La protection du consommateur à l'ère du marketing intelligent. Une approche comparative France-Québec

Mémoire
Maîtrise en droit - avec mémoire

Audrey Houle

Université Laval
Québec, Canada
Maître en droit (LL. M.)

et

Université Paris-Sud
Orsay,France
Master (M.)

La protection du consommateur à l'ère du marketing intelligent
Une approche comparative France-Québec

Mémoire
Bidiplôme – Propriété intellectuelle fondamentale et droit des technologies numériques

Audrey Houle

Sous la direction de :

Geoffray Brunaux, Université Paris-Saclay, Faculté Jean Monnet
Marc Lacoursière, Université Laval, Faculté de droit

Résumé

La publicité et le marketing, autrefois connus comme étant des moyens pour les entreprises de faire connaître leurs produits aux consommateurs, sont sournoisement devenus des armes de consommation massives ciblant le consommateur au meilleur moment pour modifier son comportement d'achat. Grâce aux technologies émergentes, comme l'intelligence artificielle, et à la multiplication des moyens pour recueillir massivement des informations sur le consommateur, les entreprises ont su créer une nouvelle forme de marketing : le marketing intelligent. Cette nouvelle méthode qui couple les données massives aux nouvelles techniques d'apprentissage machine permet aux commerçants d'en connaître plus sur le consommateur qu'il n'en connaît sur lui-même.

Armées de nouvelles techniques issues de l'intelligence artificielle, les entreprises sont en mesure de cibler de manière précise les consommateurs afin de personnaliser l'offre de manière unique. Grâce aux nouvelles technologies, le marketing opère un changement de paradigme vers une pratique individualisée. Le consommateur ne devient-il pas alors plus vulnérable à ces pratiques ciblées et à leur omniprésence dans le marché ?

Abstract

Advertising and marketing, known as methods for companies to promote their products to consumers, have steadily become massive targeting weapons to influence the consumers behavior. Emerging technologies such as artificial intelligence and big data analytics have allowed companies to create a new form of marketing: intelligent marketing. These new methods allow merchants to know more about the consumer than he knows about himself.

Armed with new techniques derived from artificial intelligence, companies are able to precisely target consumers and uniquely personalize their offerings. This begs the question: Does the consumer become more vulnerable to these growing practices and their omnipresence in the market?

Table des matières

Liste des abréviations, sigles, acronymes

C.A.I.	Commission d'accès à l'information du Québec
C.c.Q.	Code civil du Québec
C. civ.	Code civil (France)
C. com	Code de commerce
C.F.	Cour Fédérale
CNIL	Commission Nationale informatique et Liberté
CJUE	Cour de justice de l'Union Européenne
CPVPC	Commissariat à la protection de la vie privée du Canada
CRM	Customer Relationship Management
C.S.	Cour supérieure
C.S.C.	Cour Suprême du Canada
D.	Dalloz
D.G.C.C.R.F.	Direction générale de la concurrence, de la consommation et de la répression des fraudes
Harv. J. L. & Tech	Harvard Journal of Law and Technology
GAFAM	Google, Amazon, Facebook, Microsoft
LCAP	Loi canadienne anti-pourriels
LPC	Loi sur la protection du consommateur
LPRPDE	Loi sur la protection des renseignements personnels et des documents électroniques
LPRPSP	Loi sur la protection des renseignements personnels dans le secteur privé
MAC	Media Access Control
OMPI	Office Mondial de la Propriété Intellectuelle
Q.C.C.A.	Cour d'appel du Québec
Q.C.C.A.I	Commission d'accès à l'information
Q.C.C.Q.	Cour du Québec
Q.C.C.S.	Cour supérieure du Québec
R.C.S.	Recueil de la Cour Suprême du Canada
RGPD	Règlement Général sur la Protection des Données

Remerciements

Contrairement à ce que l'on pourrait croire, l'écriture est le fruit du travail, non seulement de l'auteur, mais de tous ceux qui l'accompagnent alors que les idées se transforment en mots, les mots se transforment en phrases et les phrases se transforment en pages. Je souhaite prendre le temps de remercier ma famille et mes amis qui ont été à mes côtés pour m'épauler et m'encourager au cours des dernières années dans la réalisation de ce projet. Merci spécialement à ma plus vieille amie, Alys Bouchard, qui a toujours su trouver le temps pour m'aider, m'encourager et me conseiller.

Merci à mes codirecteurs, Geoffray Brunaux et Marc Lacoursière, pour votre appui, vos précieux conseils et le temps que vous avez su m'accorder tout au long du processus.

Je veux également remercier la Fondation Claude Masse et à la Faculté de droit de l'Université Laval pour le soutien financier.

Introduction

Le développement de nouvelles technologies est aujourd'hui source de prospérité économique, de connectivité entre pairs et de progrès pour l'humanité[1]. Ce que l'homme croyait relever de l'utopie comme la voiture volante et les *homme-robots* se transforme tranquillement en réalité avec le déploiement de plusieurs innovations comme la livraison par drone[2], la voiture autonome[3] et la réalité virtuelle[4], pour en nommer que quelques-unes. Cependant, le développement rapide des technologies ne possède pas que des vertus, il est également devenu source d'insécurités autant sociales que juridiques. La rapidité d'adoption de certaines innovations opposée à la lenteur du développement du droit met en lumière les lacunes présentes dans la législation[5]. Le caractère parfois intrusif des nouvelles technologies à l'image du *Big Brother*[6] et de la surveillance de masse sollicite aujourd'hui plusieurs questions éthiques concernant l'utilisation des données personnelles. Plus que jamais le droit

[1] « Technological innovation, particularly in information technology, is at the heart of America's growing economic prosperity. » Robert D. ATKINSON et Andrew S. MACKAY, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution*, New-York, The Information Technology and Innovation Foundation, 2007, p. III.

