éclairés et à les informer de leurs droits, de leurs obligations et de leurs recours en cas de problème avec un commerçant »[202]. Pour ce faire, l'*Office* doit donc travailler à assurer que les consommateurs reçoivent toutes les informations

---

[199] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 25.

[200] *Richard c Time Inc*, [2012] 1 RCS 265 (CSC) au para 128.

[201] *Loi sur la protection du consommateur*, RLRQ c P-401, art 292 [LPC].

[202] Office de la protection du consommateur du Québec, « À propos de l'Office de la protection du consommateur », en ligne : Gouvernement du Québec <http://www.opc.gouv.qc.ca/a-propos/> (consulté le 1 juillet 2017).

nécessaires pour pouvoir faire des « choix éclairés » et, en conséquence, à remettre à l'ordre toute personne leur fournissant des informations « fausses ou trompeuses ». La loi prévoit d'ailleurs une obligation d'informer le consommateur : « Aucun commerçant, fabricant ou publicitaire ne peut, dans une représentation qu'il fait à un consommateur, passer sous silence un fait important »[203].

La procédure visant les personnes s'étant livrée ou se livrant à une pratique interdite, comme celle de la fausse représentation, se trouve à l'article 316 LPC. Il y est prévu que le président de *l'Office* ou organisme destiné à protéger le consommateur et constitué en personne morale depuis au moins un an peut demander au tribunal une injonction ordonnant à cette personne de ne plus se livrer à cette pratique[204]. Cette procédure serait donc susceptible de s'appliquer en matière de publicité afin de faire cesser quelconque individu qui enfreindrait l'article 219 LPC, faisant « par quelque moyen que ce soit » une représentation fausse ou trompeuse à un consommateur[205]. De cette manière, la Loi protège les intérêts économiques des consommateurs, en assurant qu'ils n'aient pas eux-mêmes à enclencher les poursuites contre les annonceurs malhonnêtes. Nous soulignons à nouveau que l'emploi de termes tels que « par quelques moyens que ce soit » ouvre aisément la porte à l'application de la Loi en matière de PCL.

Comme nous avons survolé les dispositions pertinentes au cadre juridique s'appliquant à la publicité, nous devons maintenant nous attarder à l'applicabilité de ces lois à l'ère d'Internet et plus précisément à la publicité en ligne.

---

[203] *Loi sur la protection du consommateur*, RLRQ c P-401, art 228 [LPC].

[204] *Loi sur la protection du consommateur*, RLRQ c P-401, art 316 [LPC].

[205] *Loi sur la protection du consommateur*, RLRQ c P-401, art 219 [LPC].

Chapitre 2 — Encadrement juridique de la publicité en ligne

Ayant à présent mieux défini le cadre juridique entourant la publicité, il importe d'observer de quelle manière il peut trouver application dans le contexte numérique de la publicité en ligne. Nous aborderons ensuite les questions spécifiques liées au profilage en matière de publicité et de protection des consommateurs.

Section 1 — Applicabilité des lois

En 2009, le professeur Gautrais publiait un texte, affirmant que la LC et la LPC, « dans la mesure où leur rédaction est très générale […], ne discrimine pas parmi les différents supports publicitaires »[206]. Ainsi, faisant écho au principe de neutralité technologique, il avançait que ces lois s'appliquaient à la cyberpublicité comme à tout autre type de publicité traditionnelle. Selon le professeur Trudel, « [la] neutralité technologique renvoie à la caractéristique d'une loi qui énonce les droits et les obligations des personnes de façon générique, sans égard aux moyens technologiques par lesquels s'accomplissent les activités visées. La loi est désintéressée du cadre technologique spécifique mis en place »[207]. Véritable création doctrinale, le principe de neutralité technologique est apparu en réponse à l'émergence des technologies de l'information[208]. Comme de nombreux concepts, celui-ci a existé avant d'être nommé. Il aura servi dans diverses circonstances sans être nécessairement

---

[206] Vincent GAUTRAIS et Adriane PORCIN, « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique » (2009) 43:3 Thémis 559 à la p 26.

[207] Pour une discussion plus approfondie sur le sujet de la neutralité technologique, voir les pages 19-21. Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Québec, Éditions Y Blais, 2012 à la p 19.

[208] Vincent GAUTRAIS, *Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques*, Montréal, Thémis, 2012 à la p 111.

identifié comme tel[209]. Ainsi, le principe, en l'absence d'encadrement législatif, émerge comme outil judiciaire servant à l'interprétation dans une perspective de cohérence du droit[210]. Cependant, de tels principes peuvent paraître problématiques, en ce qu'ils ne parviennent pas aux juges avec un manuel d'instruction. Pour autant, toujours en 2009, le Bureau de la concurrence du Canada a donné raison au professeur Gautrais, en émettant des lignes directrices signalant que :

> La Loi s'applique aux indications fausses ou trompeuses sans égard au média utilisé. Les mêmes règles de base qui régissent les pratiques commerciales et publicitaires traditionnelles s'appliquent aussi aux indications en ligne et aux pratiques commerciales par voie électronique. Quant aux dispositions pertinentes de la Loi, elles portent sur le contenu des indications plutôt que sur les moyens utilisés pour les communiquer[211].

Le Bureau confirmait ainsi que la cyberpublicité était régie par les législations traditionnelles encadrant la publicité au Canada.

Adressant particulièrement l'évolution des technologies de l'information, des dispositions récentes visent précisément les indications fausses ou trompeuses dans un message électronique (art. 52.01 (2) LC et art. 74.011 (2) LC) et dans un localisateur (art. 52.01 (3) LC et art. 74.011 (3) LC). Le message électronique est défini comme étant un « message envoyé par tout moyen de télécommunication, notamment un message alphabétique, sonore, vocal ou image » (art. 2 (1)b) LC). Quant au localisateur y est assimilée

---

[209] Cameron J HUTCHISON, « Technological Neutrality Explained (& Applied to CBC v. SODRAC) » (2015) 13:1 Canadian Journal of Law and Technology 101 à la p 106.

[210] Vincent GAUTRAIS, *Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques*, Montréal, Thémis, 2012 à la p 112; Cameron J HUTCHISON, « Technological Neutrality Explained (& Applied to CBC v. SODRAC) » (2015) 13:1 Canadian Journal of Law and Technology 101 à la p 106.

[211] Bureau de la concurrence, *Lignes directrices. Application de la Loi sur la concurrence aux indications dans Internet*, Gatineau, 2009, en ligne : <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet-2009-10-16-f.pdf/$FILE/RepresentationsInternet-2009-10-16-f.pdf> (consulté le 28 mai 2017).

« [toute] chaîne de caractères normalisés ou tout renseignement servant à identifier une source de données dans un ordinateur, notamment l'adresse URL ».

Scassa et Deturbide estiment également un autre cas qui pourrait trouver application dans la situation en l'espèce. Les auteurs soulèvent que :

> Subsection 52 (1) may have a unique application in the online environment as a weapon against spyware. The provision is similar to the "unfair and deceptive acts or practices" provisions in the *US Federal Trade Commission Act* which have been employed against spyware distributors who do not disclose that software or adware does not contain spyware[212].

En 2010, le gouvernement fédéral annonça également la mise sur pied de la *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* (ci-après « Loi Canadienne Anti Pourriel » ou « LCAP »)[213]. Entrée en vigueur le 1er juillet 2014, elle représentait à l'époque la plus importante législation antipourriel au monde, visant notamment les pourriels commerciaux, l'hameçonnage et la collecte d'adresses électroniques[214]. Elle « vise à protéger les Canadiens tout en veillant à ce

---

[212] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 65.

[213] *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, ch 23 [LCAP].

[214] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 589.

que les entreprises puissent continuer de mener concurrence sur les marchés mondiaux »[215]. Elle concerne tout organisme utilisant « des moyens électroniques pour promouvoir ou commercialiser [leurs produits ou services][216]. Son objet est défini en son article 3 :

> (3) La présente loi a pour objet de promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation des pratiques commerciales qui découragent l'exercice des activités commerciales par voie électronique pour les raisons suivantes :
>
> a) elles nuisent à l'accessibilité, à la fiabilité, à l'efficience et à l'utilisation optimale des moyens de communication électronique dans le cadre des activités commerciales ;
>
> b) elles entraînent des coûts supplémentaires pour les entreprises et les consommateurs ;
>
> c) elles compromettent la protection de la vie privée et la sécurité des renseignements confidentiels ;
>
> d) elles minent la confiance des Canadiens quant à l'utilisation des moyens de communication électronique pour l'exercice de leurs activités commerciales au Canada et à l'étranger.

Cet article nous pousse à nous questionner quant à ce qui constitue un message électronique aux fins d'application de cette loi. Cette dernière nous offre une définition à l'article 1 (1) : « [message] envoyé par tout moyen de télécommunication, notamment un message textuel, sonore, vocal ou visuel. Scassa avance que l'emploi du terme « message électronique » permet d'étendre la portée de la loi non seulement aux pourriels, mais aussi aux messages textes (SMS) et aux communications à vocation commerciale par les médias

---

[215] Industrie Canada, Gouvernement du Canada, « La Loi canadienne sur le pourriel et les autres menaces électroniques » (30 juin 2014), en ligne : La Loi canadienne anti-pourriel <http://combattrelepourriel.gc.ca/eic/site/030.nsf/fra/accueil> (consulté le 1 juillet 2017).

[216] Industrie Canada, Gouvernement du Canada, « La Loi canadienne sur le pourriel et les autres menaces électroniques » (30 juin 2014), en ligne : La Loi canadienne anti-pourriel <http://combattrelepourriel.gc.ca/eic/site/030.nsf/fra/accueil> (consulté le 1 juillet 2017).

sociaux[217]. Dans cette ligne d'idées, il est de notre avis que la portée de la loi pourrait éventuellement aussi s'étendre à d'autres types de messages électroniques dont nous ne soupçonnons toujours pas l'existence.

La loi définit aussi le message électronique *commercial* en son article 1 (2) :

> 1 (2) Pour l'application de la présente loi, est un message électronique commercial 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).

Ainsi, un « [message] envoyé par tout moyen de télécommunication, notamment un message textuel, sonore, vocal ou visuel » se qualifierait donc comme un *message électronique commercial,* s'il « a pour but, entre autres, d'encourager la participation à une activité commerciale ».

En outre, les pouvoirs de supervision relèvent du Conseil de la radiodiffusion et des télécommunications canadiennes (ci-après « CRTC ») qui a défini les règlements d'application

---

[217] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 590; Sophie DESCHÊNES-HÉBERT, « Présentation et démystification de la loi anti-pourriel : le consommateur numérique a-t-il l'unique contrôle de sa boîte de réception? » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 aux pp 224‑225.

en partenariat avec le ministère Industrie Canada[218], aujourd'hui Innovation, Sciences et Développement économique Canada.

La loi prévoit qu'est interdit l'envoi, à une adresse électronique, tout message électronique commercial que le destinataire n'a pas consenti à recevoir[219]. Suivant l'article 1 (1), l'adresse électronique est définie comme étant :

> 1 (1) Toute adresse utilisée relativement à la transmission d'un message électronique à l'un des comptes suivants :
>
> a) un compte courriel ;
>
> b) un compte messagerie instantanée ;
>
> c) un compte téléphone ;
>
> d) tout autre compte similaire. (electronic address)

La loi n'étant ainsi pas exhaustive, il est permis de croire qu'elle pourrait étendre sa portée à d'autres « adresses électroniques » n'étant toujours pas déterminée.

Quant aux obligations relatives à ce qui doit être inclus dans une télécommunication électronique commerciale, elles sont définies à l'article 6 (2) :

> 6 (2) Le message doit respecter les exigences réglementaires quant à sa forme et comporter, à la fois :
>
> a) les renseignements réglementaires permettant d'identifier la personne qui l'a envoyé ainsi que, le cas échéant, celle au nom de qui il a été envoyé ;
>
> b) les renseignements permettant à la personne qui l'a reçu de communiquer facilement avec l'une ou l'autre des personnes visées à l'alinéa a) ;
>
> c) la description d'un mécanisme d'exclusion conforme au paragraphe 11 (1).

---

[218] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 591.

[219] *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, ch 23, art 6(1)a [LCAP].

Une longue liste d'exceptions est prévue de l'article 6 (5) à 6 (8). Suivant la logique générale de la loi, le consentement est variable selon l'exception[220].

En terminant notre tour d'horizon relatif à la LCAP, l'article 2 prévoit qu'en cas d'incompatibilité avec la *Loi sur la protection des renseignements personnels et les documents électroniques* (nous utiliserons l'acronyme anglais de la loi, « PIPEDA », car il s'agit de l'acronyme le plus fréquemment employé), les dispositions de la LCAP l'emportent sur la partie I de PIPEDA.

Ayant à présent démontré que les lois, tant fédérales que provinciales, s'appliquent en matière de publicité en ligne, celles-ci ayant généralement une portée large, ne sont pas limitées à une forme de publicité particulière et englobent donc la publicité comportementale.

Section 2 — Tarification comportementale

Étant à présent en mesure de conclure qu'un corpus juridique canadien trouve application dans le domaine de la publicité en ligne, nous nous attarderons maintenant à ce qui nous apparaît être la problématique la plus importante au regard de la protection des consommateurs numériques, soit la tarification comportementale.

A. Définition

D'après Éloïse Gratton, « dynamic pricing, also known as 'adaptive pricing', 'dynamic pricing' or 'discriminatory pricing' or first-degree price discrimination, is defined as a practice where organizations attempt to perfectly exploit the differences in price sensitivity between consumers. […] Economically speaking, since a unique price for all customers would not

[220] Eloïse GRATTON et Elisa HENRY, *Practical guide to e-commerce and Internet law*, Markham, Ontario, LexisNexis, 2015 à la p 254.

maximize the retailer's profit (since certain customers may be willing to pay more than others) maximizing the profit would only be reached if each product is sold for the maximum price that the individual is willing to pay »[221].

Ainsi, 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 une pratique trompeuse soutenue par la collecte d'information sur le comportement des consommateurs.

B. Analyse juridique

Alors que la « discrimination par les prix » est commune hors ligne, comme dans la fixation de prix différents pour les étudiants et les adultes dans les musées, les données de consommation en ligne sont désormais disponibles pour les spécialistes du marketing. La tarification comportementale est l'objectif implicite du marketing comportemental, car plus on connaît d'information sur les consommateurs — et plus la forme de marketing est grande — plus il est probable que des prix particuliers puissent être conçus pour les consommateurs individuels, ce qui augmente la rentabilité d'un produit donné.

> Some businesses have attempted to use this practice. For instance, it was reported a few years ago that Coca-Cola had tested dynamic pricing in vending machines where prices would fluctuate based on the surrounding temperature since soft drink may be worth more when it is hotter outside. Amazon was also suspected of using such practices in 2000, using cookies to identify the visiting consumers. Staples Inc. was found using dynamic pricing based on users' locations and Orbitz has also been accused of price discrimination in the past, charging Mac users as much as 30% more

[221] Éloïse GRATTON, « Dynamic pricing on websites: illegal or unfair? » (26 octobre 2014), en ligne : Éloïse Gratton <http://www.eloisegratton.com/blog/2014/10/26/dynamic-pricing-on-websites-illegal-or-unfair/> (consulté le 1 juillet 2017).

> than PC users for certain products. In the offline space, retailers could profile a customer in real time (based on an RFID read of objects carried and by cross-referencing to past buying patterns) and they may offer differential service based on the "value" of the customer to the retailer[222].

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[223]. 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[224]. 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 »[225]. De cette façon, la discrimination fondée sur les prix « big data » est pratiquée, en l'absence de réglementation visant à protéger les droits des consommateurs à un prix juste pour un produit ou service donné. Une fois de plus, il est possible de soutenir que les principes généraux en matière de protection du consommateur s'appliquent en l'absence d'une législation particulière.

---

[222] Éloïse GRATTON, « Dynamic pricing on websites: illegal or unfair? » (26 octobre 2014), en ligne : Éloïse Gratton <http://www.eloisegratton.com/blog/2014/10/26/dynamic-pricing-on-websites-illegal-or-unfair/> (consulté le 1 juillet 2017).

[223] Nicola JENTZSCH, Geza SAPI et Irina SULEYMANOVA, « Targeted pricing and customer data sharing among rivals » (2013) 31:2 International Journal of Industrial Organization 131.

[224] Nicola JENTZSCH, Geza SAPI et Irina SULEYMANOVA, « Targeted pricing and customer data sharing among rivals » (2013) 31:2 International Journal of Industrial Organization 131.

[225] Allen GANNETT, « Behavioral Pricing: A Consumer's Worst Nightmare » (21 janvier 2012), en ligne : The Next Web <http://thenextweb.com/insider/2012/01/21/behavioral-pricing-a-consumers-worst-nightmare-a-merchants-dream/> (consulté le 6 décembre 2016).

À cet égard, le Bureau de la concurrence du Canada soulevait, dans un rapport paru en 2016, que :

> Big data may also allow platforms to establish pricing algorithms or other mechanisms to automate the prices charged between their users. Some panellists noted that automated price setting, with minimal intervention by humans, may enable sellers to maintain relatively high prices without the need for agreement between them. This could be a potential challenge for competition authorities and regulators, who will need to consider whether they have the right legislation, tools and frameworks to deal with these issues if and when they arise[226].

Le Bureau soulève donc un risque associé à la création de profils permettant à des algorithmes de fixer des prix selon différents critères, rendant alors l'encadrement juridique extrêmement complexe.

Parlant des données géographiques, on pourrait également être amenés à croire qu'un algorithme pourrait déterminer que la capacité de payer un article plus cher pour les gens provenant de Westmount par rapport à quelqu'un résidant dans Hochelaga-Maisonneuve, créant alors une véritable forme de discrimination, potentiellement fondée sur le milieu socio-économique. Une telle pratique peut donc aller très loin en matière de discrimination. Par exemple, il pourrait être imaginé un cas où la discrimination irait même jusqu'à déterminer la capacité de paiement d'un individu sans avoir recours à ses données bancaires, en se fondant uniquement sur sa personnalité virtuelle.