[2] AFP, « Amazon effectue sa première livraison par drone », *LaPresse*, 14 décembre 2016, en ligne : <https://www.lapresse.ca/techno/201612/14/01-5051264-amazon-effectue-sa-premiere-livraison-par-drone.php>; Stephane BAILLARGEON, « Livraison du troisième type », *Le Devoir*, 20 décembre 2019, en ligne : <https://www.ledevoir.com/societe/569506/comment-les-nouvelles-technologies-facilitent-la-logistique-de-la-vie-des-colis>

[3] Alec CASTONGUAY, « La voiture autonome arrive », *L'Actualité*, 13 avril 2018, en ligne : <https://lactualite.com/lactualite-affaires/la-voiture-autonome-arrive/>

[4] Bernard MAR, « The 7 Biggest Technology Trends In 2020 Everyone Must Get Ready For », *Forbes*, 30 septembre 2019, en ligne : <https://www.forbes.com/sites/bernardmarr/2019/09/30/the-7-biggest-technology-trends-in-2020-everyone-must-get-ready-for-now/#7dbb01cc2261>

[5] Karim SEFFAR et Karim BENYEKHLEF, « Commerce électronique et normativité alternative », (2006) 3-2 *U.O.L.T.J* 353, 356 ; Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », (2000) 32-2 *Sociologie et sociétés* 189.

[6] L'expression *Big Brother* est issue du roman *1984* de George Orwell pour qualifier les pratiques menées par certaines institutions qui portent atteinte aux droits et libertés des citoyens dans la société civile. Elle est principalement utilisée en lien avec les révélations de surveillance massive des communications électroniques des citoyens par le gouvernement américain dénoncé par Edward Snowden en 2013. Voir George ORWELL, *1984*, Angleterre, Édition Gallimard, 1950; Glen GREENWALD, Ewen MACASKILL et Laura POITRAS, « Edward Snowden : the whistleblower behind the NSA surveillance revelation », *The Guardian*, 11 juin 2013, en ligne : <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

à la vie privée est revendiqué autant sur la place publique que devant les tribunaux alors que les failles de cybersécurité se multiplient[7].

Les secteurs de la publicité et du marketing sont particulièrement touchés par ces revendications alors qu'un nombre grandissant de consommateurs se questionnent quant à l'utilisation de leurs données personnelles à des fins marketing. Autrefois connus comme étant un moyen pour les entreprises de faire connaître leurs produits aux consommateurs, la publicité et le marketing sont sournoisement devenus des armes de consommation massives qui ciblent le consommateur au meilleur moment afin d'influencer leur comportement. L'objectif du marketing : connaître, prédire et stimuler les besoins des consommateurs[8]. La publicité est alors l'outil par excellence des marketeurs afin de faire connaître aux consommateurs les produits et services désignés par l'ensemble des moyens possibles[9].

Grâce aux technologies de pointes comme l'intelligence artificielle et la multiplication des moyens pour recueillir des informations sur les consommateurs, les entreprises ont su créer une nouvelle forme de marketing, le *marketing intelligent*[10]. Ce concept réfère plus spécifiquement à l'utilisation de technologies novatrices comme l'intelligence artificielle et les données massives, aussi connues sous le nom de *big data*, pour modéliser les décisions marketing grâce à des modèles mathématiques et statistiques[11]. Ces modèles permettent de

---

[7] On peut penser dans les dernières années au scandale entourant la société *Cambridge Analytica* qui a utilisée, sans consentement valable, les données de plusieurs milliers d'utilisateurs Facebook à des fins de profilage pour la campagne présidentielle américaine du président Trump. Plus près de chez nous, tous les membres d'une institution financière phare québécoise, la société *Desjardins*, ont été touchés par fuite massive de données concernant notamment les informations bancaires des clients, leur numéro d'assurance sociale et d'autre information pouvant être recueillie par la banque. Voir à ce propos les affaires Cambridge Analytica et Desjardins : William AUDUREAU, « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », *Le Monde*, 22 mars 2018, en ligne : < https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html>; Anne-Sophie POIRÉ, « Ce qu'il faut savoir sur la fuite de données de Desjardins », Le Soleil, 21 juin 2019, en ligne : < https://www.lesoleil.com/affaires/ce-quil-faut-savoir-sur-la-fuite-de-donnees-de-desjardins-8e4743e1958d6e5e31da4439dbc111db>

[8] LAROUSSE, *Dictionnaire Larousse de la langue française*, Presses universitaire de Montréal, 2011, en ligne : <https://www.larousse.fr/dictionnaires/francais/marketing/49526> « marketing »

[9] *Id.*, « publicité »

[10] Francisco J. MARTINEZ LOPEZ et Jorge CASILLAS, « Marketing Intelligent Systems for consumer behaviour modelling by a descriptive induction approach based on Genetic Fuzzy Systems », (2009) 38 *Industrial Marketing Management* 714, 714.

[11] *Id.* ; Berend WIERENGA, « Marketing and Artificial Intelligence: Great Opportunities, Reluctant Paterns », dans Jorge CASILLAS Francisco J. MARTINEZ LOPEZ, *Marketing Intelligent Systems Using Soft Computing*, New-York, Springer, 2010, p. 1, à la p. 1.

créer des technologies d'aide à la décision grâce à des modèles prédictifs permettant de mieux segmenter, cibler et communiquer avec le consommateur[12].

Il est possible d'observer un changement de paradigme du marketing vers une individualisation de la pratique. Le marketing n'est plus le véhicule d'information de masse qu'il était autrefois, mais une pratique individualisée relativement intrusive. L'essor du marketing relationnel et la multiplication des canaux de communication ont permis d'offrir aux consommateurs des publicités spécifiques à leur profil. Le consommateur est submergé d'offres qui apparaissent selon sa localisation, son horaire ou même les périodes marquantes de sa vie afin d'assurer une vente à l'entreprise.

Naturellement, le marketing est un domaine avare d'information qui regorge d'ambition afin d'assurer la position concurrentielle de l'entreprise dans le marché et d'obtenir le meilleur retour sur ses investissements. De ce fait, la qualité et la quantité des données recueillies permettent aux entreprises d'optimiser leurs campagnes publicitaires et de transformer les dépenses marketing en profits[13]. La clé du succès face à la concurrence n'est pas seulement d'avoir des données sur les consommateurs, mais d'extraire des connaissances sur ces informations afin de prendre de meilleures décisions d'affaires[14].

Les applications des nouvelles technologies sont multiples dans le domaine du marketing comme la segmentation et le ciblage, la personnalisation tarifaire ou la gestion de la relation client[15]. Or, en raison de la précision de la technique, elle doit être utilisée avec parcimonie pour éviter de créer un malaise auprès des consommateurs. La confiance au partage des renseignements personnels demeure la clé de voute du marketing intelligent.

---

[12] B. WIERENGA, « Marketing and Artificial Intelligence: Great Opportunities, Reluctant Paterns », préc., note 11, à la p. 6-8.
[13] *Id.*, à la p. 7.
[14] F. J. MARTINEZ-LOPEZ et J. CASILLAS, « Marketing Intelligent Systems for consumer behaviour modelling by a descriptive induction approach based on Genetic Fuzzy Systems », préc. note 10, 714.
[15] Francisco J. MARTINEZ LOPEZ et Jorge CASILLAS, « Artificial intelligence-based systems applied in industrial marketing: An historical overview, current and future insights » (2013) 42 *Industrial Marketing Management* 489, 489.

L’influence du commerce électronique

L’essor du commerce électronique a su jouer un rôle important à la création de cette nouvelle forme de marketing. La réorientation des consommateurs vers le numérique a permis de multiplier les sources de données développant une réelle consécration de la personnalité numérique du consommateur[16]. Le marketing se nourrit de cette vague de données volontairement partagée par les consommateurs et celles laissées derrière en surfant sur le web. Chaque mouvement du consommateur en ligne est suivi puisqu’il possède le potentiel de créer de la valeur pour les entreprises en leur permettant d’appréhender et de mieux comprendre le comportement du consommateur.

Par ailleurs, le commerce électronique a gagné un élan de popularité grâce à la pandémie de Coronavirus qui frappe actuellement le monde entier[17]. Les consommateurs, confinés à la maison, ont dû délaisser les commerces traditionnels pour se retourner vers le numérique afin de subvenir à leurs besoins. Que ce soit pour le travail, les loisirs ou pour faire des achats, l’accroissement de la présence en ligne du consommateur fait parallèlement croître la quantité d’information que les commerçants disposent sur lui[18]. L’effet de la pandémie sur l’avenir du commerce électronique est encore inconnu, mais force est de constater qu’étant actuellement l’option la plus sécuritaire d’un point de vue épidémiologique, un lien de confiance avec les nouvelles technologies est en train d’émerger au sein de la population mondiale. Ce changement dans les habitudes de consommation est économiquement intéressant, mais il rappelle aussi l’urgence de réfléchir à l’encadrement juridique des technologies et à la protection du consommateur.

[16] Michaël BARDIN, « L’identité numérique et le droit : esquisse d’une conciliation difficile », (2018) 80-1 *Hermès* 283, 286.

[17] Une augmentation de 118% des ventes liées au commerce électronique a pu être observée au Québec par rapport à l’année précédente en raison de la pandémie. Voir : INFOPRESSE, « COVID-19 : l’opportunité du commerce électronique », *Infopresse*, 2 avril 2020, en ligne : < https://www.infopresse.com/article/2020/4/2/covid-19-l-opportunite-du-commerce-electronique> ; Krystal HU et Rebekah MATHEW, « COVID-19 Amazon: E-commerce giant raises overtime pay for warehouse workers to meet increasing online demand », *National Post*, 21 mars 2020, en ligne : < https://nationalpost.com/news/amazon-raises-overtime-pay-for-warehouse-workers-2>

[18] Alexandre PIQUARD, « La crise du coronavirus va-t-elle améliorer l’image des GAFA ? », *Le Monde*, 10 avril 2020, en ligne : <https://www.lemonde.fr/economie/article/2020/04/10/coronavirus-une-guerre-de-l-image-pour-les-geants-du-numerique_6036161_3234.html>

Le commerce électronique a bouleversé la relation entre le consommateur et le commerçant. Traditionnellement binaire, le commerce en ligne a permis à une pluralité d'acteur d'intervenir dans la relation entre les deux parties rendant diffus les contours de cette relation. De nos jours, les géants économiques comme Google, Facebook, Amazon et Microsoft, mieux connus sous l'acronyme GAFAM, sont également de la partie et recueillent une myriade d'informations sur les consommateurs. Leur rôle est incertain, même pour le commerçant, alors que leur présence pour recueillir des données sur les habitudes de consommations des internautes est plus que certaine. Les commerçants sont liés avec ces nouveaux acteurs afin d'assurer l'effectivité de leur présence en ligne. Sans activité sur Facebook et un référencement optimisé sur Google, la vitrine numérique du commerçant peut être considérée comme inexistante pour les internautes. Les consommateurs ne font plus seulement affaire avec leur commerçant préféré, mais une pluralité d'acteurs dont les géants économiques et les spécialistes en publicité et marketing.

La protection des données des consommateurs

La confiance des consommateurs envers l'environnement numérique est tributaire de la protection de leurs données. Gardienne de ce droit fondamental à la vie privée[19], la protection des données personnelles collectées à des fins marketing comporte certaines limites juridiques. Les données recueillies par les marketeurs sont de différentes natures ce qui peut rendre l'application du droit de la protection des renseignements personnels ambigüe. Elles concernent autant des informations plutôt neutres comme l'adresse IP de l'ordinateur utilisé que des informations extrêmement sensibles comme les caractéristiques socioéconomiques du consommateur (âge, genre, éducation, emploi, salaire)[20].