La tarification comportementale peut se baser sur différentes données, comme les données géographiques ou d'autres, liées à la création d'un profil, et afficher un prix variable selon l'utilisateur. Comme nous l'avons vu, les profils de ciblage sont parfois si complets qu'il est aisé de déterminer la susceptibilité d'un utilisateur à réagir à des mentions telles qu'« en quantité limitée » ou encore « en vente ». Selon leur personnalité, celles-ci répondront donc mieux à un prix affiché comme étant « réduits ». En effet, bien que la déclaration suivante ne

---

[226] Bureau de la concurrence, *Highlights from the Competition Bureau's Workshop on Emerging Competition Issues*, Gatineau, 2016, en ligne : <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04030.html> (consulté le 1 juillet 2017).

soit pas survenue dans le cadre de plaintes pour des prix discriminatoires, le Commissaire du Bureau de la concurrence a souligné que les *« [c] onsumers are naturally attracted to claims that they will save money »*[227]. Certains soulignent même que « *seeing something 'on sale' definitely impacts your decision and triggers an innate feeling of value, so you naturally look for sale products, that is why I think it is deceptive* »[228]. Cette affirmation souligne le caractère dangereux de la tarification comportementale, en ce qu'elle démontre qu'il est possible de considérer ces pratiques comme étant trompeuses. Ainsi, en matière de tarification comportementale, le caractère trompeur de cette pratique la rendrait interdite, en vertu des articles 52 (1) LC, 74.01 (1) a) LC et 219 LPC. Soulignons qu'il serait possible de se prémunir contre cette tarification comportementale en nettoyant un navigateur de ses témoins. Cependant, tel qu'évoqué précédemment, des technologies comme les témoins Flash, empreintes digitales ou inspections de paquets profonds ne permettent pas de se protéger. De plus, malgré le retrait de témoins d'un ordinateur, les serveurs informatiques utilisés par les entreprises sont tout de même en mesure de retenir les requêtes effectuées sur son site internet, et ainsi ajuster les prix en fonction des demandes dans un lieu, ou à un moment précis. À cet égard, les algorithmes développés par les entreprises comme Uber sont à même d'ajuster les prix en fonction des demandes sur leurs réseaux[229].

---

[227] NEWS et Retail & MARKETING, « Amazon Canada fined $1 million plus $100,000 costs for misleading price claims on website » (11 janvier 2017), en ligne : Financial Post <http://business.financialpost.com/news/retail-marketing/amazon-canada-fined-1-million-plus-costs-for-misleading-price-claims-on-website> (consulté le 31 juillet 2017).

[228] Lucy CORMACK, « Dynamic pricing in online shopping surging with the e-commerce boom », *The Sydney Morning Herald* (7 février 2017), en ligne : The Sydney Morning Herald <http://www.smh.com.au/business/consumer-affairs/dynamic-pricing-in-online-shopping-surging-with-the-ecommerce-boom-20170203-gu5469.html> (consulté le 1 juillet 2017).

[229] Uber, « How surge works | Drive Uber », en ligne : Uber.com <https://www.uber.com/info/how-surge-works/> (consulté le 25 juillet 2017).

Partie 2 — Protection des renseignements personnels

« Before cookies, the Web was essentially private, […] after cookies, the Web becomes a space capable of extraordinary monitoring »[230].

Si, à la fin du 20e siècle, les internautes n'avaient que peu conscience de l'existence des témoins, tout allait changer après l'affaire *DoubleClick*[231]. En agissant à titre de réseau publicitaire, *DoubleClick* procédait à la collecte de données par l'ajout de témoins. Comme la firme était de loin le plus gros réseau à cette époque, les internautes n'étant pas exposés aux témoins de *DoubleClick* représentaient l'exception. La poursuite affirmait que la création de profils utilisateurs par *DoubleClick* violait la vie privée des individus ainsi traqués. De plus, *DoubleClick* venait d'acquérir Abacus Direct, une firme de marketing direct et surtout venait de mettre la main sur une base de données impressionnante d'informations sur environ quatre-vingt-dix pour cent de la population américaine[232]. Les risques d'atteinte à la vie privée devenaient donc d'autant plus réels que l'information ainsi recueillie ne provenait plus seulement d'Internet, mais bien du monde réel. Malgré tout, les pratiques de *DoubleClick* furent jugées comme n'ayant pas enfreint la loi fédérale américaine en la matière. Cet épisode ouvrit tout de même la porte à un débat sur la légalité de l'implantation des témoins et sur les attitudes du public face à cette pratique.

---

[230] John SCHWARTZ, « Giving Web a Memory Cost Its Users Privacy », *The New York Times* (4 septembre 2001), en ligne : The New York Times <http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> (consulté le 12 avril 2017), citant Lawrence Lessig.

[231] *Re DoubleClick Inc Privacy Litigation*, 154 F Supp 2d 497 (SDNY 2001).

[232] *Re DoubleClick Inc Privacy Litigation*, 154 F Supp 2d 497 (SDNY 2001).

Dans cette partie, nous procèderons tout d'abord à une analyse du contexte social dans lequel la publicité comportementale évolue, nous intéressant particulièrement aux différents malaises que celle-ci génère (Chapitre 1). Puis, nous aborderons les aspects juridiques liés à la protection des renseignements personnels dans le contexte de la publicité comportementale en ligne (Chapitre 2).

Chapitre 1 — Internautes et conceptions de la vie privée

De nombreuses sources rapportent que les utilisateurs tendent à adopter une attitude négative face à la PCL. Certains auteurs vont jusqu'à soutenir que « *the threat to consumer privacy is aggravated by dubious, deceptive and otherwise questionable tactics employed by a handful of bad actors to collect and disseminate data about individuals without their knowledge or consent* »[233]. Nous reviendrons sur les notions de connaissance et de consentement ultérieurement. Cependant, notons immédiatement que de nombreux utilisateurs estiment qu'il y a un risque que la publicité comportementale non transparente et trompeuse viole les droits à la vie privée d'une manière dangereuse et sans précédent[234].

Section 1 — Attitudes des internautes face à la PCL

Les utilisateurs constituent le point de départ de notre réflexion. En effet, pourquoi se questionner sur les questions de préservation de vie privée si personne n'est concerné ? C'est donc dans cette perspective que cette première section abordera les attitudes des utilisateurs

---

[233] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 284.

[234] Alexander NILL et Robert J AALBERTS, « Legal and Ethical Challenges of Online Behavioral Targeting in Advertising » (2014) 35:2 Journal of Current Issues & Research in Advertising 126 à la p 126.

dans la détermination de leurs attentes de vie privée lorsqu'ils naviguent sur Internet, et ce, en relation avec la publicité comportementale.

A. Méconnaissance de la publicité comportementale en ligne

Plusieurs auteurs s'entendent pour dire que la publicité comportementale est comme une offre que les utilisateurs « ne peuvent pas refuser »[235] et que c'est en raison de l'incompréhension des utilisateurs qu'elle est aussi populaire auprès des annonceurs, précisément parce que les consommateurs ne connaissent pas, ou peu, la PCL[236]. Ce serait donc en s'appuyant sur une technologie omniprésente et méconnue que la traque massive serait effectuée[237]. Qui plus est, si la collecte d'information repose sur un mécanisme inaccessible pour la majorité des utilisateurs, ceux-ci n'ont généralement pas conscience du *qui* procède à la collecte encore moins du *pourquoi*. Ainsi, les « *[consumers] are often unaware of the existence of these entities, as well as the purposes for which they collect and use data* »[238]. Cole souligne à cet effet que les politiques de confidentialité en ligne ajoutent à

---

[235] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273.

[236] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 273.

[237] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 284.

[238] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, 2012 à la p 68, en ligne : <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> (consulté le 18 avril 2017).

la confusion des utilisateurs par leur manque de clarté et leur longueur[239]. Cette méconnaissance tend à entraîner chez les utilisateurs un véritable inconfort, allant jusqu'à considérer les pratiques de la PCL comme étant trompeuses, injustes ou à l'encontre de leur volonté personnelle[240]. Certains en viennent même à considérer la traque en ligne comme étant dangereuse, rendant les internautes « transparents et contrôlables »[241].

Hoofnagle et al. soutiennent qu'il existe au sein de l'industrie, une véritable volonté d'empêcher les utilisateurs de mettre un frein à la publicité comportementale[242].

> Behavioral advertising and the tracking that goes with it is the offer you cannot refuse, not necessarily because you are tempted by it, but because sophisticated, market-dominant actors control the very platforms you use to access the web[243].

Ainsi, à chaque problème sa solution. Les *témoins* traditionnels peuvent être supprimés ? Pas de problème, les témoins flash prendront le relais. Ces derniers sont sujets à controverse ? L'industrie utilisera l'empreinte *numérique* de votre ordinateur !

---

[239] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 284; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, 2012 à la p 61, en ligne : <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> (consulté le 18 avril 2017); Cette conclusion est partagée par de nombreux auteurs soulignant que les politiques de vie privée sont vides de sens tant elles sont amigües Joel R REIDENBERG et al, « Ambiguity in Privacy Policies and the Impact of Regulation » (2016) 45:S2 J Legal Stud S163.

[240] Paul SCHWARTZ et Daniel SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814 à la p 1853; Joseph TUROW et al, *Americans Reject Tailored Advertising and Three Activities that Enable It*, 2009 à la p 14, en ligne : <https://papers.ssrn.com/abstract=1478214> (consulté le 18 avril 2017).

[241] Thomas MANDL, Wiebke THODE et Joachim GRIESBAUM, *« I would have never allowed it »: User Perception of Third-party Tracking and Implications for Display Advertising*, *14th International Symposium on Information Science*, 2015, 445 à la p 451, en ligne : 14th International Symposium on Information Science <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1008.601&rep=rep1&type=pdf>.

[242] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 273.

[243] Chris HOOFNAGLE et al, « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273 à la p 278.

Si certains utilisateurs sont conscients de l'existence de la publicité comportementale, ils ont généralement une mauvaise compréhension de la publicité sur Internet et restent persuadés que leurs actions en ligne sont anonymes[244].

Assumant qu'un certain nombre de participants à leur étude étaient familiers avec la PCL et avec les témoins, McDonald et Cranor ont constaté que la majorité des personnes interrogées n'étaient pas conscientes du rôle des témoins dans la collecte des données, croyant pour la plupart qu'ils ne servaient qu'à la sauvegarde des mots de passe[245]. Ultimement, seuls dix-huit pour cent des participants ont répondu qu'ils appréciaient avoir de la publicité personnalisée plutôt qu'une publicité générique[246].

Lorsque des outils sont mis à la disposition des internautes afin de prévenir ou empêcher la collecte de données aux fins de publicité comportementale, on constate que ceux-ci n'ont souvent pas eu d'impact sur les utilisateurs qui ne se désengagent pas du suivi[247]. Ce constat survient malgré le fait que les études démontrent une forte propension de la part des internautes à refuser, s'ils le pouvaient, la traque aux fins de publicité comportementale[248]. S'il existe un désir de la part des internautes de mettre fin à cette traque, ceux-ci y parviennent

---

[244] Aleecia M MCDONALD et Lorrie Faith CRANOR, *An Empirical Study of How People Perceive Online Behavioral Advertising*, CMU-CyLab-09-015, 2009.

[245] Aleecia M MCDONALD et Lorrie Faith CRANOR, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, Arlington, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), 16 août 2010 à la p 9.

[246] Aleecia M MCDONALD et Lorrie Faith CRANOR, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, Arlington, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), 16 août 2010 à la p 22.

[247] Pedro LEON et al, *Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising*, New York, New York, USA, ACM, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 5 mai 2012, 589.

[248] Pedro LEON et al, *Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising*, New York, New York, USA, ACM, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 5 mai 2012, 589 à la p 589.

rarement à la hauteur de leurs attentes personnelles. En effet, les différents mécanismes, qu'ils soient d'*opt-out*, de bloqueur de publicité (de type *ad-block*) ou encore les solutions propres aux navigateurs (de type *do-not-track*) sont déficientes, difficiles à configurer et manquent cruellement d'informations[249].

B. Perceptions de violations de la vie privée

Certains chercheurs ont démontré que les utilisateurs d'Internet ne percevaient pas de bénéfices particuliers dans la PCL et considéraient que le type de publicité basée sur le suivi de leurs activités était en fait une forme de manipulation et, par conséquent, avaient tendance à l'évitement[250].

Si plusieurs études se sont penchées sur les attitudes des internautes face à la protection de leurs renseignements personnels, d'autres ont cherché à comprendre les impacts de la publicité comportementale sur les utilisateurs[251]. Ils ont, en outre, constaté que certains utilisateurs pouvaient être affectés de manière défavorable par le jugement sous-entendu de certaines annonces ciblées qu'ils ont reçues. Celles-ci iraient même jusqu'à affecter leur perception d'eux-mêmes en fonction des annonces ayant résulté de leurs historiques de

---

[249] Pedro LEON et al, *Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising*, New York, New York, USA, ACM, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 5 mai 2012, 589 aux pp 593, 598.

[250] Chang-Dae HAM et Sann RYU, *Exploring How Consumers Cope with Online Behavioral Advertising: An Integration of the Persuasion Knowledge Model and the Protection Motivation Theory*, Lubbock, United States, American Academy of Advertising, 2014, 165.

[251] Christopher A SUMMERS, Robert W SMITH et Rebecca Walker RECZEK, « An Audience of One: Behaviorally Targeted Ads as Implied Social Labels » [2016] J Cons Res.

recherche. Certains profils peuvent être embarrassants, notamment lorsqu'ils portent sur des sujets sensibles comme la perte de poids ou les problèmes financiers[252].

D'autres auteurs ont concentré leurs recherches sur la manipulation du marché et, sans aller jusqu'à la qualification de subliminal, reconnaissent que les impacts de la publicité comportementale s'y apparentent :

> Digital market manipulation presents an easy case: firms purposefully leverage information about consumers to their disadvantage in a way that is designed not to be detectable to them […] A consumer who receives an ad highlighting the limited supply of a product will not usually understand that the next person, who has not been associated with a fear of scarcity, sees a different pitch based on her biases. Such a practice does not just tend to mislead; misleading is the entire point[253].

Lorsqu'exposés à la PCL, un nombre important d'internautes adopte une attitude négative. Malgré la prolifération de cette pratique, loin d'être résolus, ils continuent de

---

[252] Sol TANGUAY, « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, *Le consommateur numérique: une protection à la hauteur de la confiance?*, Éditions Yvon Blais, 2016 à la p 169.

[253] Ryan CALO, « Digital Market Manipulation » (2014) 82:4 Geo Wash L Rev 995 à la p 1041; Certaines études vont même jusqu'à conclure que les algorithmes nous connaissent mieux que quiconque « by harvesting Facebook « Likes, » the researchers' computer model proved more accurate at divining a person's self-reported personality traits than their own kith and kin » Gwynn GUILFORD, « Facebook data know you better than your own mother », en ligne : Quartz <https://qz.com/325129/facebook-data-know-you-better-than-your-own-mother/> (consulté le 10 avril 2017).

percevoir cette dernière comme étant intrusive[254]. Les utilisateurs se disent inquiets de la protection de leurs renseignements personnels et cette inquiétude se fait particulièrement ressentir dans les situations où il n'y a pas, ou peu de divulgation préalable sur le fait que de telles informations soient recueillies[255].

Un des facteurs psychologiques affectant le plus les utilisateurs est l'absence de contrôle sur les informations personnelles recueillies[256]. Lorsqu'informés sur les pratiques marketing de traque et de publicité comportementale, certains internautes soutiennent qu'ils n'auraient jamais accepté une telle traque[257]. Les préoccupations en matière de protection de la vie privée semblent être moindres lorsqu'il existe une véritable divulgation concernant la

---

[254] Sangdow ALNAHDI, Maged ALI et Kholoud ALKAYID, « The effectiveness of online advertising via the behavioural targeting mechanism » (2014) 5:1 The Business & Management Review 22 à la p 28; Pedro Giovanni LEON et al, *What matters to users?: factors that affect users' willingness to share information with online advertisers*, *Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013*, New York, New York, USA, ACM, juillet 2013, 7, DOI : 10.1145/2501604.2501611; Blase UR et al, *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, *Proceedings of the Eighth Symposium on Usable Privacy and Security*, coll SOUPS '12, New York, NY, USA, ACM, 2012, 4:1; Annie I ANTÓN, Julia B EARP et Jessica D YOUNG, « How internet users' privacy concerns have evolved since 2002 » (2010) 8:1 IEEE Security & Privacy; Aleecia M MCDONALD et Lorrie Faith CRANOR, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, Arlington, 38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference), 16 août 2010; Aleecia M MCDONALD et Lorrie Faith CRANOR, *An Empirical Study of How People Perceive Online Behavioral Advertising*, CMU-CyLab-09-015, 2009.

[255] Blase UR et al, *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, *Proceedings of the Eighth Symposium on Usable Privacy and Security*, coll SOUPS '12, New York, NY, USA, ACM, 2012, 4:1 à la p 1.

[256] Laurence ASHWORTH et Clinton FREE, « Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns » (2006) 67:2 Journal of Business Ethics 107 à la p 110.

[257] « It's one thing if I'd knew what is happening when I go online, then it's my decision and I could live with it but I would have never permitted it if I'd known what it means to go online. Consciously, I would have never allowed it. » Thomas MANDL, Wiebke THODE et Joachim GRIESBAUM, *« I would have never allowed it »: User Perception of Third-party Tracking and Implications for Display Advertising*, *14th International Symposium on Information Science*, 2015, 445 à la p 452, en ligne : 14th International Symposium on Information Science <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1008.601&rep=rep1&type=pdf>.

collecte de ces renseignements, mais que, dans l'ensemble, il serait difficile pour les consommateurs de prendre connaissance du volume de renseignements personnels recueillis sur leurs comportements dans l'objectif d'être utilisés par les spécialistes du marketing en ligne. Dans cette ligne d'idée, Ashworth et Free[258] soutiennent que les utilisateurs sont réfractaires à la collecte de données puisqu'ils perçoivent l'échange comme étant injuste affirmant ne rien recevoir dans cet « échange »[259].

La valeur économique des données collectées justifie, sur le plan commercial, d'acquérir plus d'information, afin de nourrir des profils encore plus détaillés et ainsi avoir un potentiel commercial plus élevé. Or, cette incessante collecte préoccupe les utilisateurs qui constatent que leurs intérêts entrent dès lors en contradiction avec ceux des entreprises tirant profit de cette collecte[260]. Comme les informations proviennent d'une myriade de sources différentes, il est possible que certaines bases de données possèdent de l'information extrêmement détaillée sur un individu, allant même notamment jusqu'à posséder les renseignements personnels comme un numéro de sécurité sociale, des données de santé, des données financières, un dossier criminel, une affiliation religieuse ou politique[261]. Ces données peuvent ensuite être converties en informations à travers différents segments tels que

---

[258] Laurence ASHWORTH et Clinton FREE, « Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns » (2006) 67:2 Journal of Business Ethics 107.

[259] Laurence ASHWORTH et Clinton FREE, « Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns » (2006) 67:2 Journal of Business Ethics 107 à la p 107; Dans une étude réalisée sur la PCL une participante s'est exclamée : « I see no advantages for the user. If I want to find something online I got ways to do so and I don't need advertisements telling me that there is something » Thomas MANDL, Wiebke THODE et Joachim GRIESBAUM, *« I would have never allowed it »: User Perception of Third-party Tracking and Implications for Display Advertising*, *14th International Symposium on Information Science*, 2015, 445 à la p 451, en ligne : 14th International Symposium on Information Science <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1008.601&rep=rep1&type=pdf>.

[260] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 290.

[261] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 290.