La notion de renseignement personnel se définit en droit canadien comme étant « […] tout renseignement concernant un individu identifiable.»[21] En sol québécois, le législateur a repris essentiellement la même formule en la définissant comme étant « […] tout renseignement

[19] *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. 8.
[20] B. WIERENGA, « Marketing and Artificial Intelligence: Great Opportunities, Reluctant Paterns », préc., note 11, à la p. 6.
[21] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c. 5, art. 3

qui concerne une personne physique et qui permet de l'identifier.»[22] De même que de l'autre côté de l'Atlantique, le législateur européen a adopté une formule similaire définissant la notion de données à caractère personnelles comme étant « […] toute information se rapportant à une personne physique identifiée ou identifiable »[23]. Ces définitions larges donnent à la notion de renseignement personnel un caractère protéiforme qui impose aux tribunaux d'interpréter ponctuellement la notion lui permettant d'évoluer au gré des développements technologiques[24].

De manière générale, pour être qualifiée de renseignement personnel, l'information recueillie doit permettre d'identifier un individu qu'il soit seul ou en combinaison avec d'autres renseignements[25]. Le *Règlement Général sur la Protection des Données* (RGPD) a offert plus de précisions aux tribunaux européens quant à savoir quelles données pouvaient être considérées comme des renseignements personnels : « […] nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[26]. Les données recueillies par les différentes pratiques marketing peuvent être protégées par le régime juridique du droit à la protection des renseignements personnels considérant le potentiel de réidentification de l'individu qu'elles possèdent. Toutefois, la notion de renseignement personnel à elle seule n'est pas suffisante pour offrir une protection optimale aux consommateurs en raison de certaines lacunes entre la théorie et la pratique.

Le corpus législatif entourant le droit à la vie privée est rapidement déjoué par l'abus de la notion de consentement. Au Canada, le Commissariat à la protection de la vie privée avait émis certaines réserves déjà en 2016 sur la notion de consentement dans un rapport portant sur l'amélioration possible de la *Loi sur la protection des renseignements personnels et des documents électroniques*[27]. C'est face à la capacité de consentir que le bât blesse dans le

[22] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ, c. P-39.1, art. 2.
[23] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),* J.O. L 119 du 4.5.2016, p. 1–88, art. 4, par. 11.
[24] *Dagg c. Canada (Ministre des Finances),* [1997] 2 RCS 403, par. 68.
[25] *Gordon c. Canada (Santé),* 2008 CF 258, par. 33.
[26] *Règlement (UE) 2016/679*, préc., note 23, par. 11.
[27] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consentement et protection de la vie privée,* Document de discussion sur les améliorations possibles au consentement sous le régime de la *Loi sur la*

contexte des nouvelles technologies. En pratique, le consommateur consent à un moment ou un autre à partager ses renseignements personnels pour avoir accès à un programme de fidélité ou pour qu'un témoin (*cookie*)[28] soit installé dans son navigateur. Or, la qualité de ce consentement est définitivement critiquable considérant que celui-ci est préalable à la collecte, l'utilisation ou à la communication du renseignement visé[29] et qu'il doit être donné à des fins spécifiques de manière manifeste, libre et éclairée[30].

Théoriquement, les entreprises devraient expliquer clairement quels renseignements seront recueillis, de quelle manière, comment ils seront utilisés, à qui ils pourront être partagés et sous quelles conditions. Par ailleurs, le consentement peut seulement être valable lorsqu'il est raisonnable de s'attendre à ce que l'individu puisse comprendre la nature des renseignements visés, l'usage qui va en être fait et les conséquences qui sont en jeu[31]. Une application stricte du droit imposerait aux entreprises d'obtenir un consentement distinct et répété pour chaque plateforme et site web que le consommateur visite. La théorie semble difficilement applicable à la pratique. Le consommateur qui se voit noyé dans les méandres des politiques d'utilisation des données et la navigation sur le web peut devenir un fardeau juridique pour le consommateur. La lourdeur du processus fait courir le risque de décourager les consommateurs à réellement jouir de leur capacité à consentir en acceptant aveuglément les conditions d'utilisations pour réussir à accéder au site souhaité. Il faut toutefois rappeler que les lois canadiennes et québécoises ont été adoptées il y a déjà plus d'une décennie et font l'objet de projets de réforme[32].

---

protection des renseignements personnels et les documents électroniques, Québec, 2016, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/consent_201605/>

[28] Les cookies, appelés aussi communément traceurs ou témoins sont des fichiers textes invisibles déposés sur le disque dur de l'ordinateur de l'utilisateur lorsqu'il navigue sur le web. David M. KRISTOL, « HTTP Cookies : Standards, Privacy and Politics », (2001) 1-2 *ACM Transaction on Technology* 151, 153.

[29]*Loi sur la protection des renseignements personnels et les documents électroniques,* préc., note 21, Principe 4.3.1

[30] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 14. ; *Règlement (UE) 2016/679*, préc., note 24, par. 11.

[31]*Id.*; *Loi sur la protection des renseignements personnels et les documents électroniques,* préc., note 21, art. 6.1

[32] Voir *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi no. 64 (présentation – 12 juin 2020), 1re session, 42e légis. (Qc).

Le niveau de protection requis par le corpus juridique de la protection des renseignements personnels varie en fonction de la sensibilité des informations recueillies[33]. En soi, la préférence pour une marque de croustilles recueillie par un programme de fidélité ou le fait qu'un témoin emmagasine les informations concernant l'adresse IP d'un ordinateur suite à la consultation de certains sites web peut sembler relativement dérisoire. La donnée unitaire ne révèle que très peu de choses, ce n'est qu'une fois corrélée avec les autres renseignements recueillis que l'information se précise et que son degré de sensibilité augmente. Le même sac de croustilles peut révéler une dépendance à la malbouffe et une prédisposition à certaines maladies cardiovasculaires seulement en considérant les habitudes d'achat du consommateur. En matière de marketing, les habitudes d'achat peuvent se transformer en moment de vulnérabilité. Par exemple, un épicier pourrait proposer au consommateur une publicité de croustilles à un créneau horaire précis sachant que celui-ci est susceptible de s'arrêter faire des courses en fonction de ses statistiques. En ciblant une période précise où le consommateur est plus enclin à avoir faim, la publicité peut générer un comportement d'achat impulsif[34]. Le marketing intelligent permet aux entreprises de profiter d'une meilleure compréhension des facteurs cognitifs du comportement du consommateur afin de révéler ou même accentuer le caractère vulnérable du consommateur[35]. Les renseignements recueillis à des fins marketing sont de nature extrêmement sensible, non seulement au regard du droit à la vie privée, mais également au regard du droit de la consommation. Pourtant, le droit à la vie privée semble être le principal droit revendiqué face à ces enjeux alors qu'il n'est pas l'unique régime de protection applicable au marketing intelligent.

Le rôle du droit de la consommation

À une autre époque, l'essor de la société de consommation a transformé les rapports juridiques entre les consommateurs et les commerçants imposant la création d'un régime juridique propre à la protection du consommateur[36]. Caractérisé par le déséquilibre entre les parties, le droit de la consommation s'est construit parallèlement au développement de la

[33] *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 21, Principe 4.7
[34] Nicole L'HEUREUX et Marc LACOURSIÈRE, *Droit de la consommation*, 6e éd., Cowansville, Éditions Yvon Blais, 2011, p. 3.
[35] Ryan CALO, « Digital Market Manipulation », (2014) 82 *George Washington Law Review* 995, 995.
[36] N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 2-3.

société de consommation que l'on connaît aujourd'hui offrant au consommateur les outils juridiques nécessaires pour rétablir l'équilibre entre les prestations. La notion de déséquilibre vient de la présomption prévue par le législateur que le consommateur, en raison de son manque d'expertise, n'est pas en mesure d'apprécier la valeur de la prestation et devient plus susceptible d'adhérer à un contrat dont les obligations sont disproportionnées[37]. Avec les nouvelles technologies, le déséquilibre est plus que jamais présent dans les relations contractuelles entre le consommateur et le commerçant en raison du manque d'expérience des consommateurs avec les nouvelles technologies face à l'expertise développée par les entreprises.

Méthodologie

La nouvelle forme de marketing intelligent incite à un certain rapprochement entre l'optimisation du marketing et l'exploitation de l'état de vulnérabilité du consommateur. La question générale de recherche vise à évaluer dans quelle mesure le marketing intelligent affecte les droits des consommateurs. De manière spécifique, cette recherche s'intéresse à savoir si la protection du consommateur est pleinement considérée par le régime juridique québécois à l'ère du marketing intelligent et surtout, quel est le rôle du droit de la consommation face à ces nouveaux enjeux.

Cette recherche se base sur l'hypothèse que le marketing intelligent affecte une pluralité de droits et accentue le déséquilibre entre le consommateur et le commerçant sollicitant l'intervention du droit de la consommation.

Le rôle du droit de la consommation face aux enjeux que soulève le marketing intelligent peut être envisagé selon deux principales écoles de pensée comprenant un éventail varié d'opinions nuancées. La première école, chapeautée par la Cour Suprême du Canada[38], appréhende le droit comme étant nécessaire à la protection du consommateur vulnérable et même parfois crédule face aux commerçants[39]. La notion de vulnérabilité du consommateur est un état de fait dans lequel se trouve le consommateur en raison de la disparité des

[37] N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 622 ; *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 8.
[38] *Richard c. Times*, [2012] 1 R.C.S. 265, *infra* p. 72-73; *Banque de Montréal c. Marcotte*, [2014] 2 RCS 725.
[39] *Id.*

conditions socioéconomiques entre lui et le commerçant[40]. La pluralité de produits et de services offerts, leur complexité, l'expertise du commerçant opposé au manque d'expérience du consommateur, le caractère unilatéral des contrats de consommation et l'influence de la publicité sur le comportement du consommateur accentuent la position de vulnérabilité du consommateur. Le rôle du droit de la consommation s'inscrit alors dans l'idée de protéger le consommateur afin de rétablir l'équilibre entre les parties en raison du caractère inégal des prestations[41]. En ce sens, le droit de la consommation doit déroger du principe d'autonomie de volonté établi par le droit civil pour atteindre de nouveau l'équilibre contractuel.

La seconde école s'éloigne de la présomption que le consommateur représente la partie faible dans la relation d'affaires et affirme que les entreprises peuvent également avoir une position vulnérable. L'affaire *Dell Computer Corp. c. Union des consommateurs,* où des consommateurs ont profité d'une erreur de prix notable en contournant les mesures mises en place par *Dell* pour obtenir des ordinateurs à un prix affiché par erreur[42], peut illustrer ce propos. L'ingéniosité des consommateurs dans cette affaire et le caractère très protecteur du droit de la consommation sont susceptibles de créer un nouveau déséquilibre, au désavantage du commerçant.

La recherche s'accorde davantage avec la première école de pensée qui adopte comme critère de référence le consommateur moyen. Dans le cadre de ce mémoire, le caractère inégal des prestations s'observe non seulement en raison de la puissance économique des entreprises

[40]N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 26 ; Marc LACOURSIÈRE, « Richard C Time Inc : à la recherche de la définition du « consommateur moyen »! », 2012 90-2 *Revue du Barreau canadien* 493, 502.