« *'Expectant Parent', 'Bible Lifestyle', 'Financially Challenged', 'Allergy Sufferer', 'Discount Shopper', 'Diabetes Interest', and 'Thrifty Elders'* »[262].

Section 2 — Questions de vie privée

La vie privée est un concept abstrait et difficile à saisir. Daniel J. Solove disait à cet égard que le concept de « *[privacy] seems to be about everything, and therefore it appears to be nothing* »[263]. La vie privée souffre donc d'un problème définitionnel, dont l'impasse trouve sa source dans l'interprétation que s'en fait tout un chacun. La vie privée comme concept est donc intimement liée aux individus qui la construisent et déconstruisent.

> Privacy is difficult to define. It means different things to different people […] While seemingly different, these definitions are related, because they pertain to the boundaries between the self and the others, between private and shared, or, in fact, public.
>
> As individuals and as consumers, we constantly navigate those boundaries, and the decisions we make about them determine tangible and intangible benefits and costs, for ourselves and for society[264].

À cet égard le professeur Pelletier souligne que :

> [la] vie privée est une notion très élastique qui recouvre une panoplie indéfinie de situations où il peut être porté atteinte à celle-ci. Bien qu'elle soit un sujet relativement imprécis et indéfinissable, la protection de la vie privée comporte différents aspects, lesquels sont plus ou moins régis par le droit existant : confidentialité des données à

---

[262] Gregory MAUS, « How data brokers sell your life, and why it matters » (24 août 2015), en ligne : The Stack <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/> (consulté le 11 avril 2017).

[263] Daniel J SOLOVE, « A Taxonomy of Privacy » (2006) 154:3 U Pa L Rev 477 à la p 479.

[264] Alessandro ACQUISTI, Curtis R TAYLOR et Liad WAGMAN, « The Economics of Privacy » (2016) 52:2 Journal of Economic Literature 442 à la p 443.

> caractère personnelles [...] droit à l'honneur et à la dignité [...] développements technologiques et respect des télécommunications [...] droit à l'intimité, etc[265].

Ainsi donc, comme le souligne Éloïse Gratton, la vie privée est indispensable dans la protection d'autres catégories de droit, notamment la liberté d'expression et la liberté d'association[266].

A. Conception de la vie privée

Si le concept de vie privée peut être perçu comme émanant du droit naturel[267], celui-ci semble trouver écho chez les philosophes Kant et Aristote[268]. Or, juridiquement parlant, l'évolution du concept de vie privée ou *Privacy* se serait faite sur trois phrases distinctes. La première prendrait ses racines principalement en 1890[269] lors de la publication par Samuel Warren et Louis Brandeis d'un article intitulé « *The right to privacy* »[270] que l'emploi de ce concept fut consacré en droit américain. Le droit à la vie privée y était défini comme étant

---

[265] Benoit Pelletier, « Droit constitutionnel: La protection de la vie privee au Canada » (2001) 35 La Revue Juridique Themis 485 aux pp 487‑488.

[266] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p xxiii.

[267] « [to] say that the common law right to privacy is grounded in natural law, is simply to state an empirical fact » Anita L ALLEN, « Natural Law, Slavery, and the Right to Privacy Tort Colloquium: The Natural Law Origins of the American Right to Privacy » (2012) 81 Fordham L Rev 1187 à la p 1191.

[268] Anita L ALLEN, « Natural Law, Slavery, and the Right to Privacy Tort Colloquium: The Natural Law Origins of the American Right to Privacy » (2012) 81 Fordham L Rev 1187 à la p 1211.

[269] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p 2.

[270] Samuel WARREN et Louis BRANDEIS, « The Right to Privacy » (1890) IV:5 Harv L Rev, en ligne : Harvard Law Review <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm> (consulté le 12 février 2017).

« *the right to be left alone* »[271]. Cette définition du droit à la vie privée par Warren et Brandeis lie celle-ci aux droits de personnalité[272] et établit principalement celle-ci dans la dichotomie que représente l'espace privé opposé à l'espace public, rappelant les écrits de Locke[273]. Un des risques soulevés par Warren et Brandeis est le développement de nouvelles technologies, alors précisément que l'appareil photo qui devenait de plus en plus accessible et abordable à leur époque[274].

La deuxième phase aurait débuté au sortant et en réponse aux atrocités de la Seconde Guerre mondiale[275], à la suite à l'adoption en 1948, par les *Nations Unies*, de la *Déclaration universelle des droits de l'Homme*[276] qui déclarait en son article 12 que :

> **12.** Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes[277].

---

[271] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p xxiii.

[272] Paul SCHWARTZ et Daniel SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814 à la p 1819.

[273] « Chez Hobbes et chez Locke, l'individu dans l'état de nature, donc décentré par rapport à l'univers politique, est l'ultime lieu de légitimité tant de l'État que de la société civile. Cette double distanciation, entre la sphère politique et la sphère privée d'une part, et entre le lieu de la légitimité et le lieu d'exercice de cette souveraineté d'autre part » J Yvon THÉRIAULT, « De l'utilité de la distinction moderne privé/public » [1992] 21 Politique 37 à la p 53.

[274] Daniel J SOLOVE et Paul M SCHWARTZ, *Information privacy law*, 5e éd, coll Aspen casebook series, New York, Wolters Kluwer Law & Business, 2015 aux pp 11‑12.

[275] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p 3.

[276] *Déclaration universelle des droits de l'homme*, Rés AG 217(III), Doc off AG NU, 3e sess, sup no 13, Doc NU A/810 (1948) 71.

[277] *Déclaration universelle des droits de l'homme*, Rés AG 217(III), Doc off AG NU, 3e sess, sup no 13, Doc NU A/810 (1948) 71, art 12.

Cette phase serait donc particulièrement liée à l'émergence d'une protection entourant les droits humains, contrairement à la toute première phase (et la troisième) qui serait intimement liée aux développements technologiques.

Finalement, à l'instar de la première, la troisième phase serait, liée aux avancées technologiques. De ce fait, au courant des années 60 et 70[278] les débats entourant la vie privée étaient constants et occupaient une place centrale dans les milieux politiques et sociaux, particulièrement en raison du développement de surveillance électronique et des bases de données[279]. Conséquemment, la vie privée sera dès lors perçue dans une perspective de contrôle des individus sur leurs informations personnelles[280].

Ainsi, si en 1960-1970, l'émergence de l'utilisation des bases de données et des ordinateurs faisait craindre le pire, particulièrement en ce que ceux-ci étaient devenus indispensables[281], Éloïse Gratton soutient qu'aujourd'hui « *[the] recent changes triggered by the Internet and related technologies are important enough to suggest that we have entered a fourth wave, and we should therefore go back to the drawing board* »[282].

---

[278] Daniel J SOLOVE et Paul M SCHWARTZ, *Information privacy law*, 5e éd, coll Aspen casebook series, New York, Wolters Kluwer Law & Business, 2015 à la p 37.

[279] Daniel J SOLOVE et Paul M SCHWARTZ, *Information privacy law*, 5e éd, coll Aspen casebook series, New York, Wolters Kluwer Law & Business, 2015 à la p 37.

[280] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p 6.

[281] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p 7.

[282] Éloïse GRATTON, *Understanding personal information: managing privacy risks*, Markham, Ont, LexisNexis, 2013 à la p 56.

B. Discussion sur la vie privée

Mais pourquoi tant de discussions entourant la vie privée ? Le professeur Westin soutient dès 1967 que « *[privacy] is the claim of individuals, groups or institutions to* ***determine for themselves*** *when, how, and to what extent information about them is communicated to others* »[283]. Le professeur Hunt, quant à lui, souligne que « *[the] claim to control personal information is closely associated with the values underpinning privacy (especially the values of* ***dignity*** *and* ***autonomy***) »[284] établissant alors un lien entre des valeurs universelles comme la dignité et l'autonomie, toutes deux reconnues dans la *Déclaration universelle* de 1948[285].

Dans l'affaire *Campbell v MGM*[286], Lord Nicholls souligna que « *[a] proper degree of privacy is essential for the [well-being] and development of an individual* »[287]. Toujours dans la même affaire, Lord Hoffmann pour sa part ajouta que « *[the] protection of human* ***autonomy*** *and* ***dignity****—the* ***right to control*** *the dissemination of information about one's private life and the right to the esteem and respect of other people* »[288].

Solove et Schwartz soulèvent que, dans une ère gouvernée par la technologie, la vie privée incarne :

> [an] issue of paramount significance for freedom, democracy, and security. One of the central issues of information privacy concerns the power of commercial and

---

[283] Alan F WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967 à la p 7.

[284] Chris DL HUNT, « Conceptualizing Privacy and Elucidating its importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011) 37 Queen's LJ 167 à la p 182.

[285] L'article premier de la *Déclaration universelle* s'énonce comme suit : « Tous les êtres humains naissent libres et égaux en **dignité** et en droits » *Déclaration universelle des droits de l'homme*, Rés AG 217(III), Doc off AG NU, 3e sess, sup no 13, Doc NU A/810 (1948) 71, art premier.

[286] *Campbell v MGN Ltd*, [2004] UKHL 22.

[287] *Campbell v MGN Ltd*, [2004] UKHL 22 au para 12.

[288] *Campbell v MGN Ltd*, [2004] UKHL 22 au para 51.

> government entities over individual autonomy and decision-making. Privacy also concerns the drawing of rules that may limit this autonomy and decision-making by necessarily permitting commercial and government entities access to personal information[289].

Notons en terminant cet aperçu (non exhaustif nous en conviendrons) que nous souscrivons aux propos soulevés par Hyman Gross en 1967 : « *[the] law does not determine what privacy is, but only what situations of privacy will be afforded legal protection* »[290]. Ainsi, la définition de ce qu'est la vie privée ne peut, ou ne doit pas nécessairement être encastrée dans un corpus juridique, mais puisque les lois en gèrent certaines facettes, il est nécessaire d'en déterminer les pourtours.

Chapitre 2 — Aspects juridiques des renseignements personnels

De nombreuses problématiques liées à la vie privée semblent faire surface en matière de publicité comportementale, un des problèmes qu'on ne saurait éclipser est celui de la détermination du cadre juridique applicable. En effet, quelle est la nature de la donnée recueillie et quelles lois garantissent sa protection. Également, la pratique qui consiste en la création de profils utilisateurs, est-elle conforme avec les lois en vigueur. Ainsi, dans ce chapitre, nous aborderons le cadre juridique en matière de publicité comportementale et tenterons de déterminer si les lois en la matière constituent une protection adéquate pour les renseignements personnels.

---

[289] Daniel J SOLOVE et Paul M SCHWARTZ, *Information privacy law*, 5e éd, coll Aspen casebook series, New York, Wolters Kluwer Law & Business, 2015 à la p 2.

[290] Hyman GROSS, « The Concept of Privacy » (1967) 42 NYU L Rev 34 à la p 36.

Section 1 — La protection de la vie privée

Le droit de *Privacy* tel qu'énoncé par Warren et Brandeis aux États-Unis n'est pas étranger au Canada et émane d'ailleurs d'un curieux mélange d'influences. Tout d'abord développé dans le cadre de certaines lois[291] — sans qu'il ne soit expressément nommé — ce concept fut par la suite reconnu comme droit fondamental, suite à l'interprétation des tribunaux canadiens comme étant enchâssé dans la *Charte canadienne des droits et libertés*[292] (ci-après « CCDL » ou « Charte canadienne ») (adoptée en 1982) aux articles 7 et 8. L'outil constitutionnel, que représente la Charte canadienne ne s'applique cependant qu'aux acteurs étatiques et ne vise donc pas les acteurs privés[293].

Si la publicité comportementale apparaît comme étant un phénomène récent, les problématiques qui en découlent et particulièrement celles visant la protection de la vie privée ne le sont pas. Puisqu'au tournant des années 1970, l'Occident chercha à établir un cadre entourant la protection des données à caractère personnel[294], les instances internationales allaient donner un coup de pouce au développement du cadre juridique canadien. C'est ainsi

---

[291] À cet égard voir par exemple : « Commet une infraction quiconque, sans y être expressément autorisé sous le régime de la présente loi, de la Loi sur les douanes ou de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes et en connaissance de cause, ouvre, cache ou retient un contenant postal, un envoi ou un récipient ou un dispositif que la Société destine au dépôt ou permet que soient commises ces actions ». *Loi sur la société canadienne des postes*, LRC 1985, c C-10, art 48; Voir également : « Sauf exception réglementaire, il est interdit d'intercepter et soit d'utiliser, soit de communiquer toute radiocommunication sans l'autorisation de l'émetteur ou du destinataire » *Loi sur la radiocommunication*, LRC 1985, c R-2, art 9(2); Ou encore : « La présente loi affirme le caractère essentiel des télécommunications pour l'identité et la souveraineté canadiennes; la politique canadienne de télécommunication vise à : [...] contribuer à la protection de la vie privée des personnes » *Loi sur les télécommunications*, LC 1993, c 38, art 7(i).

[292] *Charte canadienne des droits et libertés*, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11, art 7, 8 [CCDL].

[293] Pour une discussion sur le contexte de l'application de la vie privée en droit canadien voir Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 82.

[294] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 86.

qu'en septembre 1980, l'*Organisation de coopération et de développement économiques* (OCDE) adopta les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*[295]. Ces lignes directrices contenaient huit grands principes de gestion de l'information[296] et donnèrent naissance à la première loi fédérale de gestion des renseignements personnels à savoir la *Loi sur la protection des renseignements personnels*[297] (ci-après « LPRP ») en 1983[298]. Cependant, la LPRP[299] ne s'applique qu'aux institutions fédérales[300].

En outre, avant l'émergence d'un cadre propre au secteur privé, certains aspects de la vie privée ou de la protection des données se trouvaient pour leurs parts encadrés par différentes lois et règlements, entre autres celles réglementant le secteur bancaire, certaines professions et le domaine de la santé[301]. Ce mouvement vers un accroissement de la protection de la vie privée, ainsi que l'avancement des technologies fit en sorte qu'avec l'émergence d'Internet, le gouvernement eut à établir les principes encadrant la protection des renseignements personnels dans le secteur privé.

---

[295] OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », en ligne : <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm> (consulté le 26 mars 2017).

[296] (1) principe de la limitation de la collecte (2) de la qualité des données (3) de la spécification des finalités (4) de la limitation de l'utilisation (5) des garanties de sécurité (6) de la transparence (7) de la participation individuelle (8) de la responsabilité OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », en ligne : <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm> (consulté le 26 mars 2017).

[297] *Loi sur la protection des renseignements personnels*, LRC (1985) ch P-21 [LPRP].

[298] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 87.

[299] *Loi sur la protection des renseignements personnels*, LRC (1985) ch P-21 [LPRP].

[300] *Loi sur la protection des renseignements personnels*, LRC (1985) ch P-21, art 2 [LPRP].

[301] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 84.

En raison des avancées technologiques, des pressions politiques locales et internationales, de la disparité des lois régionales, et surtout suite à l'adoption en 1995 par le Parlement européen de la *Directive 95/46/CE*[302], sur la protection des données, le Gouvernement fédéral canadien se senti pressé de mettre sur pied une loi d'application dans le secteur privé[303]. En effet, en raison de la *Directive 95/46/CE*, aucune juridiction canadienne (outre le Québec, nous le verrons ci-après[304]) ne pouvait déclarer qu'elle offrait un niveau de protection « adéquat » dans le transfert des données depuis un pays membre de l'UE[305]. Ainsi, en 2000, la *Loi sur la protection des renseignements personnels et les documents*

---

[302] *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] JO L281.

[303] Collin J BENNETT, Christopher A PARSONS et Adam MOLNAR, « Real and Substantial Connections: Enforcing Canadian Privacy Laws against American Social Networking Campaigns » (2014) 23 J L Inf & Sci 50 à la p 53.

[304] « Le 20 janvier 2001, la Commission européenne a décrété que la LPRPDE remplissait les conditions fixées par la Directive sur la protection des données qu'avait adoptée l'Union européenne en 1995 dans le but de protéger les renseignements personnels et d'harmoniser les lois respectives de ses membres sur la protection de la vie privée. Par la suite, les données à caractère personnel des États membres de l'Union européenne peuvent être transférées au Canada » *Englander c Telus Communications Inc*, 2004 CAF 387 au para 17.

[305] Collin J BENNETT, Christopher A PARSONS et Adam MOLNAR, « Real and Substantial Connections: Enforcing Canadian Privacy Laws against American Social Networking Campaigns » (2014) 23 J L Inf & Sci 50 à la p 53; Le nouvel article 44 de la Directive européenne prévoit les mêmes conditions « Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. » *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, (2016) Official Journal of the European Union 1‑88, art 44 [GDPR]; La nouvelle directive de l'Union Européenne risque d'ailleurs d'avoir des conséquences juridiques en matière de publicité comportementale « It may even apply to companies that track the online activity of EU citizens, potentially including those companies doing it for targeted advertising purposes, warns Thompson », Danny BRADBURY, « Getting ready for GDPR » (24 avril 2017), en ligne : Canadian Lawyer Guide <http://www.canadianlawyermag.com/6418/Getting-ready-for-GDPR.html> (consulté le 7 juillet 2017).

électroniques[306] (« PIPEDA ») fut le résultat de cette réflexion[307]. Fait intéressant soulevé par le professeur Vincent Gautrais, le cœur de cette loi est en fait une annexe (l'annexe 1) et provient pour sa part d'un code qu'il qualifie de communautaire[308].

L'objectif de la loi est contenu en son article 3 et fait état de ce besoin de clarification dans un monde en constante évolution technique, mais suggère également la nécessité de mettre en balance le droit des individus à la vie privée et les besoins du secteur privé :

> **3.** La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Voyant le développement de la notion de vie privée comme une conséquence directe du développement des technologies, le professeur Trudel souligne que :

> [l] a notion de vie privée est apparue comme une catégorie juridique autonome [...] son importance s'est accrue dans plusieurs systèmes juridiques comme conséquence de la multiplication des technologies permettant de traiter toujours plus d'informations, rendant de ce fait possibles des intrusions ou divulgations autrefois inconcevables[309].

---

[306] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 [LPRPDE].

[307] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 87.

[308] Vincent GAUTRAIS, « Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle » (2004) 9:2 Lex Electronica à la p 6, en ligne : Lex Electronica <http://www.lex-electronica.org/articles/vol9/num2/le-defi-de-la-protection-de-la-vie-privee-face-aux-besoins-de-circulation-de-linformation-personnelle/>; *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96.

[309] Benoit Pelletier, « Droit constitutionnel: La protection de la vie privee au Canada » (2001) 35 La Revue Juridique Themis 485 à la p 486 citant ; Pierre TRUDEL et al, *Droit du cyberespace*, Montréal, Thémis, 1997 aux pp 11‑20.

Pour sa part, le Québec, par l'entremise de la *Charte des droits et libertés* [310](ci-après « CDLP ») (adoptée en 1975) en son article 5 ainsi que le *Code civil du Québec*[311] (ci-après « CcQ ») (adopté en 1991) aux articles 3, 35 et 36 élèvent expressément la vie privée au rang de droit protégé.

Parallèlement, de son côté, le Québec avait entamé une démarche similaire qui mena à l'adoption, dès 1993, de la *Loi sur la protection des renseignements personnels dans le secteur privé*[312] (ci-après « LPRPSP »). Cette loi fut la toute première en Amérique du Nord à encapsuler les obligations légales en matière de protection de renseignements personnels par les organisations privées[313]. Elle mit ensuite sur pied, en 2001, la *Loi concernant le cadre juridique des technologies de l'information*[314] (ci-après « LCCJTI »). À ce sujet, le professeur Pierre Trudel soutient que « le droit de la protection des données personnelles a été conçu pour protéger la vie privée contre les écueils que laissait craindre l'utilisation des technologies de l'information à des fins de surveillance »[315]. Comme élément du droit de la vie privée, les *données personnelles* ou renseignements personnels sembleraient donc avoir pour objectif

---

[310] « Toute personne a droit au respect de sa vie privée ». À noter que contrairement à la *Charte canadienne*, la Charte québécoise régit à la fois les rapports entre les personnes ainsi que les relations entre l'État et les personnes. *Charte des droits et libertés de la personne*, RLRQ c C-12, art 5 [CDLP]; Voir aussi Benoit Pelletier, « Droit constitutionnel: La protection de la vie privee au Canada » (2001) 35 La Revue Juridique Themis 485 à la p 495.

[311] *Code civil du Québec*, RLRQ c C-1991 [CcQ].

[312] Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1 [LPRPSP].

[313] Collin J BENNETT, Christopher A PARSONS et Adam MOLNAR, « Real and Substantial Connections: Enforcing Canadian Privacy Laws against American Social Networking Campaigns » (2014) 23 J L Inf & Sci 50 à la p 52.

[314] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-11 [LCCJTI].

[315] Pierre TRUDEL, « La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives » (2006) 61:7 Annales Des Télécommunications 950 à la p 953.

principal de faciliter la sauvegarde de la vie privée d'un individu. Ainsi, Trudel fait principalement référence au contrôle qu'un individu peut exercer sur ses données[316].

A. Protection des renseignements personnels et PCL

La protection des renseignements personnels en droit canadien repose donc largement sur l'application de PIPEDA et de la LCAP au niveau fédéral, ainsi que sur la LPRPSP, le CcQ et LCCJTI au Québec. D'autres provinces ont également adopté des lois encadrant la gestion des renseignements personnels, à savoir la Colombie-Britannique par l'adoption du *Personnal Information Protection Act (BC)*[317] (ci-après « PIPABC ») et l'Alberta avec le *Personnal Information Protection Act (Alberta)*[318] (ci-après « PIPAA »).

(i) Champ d'application

La loi fédérale PIPEDA s'applique sur l'ensemble du territoire canadien à l'exception des provinces disposant d'une loi sur la protection de la vie privée qui répond aux exigences de l'article 26 (2)[319], à savoir qu'elle doit être « essentiellement similaire » aux protections offertes par la loi fédérale. Par « essentiellement similaire », il semblerait que la loi doit offrir une protection également bonne, ou supérieure, sans quoi elle ne peut être similaire[320]. Ainsi,

---

[316] « [la] possibilité effective pour une personne de maîtriser la circulation de l'information la concernant » Pierre TRUDEL, « La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives » (2006) 61:7 Annales Des Télécommunications 950 à la p 954.

[317] *Personal Information Protection Act BC*, SBC 2003, c 63 [PIPABC].

[318] *Personal Information Protection Act Alberta*, SA 2003, c P-65 [PIPAA].

[319] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 [LPRPDE].

[320] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 97.

les provinces de l'Alberta, la Colombie-Britannique, l'Ontario (seulement en ce qui concerne les renseignements de santé en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*[321]) et le Québec bénéficient de l'exception de l'article 26 (2). Malgré l'exemption de l'application générale de PIPEDA, il importe de souligner qu'elle s'applique tout de même dans un contexte interprovincial ou international[322].

Nous retrouvons à l'article 4 de PIPEDA le champ d'application de la loi. Cet article stipule que :

> **4 (1)** La présente partie s'applique à toute organisation à l'égard des renseignements personnels
>
> a) soit qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales ;

Trois éléments clés se trouvent au cœur de l'article : (1) la loi s'applique à une organisation (2) elle vise les renseignements personnels et (3) elle concerne des activités commerciales. Il est donc clair que PIPEDA ne s'applique donc qu'aux entreprises engagées dans une activité commerciale[323]. Il faudra alors évaluer si la publicité comportementale est effectuée par une entreprise, dans le cadre d'une activité commerciale, afin de déterminer l'application de PIPEDA.

Or, la loi québécoise prévoit, en son article premier, qu'elle s'applique à toutes les entreprises du secteur privé, telle que définie à l'article 1525 al. 3 CcQ :

---

[321] *Loi de 2004 sur la protection des renseignements personnels sur la santé*, LO 2004, c 3, Annexe A; Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 99.

[322] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 97.

[323] « [A]ctivité commerciale : Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds. » *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 2(1) [LPRPDE].

> Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, **qu'elle soit ou non à caractère commercial**, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services[324] [notre emphase].

La PIPAA s'applique, quant à elle, à « *every organization and in respect of all personal* information »[325]. Finalement la PIPABC prévoit que cet « *Act applies to every organization* »[326], entendue comme incluant « *a person, an unincorporated association, a trade union, a trust or a not for profit organization* »[327]. En l'espèce, il importe peu de savoir si la publicité comportementale est faite dans le cadre d'une activité à caractère commercial pour permettre l'application de la LPRPSP, la PIPAA ou de la PIPABC.

(ii) Une question d'équilibre ?

À la lecture de PIPEDA, on peut aisément conclure que celle-ci cherche à établir un équilibre entre les droits des utilisateurs à la protection de leurs renseignements personnels, ainsi que les besoins de l'industrie d'avoir accès à des informations. L'article 3 se lit comme suit :

> La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte **du droit des individus à la vie privée à l'égard des renseignements personnels** qui les concernent et **du besoin des organisations de recueillir, d'utiliser**

---

[324] « Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services. » *Code civil du Québec*, RLRQ c C-1991, art 1525 al. 3 [CcQ].

[325] *Personal Information Protection Act Alberta*, SA 2003, c P-65, art 4(1) [PIPAA].

[326] *Personal Information Protection Act BC*, SBC 2003, c 63, art 3(1) [PIPABC].

[327] *Personal Information Protection Act BC*, SBC 2003, c 63, art 1 [PIPABC].

> **ou de communiquer des renseignements personnels** à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[328].

Cette proposition est tout de même tempérée par l'ajout de la mention voulant que les fins de cette cueillette, utilisation ou communication soit celles « [qu'une] personne raisonnable estimerait acceptables dans les circonstances »[329]. En d'autres termes, PIPEDA vise « à concilier le droit d'un individu à la vie privée et le besoin raisonnable qu'ont les organisations de recueillir, d'utiliser et de communiquer des renseignements à des fins économiques »[330].

De son côté, la loi québécoise a pour objectif de permettre la mise en exercice des droits conférés aux articles 35 à 40 CcQ[331]. Dans un discours prononcé en 1993, Lawrence Cannon, alors ministre des Communications, affirma que :

> [Le] Québec était mûr pour une loi qui protégerait les renseignements personnels détenus dans le secteur privé […] une telle législation ne devait pas freiner la compétitivité des entreprises du Québec. Bien au contraire, la législation québécoise devait permettre à nos entreprises d'échanger des renseignements personnels avec des firmes œuvrant dans des pays qui se sont donné des règles équivalentes de protection des renseignements personnels. L'intervention québécoise s'harmonisait alors avec les nombreux efforts qui sont faits sur le plan international, que ce soit à l'OCDE ou à la Communauté économique européenne, pour faciliter la circulation de données

---

[328] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 3 [LPRPDE].

[329] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 3 *in fine* [LPRPDE].

[330] Nancy HOLMES, *Les lois fédérales du Canada sur la protection de la vie privée*, PRB 07-44F, Division du droit et du gouvernement, 2008 à la p 6, en ligne : <https://lop.parl.ca/content/lop/researchpublications/prb0744-f.pdf> (consulté le 28 mai 2017).

[331] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 1 al. 1 [LPRPSP].

> personnelles tout en s'assurant que celles-ci soient protégées également d'un pays à l'autre[332].

Il semble donc y avoir une véritable intention d'établir une forme d'équilibre dans le développement de la législation québécoise en matière de protection des renseignements personnels.

Dans une perspective économique, les acteurs de l'industrie de la publicité comportementale soutiennent que si, dans les marchés traditionnels, l'échange de biens et services se concrétise par la remise d'une somme en argent, dans le marché virtuel, et relativement aux données personnelles, cet échange est généralement effectué sous forme de services fournis gratuitement. Pour cela, il n'y a qu'à penser aux principaux sites Internet qu'un internaute visitera dans une journée, qu'il s'agisse de médias sociaux, fournisseurs d'adresses courriel, moteurs de recherche ou plateformes de nouvelles[333]. Ainsi, le prix à payer pour l'internaute : la collecte de ses données. Sur l'échange que représente cette conciliation, la Commissaire à la vie privée Jennifer Stoddart souligna que :

> Les renseignements personnels sont devenus une devise importante dans l'économie actuelle. Les gens sont prêts à échanger une certaine quantité d'information pour obtenir les produits et services qu'ils désirent.
>
> Mais cet échange doit être **mesuré et juste**[334]**.**

---

[332] ASSEMBLÉE NATIONALE DU QUÉBEC, *Journal des débats de la Commission de la culture, 34e législature, 2e session (19 mars 1992 au 10 mars 1994) Le mardi 23 février 1993 - Vol. 32 N° 11*, février 1993, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cc-34-2/journal-debats/CC-930223.html> (consulté le 28 mai 2017).

[333] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, « The Value of Personal Information: Evidence from Empirical Economic studies » (2012) 1:88 Communications & Strategies 41 aux pp 44‑45.

[334] Jennifer STODDART, « Discours: Sécurité et protection de la vie privée : Protéger l'information dans un monde transparent » (juin 2011), en ligne : Commissariat à la protection de la vie privée du Canada <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2011/sp-d_20110601/> (consulté le 28 mai 2017).

Bien que cette notion d'équilibre est controversée, il nous apparaît nécessaire de la souligner, car elle semble bien être la pierre d'assise sur laquelle sont fondées les lois canadiennes protégeant les relations entre consommateurs et entreprises. En effet, comme société nous savons accepter qu'il existe une forme d'échange entre les droits des consommateurs et les besoins des entreprises. Celles-ci se nourrissent des informations des consommateurs et en retour les consommateurs reçoivent des produits, publicités et autres qui leur ressemblent, ou que l'on souhaite leur imposer.

Evans soutient que le marché des renseignements personnels en est un de compétition en ce que les intermédiaires de la publicité compétitionnent à la fois pour acquérir les annonceurs et les consommateurs[335] — par l'exposition d'une publicité qui leur conviendra. Il soutient à cet égard que si un marché du renseignement leur était ouvert, et s'ils avaient conscience de la valeur de celui-ci, les consommateurs pourraient prendre part au processus décisionnel et transactionnel, en rendant accessibles certaines informations personnelles et la vendant au plus offrant[336]. À cet égard, une étude réalisée en 2013 concluait que l'utilisateur moyen évaluait son historique de navigation à environ 7 euros, alors que les informations telles que l'âge et l'adresse étaient considérées comme ayant une valeur supérieure, atteignant environ 25 euros[337]. Les auteurs notaient tout de même, et plus particulièrement que la valorisation variait selon le contexte de la navigation.

---

[335] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 57.

[336] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 56; Dans un manifeste intitulé « Who owns the Future? », « prophète du digital » appelle à une changement du monde digital : « a shift away from the few at the top making huge sums from the masses, by monetising the information we currently hand over for free » « Jaron Lanier on how to make the internet pay » (4 mars 2013), en ligne : Channel 4 News <https://www.channel4.com/news/jaron-lanier-on-how-to-make-the-internet-pay> (consulté le 28 avril 2017).

[337] Juan Pablo CARRASCAL et al, *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, *Proceedings of the 22nd International Conference on World Wide Web*, coll WWW '13, New York, NY, USA, ACM, 2013, 189 à la p 189, DOI : 10.1145/2488388.2488406.

Lors de leurs visites en ligne, les utilisateurs devraient prendre en compte les risques inhérents, tels que la perte, le vol ou la distribution des renseignements personnels afin de faire le choix ou non de les divulguer[338]. Ce choix existe déjà et des utilisateurs avertis évitent, ou non, certains sites Internet, adoptent des pratiques de protection des renseignements privés comme la suppression des témoins, la navigation incognito et autres moyens. Or, Evans insiste sur trois facteurs qui rendent difficile le délicat exercice de conciliation entre vie privée (« privacy ») et publicité ciblée. Premièrement, les utilisateurs ne sont pas conscients que leurs renseignements personnels sont collectés et sauvegardés. Deuxièmement, les utilisateurs peuvent accepter de divulguer leurs informations (tacitement ou expressément) sans nécessairement prendre en compte la possibilité que celles-ci soient vendues à des tiers qui les combineraient à d'autres informations à leur sujet. Troisièmement, il s'agit d'un milieu compétitif, où de nombreux acteurs sont présents. La publicité en ligne implique plusieurs intermédiaires sur différentes plateformes qui se livrent à une compétition tant pour la vente et l'achat de données, que pour l'acquisition et la vente de publicité[339].

Roger Allan Ford avance que la collecte des données est souvent une décision prise unilatéralement par une tierce partie[340]. Il estime qu'il en est ainsi pour différentes raisons. D'abord, de nombreux individus ignoreraient qu'ils sont suivis et que leurs informations sont emmagasinées[341], alors que d'autres ne seraient que partiellement sensibilisés à cette pratique[342]. Ensuite, il souligne que même si de nombreux utilisateurs sont au courant des

---

[338] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 56.

[339] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 57.

[340] Roger Allan FORD, « Unilateral invasions of privacy » (2015) 91 Notre Dame L Rev 1075 à la p 1094.

[341] Roger Allan FORD, « Unilateral invasions of privacy » (2015) 91 Notre Dame L Rev 1075 à la p 1094. Plus précisément voir ci-dessus notre discussion à la Partie 2, Chapitre 1, Section 1 (A) « Méconnaissance de la publicité comportementale ».

[342] Roger Allan FORD, « Unilateral invasions of privacy » (2015) 91 Notre Dame L Rev 1075 à la p 1095.

pratiques de collecte de leurs données, ils n'ont aucune idée de ce qui doit être fait pour préserver leurs informations[343]. De manière critique, il se demande donc comment, dans de telles circonstances, les individus pourraient avoir un quelconque choix[344] dans ce processus qui laisse le champ libre à une décision unilatérale de la circulation des informations personnelles aux agrégateurs de données.

B. Quelle est cette donnée qu'on ne saurait cacher ?

Il semble à présent clair que les lois trouvent une application directe s'il y a transmission d'informations identifiables à des tiers (telles que le nom, l'adresse courriel et ainsi de suite). Il apparaît maintenant nécessaire de procéder à la qualification du renseignement. Il importe alors de se demander s'il existe un risque que le renseignement, combiné à un autre, résulte en la création de profils détaillés ou facilement identifiables.

Ainsi, il nous apparaît nécessaire, en guise de première étape, de déterminer la nature de la donnée. Une question s'impose alors : s'agit-il d'un renseignement personnel ? L'*Office québécois de la langue française* énonce : qu'un renseignement personnel « [**porte] sur un individu** et [**permet**] **d'établir son identité**. »[345]. PIPEDA définit en son article 2 (1) le « renseignement personnel » comme étant : « tout renseignement concernant un **individu identifiable,** à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse

---

[343] Roger Allan FORD, « Unilateral invasions of privacy » (2015) 91 Notre Dame L Rev 1075 à la p 1095.

[344] Voir ci-dessus notre discussion à la Partie 2, Chapitre 1, Section 1 (A) « Méconnaissance de la publicité comportementale ». Concernant les différentes problématiques lié à la volonté des individus, voir les techniques employés par l'industrie de la publicité comportementale au chapitre préliminaire, Section 3, intitulé « Technologies du ciblage ». Les différentes technologies sur lesquelles reposent la PCL rendent l'exercice d'une autonomie citoyenne difficile à mettre en pratique.

[345] Office québécois de la langue française, 2005, *sub verbo* « Renseignements personnels », en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8398805> (consulté le 28 juillet 2017).

et numéro de téléphone de son lieu de travail »[346]. La loi québécoise, pour sa part, établie qu' « [est] un renseignement personnel, tout renseignement qui concerne une **personne physique** et **permet de l'identifier** »[347]. Si la PIPEDA vise expressément les documents électroniques, notons que la LPRPSP prévoit à l'art 1 al. 2 qu' « [elle] s'applique à ces renseignements 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 autre ».

De ces définitions, il est alors possible d'identifier deux éléments clés, à savoir, le renseignement porte sur une « personne physique » et « permet son identification ». Cette notion est importante, car elle supporte l'idée d'une distinction entre deux individus.

Il ressort de ces définitions un risque d'identification d'un individu à partir d'un renseignement donné, et ce, peu importe le moyen par lequel l'identification a lieu. À cet égard, la Cour fédérale eut l'occasion de se prononcer sur la notion de « renseignements concernant un individu » dans l'affaire *Rousseau c Wyndowe*[348]. Comme le souligne le juge Teitelbaum, cette affaire marque la première décision rendue sur la base de la PIPEDA et tente d'interpréter la notion de renseignements personnels. S'appuyant sur la LPRP, il souligne d'emblée que le renseignement personnel sous PIPEDA doit être interprété de manière à englober la définition de la LPRP[349], assez large pour y inclure d'autres renseignements, à l'exception de ceux qui sont « véritablement anonymes », échappant dès lors à la qualification de personnel[350].

---

[346] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 2(1) [LPRPDE].

[347] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 2 [LPRPSP].

[348] *Rousseau c Wyndowe*, 2006 CF 1312.

[349] *Rousseau c Wyndowe*, 2006 CF 1312 au para 30.

[350] *Rousseau c Wyndowe*, 2006 CF 1312 aux paras 31‑32.

Or, cette définition est loin de plaire à tous. En effet, les professeurs Trudel et Benyekhlef évoquaient que le caractère large de la définition de renseignements personnels risquait d'entraîner des conséquences fâcheuses, puisque « [la] loi ne vise donc pas seulement les renseignements susceptibles de concerner la vie privée d'une personne, mais la **totalité des renseignements susceptibles de l'identifier** »[351]. Ils soulignent que c'est probablement en raison de la possibilité d'agglomération de renseignements que la définition s'est vue acquérir une portée si large et englobante.