[41] N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 3 ; Jacob S. ZIEGEL, « The Future of Canadian Consumerism », (1973) 51 *R. du B. can.* 191, 193 ; Pierre-Claude LAFOND (dir.), *L'équité au service du consommateur*, Cowansville, Éditions Yvon Blais, 2010 ; Benoit MOORE, « Autonomie ou dépendance : réflexions sur les liens unissant le droit contractuel de la consommation au droit commun », dans Pierre-Claude Lafond, *Le droit de la consommation sous influences*, Cowansville, Les Éditions Yvon Blais Inc., 2007 ; Claude MASSE « Fondement historique de l'évolution du droit québécois de la consommation », dans Pierre-Claude Lafond, dir., *Mélanges Claude Masse – En quête de justice et d'équité*, Cowansville, 2003 ; Thierry BOURGOIGNIE, « Un droit de la consommation est-il encore nécessaire en 2006 ? », dans Thierry BOURGOIGNIE, *Regards croisés sur les enjeux contemporains du droit de la consommation*, Cowansville (Qué.), Les Éditions Yvon Blais Inc., 2006, p. 1 ; Thierry BOURGOIGNIE, *Éléments pour une théorie du droit de la consommation : au regard des développements du droit belge et du droit de la Communauté économique européenne*, Bruxelles, Story Scientia, 1988 ; Philippe STOFFEL-MUNCK, « L'autonomie du droit contractuel de la consommation : d'une logique civiliste à une logique de régulation », *RTD com.* 2012, p. 705.

[42] *Dell Computer Corp. c. Union des consommateurs,* [2007] 2 RCS 801, par. 4.

étudiées, mais également en raison du manque d'expérience d'une majeure partie des consommateurs avec les nouvelles technologies.

L'interprétation de l'esprit du droit de la consommation apporte un regard nouveau sur une question récurrente : celle de la protection des données des consommateurs. Ce mémoire a pour ambition de se démarquer d'un point de vue scientifique par l'originalité de son approche en abordant non seulement le droit à la protection des renseignements personnels, mais aussi le droit de la consommation.

Une analyse exégétique du droit applicable à la question en France et au Québec sera effectuée afin de démontrer dans quelles mesures les droits des consommateurs sont affectés par l'utilisation des technologies à des fins marketing. Une posture de cherche interne au droit conjugué à une approche de droit comparé sera naturellement adoptée dans le but d'observer l'état actuel du droit dans les deux juridictions. Cette approche permet d'envisager comment, face à l'état de la technique, le droit pourrait évoluer au Canada pour assurer la protection optimale du consommateur à l'ère du marketing intelligent. Le lien historique entre les deux territoires, leur évolution juridique distincte et la tradition civiliste partagée offre une occasion de comparer les régimes juridiques et d'extraire les forces et les faiblesses de chacun afin d'avoir une perspective nouvelle sur la question de recherche[43]. Au niveau technologique, l'étude du droit français et même européen comporte plusieurs avantages en raison du caractère très réactif et avant-gardiste de la législation face aux nouvelles technologies[44].

Les deux régimes juridiques seront interprétés en vertu de l'esprit du droit de la consommation en un effectuant un retour sur ses fondements historiques[45]. Cette méthodologie avec une dimension herméneutique entre en adéquation avec l'hypothèse de recherche qui suppose que la nature du droit de la consommation est de rétablir l'équilibre

[43]Béatrice JALUZOT, « Méthodologie du droit comparé : bilan et prospective », préc., note 18. ; John C. REITZ, « How to Do Comparative Law », (1998) 4-46 *Amercian Journal of Comparative Law* 617, 620.
[44] L'Union Européenne a été vu dans le monde comme étant une pionnière dans le monde face aux enjeux de protection de la vie privée à l'épreuve des nouvelles technologies en adoptant en 2016 le *Règlement Général sur la Protection des Données*. Martin UNTERSINGER, « Données personnelles : un nouveau règlement européen contraignant », *Le Monde*, 24 janvier 2018, en ligne : <https://www.lemonde.fr/pixels/article/2018/01/24/un-nouveau-reglement-contraignant_5246333_4408996.html>
[45]B. JALUZOT, préc., note 43, 33.

entre le consommateur et le commerçant[46]. L'étude des différentes manières dont le marketing intelligent affecte les droits des consommateurs permet de démontrer le déséquilibre présent entre les parties susceptible d'intéresser le droit de la consommation. Toutefois, ce mémoire délaisse les enjeux de publicités trompeuses et les pratiques déloyales qui s'éloignent de l'objet de la recherche.

Une étude approfondie des pratiques marketing sera faite par l'entremise de la littérature scientifique afin d'avoir accès aux pratiques les plus récentes tout en permettant à la recherche d'avoir une approche interdisciplinaire sur la question. Le choix d'une démarche plus technique permet de comprendre adéquatement les rouages du marketing intelligent pour mieux observer les lacunes juridiques des différents régimes applicables. Cette recherche entend donc qualifier juridiquement la problématique reliée au développement du marketing intelligent en ouvrant la voie à la protection potentielle du régime juridique du droit de la consommation. Sans s'étendre sur la manière dont le droit québécois devrait saisir la question, la démonstration vise à justifier pourquoi le droit de la consommation devrait prendre part au débat et non à savoir comment il devrait le faire.

Le mémoire sera divisé en deux chapitres qui représentent des technologies émergentes qui interviennent consécutivement dans la pratique, soit les données massives et l'intelligence artificielle. Dans un premier temps, la collecte massive de données sera étudiée sous l'angle du suivi du consommateur dans son environnement physique et ses activités numériques. Les consommateurs sont plus que jamais connectés par les téléphones intelligents, les réseaux sociaux et les objets connectés. L'activité en ligne du consommateur peut être épiée par les entreprises grâce à différentes techniques comme l'installation de témoins, de traceurs ou tout simplement avec les réseaux sociaux. Les récents développements technologiques ont permis d'assurer un suivi du consommateur dans son quotidien. Les entreprises diversifient leurs méthodes de collecte de données pour recueillir des informations sur la géolocalisation de leurs clients ou en utilisant des techniques de reconnaissance faciale à diverses fins. Cette collecte à grande échelle ouvre la porte de nouveaux canaux de communication, et permet de mieux connaître le profil du public ciblé afin de personnaliser l'offre de publicité.

[46] *Supra.* p. 12.

L’utilisation de l’intelligence artificielle sera examinée dans un second chapitre afin d’évaluer comment la technologie façonne aujourd’hui le marketing intelligent. L’influence des technologies sur le ciblage et le profilage à des fins publicitaire sera analysée pour se consacrer, par la suite, à la personnalisation des offres publicitaires. Ces pratiques comportent chacune de multiples lacunes autant juridiques et éthiques qui forgent les inégalités entre le consommateur et le commerçant. Cette structure permet de suivre le parcours des données utilisées à des fins marketing de manière concrète dans l’objectif de dégager le préjudice potentiel ou réel que peut subir le consommateur.

Chapitre I – Les données massives et le marketing

« Le tout est plus grand que la somme des parties. »[47]

Aristote

Le marketing intelligent puise sa force dans la masse de données générées par les consommateurs. Concrètement, les données massives sont de volumineuses bases de données hétérogènes dont la complexité croit continuellement en se construisant à travers une multitude de sources[48]. De nos jours, tout mouvement peut constituer une donnée, et même la donnée en soi crée de l'information, appelée métadonnée, qui permet aux analystes et aux modèles prédictifs d'inférer beaucoup d'informations sur les consommateurs en fonction de l'effet de la masse.

L'augmentation des capacités de stockage des données jumelée à la multiplication des sources de collecte a encouragé la réorientation du modèle d'affaire des entreprises vers une pratique axée sur l'analyse de données. Par exemple, l'analyse des préférences de visionnement chez les abonnés de la plateforme *Netflix* a permis à l'entreprise de prédire qu'une réadaptation de la célèbre série *House of Cards* serait bien accueillie par les utilisateurs, en laissant de côté l'instinct du directeur créatif de l'entreprise[49]. Cette approche prédictive permet aux entreprises de réagir promptement aux nouvelles tendances dans le marché et d'adapter leur offre de produit[50].

Toutefois cette masse de données pose le défi de développer des techniques d'analyse rapides afin de leur permettre d'utiliser l'extrant au bon moment tout en protégeant les droits des consommateurs[51]. Il est d'ailleurs attendu que 44 *zettaoctets* (10^{21} octets)[52] de données soient

[47] W D. ROSS, *Aristotle's Metaphysics*, Oxford, Clarendon Press, 1981.
[48] Xindong WU *et al.*, « Data mining with the big data », (2014) 26-1 *EEE Transactions on Knowledge and Data Engineering* 97, 98.
[49] David CARR, « Giving user what they want », *The New York Times*, 24 février 2013, en ligne : < https://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?auth=linked-facebook>
[50] Sunil EREVELLES, Nobuyuki FUKAWA et Linda SWAYNES, « Big data consumer analytics and the transformation of marketing », (2016) 69 *Journal of Business Research* 897, 900.
[51] X. WU *et al.*, préc., note 48, 97; S. EREVELLES, N. FUKAWA et L. SWAYNES, préc., note 50, 897.
[52] En information, un octet représente un multiplet de 8 bits permettant de coder des valeurs numériques. Cette information est une unité de mesure informatique permettant de représenter la capacité de stockage. (Voir Annexe I pour plus de détails) Un zettaoctets représente un sextillion d'octets (10^{21} = 1 000 000 000 000 000 000 000).

générés par les internautes en 2020 représentant 40 fois plus d'octets de données que le nombre d'étoiles dans le ciel[53]. Le marketing intelligent doit savoir composer avec une quantité astronomique d'informations qui lui donne l'avantage de connaître, presque en temps réel, les intérêts des consommateurs.

En 2012, les réseaux sociaux s'étaient enflammés lors du premier débat présidentiel de Barack Obama et Mitt Romney engendrant plus de 10 millions de gazouillis (*tweet*) en quelques heures[54]. L'analyse des mots-clés (*hashtag*) a permis de générer une réponse face au débat de manière presque instantanée. De ce fait, l'entreprise capable de dompter la masse de données bénéficie d'un avantage concurrentiel majeur dans le marché, mais à quel prix pour le consommateur?

L'avènement du *big data* a bouleversé les pratiques de marketing traditionnelles qui reposaient sur l'idée de « connaître son client ». Aujourd'hui, cette connaissance dépasse la simple courtoisie et s'invite dans l'intimité des consommateurs pour mieux comprendre et appréhender son comportement. Que ce soit lors de ces activités de tous les jours (1.1) ou lorsqu'il navigue en ligne (1.2), les entreprises agrègent une masse de données sensibles sur le comportement du consommateur au grand bonheur des commerçants laissant le consommateur sans même l'ombre d'une intimité.

1.1 Les données comportementales physiques

La collecte massive de données ne concerne pas seulement les activités en ligne des consommateurs. Avec le développement de nouvelles technologies comme les systèmes de géorepérage, la reconnaissance faciale ou les caméras infrarouges, les activités hors ligne des consommateurs peuvent également être numérisées. Pour les marketeurs, ces données permettent d'améliorer l'offre de produits, de simplifier les différentes étapes du processus d'achat du consommateur et d'intégrer la publicité de manière innovante. Les entreprises peuvent influencer le comportement du consommateur par une publicité ciblée, hors ligne, propulsée grâce à différentes méthodes numériques.

[53] Richard CHUNG, « How much data is generated each day », *World Economic Forum*, 17 avril 2019, en ligne : < https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>
[54] X. WU *et al.*, préc., note 48, 97.

L'une de ces pratiques exploite les téléphones intelligents et autres objets connectés afin de connaître la position géographique du consommateur pour lui offrir une publicité ciblée selon le lieu où il se trouve (1.1.1.). Le consommateur est alors intercepté au moment où il est le plus susceptible d'avoir un comportement d'achat spontané permettant aux entreprises de saisir chacune des opportunités et de transformer une simple sortie en dépense pour le consommateur.