À cet effet, en 2008, la Cour fédérale eut à nouveau à se pencher sur la définition du renseignement personnel et conclut dans l'affaire *Gordon c Canada* que :

> Les renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de **fortes possibilités que l'individu puisse être identifié** par l'utilisation de ces renseignements, **seuls ou en combinaison avec des renseignements d'autres sources**[352].

Le juge Gibson souligne dès lors, que la combinaison de renseignements (tels que ceux contenus dans un profil utilisateur par exemple) peut engendrer la qualification de personnels, dans la mesure, où mis ensembles, ils augmentent le risque d'identification de l'individu. Dans cette affaire, il était question d'un renseignement contenu dans le champ « province » d'un dossier et la divulgation de cette information portait un risque à l'identification de la personne s'il était aggloméré à des informations publiquement accessibles[353].

Une question émerge dès lors, quels sont ces renseignements pouvant être agglomérés afin d'évoluer au rang de renseignements personnels ? Les données recueillies dans le cadre d'un programme de publicité comportementale sont variées, allant de l'adresse IP, à la géolocalisation, en passant par l'historique de navigation jusqu'à la configuration du

---

[351] Pierre TRUDEL et Karim BENYEKHLEF, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Rapport / Report, CAI, 1997 à la p 3, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/71> (consulté le 26 mai 2017).

[352] *Gordon c Canada*, 2008 CF 258 au para 34.

[353] *Gordon c Canada*, 2008 CF 258 aux paras 43‑47.

navigateur. En la matière, le *Commissariat à la protection de la vie privée du Canada* soutient qu'une adresse IP constitue un renseignement personnel lorsqu'il peut être associé avec un individu[354].

Comme le souligne à juste titre Éloïse Gratton, les adresses IP, tout comme les témoins de connexion, peuvent devenir un véritable casse-tête lorsque l'on tente de déterminer s'ils sont ou non des renseignements personnels. S'il est vrai que les témoins de connexion ne renferment pas systématiquement d'informations personnellement identifiables et restent relativement anonymes, ceux-ci sont susceptibles de transmettre un certain nombre d'informations, qui une fois agglomérées, permettent l'identification[355]. Or, le commissaire à

---

[354] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 105; Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2001-25 Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2001/lprpde-2001-025/> (consulté le 2 avril 2016); Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-315 Mesures de sécurité d'une société Internet et traitement d'une demande d'accès à l'information et d'une plainte relative à la protection des renseignements personnels mis en doute*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-315/> (consulté le 2 avril 2016); Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-319 Mesures anti-pourriel du FSI contestées*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-319/> (consulté le 2 avril 2016); Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-010 La commissaire adjointe recommande à Bell Canada d'informer les clients au sujet de l'inspection approfondie des paquets*, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/2009_010_rep_0813/> (consulté le 2 avril 2016).

[355] Eloïse GRATTON, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, CCH Canadian Limited, 2003 à la p 46.

la vie privée a conclu que « les renseignements emmagasinés par les témoins temporaires et permanents constituaient des renseignements personnels aux fins de la Loi »[356].

En outre, Éloïse Gratton soulève qu'un appareil peut être utilisé par plus d'un individu et qu'il est souvent très difficile d'identifier un individu correctement[357]. À cet égard, Scassa et Deturbide soulignent que malgré l'utilisation par plusieurs individus d'un appareil, celui-ci reste tout de même largement attaché à son propriétaire[358].

Bien que les définitions proposées dans les lois concernées soient très larges, il nous apparaît important que son interprétation le soit tout autant afin de s'assurer que les renseignements personnels collectés dans la création d'un profil d'utilisateur entrent dans le spectre des lois en la matière.

À cet égard aux États-Unis, Schwartz et Solove soulignent que le FTC joue un rôle essentiel dans la détermination de ce qu'est un renseignement identifiable ou non, et que la tendance actuelle se maintient vers un élargissement de la définition[359].

Dans cette perspective, Chung rappelle une étude réalisée par Latanya Sweeney démontrant que le caractère anonyme de ces renseignements le serait seulement en apparence. En effet, les résultats révèlent que « *87.1% of people in the United States can be identified by the combination of their ZIP code, birth date and gender. More significantly, her study*

---

[356] Commissariat à la protection de la vie privée du Canada, *Un client se plaint de la présence de « témoins » sur le site Web d'une compagnie aérienne, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2003-162*, Conclusion #162, Commissariat à la protection de la vie privée du Canada, 2003, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-162/>.

[357] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299 à la p 300.

[358] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 105.

[359] Paul SCHWARTZ et Daniel SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814 à la p 1876.

showed that even less-specific data combinations such as city, birth date and sex can identify 53% of United States citizens »[360]. Ainsi, même si elles semblent banales, ces trois informations censées être anonymes rendent plutôt simple l'identification d'un individu[361]. Pour cette raison, Reidenberg compare le processus de combinaison d'informations disparates et à l'apparence inoffensive à la création d'une nudité technologique, permettant de défier la barrière entre le public et le privé[362]. Sans nous étendre trop longuement sur la question, nous trouvons intéressants de soulever que Reidenberg s'interroge même sur l'impact social que peut avoir cette translucidité individuelle constamment accrue et qu'il soulève les dangers qu'elle suppose dans un contexte démocratique fondé sur l'État de droit[363]. Après tout, comme le rappelle Cohen, les juristes sont souvent frileux quand vient le temps d'aborder la relation entre la surveillance et l'État de droit, même s'il s'agit d'une question fondamentale qui ne doit nullement être négligée dans nos sociétés démocratiques[364].

Il serait alors facile de soutenir que la définition large des données à caractères personnelles limite les possibilités pour les commerçants. Or, le risque inhérent à une interprétation restrictive réside dans la facilité avec laquelle on peut parvenir à identifier un individu.

---

[360] Yuen Yi CHUNG, « Goodbye PII: Contextual Regulations For Online Behavioral Targeting » (2014) XIV:2 J High Tech L 414 à la p 424; Paul OHM, « Broken promises of privacy: responding to the surprising failure of anonymization » (2010) 57:6 UCLA Law Review 1701 à la p 1719.

[361] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 448.

[362] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 aux pp 448‑449.

[363] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 aux pp 448‑449.

[364] Julie COHEN, « Studying Law Studying Surveillance » (2014) 13:1 Surveillance & Society 91 à la p 92.

Section 2 — Examen de l'application des lois dans le cadre de PCL

Nous sommes à présent enclins à conclure à l'application des lois en matière de protection des renseignements personnels dans le cadre de la collecte de données aux fins de publicité comportementale. Dans la présente section, nous explorerons tout d'abord (A) les limites légales à la collecte, (B) la notion de consentement, (C) la collecte dans le contexte de gratuité et (D) l'autoréglementation comme solution.

A. Limites légales à la collecte

Si la loi autorise la collecte de renseignements personnels, elle cherche inévitablement à encadrer cette pratique. Nous explorerons donc immédiatement les différentes limites imposées à la collecte tant par PIPEDA que la LPRPSP.

(i) Identification de la finalité et PCL

Suivant le principe 4.2 de PIPEDA, l'organisation doit déterminer l'objectif de la collecte des renseignements personnels. À cet effet, la détermination de ces objectifs doit précéder la collecte. Elle est en outre soumise à d'autres conditions, à savoir que la finalité doit être documentée dans une perspective de transparence[365].

La condition est similaire du côté du Québec :

> 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**

[365] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4.2.1 [LPRPDE].

spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé[366].

Ainsi les deux articles évoquent la même nécessité de détermination de la finalité. Or, dans le cas de la loi fédérale, celle-ci précise le moment où l'objectif doit être déterminé, soit au plus tard avant la collecte[367]. La loi québécoise pour sa part ne précise pas le moment où l'utilisateur doit être informé, mais puisqu'elle requiert (elle aussi) le consentement (« manifeste, libre, éclairé ») de l'utilisateur, elle ne saurait se produire après la collecte.

Or, dans le contexte de la publicité comportementale, nous l'avons indiqué[368], il s'agit la plupart du temps, de tierces parties qui collectent l'information et non pas les éditeurs de contenu. Dès lors, comment affirmer que l'utilisateur a été adéquatement informé de la collecte et des finalités de celle-ci ?

Sur cette question, l'article 6 de la LPRPSP prévoit que « [la] personne qui recueille des renseignements personnels sur autrui doit les recueillir auprès de la personne concernée, à moins que celle-ci ne consente à la cueillette auprès de tiers ». La tierce partie qui voudra collecter des données sur un individu devra dès lors obtenir non seulement son consentement, mais informer celui-ci. PIPEDA prévoit, en son article 4.3.7 (b), qu'une organisation, à moins d'avis contraire, peut inférer de l'inaction d'un utilisateur qu'il consent. Cependant, comment justifier que celui-ci aura été adéquatement informé des finalités de la collecte ? Cette déclaration semble à notre avis être porteuse de bien peu d'information et porte à confusion. Si l'article 4.2 prévoit que « [les] fins auxquelles des renseignements personnels sont recueillis **doivent être déterminées par l'organisation** avant la collecte ou au moment de celle-ci »,

---

[366] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 14 [LPRPSP].

[367] « Organizations must identify the purposes for which they intend to use individuals' personal information no later than the time of collection » Christopher SCOTT, « Our Digital Selves: Privacy Issues in Online Behavioural Advertising » (2013) 17:1 Appeal: Review of Current Law and Law Reform 63 à la p 72.

[368] Voir chapitre préliminaire, section 2 « Industrie du ciblage ».

c'est donc à celle-ci qu'incombe l'obligation d'informer. En outre, le principe 4.9 prévoit qu' « [une] organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter ».

En l'espèce, nous pouvons inférer de ces articles que l'organisation collectrice est responsable d'informer les internautes de la collecte de leurs renseignements. Sur Internet, cette divulgation prend souvent la forme d'une « politique de confidentialité » ou « politique d'utilisation » que l'on retrouve la plupart du temps dans un menu en bas de page. Or, il existe plusieurs problématiques relativement à ces politiques, souvent en lien avec leur précision et leur clarté, comme il a été soulevé par les professeurs Gautrais[369] et Reidenberg (et al.)[370]. Gautrais souligne d'abord qu'il est fondamental qu'elles fournissent à l'utilisateur « toute l'information dont il peut avoir besoin »[371], en évitant pour autant « l'accumulation de textes à l'infini »[372], pratique ayant pour effet de diluer l'information. Il s'interroge ainsi sur la validité des politiques d'utilisation si volumineuses qu'elles rendent impossible pour l'utilisateur de savoir à quoi son utilisation l'engage[373]. Reidenberg (et al.) soulignent, quant à eux, l'importance que ces politiques soient rédigées dans un langage précis, car si elles sont trop ambiguës, elles risquent de cacher les pratiques concernant la collecte de données sur le site en

---

[369] Vincent GAUTRAIS, « La protection du « cyberconsommateur » selon le droit québécois » dans Vincent Gautrais, dir, *Le droit du commerce électronique*, Montréal, Thémis, 2002.

[370] Joel R REIDENBERG et al, « Ambiguity in Privacy Policies and the Impact of Regulation » (2016) 45:S2 J Legal Stud S163.

[371] Vincent GAUTRAIS, « La protection du « cyberconsommateur » selon le droit québécois » dans Vincent Gautrais, dir, *Le droit du commerce électronique*, Montréal, Thémis, 2002 aux pp 267‑268.

[372] Vincent GAUTRAIS, « La protection du « cyberconsommateur » selon le droit québécois » dans Vincent Gautrais, dir, *Le droit du commerce électronique*, Montréal, Thémis, 2002 aux pp 267‑268.

[373] Vincent GAUTRAIS, « La protection du « cyberconsommateur » selon le droit québécois » dans Vincent Gautrais, dir, *Le droit du commerce électronique*, Montréal, Thémis, 2002 à la p 268.

question et d'échouer à donner aux utilisateurs l'information juste et complète du traitement qu'il y est fait de leurs données personnelles[374].

Ainsi, nous soutenons qu'à défaut d'informer les utilisateurs des différentes tierces parties qui sont susceptibles de placer un témoin, ou de recueillir des renseignements personnels sur un site Internet donné, tant l'éditeur de contenu que la tierce partie échouent dans leur obligation d'informer les internautes, laissant ceux-ci dans l'incapacité de se renseigner sur les pratiques ou utilisations de leurs données.

(ii) Une collecte nécessaire en vue de la PCL

Les lois canadienne et québécoise, à l'instar de la majorité des lois encadrant la protection des données[375], s'appuient sur la collecte d'informations « nécessaires ».

PIPEDA prévoit que :

> [une] 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[376].

Du côté du Québec, la LPRPSP prévoit à l'article 5 LPRPSP que seuls les renseignements *nécessaires* peuvent faire l'objet d'une collecte.

---

[374] Joel R REIDENBERG et al, « Ambiguity in Privacy Policies and the Impact of Regulation » (2016) 45:S2 J Legal Stud S163 à la p S185.

[375] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299 à la p 308.

[376] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4.3.3 [LPRPDE].

> La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les **renseignements nécessaires** à l'objet du dossier[377].

L'article 9, quant à lui prévoit que :

> [nul] ne peut refuser d'acquiescer à une demande de bien ou de service […] à cause du refus de la personne qui formule la demande de lui fournir un renseignement personnel sauf [lorsque] la collecte est **nécessaire à la conclusion ou à l'exécution du contrat**[378].

Lorsque le critère de nécessité n'est pas rempli ou qu'il subsiste un doute sur la nécessité de la collecte, il semble qu'elle soit alors réputée comme non nécessaire[379]. La PCL ne semble pas être en mesure de respecter ce critère de nécessité, puisqu'à défaut d'offrir une publicité comportementale, un site internet pourrait toujours offrir une publicité générale.

(iii) PCL et attentes raisonnables

Une autre limite au droit de collecte par le secteur privé émane de la rédaction de l'article 4.3.5 PIPEDA. En effet, celui-ci précise qu'il importe de prendre en considération les attentes *raisonnables* de l'utilisateur. Or, quelles sont ces attentes raisonnables ? Dans l'affaire *R c Spencer*, la Cour suprême a conclu qu'il était raisonnable qu'un utilisateur s'attende au respect de sa vie privée en ligne.

> À mon avis, compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La communication de ces renseignements permettra souvent

---

[377] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 5 [LPRPSP].

[378] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 9 [LPRPSP].

[379] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-391, art 9 *in fine* [LPRPSP].

> d'identifier l'utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes[380].

Finalement, une ultime limite à la collecte résiderait dans la sous-section 5 (3) PIPEDA, voulant qu'elle se fasse à des fins qu'une personne raisonnable jugerait appropriées dans les circonstances. Or, l'application *in concreto* de ce critère semble représenter un défi[381]. Dans l'affaire *Turner c Telus*[382], la Cour fédérale a été appelée à trancher sur la qualification des caractéristiques de la voix comme renseignements personnels ; elle s'exprima ainsi :

> La protection de la vie privée est une notion variable et évolutive, c'est-à-dire « protéiforme ». Les droits en matière de vie privée ne sont ni absolus ni insignifiants. Situés entre ces deux extrêmes, ils varient selon le contexte factuel dans lequel s'inscrit leur examen[383].

Cette décision rendue par le juge Gibson souligna alors que le critère « d'approprié selon les circonstances », devait prendre en considération différents facteurs, dont notamment le degré de sensibilité des données, l'objectif légitime de l'entreprise et les mesures de sécurité mises en place[384].

En outre, il ne s'agit pas de déterminer si les fins de la collecte, de l'utilisation et de la communication sont acceptables, mais bien si chacune des finalités le sont. Ainsi, « [les] fins acceptables de la collecte peuvent différer des fins acceptables de l'utilisation et des fins acceptables de la communication des renseignements recueillis, ce qui laisse supposer une flexibilité et une variabilité en fonction des circonstances »[385].

---

[380] *R c Spencer*, [2014] 2 RCS 212 (CSC) à la p 66.

[381] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 126.

[382] *Turner c Telus Communications Inc*, 2005 CF 1601.

[383] *Turner c Telus Communications Inc*, 2005 CF 1601 au para 41.

[384] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 126.

[385] *Eastmond c Canadien Pacifique Ltée*, 2004 CF 852 au para 131.

B. Une collecte qui repose sur le consentement

S'il appert légitime de « recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances », la contrepartie reposerait inévitablement sur le consentement de l'utilisateur. C'est donc en son article 4.3 que PIPEDA prévoit les obligations de consentement licite à la collecte. En effet, sous réserve des exceptions de l'article 7, l'organisation est tenue d'obtenir le consentement de l'internaute dans le cas de la collecte de ses renseignements personnels.

> The consent that an individual gives to the collection of his or her personal information must be for purposes that are clearly specified. […] The purpose for which consent is being sought **must also be reasonable**[386].

Dans cet esprit, l'article 4.3.2 PIPEDA exige que l'utilisateur soit informé des fins auxquelles l'information sera utilisée, afin de donner pleine valeur à son consentement. En outre, l'organisation a une obligation de faire des efforts raisonnables pour documenter les fins de la collecte. À cet effet, la commissaire Elizabeth Denham s'exprima :

> je suis préoccupée à l'idée qu'à certains égards, Facebook ne fait pas des **efforts raisonnable**s, conformément au principe 4.3.2, pour documenter, préciser et expliquer les fins de la collecte de la date de naissance des utilisateurs […] Le principe 4.3.3 stipule que les fins doivent non seulement être légitimes, mais « **explicitement indiquées** »[387].

Au Québec, le consentement à la collecte repose sur l'article 14 LPRPSP qui exige que le consentement soit « manifeste, libre, éclairé et [donné] à des fins spécifiques ». Ce type de consentement semble en être un qui nécessite un consentement explicite.

---

[386] Teresa SCASSA et Michael Eugene DETURBIDE, dir, *Electronic commerce and internet law in Canada*, 2e éd, Toronto, CCH Canadian, 2012 à la p 136.

[387] Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques* aux paras 50‑51, en ligne : <https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.asp> (consulté le 2 avril 2016).

Du côté de la loi fédérale, la forme de consentement pourra varier selon les circonstances. En effet, l'article 4.3.4 PIPEDA prévoit qu'elle pourra être influencée à la fois par les circonstances et par la nature des renseignements qu'elle collecte. Pour se faire, il faudra prendre en compte le degré de sensibilité des données. L'article prévoit en outre que certains types de renseignements auront *de facto* le statut de renseignements sensibles[388]. L'article 4.3.6 PIPEDA confirme le degré variable du consentement, soulignant que « [en] général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant »[389].

Le Commissariat a eu l'occasion de se prononcer sur le type de consentement exigé lors de l'application de la PIPEDA en matière de publicité comportementale et souligna qu'il :

> [était] d'avis que le consentement explicite (aussi appelé « consentement positif ») est nécessaire pour la diffusion de PCL. Comme il est indiqué dans nos lignes directrices sur la PCL, le consentement implicite (aussi appelé « consentement négatif ») à des fins de publicité comportementale peut être acceptable si les renseignements recueillis et utilisés se limitent, dans la mesure du possible, aux renseignements non sensibles (éviter les renseignements sensibles comme les renseignements médicaux et les renseignements sur l'état de santé)[390].

Ce consentement serait donc suffisant pour la plupart des données, considérées comme non sensibles. On serait alors tenté de se demander si la notion de consentement, qu'il soit

---

[388] « Si 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 » *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4.3.4 [LPRPDE].

[389] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4.3.6 [LPRPDE].

[390] Commissariat à la protection de la vie privée, *Rapport des conclusions en vertu de la LPRPDE no 2014-001, 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*, 2014 au para 27, en ligne : <http://canlii.ca/t/g2wr8> (consulté le 7 juillet 2017).

manifeste ou exprès, est adaptée aux réalités d'Internet. En effet, **comment parvenir à déterminer si le consentement de l'utilisateur est éclairé dans un univers où tout se passe à une vitesse impressionnante ?**

Une question se pose dès lors : est-ce que l'utilisateur a consenti au moment où la collecte a débuté ? À quel moment sont déposés les témoins et qu'arrive-t-il si un utilisateur ne consent pas, ou ne souhaite pas consentir à la collecte de ses informations ? Il semble dès lors que la seule option envisageable soit celle de retirer son consentement, par l'effacement des témoins. Cependant, nous l'avons mentionné, les moyens de traque sont développés et il existe des technologies, telles que le témoin Flash, qui permettent la régénération des témoins supprimés[391]. Qui plus est, les technologiques d'empreintes numériques et d'inspection des paquets profonds ne semblent que très peu se soucier du consentement[392], puisqu'il n'existe pas de manière valable de le retirer.

À ce propos, Angela Daly soulève les dangers liés à l'utilisation de la technologie d'IAP, si les témoins permettent de collecter un certain nombre de renseignements prédéterminer, l'IAP, quant à lui, rend accessible l'ensemble de l'utilisation Internet d'un utilisateur « *everything that a user is doing on the Internet is accessible via DPI* »[393]. Dès lors l'on pourrait se demander si le débat entourant le consentement, ou l'utilisation de témoins traceurs n'en est pas un qui soit déjà réglé par la prolifération d'une nouvelle technologie de surveillance omniprésente et d'autant plus invisible.

---

[391] Nous traitons particulièrement des difficultés posés par les témoins Flash au chapitre préliminaire, section 3 « Technologies du ciblage ».

[392] Tel que mentionné au chapitre préliminaire, section 3, les technologies reposant sur l'empreinte numérique et de l'inspection des paquets profonds ont lieu, non seulement en l'absence de tout consentement, mais également elles ont lieu à l'insu des individus.

[393] Angela DALY, *The Legality of Deep Packet Inspection*, University of Glasgow, First Interdisciplinary Workshop on Communications Policy and Regulation « Communications and Competition Law and Policy – Challenges of the New Decade », 17 juin 2010 à la p 6, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).

Une autre question émerge : un site Internet peut-il *forcer* un utilisateur à accepter les témoins de connexion, à défaut de quoi il ne pourra accéder au contenu ? Les articles 4.3.3 PIPEDA et 9 LPRPSP indiquent qu'il est interdit de refuser de fournir un service à un individu qui refuse la collecte de ses renseignements personnels[394].

En vertu de cet article, l'organisation ne pourrait interdire l'accès à un site Internet pour motif que l'utilisateur ne consent pas à la collecte de ses renseignements. Il faut dès lors déterminer les fins de la collecte et de l'utilisation des renseignements personnels afin de déterminer si celles-ci sont légitimes et explicites. Dans le cas en l'espèce, nous pouvons en déduire que l'intérêt réside dans le fait que l'on souhaite exposer un utilisateur à une publicité. Bien que cette fin soit légitime en soi, lorsque la publicité est comportementale, elle nous apparaît difficilement conciliable avec l'intérêt du consommateur. L'intérêt de la publicité comportementale, nous l'avons dit, est de mieux cibler le consommateur. Mais quoi faire si celui-ci ne veut pas être ciblé ? Nous soutenons qu'il serait plus approprié de laisser un véritable choix et ainsi laisser le consommateur fournir un véritable consentement. Si celui-ci refuse, les fins de publicité peuvent être accomplies par d'autres moyens, notamment celui de ne fournir qu'une publicité générique et non ciblée.

> **9. Nul ne peut refuser d'acquiescer** à une demande de bien ou de service ni à une demande relative à un emploi **à cause du refus** de la personne qui formule la demande de lui fournir un renseignement personnel sauf dans l'une ou l'autre des circonstances suivantes :
>
> 1° la collecte est nécessaire à la conclusion ou à l'exécution du contrat ;
>
> 2° la collecte est autorisée par la loi ;
>
> 3° il y a des motifs raisonnables de croire qu'une telle demande n'est pas licite.

---

[394] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4.3.3 [LPRPDE].

La Directive 2002/58/CE du Parlement européen[395] est fondée sur une obligation proactive d'informer adéquatement les utilisateurs, tout en leur offrant immédiatement un choix. Ainsi, « the ePrivacy Directive lays down specific requirements for the legitimate use of cookies, requiring that the user or the subscriber is properly informed about the use of cookies and that the consent of the user or the subscriber is provided before their installation and use »[396]. Suivant cette pratique, l'internaute est informé au moment d'arriver sur la page internet qu'un témoin traceur sera installé. Bien que cette pratique soit plus proactive que l'approche canadienne, où cette même information est généralement enterrée dans une interminable page de politiques d'utilisation et de vie privée, l'utilisateur ne possède aucun choix.

Aux États-Unis, la FTC, organisme de régulation du commerce, a pour sa part émis des lignes directrices en 2009 concernant la publicité comportementale. Essentiellement elle prévoit quatre grands principes :

> First, Web sites should provide clear and conspicuous notice of behavioral advertising, and a simple way for consumers to choose whether to participate. In announcing this principle, the FTC criticized typical posted privacy policies as "long and difficult to understand," and urged companies to do better. Second, companies should provide reasonable security for data they collect for behavioral advertising and retain it only as long as necessary to fulfill legitimate business needs. Third, changes in behavioral advertising policies should be given prominent notice that includes a consumer opt-out choice. The fourth principle reflects heightened concern with sensitive information, including that pertaining to health, finances, or children, and urges companies to obtain express consent before collecting it
>
> The FTC's approach is part of an international trend. In a recent speech, the European Union's consumer affairs commissioner criticized many companies' behavioral advertising policies as hard to understand, with consumer opt-out provisions too difficult to find. She singled out Facebook for its practice of sharing data with

---

[395] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, [2002] JO L201.

[396] Ronald LEENES et Eleni KOSTA, « Taming the cookie monster with Dutch law – A tale of regulatory failure » (2015) 31:3 CLSR 317 à la p 318.

> commercial partners that are not bound by its policies, and hinted that more aggressive law enforcement is coming. In apparent anticipation of such a development, a consortium of British Internet advertisers has adopted "best practices" guidelines that look very much like the FTC's principles[397].

Ainsi, il est intéressant de constater que la FTC appelle à un encadrement de la PCL qui requerrait un consentement exprès de la part des utilisateurs avant de pouvoir collecter leurs informations, de même qu'une possibilité d'opting-out pour ceux qui refuseraient la traque.

C. La collecte dans un contexte gratuit

Alors qu'on aurait tendance à se demander pourquoi tolérer la traque, une réponse semble s'imposer. Plusieurs services en ligne sont offerts gratuitement, à condition d'accepter d'y laisser quelques informations personnelles[398]. Or, ces données sont une véritable mine d'or pour les entreprises offrant ces services. En effet, les revenus de *Facebook* par utilisateur s'élevaient à 12.76 $ US en 2015, et ceux de Twitter à 7.75 $ US[399]. Toutefois, même si la collecte de données permet de soutenir financièrement certains services gratuits, ceux-ci doivent tout de même se conformer aux règles en matière de droit à la vie privée.

---

[397] John M CONLEY, « Behavioral Advertising: The Next Frontier for Privacy Law? » (avril 2009), en ligne : Robinson Bradshaw Publication <http://www.robinsonbradshaw.com/newsroom-publications-Behavioral-Advertising-The-Next-Frontier-for-Privacy-Law-04-23-2009.html> (consulté le 11 décembre 2016).

[398] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299 à la p 299.

[399] Alex HERN, « Facebook is making more and more money from you. Should you be paid for it? » (25 septembre 2015), en ligne : The Guardian <https://www.theguardian.com/technology/2015/sep/25/facebook-money-advertising-revenue-should-you-be-paid> (consulté le 28 mars 2016), selon l'auteur « advertisers [are] paying more to sell products on social networks, and social networks working out more ways to show you adverts » ce qui explique la valeur de cette industrie.

On peut dès lors procéder au constat suivant : l'application des lois concernant la collecte de renseignements personnels semble être plus souple dans le cadre de services offerts gratuitement puisqu'elle permet de générer un revenu, de soutenir une industrie et de maintenir les services gratuits[400]. À cet égard, la Commissaire Elizabeth Denham souligna, au terme d'une enquête menée contre *Facebook*, que :

> [Le] modèle organisationnel de Facebook est différent de ceux des organisations sur lesquelles nous nous sommes penchés jusqu'à maintenant. Si le site est gratuit pour les utilisateurs, il ne l'est pas pour Facebook qui a besoin de revenus publicitaires afin de fournir le service. De ce point de vue, la publicité est essentielle à la prestation de ce service. **Ceux et celles qui souhaitent utiliser le service doivent donc accepter de recevoir une certaine quantité de publicité**[401].

Il semble alors surgir l'idée que cette quête se traduit en la recherche d'une balance entre les attentes des utilisateurs et le droit des entreprises d'utiliser les outils techniques pour accomplir leurs divers desseins[402].

En 2004, la Cour d'appel fédérale discuta de la balance des intérêts dans l'affaire *Englander*. Elle rappellera que, si la PIPEDA a pour objectif de protéger la vie privée, elle permet également la collecte de renseignements personnels, allant même jusqu'à en faciliter le processus. En l'occurrence, lors de son analyse, « [la] Cour doit interpréter cette législation en trouvant le juste milieu entre deux intérêts concurrents »[403].

---

[400] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299 à la p 309.

[401] Commissariat à la protection de la vie privée du Canada, *Résumé de conclusions d'enquête en vertu de la PIPEDA no 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, 2009 au para 131, en ligne : <https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.asp> (consulté le 2 avril 2016).

[402] Eloise GRATTON, « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299 à la p 311.

[403] *Englander c Telus Communications Inc*, 2004 CAF 387 au para 46.

> « [...] lesdites collecte, utilisation et communication soient exécutées d'une manière qui concilie, dans toute la mesure du possible, le droit de la personne à la vie privée et les besoins de l'organisation. Il y a donc deux intérêts concurrents dans l'objet de la LPRPDE : le droit de la personne à la vie privée d'une part, et le besoin commercial d'accès aux renseignements personnels d'autre part [...] le droit à la vie privée n'est pas absolu »[404].

Relativement à la PCL, Tene et Polonetsky[405], soutiennent qu'il est crucial d'établir un équilibre entre les « utilisations bénéfiques des données » et la protection de la vie privée des individus[406]. Pour y parvenir, il serait nécessaire d'étendre la définition du consentement, la « limitation de l'objet et la minimisation des données », ainsi qu'une définition robuste de ce que sont les « informations d'identification personnelle »[407]. Or, comment parvenir à la réalisation de ce curieux équilibre entre une quête de contrôle grandissante et la publicité comportementale reposant nécessairement sur la collecte d'informations personnelles ?

D. Quelle alternative ?

Cette démonstration semble suggérer qu'il n'existe jusqu'à présent aucune alternative à la traque et à la publicité comportementale. Plusieurs initiatives ont été prises afin d'encadrer les pratiques de l'industrie. La pratique générale veut qu'un site Internet dispose d'une page contenant les modalités et conditions, dans laquelle elle divulguera par exemple, l'installation de témoins de connexion. On parlera alors d'une acceptation tacite des conditions, puisque le fait poursuivre la navigation sur le site constitue une acceptation des modalités.

---

[404] *Englander c Telus Communications Inc*, 2004 CAF 387 au para 38.

[405] Omer TENE et Jules POLONETSKY, « Privacy in the Age of Big Data: A Time for Big Decisions » (2012) 64 Stan L Rev 63.

[406] Omer TENE et Jules POLONETSKY, « Privacy in the Age of Big Data: A Time for Big Decisions » (2012) 64 Stan L Rev 63 à la p 63.

[407] Omer TENE et Jules POLONETSKY, « Privacy in the Age of Big Data: A Time for Big Decisions » (2012) 64 Stan L Rev 63 à la p 64.

Nous l'avons évoqué ci-dessus, certains sites Internet emploient l'utilisation de bandeaux persistants qui empêchent une partie de la navigation jusqu'à ce que l'utilisateur « accepte » les conditions d'utilisation — et les témoins. Il y a alors une acceptation expresse des conditions. Malgré tout, si l'information que l'on recherche se trouve devant nous, au bout de nos doigts et qu'un bandeau nous empêche d'y accéder, serons-nous tentés « d'accepter » les conditions simplement afin de nous en débarrasser ? Est-ce que ce consentement peut réellement être considéré comme valable ? Quel choix pour le consommateur dans de telles circonstances ? S'il existe un bouton « accepter », il n'existe pas son pendant négatif. Évidemment, l'utilisateur maintient toujours une portion de contrôle sur ses données personnelles. Il aura toujours le choix de visiter ou non des sites Internet qui installent des témoins et qui procèdent à la collecte de données[408]. Il se trouvera cependant pénalisé dans le monde virtuel.

Certains programmes d'autorégulation ont vu le jour au cours des dernières années. C'est notamment le cas du programme « AdChoice »[409], qui propose une forme de *opt-out* à la publicité ciblée. En cliquant sur l'icône *AdChoice* d'un site Internet donné, l'utilisateur est redirigé vers une page où on lui fournit de l'information sur le service et à partir de laquelle il peut se « désinscrire » du programme.

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.

---

[408] David S EVANS, « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37 à la p 56.

[409] Digital Advertising Alliance of Canada, « YourAdChoices.com », en ligne : <http://youradchoices.com/> (consulté le 2 avril 2016).

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 renseignements personnels alors qu'il met plutôt fin à publicité comportementale[410].

> The only right that online advertisers are willing to give users is the ability not to have ads served to them based on their web histories. Curran himself admits this: "There is a vital distinction between limiting the use of online data for ad targeting, and banning data collection outright"[411].

Les témoins de connexion sont toujours installés sur l'appareil de l'individu et continuent de collecter de l'information personnelle. De plus, une *The Economist* soulève que les utilisateurs qui suppriment systématiquement ou régulièrement leurs témoins, seront automatiquement *opted-in* puisque le système repose lui aussi sur l'installation de témoins[412].

---

[410] « Getting to know you » (13 septembre 2014), en ligne : The Economist <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party> (consulté le 18 avril 2016).

[411] Alexis C MADRIGAL, « I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web » (29 février 2012), en ligne : The Atlantic <http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/> (consulté le 2 avril 2016).

[412] « Getting to know you » (13 septembre 2014), en ligne : The Economist <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party> (consulté le 18 avril 2016).

Conclusion

Depuis son avènement, la publicité en ligne est véritablement devenue incontournable pour les annonceurs et les publicitaires, générant annuellement des revenus de plus de 150 milliards de dollars. Profitant de la révolution numérique, ces derniers ont graduellement compris comment recueillir des informations permettant d'en connaître beaucoup plus sur les utilisateurs que toute autre forme de publicité. Est ainsi née la publicité comportementale en ligne. Cette méthode consiste en une vaste cueillette d'informations à l'aide de « cookies », permettant ainsi la création de profils utilisateurs remarquablement complets, dans l'objectif précis de cibler chaque utilisateur pour lui présenter du contenu publicitaire conforme à son profil d'intérêts, d'habitudes et de comportements. En choisissant alors d'uniquement présenter des publicités susceptibles d'attirer l'attention du consommateur. Cette méthode est rapidement devenue le Saint Graal de la publicité, permettant de décupler le retour sur l'investissement.

Si l'industrie numérique de la publicité permet de chiffrer l'importance du marché, d'autres domaines sont également affectés par la publicité comportementale d'une manière plus subtile. Outre les considérations économiques, la protection des renseignements personnels, les questions de concurrence ou de droit de la consommation, la collecte de renseignements personnels dans le cadre d'une traque massive sur Internet comporte une facette sociale qu'on ne saurait négliger, soit des questions de « *personal autonomy, freedom from scrutiny or categorization, and similar values grounded in normative theories of social identity* »[413]. En effet, les profils créés à la suite d'un tel processus n'établissent pas qu'un portrait individuel de nos habitudes de navigation et de consommation, mais deviennent également des points de référence permettant de comparer les individus. Dans cette optique, grâce à son profil, tout le monde devient un point de comparaison. Il y a alors normalisation de

[413] Agatha M COLE, « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283 à la p 291.

certains types de comportements et mise à l'écart d'autres : ceux qui n'entrent pas dans la norme et qui semblent suspects. Comment alors protéger adéquatement les internautes ?

La collecte de renseignements personnels est, nous l'avons expliqué, extrêmement répandue et les entreprises sont à même de collecter de l'information de plus en plus personnelle afin d'offrir une publicité ciblée qui *correspond* aux intérêts individuels de chacun. Si cette personnalisation massive de la publicité semble souhaitable, elle effraye également puisqu'elle repose sur la collecte d'un nombre incalculable de renseignements personnels.

Les renseignements personnels collectés représentent une mine d'or pour les entreprises et elles ne semblent pas, à ce titre, souhaiter mettre fin à de telles activités. Si elles acceptent parfois de se soumettre aux lois en matière de protection des renseignements personnels, elles semblent tout de même œuvrer dans une zone grise, car conscientes du potentiel énorme qui dort dans les profils personnels, elles ne souhaitent pas toutes respecter les législations applicables.

Cette tendance est inquiétante. D'autant que 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[414], 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

---

[414] Liat CLARK, « Tim Berners-Lee: We need to re-decentralize the Web », *Ars Technica* (6 février 2014), en ligne : Ars Technica <https://arstechnica.com/tech-policy/2014/02/tim-berners-lee-we-need-to-re-decentralize-the-web/> (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 <https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-online-political-advertising-regulation> (consulté le 25 mars 2017).

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 discrimination raciale, de même que celle fondée sur la classe sociale[415]. En ce sens, la publicité ciblée présenterait un risque pour l'autonomie et la dignité humaine[416].

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[417], 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[418]. 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[419]. 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.

Une première étape pour se prémunir d'une telle dérive concernerait les juristes. D'après Cohen, bien qu'il s'agisse d'une approche généralement contre-intuitive pour ces derniers, à titre d'artisans des stratégies normatives et du droit régissant nos sociétés démocratiques, ils auraient la responsabilité de reconnaître l'idéologie libérale fondant culturellement le discours à la source de la distinction entre les sphères privées et publiques, de manière à se soucier tout autant des intrusions commerciales qu'étatiques au sein de la vie

---

[415] Shaun B SPENCER, « Privacy and Predictive Analytics in E-Commerce » (2015) 49 New Eng L Rev 629.

[416] Shaun B SPENCER, « Privacy and Predictive Analytics in E-Commerce » (2015) 49 New Eng L Rev 629 à la p 640.

[417] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 449.

[418] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 447.

[419] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 449.

privée[420]. De cette manière, en travaillant à circonscrire la liberté des entreprises à collecter l'information comme on aurait tendance à se méfier des mêmes activités de la part des gouvernements, on limiterait aussi les risques de dissémination, et donc de publicisation, des informations personnelles, qui comme nous l'avons vu, deviennent susceptibles d'être utilisées à d'autres fins que leur fonction marketing utilitaire[421].

En nous recentrant sur notre objet de recherche et de manière tout de même moins dramatique, nous ne pouvons qu'insister sur les nombreux défis qui attendent les consommateurs de demain. D'une part, ils devront prendre conscience de cette traque et choisir d'adopter des comportements plus sécuritaires en ligne. D'autre part, les pratiques sociales devront évoluer au rythme des technologies, afin que la réalité quotidienne puisse rejoindre celle des technologies et ainsi combler le fossé qui s'installe. Ainsi, nous ne pouvons que souligner et réitérer l'importance que doit prendre l'éducation citoyenne quant à l'enjeu que représente la PCL. Finalement, il semble nécessaire pour la frange juridique de poursuivre ses questionnements sur la protection des renseignements à caractère personnel, afin d'assurer que soit maintenue une protection qui est satisfaisante, voire même optimale, dans le cadre de la publicité en ligne.

---

[420] Julie COHEN, « Studying Law Studying Surveillance » (2014) 13:1 Surveillance & Society 91 à la p 92; Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437 à la p 463.

[421] Joel R REIDENBERG, « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437.

Bibliographie

LEGISLATION : CANADA

Charte canadienne des droits et libertés, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11.

Charte des droits et libertés de la personne, RLRQ c C-12.

Code civil du Québec, RLRQ c C-1991.

Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96.

Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-11.

Loi de 2004 sur la protection des renseignements personnels sur la santé, LO 2004, c 3, Annexe A.

Loi sur la concurrence, LRC 1985, c C-34.

Loi sur la protection des renseignements personnels, LRC (1985) ch P-21.

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-391.

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

Loi sur la protection du consommateur, RLRQ c P-401.

Loi sur la radiocommunication, LRC 1985, c R-2.

Loi sur la société canadienne des postes, LRC 1985, c C-10.

Loi sur les télécommunications, LC 1993, c 38.

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, ch 23.

Personal Information Protection Act Alberta, SA 2003, c P-65.

Personal Information Protection Act BC, SBC 2003, c 63.

LEGISLATION : AUTRES

Déclaration universelle des droits de l'homme, Rés AG 217(III), Doc off AG NU, 3e sess, sup nº 13, Doc NU A/810 (1948) 71.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, [1995] JO L281.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le

secteur des communications électroniques (directive vie privée et communications électroniques), [2002] JO L201.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) Official Journal of the European Union 1‑88.

JURISPRUDENCE : CANADA

Commissioner of Competition v Yellow Page Marketing, 2012 ONSC 927.
Dumont c Sears Canada inc, 2015 QCCQ 13883.
Eastmond c Canadien Pacifique Ltée, 2004 CF 852.
Englander c Telus Communications Inc, 2004 CAF 387.
Faucher c Costco Wholesale Canada Ltd, 2015 QCCQ 3366.
Gordon c Canada, 2008 CF 258.
Lelièvre c Magasin La clé de sol inc, 2011 QCCQ 5774.
R c Spencer, [2014] 2 RCS 212 (CSC).
R v Imperial Tobacco Products Limited, 1971 ALTASCAD 44 (CanLII), [1971] 5 WWR.
Richard c Time Inc, [2012] 1 RCS 265 (CSC).
Rousseau c Wyndowe, 2006 CF 1312.
Turner c Telus Communications Inc, 2005 CF 1601.

JURISPRUDENCE : AUTRES

Campbell v MGN Ltd, [2004] UKHL 22.

Aronberg v Federal Trade Commission, 132 F.2d 165 (7th Cir. 1942).
F T C v STERLING DRUG, INC, 215 F.Supp. 327 (1963).
Re DoubleClick Inc Privacy Litigation, 154 F Supp 2d 497 (SDNY 2001).

RAPPORTS OFFICIELS

ASSEMBLÉE NATIONALE DU QUÉBEC. Journal des débats de la Commission de la culture, 34e législature, 2e session (19 mars 1992 au 10 mars 1994) Le mardi 23 février 1993 - Vol. 32 N° 11, février 1993.
Bureau de la concurrence. Lignes directrices. Application de la Loi sur la concurrence aux indications dans Internet, Gatineau, 2009, en ligne : <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/vwapj/RepresentationsInternet-2009-10-16-f.pdf/$FILE/RepresentationsInternet-2009-10-16-f.pdf> (consulté le 28 mai 2017).

Commissariat à la protection de la vie privée. Rapport des conclusions en vertu de la LPRPDE no 2014-001, 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, 2014, en ligne : <http://canlii.ca/t/g2wr8> (consulté le 7 juillet 2017).

———. Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique, 2011, en ligne : <https://www.priv.gc.ca/media/1964/report_201105_f.pdf> (consulté le 5 février 2017).

———. Position de principe sur la publicité comportementale en ligne, 2015, 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 20 février 2017).

———. Résumé de conclusions d'enquête en vertu de la LPRPDE no 2001-25 Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2001/lprpde-2001-025/> (consulté le 2 avril 2016).

———. Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-315 Mesures de sécurité d'une société Internet et traitement d'une demande d'accès à l'information et d'une plainte relative à la protection des renseignements personnels mis en doute, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-315/> (consulté le 2 avril 2016).

———. Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-319 Mesures anti-pourriel du FSI contestées, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-319/> (consulté le 2 avril 2016).

———. Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques, en ligne : <https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.asp> (consulté le 2 avril 2016).

———. Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-010 La commissaire adjointe recommande à Bell Canada d'informer les clients au sujet de l'inspection approfondie des paquets, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/2009_010_rep_0813/> (consulté le 2 avril 2016).

———. Un client se plaint de la présence de « témoins » sur le site Web d'une compagnie aérienne, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2003-162, Conclusion #162, Commissariat à la protection de la vie privée du Canada, 2003, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-162/>.

Federal Trade Commission. FTC Staff Revises Online Behavioral Advertising Principles, 2009, en ligne : <https://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles> (consulté le 2 avril 2016).

———. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, 2012, en ligne : <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> (consulté le 18 avril 2017).

OCDE. « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », en ligne : <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm> (consulté le 26 mars 2017).

U.S. Senate, Committee on Commerce, Science and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes., 2013, en ligne : <https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf> (consulté le 9 janvier 2017).

DOCTRINE : MONOGRAPHIES

BORSCI, Simone, Masaaki KUROSU, Stefano FEDERICI et Maria Laura MELE. Computer Systems Experiences of Users with and Without Disabilities: An Evaluation Guide for Professionals, Boca Raton, FL, USA, CRC Press, 2013.

GAUTRAIS, Vincent. Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques, Montréal, Thémis, 2012.

GOLDMAN, Calvin S. et J. D. BODRUG. Competition Law of Canada, Juris Publishing, Inc, 2013.

GRATTON, Eloïse. Internet and Wireless Privacy: A Legal Guide to Global Business Practices, CCH Canadian Limited, 2003.

GRATTON, Éloïse. Understanding personal information: managing privacy risks, Markham, Ont, LexisNexis, 2013.

GRATTON, Eloïse et Elisa HENRY. Practical guide to e-commerce and Internet law, Markham, Ontario, LexisNexis, 2015.

LAMBERT, Paul. Gringras, the Laws of the Internet, 4e éd, Haywards Heath, West Sussex, Bloomsbury Professional, 2015.

LUE, Henry et Sangeetha PUNNIYAMOORTHY. Canadian marketing law handbook, 2e éd, Toronto, Carswell, 2012.

MURRAY, Andrew. Information Technology Law: The Law and Society, 2e éd, Oxford, United Kingdom, Oxford University Press, 2013.

PRICE, Monroe Edwin, Stefaan VERHULST et Libby MORGAN. Routledge Handbook of Media Law, Abingdon, Oxon ; New York, Routledge, 2013.

PRITCHARD, Brenda L, Susan VOGT et Association of Canadian Advertisers. Advertising and Marketing Law in Canada, 5e éd, Markham, Ontario, LexisNexis, 2015.

SCASSA, Teresa et Michael Eugene DETURBIDE, dir. Electronic commerce and internet law in Canada, 2e éd, Toronto, CCH Canadian, 2012.

SCHLEE, Christian. Targeted advertising technologies in the ICT space: a use case driven analysis, Wiesbaden, Springer Vieweg, 2013.
SMITH, Mike. Targeted: how technology is revolutionizing advertising and the way companies reach consumers, New York, American Management Association, 2015.
SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age, Fredericksburg, NYU Press, 2006.
SOLOVE, Daniel J. et Paul M. SCHWARTZ. Information privacy law, 5e éd, coll Aspen casebook series, New York, Wolters Kluwer Law & Business, 2015.
TRUDEL, Pierre. Introduction à la Loi concernant le cadre juridique des technologies de l'information, Cowansville, Québec, Éditions Y Blais, 2012.
TRUDEL, Pierre, France ABRAN, Karim BENYEKHLEF et Sophie HEIN. Droit du cyberespace, Montréal, Thémis, 1997.
WESTIN, Alan F. Privacy and Freedom, New York, Atheneum, 1967.
WILDE, Erik. Wilde's WWW: technical foundations of the World Wide Web, Berlin ; New York, Springer, 1999.
YOUNG, David M. W. et Brian R. FRASER. Canadian advertising & marketing law, Toronto, Carswell, 1990.

DOCTRINE : OUVRAGES COLLECTIFS

DESCHÊNES-HÉBERT, Sophie. « Présentation et démystification de la loi anti-pourriel : le consommateur numérique a-t-il l'unique contrôle de sa boîte de réception? » dans Pierre-Claude Lafond et Vincent Gautrais, dir, Le consommateur numérique: une protection à la hauteur de la confiance?, Éditions Yvon Blais, 2016.
GAUTRAIS, Vincent. « La protection du « cyberconsommateur » selon le droit québécois » dans Vincent Gautrais, dir, Le droit du commerce électronique, Montréal, Thémis, 2002.
———. « Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle » (2004) 9:2 Lex Electronica, en ligne : Lex Electronica <http://www.lex-electronica.org/articles/vol9/num2/le-defi-de-la-protection-de-la-vie-privee-face-aux-besoins-de-circulation-de-linformation-personnelle/>.
GAUTRAIS, Vincent et Adriane PORCIN. « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique » (2009) 43:3 Thémis 559.
MASSEY, Aaron K. et Annie I. ANTÓN. « Behavioral Advertising Ethics » dans Melissa Jane Dark, dir, Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives, IGI Global, 2011, 162.
TANGUAY, Sol. « Le ciblage publicitaire en ligne » dans Pierre-Claude Lafond et Vincent Gautrais, dir, Le consommateur numérique: une protection à la hauteur de la confiance?, Éditions Yvon Blais, 2016.

ABAD, Véronique. « L'effectivité des recours en matière de publicité sur Internet » (2005) 10:2 Lex Electronica, en ligne : Lex Electronica <http://www.lex-electronica.org/articles/vol10/num2/leffectivite-des-recours-en-matiere-de-publicite-sur-internet/> (consulté le 29 juillet 2017).

ACQUISTI, Alessandro, Curtis R. TAYLOR et Liad WAGMAN. « The Economics of Privacy » (2016) 52:2 Journal of Economic Literature 442.

ALLEN, Anita L. « Natural Law, Slavery, and the Right to Privacy Tort Colloquium: The Natural Law Origins of the American Right to Privacy » (2012) 81 Fordham L Rev 1187.

ALNAHDI, Sangdow, Maged ALI et Kholoud ALKAYID. « The effectiveness of online advertising via the behavioural targeting mechanism » (2014) 5:1 The Business & Management Review 22.

AMMORI, Marvin et Luke PELICAN. « Media Diversity and Online Advertising » (2012) 76:1 Alb L Rev 665.

ANTÓN, Annie I., Julia B. EARP et Jessica D. YOUNG. « How internet users' privacy concerns have evolved since 2002 » (2010) 8:1 IEEE Security & Privacy.

ASHWORTH, Laurence et Clinton FREE. « Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns » (2006) 67:2 Journal of Business Ethics 107.

AYENSON, Mika D., Dietrich James WAMBACH, Ashkan SOLTANI, Nathan GOOD et Chris Jay HOOFNAGLE. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, SSRN, 2011, en ligne : <https://papers.ssrn.com/abstract=1898390> (consulté le 5 mars 2017).

BENNETT, Collin J., Christopher A. PARSONS et Adam MOLNAR. « Real and Substantial Connections: Enforcing Canadian Privacy Laws against American Social Networking Campaigns » (2014) 23 J L Inf & Sci 50.

BENNETT, Steven C. « Regulating Online Behavioral Advertising » (2010) 44 John Marshall L Rev 899.

Benoit Pelletier. « Droit constitutionnel: La protection de la vie privee au Canada » (2001) 35 La Revue Juridique Themis 485.

BERGER, Dustin. « Balancing Consumer Privacy with Behavioral Targeting » (2010) 27:1 Santa Clara Computer & High Tech LJ 3.

BORGESIUS, Frederik J Zuiderveen. « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation » (2016) 32:2 CLSR 256.

BRANDON, Sarah Cathryn. « What's Mine is Yours: Targeting Privacy Issues and Determining the Best Solutions for Behavioral Advertising » (2011) 29 Marshall J Computer Info L 637.

CALO, Ryan. « Digital Market Manipulation » (2014) 82:4 Geo Wash L Rev 995.

CARRASCAL, Juan Pablo, Christopher RIEDERER, Vijay ERRAMILLI, Mauro CHERUBINI et Rodrigo DE OLIVEIRA. « Your Browsing Behavior for a Big Mac: Economics of Personal Information Online » dans Proceedings of the 22nd International Conference on World Wide Web, coll WWW '13, New York, NY, USA, ACM, 2013, 189.

CHEN, Jianqing et Jan STALLAERT. « An Economic Analysis of Online Advertising Using Behavioral Targeting » (2014) 38:2 MIS Quaterly 429.
CHUNG, Yuen Yi. « Goodbye PII: Contextual Regulations For Online Behavioral Targeting » (2014) XIV:2 J High Tech L 414.
COHEN, Julie. « Studying Law Studying Surveillance » (2014) 13:1 Surveillance & Society 91.
COLE, Agatha M. « Internet advertising after Sorrell v. IMS Health: a discussion on data privacy & the First Amendment » (2012) 30:2 Cardozo Arts & Ent LJ 283.
DALY, Angela. The Legality of Deep Packet Inspection, University of Glasgow, 2010, en ligne : <https://papers.ssrn.com/abstract=1628024> (consulté le 28 mars 2017).
EVANS, David S. « The Online Advertising Industry: Economics, Evolution, and Privacy » (2009) 23:3 Journal of Economic Perspectives 37.
FORD, Roger Allan. « Unilateral invasions of privacy » (2015) 91 Notre Dame L Rev 1075.
GODEL, Moritz, Annabel LITCHFIELD et Iris MANTOVANI. « The Value of Personal Information: Evidence from Empirical Economic studies » (2012) 1:88 Communications & Strategies 41.
GRATTON, Eloise. « Personalization, analytics, and sponsored services: The challenges of applying PIPEDA to online tracking and profiling activities » (2010) 8:2 CJLT 299.
GROSS, Hyman. « The Concept of Privacy » (1967) 42 NYU L Rev 34.
HAM, Chang-Dae et Sann RYU. Exploring How Consumers Cope with Online Behavioral Advertising: An Integration of the Persuasion Knowledge Model and the Protection Motivation Theory, Lubbock, United States, American Academy of Advertising, 2014, 165.
HOLMES, Nancy. Les lois fédérales du Canada sur la protection de la vie privée, PRB 07-44F, Division du droit et du gouvernement, 2008, en ligne : <https://lop.parl.ca/content/lop/researchpublications/prb0744-f.pdf> (consulté le 28 mai 2017).
HOOFNAGLE, Chris, Ashkan SOLTANI, Nathaniel GOOD et Dietrich WAMBACH. « Behavioral Advertising: The Offer You Can't Refuse » [2012] Harv L & Pol'y Rev 273.
HOTALING, Andrew. « Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting » (2008) 16:2 CommLaw Conspectus 529.
HUNT, Chris DL. « Conceptualizing Privacy and Elucidating its importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011) 37 Queen's LJ 167.
HUTCHISON, Cameron J. « Technological Neutrality Explained (& Applied to CBC v. SODRAC) » (2015) 13:1 Canadian Journal of Law and Technology 101.
International Telecommunication Union. Measuring the Information Society Report 2016, ITU MIS Report, 2016, en ligne : <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf> (consulté le 12 février 2017).
JENTZSCH, Nicola, Geza SAPI et Irina SULEYMANOVA. « Targeted pricing and customer data sharing among rivals » (2013) 31:2 International Journal of Industrial Organization 131.
JÉZÉQUEL, Myriam. « Historique de la Loi sur la protection du consommateur » (2003) 35:21 Journal du Barreau, en ligne : Journal du Barreau

<http://www.barreau.qc.ca/pdf/journal/vol35/no21/historique.html> (consulté le 24 août 2017).

JUELS, Ari. « Targeted Advertising ... And Privacy Too » dans Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA, coll CT-RSA 2001, London, UK, Springer-Verlag, 2001, 408.

KING, Nancy. « When Mobile Phones are RFID-Equipped - Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce » (2008) 15:1 Mich Telecomm & Tech L Rev 107.

KRISTOL, David M. « HTTP Cookies: Standards, Privacy, and Politics » (2001) 1:2 ACM Transactions on Internet Technology 151.

KUEHN, Andreas et Milton MUELLER. Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States, Syracuse NY, Syracuse University, School of Information Studies, 2012, en ligne : <https://papers.ssrn.com/abstract=2014181> (consulté le 27 mars 2017).

LEENES, Ronald et Eleni KOSTA. « Taming the cookie monster with Dutch law – A tale of regulatory failure » (2015) 31:3 CLSR 317.

LEGGE, Adam. « Online behavioural advertising: A comparative study of regulation between the EU and Hong Kong » (2015) 31:3 CLSR 422.

LEON, Pedro Giovanni, Blase UR, Yang WANG, Manya SLEEPER, Rebecca BALEBAKO, Richard SHAY, Lujo BAUER, Mihai CHRISTODORESCU et Lorrie Faith CRANOR. « What matters to users?: factors that affect users' willingness to share information with online advertisers » dans Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, New York, New York, USA, ACM, 2013, 7, DOI : 10.1145/2501604.2501611.

LEON, Pedro, Blase UR, Richard SHAY, Yang WANG, Rebecca BALEBAKO et Lorrie CRANOR. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising, New York, New York, USA, ACM, 2012, 589.

MANDL, Thomas, Wiebke THODE et Joachim GRIESBAUM. « "I would have never allowed it": User Perception of Third-party Tracking and Implications for Display Advertising » dans 14th International Symposium on Information Science, 2015, 445, en ligne : 14th International Symposium on Information Science <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1008.601&rep=rep1&type=pdf>.

MARSTON, Bette. « Where in the world? (Core Concepts: Geotargeting) » (2010) 44:12 Marketing News 6.

MASSEY, Aaron. « Getting to October: Why Understanding Technology Is Essential for Privacy Law » (2014) 51 Idaho L Rev 695.

MATHEWS-HUNT, Kate. « CookieConsumer: Tracking online behavioural advertising in Australia » (2016) 32:1 CLSR 55.

MCDONALD, Aleecia M. et Lorrie Faith CRANOR. An Empirical Study of How People Perceive Online Behavioral Advertising, CMU-CyLab-09-015, 2009.

———. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, Arlington, 2010.

MUELLER, Milton L. et Hadi ASGHARI. « Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States » (2012) 36:6 Telecomm Pol'y 462.

NIKIFORAKIS, Nick, Alexandros KAPRAVELOS, Wouter JOOSEN, Christopher KRUEGEL, Frank PIESSENS et Giovanni VIGNA. « Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting » dans Proceeding SP '13 Proceedings of the 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, 541.

NILL, Alexander et Robert J. AALBERTS. « Legal and Ethical Challenges of Online Behavioral Targeting in Advertising » (2014) 35:2 Journal of Current Issues & Research in Advertising 126.

NIZIO, Angelica. « Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a Do Not Track Mechanism » (2014) 2014:1 U Ill JL Tech & Pol'y 283.

OHM, Paul. « Broken promises of privacy: responding to the surprising failure of anonymization » (2010) 57:6 UCLA Law Review 1701.

———. « The Underwhelming Benefits of Big Data » (2013) 161:1 U Pa L Rev 339.

OUAKRAT, Alan. « Le ciblage comportemental, une perte de contrôle des éditeurs sur les données de l'audience » (2012) 6:1 Tic&société, en ligne : Tic&société <http://ticetsociete.revues.org/1251>.

PENN, Joanna. « Behavioral Advertising: The Cryptic Hunter and Gatherer of the Internet » (2011) 64:3 Fed Comm LJ 599.

PERSON, Andrea. « Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience » (2010) 62:2 Fed Comm LJ 435.

REIDENBERG, Joel R. « The Transparent Citizen » (2015) 47 Loy U Chi LJ 437.

REIDENBERG, Joel R., Jaspreet BHATIA, Travis D. BREAUX et Thomas B. NORTON. « Ambiguity in Privacy Policies and the Impact of Regulation » (2016) 45:S2 J Legal Stud S163.

ROOSENDAAL, Arnold. Facebook Tracks and Traces Everyone: Like This!, coll Tilburg Law School Legal Studies Research Paper Series No 03/2011, 2010, en ligne : <https://papers.ssrn.com/abstract=1717563> (consulté le 29 novembre 2016).

SCHWARTZ, Paul et SOLOVE, Daniel « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 NYU L Rev 1814.

SCOTT, Christopher. « Our Digital Selves: Privacy Issues in Online Behavioural Advertising » (2013) 17:1 Appeal: Review of Current Law and Law Reform 63.

SOLOVE, Daniel J. « A Taxonomy of Privacy » (2006) 154:3 U Pa L Rev 477.

SOLTANI, Ashkan, Shannon CANTY, Quentin MAYO, Lauren THOMAS et Chris Jay HOOFNAGLE. Flash Cookies and Privacy, SSRN, 2009, en ligne : <https://papers.ssrn.com/abstract=1446862> (consulté le 5 avril 2017).

SPENCER, Shaun B. « Privacy and Predictive Analytics in E-Commerce » (2015) 49 New Eng L Rev 629.

STALLA-BOURDILLON, Sophie, Evangelia PAPADAKI et Tim CHOWN. « From Porn to Cybersecurity Passing by Copyright: How mass Surveillance Technologies are Gaining Legitimacy... The Case of Deep Packet Inspection Technologies » (2014) 30:6 CLSR 670.

STODDART, Jennifer. « Discours: Sécurité et protection de la vie privée : Protéger l'information dans un monde transparent » (juin 2011), en ligne : Commissariat à la protection de la vie privée du Canada <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2011/sp-d_20110601/> (consulté le 28 mai 2017).

SUMMERS, Christopher A., Robert W. SMITH et Rebecca Walker RECZEK. « An Audience of One: Behaviorally Targeted Ads as Implied Social Labels » [2016] J Cons Res.

TENE, Omer et Jules POLONETSKY. « To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising » (2012) 13:1 Minn J L Sci & Tech 281.

———. « Privacy in the Age of Big Data: A Time for Big Decisions » (2012) 64 Stan L Rev 63.

———. « Big Data for All: Privacy and User Control in the Age of Analytics » (2013) 11:5 NW J Tech & IP 239.

THÉRIAULT, J. Yvon. « De l'utilité de la distinction moderne privé/public » [1992] 21 Politique 37.

TRUDEL, Pierre. « La protection de la vie privée dans les réseaux: des paradigmes alarmistes aux garanties effectives » (2006) 61:7 Annales Des Télécommunications 950.

TRUDEL, Pierre et Karim BENYEKHLEF. Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes, Rapport / Report, CAI, 1997, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/71> (consulté le 26 mai 2017).

TUROW, Joseph, Jennifer KING, Chris Jay HOOFNAGLE, Amy BLEAKLEY et Michael HENNESSY. Americans Reject Tailored Advertising and Three Activities that Enable It, 2009, en ligne : <https://papers.ssrn.com/abstract=1478214> (consulté le 18 avril 2017).

UR, Blase, Pedro Giovanni LEON, Lorrie Faith CRANOR, Richard SHAY et Yang WANG. « Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising » dans Proceedings of the Eighth Symposium on Usable Privacy and Security, coll SOUPS '12, New York, NY, USA, ACM, 2012, 4:1.

WARNER, Richard et Robert H SLOAN. « Behavioral advertising: From one-sided chicken to informational norms » [2012] 15 Vand J Ent & Tech L 49.

WARREN, Samuel et Louis BRANDEIS. « The Right to Privacy » (1890) IV:5 Harv L Rev, en ligne : Harvard Law Review <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm> (consulté le 12 février 2017).

ZUKINA, Julia. « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation within the Internet Behavioral Advertising Industry » (2012) 7:1 Brooklyn Journal of Corporate, Financial Commercial Law 277.

DICTIONNAIRES ET GLOSSAIRES

CAIJ. JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien, 2016, en ligne : JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien <https://dictionnairereid.caij.qc.ca/recherche#q=public%20&t=edictionnaire&sort=relevancy&m=search> (consulté le 4 août 2017).

———. JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien, 2016, en ligne : JuriBistro eDICTIONNAIRE, Dictionnaire de droit québécois et canadien <https://dictionnairereid.caij.qc.ca/> (consulté le 4 août 2017).

Gouvernement du Canada, Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). Glossaire concernant la télécommunication, 2009, en ligne :

Glossaire concernant la télécommunication <http://www.crtc.gc.ca/multites/mtwdk.exe?k=glossaire-glossary&l=60&w=262&n=1&s=5&t=2> (consulté le 21 février 2017).

Office québécois de la langue française. 2005, en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8398805> (consulté le 28 juillet 2017).

AUTRES : ARTICLES DE JOURNAUX ET BILLETS DE BLOG

ANGWIN, Julia. « Meet the Online Tracking Device That is Virtually Impossible to Block » (21 juillet 2014), en ligne : ProPublica <http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block> (consulté le 10 avril 2017).

BUSINESS, Author: Robert McMillan Robert McMillan. « Not on a Social Network? You've Still Got a Privacy Problem », en ligne : WIRED <https://www.wired.com/2014/10/privacy-friendster/> (consulté le 10 avril 2017).

Business News Daily. « Has Online Targeted Advertising Gone Too Far? » (7 avril 2011), en ligne : <http://www.businessnewsdaily.com/841-online-targeted-advertising.html> (consulté le 11 avril 2017).

CLARK, Liat. « Tim Berners-Lee: We need to re-decentralize the Web », Ars Technica (6 février 2014), en ligne : Ars Technica <https://arstechnica.com/tech-policy/2014/02/tim-berners-lee-we-need-to-re-decentralize-the-web/> (consulté le 10 avril 2017).

CONLEY, John M. « Behavioral Advertising: The Next Frontier for Privacy Law? » (avril 2009), en ligne : Robinson Bradshaw Publication <http://www.robinsonbradshaw.com/newsroom-publications-Behavioral-Advertising-The-Next-Frontier-for-Privacy-Law-04-23-2009.html> (consulté le 11 décembre 2016).

CORMACK, Lucy. « Dynamic pricing in online shopping surging with the e-commerce boom », The Sydney Morning Herald (7 février 2017), en ligne : The Sydney Morning Herald <http://www.smh.com.au/business/consumer-affairs/dynamic-pricing-in-online-shopping-surging-with-the-ecommerce-boom-20170203-gu5469.html> (consulté le 1 juillet 2017).

CURRAN, Charles. « Study finds behaviorally targeted ads more than twice as valuable and effective as non-targeted online ads » (24 mars 2010), en ligne : NAI : Network Advertising Initiative <https://www.networkadvertising.org/blog/study-finds-behaviorally-targeted-ads-more-twice-valuable-and-effective-non-targeted-online-ads> (consulté le 11 avril 2017).

DESCHÊNES-HÉBERT, Sophie. « La publicité comportementale en ligne, une nouvelle ère de la publicité : les internautes doivent-ils s'inquiéter de leur vie privée ? », en ligne : Legault Joly Thiffault <http://www.ljt.ca/fr/publications/publication_123.sn> (consulté le 3 avril 2016).

GANNETT, Allen. « Behavioral Pricing: A Consumer's Worst Nightmare » (21 janvier 2012), en ligne : The Next Web <http://thenextweb.com/insider/2012/01/21/behavioral-

pricing-a-consumers-worst-nightmare-a-merchants-dream/> (consulté le 6 décembre 2016).

GRATTON, Éloïse. « Dynamic pricing on websites: illegal or unfair? » (26 octobre 2014), en ligne : Éloïse Gratton <http://www.eloisegratton.com/blog/2014/10/26/dynamic-pricing-on-websites-illegal-or-unfair/> (consulté le 1 juillet 2017).

GREENFIELD, Rebecca. « The Trailblazing, Candy-Colored History Of The Online Banner Ad », Fast Company (27 octobre 2014), en ligne : Fast Company <https://www.fastcompany.com/3037484/most-creative-people/the-trailblazing-candy-colored-history-of-the-online-banner-ad> (consulté le 23 janvier 2017).

GROGAN, Samuel et Aleecia M MCDONALD. Access Denied! Contrasting Data Access in the United States and Ireland, 3, 2016, 191, en ligne : <http://www.degruyter.com/view/j/popets.2016.2016.issue-3/popets-2016-0023/popets-2016-0023.xml>.

GUILFORD, Gwynn. « Facebook data know you better than your own mother », en ligne : Quartz <https://qz.com/325129/facebook-data-know-you-better-than-your-own-mother/> (consulté le 10 avril 2017).

HERN, Alex. « Facebook is making more and more money from you. Should you be paid for it? » (25 septembre 2015), en ligne : The Guardian <https://www.theguardian.com/technology/2015/sep/25/facebook-money-advertising-revenue-should-you-be-paid> (consulté le 28 mars 2016).

HILL, Kashmir. « How A Strange Internet Glitch Turned This Kansas Farm Into A Digital Hell », en ligne : Fusion <http://fusion.net/story/287592/internet-mapping-glitch-kansas-farm/> (consulté le 13 novembre 2016).

KHAN, Azam. « The Inner Workings of Ad Networks and Ad Exchanges » (11 octobre 2011), en ligne : <http://www.adweek.com/digital/the-inner-workings-of-ad-networks-and-ad-exchanges/> (consulté le 5 avril 2017).

KROFT, Steve. « The Data Brokers: Selling your personal information » (9 mars 2014), en ligne : <http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/> (consulté le 10 avril 2017).

MADRIGAL, Alexis C. « I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web » (29 février 2012), en ligne : The Atlantic <http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/> (consulté le 2 avril 2016).

MAUS, Gregory. « How data brokers sell your life, and why it matters » (24 août 2015), en ligne : The Stack <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/> (consulté le 11 avril 2017).

NEWS et Retail & MARKETING. « Amazon Canada fined $1 million plus $100,000 costs for misleading price claims on website » (11 janvier 2017), en ligne : Financial Post <http://business.financialpost.com/news/retail-marketing/amazon-canada-fined-1-million-plus-costs-for-misleading-price-claims-on-website> (consulté le 31 juillet 2017).

SCHWARTZ, John. « Giving Web a Memory Cost Its Users Privacy », The New York Times (4 septembre 2001), en ligne : The New York Times <http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> (consulté le 12 avril 2017).

SOLON, Olivia. « Tim Berners-Lee calls for tighter regulation of online political advertising », The Guardian (12 mars 2017), en ligne : The Guardian <https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-online-political-advertising-regulation> (consulté le 25 mars 2017).

TALBOT, David. « A Phone that Knows Where You're Going », en ligne : MIT Technology Review <https://www.technologyreview.com/s/428441/a-phone-that-knows-where-youre-going/> (consulté le 10 avril 2017).

TANNER, Adam. « The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next », Forbes, en ligne : Forbes <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/> (consulté le 10 avril 2017).

ZITTRAIN, Jonathan. « Meme patrol: "When something online is free, you're not the customer, you're the product." » (21 mars 2012), en ligne : Future of the Internet - And how to stop it. <http://blogs.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/> (consulté le 28 mars 2017).

AUTRES : SITES INTERNET

BLG. Cibler le consommateur Canadien — Un important exposé sur le droit de la publicité et du marketing au Canada, 2014, en ligne : <http://blg.com/fr/Nouvelles-Et-Publications/Documents/Cibler_le_consommateur_Canadien_-_SEP2016.pdf> (consulté le 29 mars 2017).

BRADBURY, Danny. « Getting ready for GDPR » (24 avril 2017), en ligne : Canadian Lawyer Guide <http://www.canadianlawyermag.com/6418/Getting-ready-for-GDPR.html> (consulté le 7 juillet 2017).

Bureau de la concurrence. « Notre organisme » (31 mars 2005), en ligne : Gouvernement du Canada <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/h_00125.html> (consulté le 29 mai 2017).

———. « Promotion de l'éthique publicitaire » (20 avril 2005), en ligne : Gouvernement du Canada <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/h_00529.html> (consulté le 29 mai 2017).

———. Highlights from the Competition Bureau's Workshop on Emerging Competition Issues, Gatineau, 2016, en ligne : <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04030.html> (consulté le 1 juillet 2017).

———. « Bureau de la concurrence » (24 mai 2017), en ligne : Gouvernement du Canada <https://www.canada.ca/fr/bureau-concurrence.html> (consulté le 29 mai 2017).

Digital Advertising Alliance of Canada. « YourAdChoices.com », en ligne : <http://youradchoices.com/> (consulté le 2 avril 2016).

Electronic Frontier Foundation. « Do Not Track », en ligne : <https://www.eff.org/issues/do-not-track> (consulté le 13 janvier 2017).

eMarketers et Cindy LIU. Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 2015–2020, 2016, en ligne :

<https://www.emarketer.com/Report/Worldwide-Ad-Spending-eMarketers-Updated-Estimates-Forecast-20152020/2001916> (consulté le 10 mars 2017).

Future of Privacy Forum. « All About DNT », en ligne : All About DNT <https://allaboutdnt.com/> (consulté le 23 février 2017).

GAYLOR, Brett. « Do Not Track Documentary », en ligne : Do Not Track <https://donottrack-doc.com/> (consulté le 23 février 2017).

Industrie Canada, Gouvernement du Canada. « La Loi canadienne sur le pourriel et les autres menaces électroniques » (30 juin 2014), en ligne : La Loi canadienne anti-pourriel <http://combattrelepourriel.gc.ca/eic/site/030.nsf/fra/accueil> (consulté le 1 juillet 2017).

Interactive Advertising Bureau of Canada. 2015 Actual + 2016 Estimated Canadian Internet Advertising Revenue Survey, Annual Internet Advertising Revenue Reports, 2016, en ligne : <http://iabcanada.com/research/annual-internet-advertising-revenue-reports/> (consulté le 10 mars 2017).

KANARICK, Craig et Otto TIMMONS. « The "First" Banner Ad » (2014), en ligne : The First Banner Ad <http://thefirstbannerad.com/> (consulté le 23 janvier 2017).

LESINSKI, Mike. « Understanding the Difference Between Third-Party and First-Party Data », en ligne : Allant <http://www.allantgroup.com/blog/understanding-the-difference-between-third-party-and-first-party-data> (consulté le 10 août 2016).

Office de la protection du consommateur du Québec. « À propos de l'Office de la protection du consommateur », en ligne : Gouvernement du Québec <http://www.opc.gouv.qc.ca/a-propos/> (consulté le 1 juillet 2017).

PricewaterhouseCoopers. « Internet advertising - Key insights at a glance », en ligne : PwC.com <http://www.pwc.com/gx/en/industries/entertainment-media/outlook/segment-insights/internet-advertising.html> (consulté le 17 janvier 2017).

Uber. « How surge works | Drive Uber », en ligne : Uber.com <https://www.uber.com/info/how-surge-works/> (consulté le 25 juillet 2017).

« Jaron Lanier on how to make the internet pay » (4 mars 2013), en ligne : Channel 4 News <https://www.channel4.com/news/jaron-lanier-on-how-to-make-the-internet-pay> (consulté le 28 avril 2017).

« Getting to know you » (13 septembre 2014), en ligne : The Economist <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party> (consulté le 18 avril 2016).

« Facebook tracks users, even those who don't use it, says privacy report » (3 avril 2015), en ligne : HackRead <https://www.hackread.com/facebook-tracks-users-even-those-who-dont-use-it-report/> (consulté le 10 avril 2017).

« Cost of Super Bowl Advertising Breakdown by Year », en ligne : Superbowl-ads.com <http://superbowl-ads.com/cost-of-super-bowl-advertising-breakdown-by-year/> (consulté le 4 avril 2017).

« Do Not Track - Universal Web Tracking Opt Out », en ligne : <http://donottrack.us/> (consulté le 28 février 2017).