Il existe également des technologies autonomes comme la reconnaissance faciale (1.1.2.) qui offrent plusieurs possibilités autant pour le consommateur que pour le commerçant. Elle permet entre autres de simplifier le processus d'achat en accélérant l'authentification du client. Cette fonction facilite les transactions qui nécessitent une preuve d'identité comme les opérations bancaires courantes. Pour les commerçants, elle offre une multitude d'avenues allant de la reconnaissance des émotions à la publicité personnalisée. Pour le consommateur, il reste toutefois difficile de s'en extraire.

1.1.1 Le positionnement géographique

Les technologies de géolocalisation font partie du quotidien des consommateurs, et ce, sans nécessairement que celui-ci en soit pleinement conscient. Que ce soit pour enregistrer les statistiques d'une course à pied avec une montre intelligente[55], commander un Uber[56] ou identifier les lieux visités sur les réseaux sociaux, les consommateurs partagent déjà leur localisation à grande échelle. C'est grâce aux dispositifs installés dans les appareils mobiles que les différentes entreprises sont en mesure de détecter la position des consommateurs. De nos jours, la majorité des téléphones et appareils électroniques sont munis d'un système de positionnement par satellite (GPS)[57] qui assure le suivi des individus avec une précision

[55] STRAVA, *Suivez et analysez chaque aspect de votre activité*, en ligne : <https://www.strava.com/features?hl=fr-FR#:~:text=Strava%20est%20le%20r%C3%A9seau%20social,chacun%2C%20et%20laisser%20des%20commentaires.>

[56] UBER, *Utilisation des informations de localisation des passagers par Uber (IOS),* en ligne : <https://help.uber.com/fr-FR/riders/article/utilisation-des-informations-de-localisation-des-passagers-par-uber%C2%A0ios?nodeId=741744cb-125c-4efc-ab3f-4a977940ac87>

[57] *Global Positioning System*.

d'environ 7 à 12 mètres[58] dans un environnement urbain[59]. Cette précision permet d'identifier de manière presque parfaite les différents lieux que le consommateur fréquente de manière quotidienne passent et même de prédire le lieu potentiel où le consommateur se trouvera à un moment donné et lui proposer la publicité appropriée (1.1.1.1)[60].

En raison de son caractère instantané, cette technologie à la capacité de s'adapter aux changements dans les habitudes de consommation des individus qui sont de plus en plus nomades[61]. Grâce aux données collectées, l'offre de publicité peut s'adapter si le consommateur est à la maison, au travail, en voyage d'affaires ou s'il change de lieu de résidence. Cette forme de marketing direct permet d'entretenir un lien étroit avec le consommateur et d'en connaître davantage sur ces habitudes seulement grâce à sa position (1.1.1.2).

1.1.1.1 Proposer de la publicité

Dans le quotidien des consommateurs, l'exploitation des données de géolocalisation peut prendre différentes formes. Les systèmes de géorepérage permettent notamment aux entreprises de générer des publicités ciblées dans un périmètre précis afin d'offrir la bonne publicité au bon moment. La publicité sera envoyée par courriel, message texte ou comme notification sur le téléphone mobile du consommateur lorsque le téléphone ou l'objet connecté traversera la frontière déterminée[62]. Par exemple, Starbucks est une entreprise bien connue pour ces offres géolocalisées. Elle invite les consommateurs ayant téléchargé l'application à se présenter dans le café le plus près afin de bénéficier d'un rabais sur leur breuvage préféré selon leurs habitudes de consommation recensé par le programme de fidélité[63]. Cette pratique, fort intéressante pour les entreprises, peut toutefois devenir abusive pour les consommateurs qui sont sollicités à tout moment.

[58]La précision de la localisation peut varier d'un modèle d'appareil à un autre. Krista MERRY et Pete BETTINGER, « Smartphone GPS accuracy study in an urban environment », (2019) 14-7 *Plos ONE* 1, 1.
[59] Kristen E. EDMUNDSON, « Global Position System Implants: Must Consumer Privacy Be Lost in order for People to Be Found? », (2005) 38 *Ind. L. Rev.* 207, 209.
[60] S. EREVELLES, N. FUKAWA et L. SWAYNES, préc., note 50, 900.
[61] Delphine DION et Aurélie MICHAUD-TREVINAL, « Les enjeux de la mobilité des consommateurs », (2004) 34 *Décisions Marketing* 17, 17.
[62] Sarit K. MIZRAHI, *The Legal Implications of Internet Marketing: Exploiting the Digital Marketplace Within the Boundaries of the Law*, Cowansville, Éditions Yvon Blais, 2015, p. 34.
[63] *Id.*, p. 34.

Juridiquement, les consommateurs ont préalablement consenti à recevoir ce type de publicité en acceptant les conditions d'utilisation de l'application et ont le choix de retirer leur consentement[64]. De cette manière, l'entreprise qui utilise ce genre de stratégie s'assure de respecter autant les lois entourant la concurrence, la protection des renseignements personnels, mais aussi le cadre juridique entourant les pourriels[65].

Ces lois protègent les consommateurs contre l'utilisation abusive des technologies numériques à des fins de sollicitation[66]. En France, l'article L. 34-5 du *Code des postes et des communications électroniques* prohibe spécifiquement la sollicitation non consentie auprès des consommateurs[67]. Cette disposition phare en matière de prospection commerciale par voie électronique fait partie intégrante du régime juridique entourant à la protection des renseignements personnels[68]. Introduite par la directive *vie privée et communication électronique*[69], elle complète aujourd'hui l'application du RGPD. Elle impose un consentement explicite (*opt-in*) de la part du consommateur conformément à l'article 4 du RGPD et prévoit que « [p]our l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. » [70] Par ailleurs, le message envoyé doit permettre au consommateur de pouvoir se désinscrire de manière définitive.

---

[64] STARBUCKS, *Conditions de l'application : communications par courriel, notifications poussées et messages in-app*, 2019.

[65] *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, LC 2010, c. 23. (Loi canadienne anti-pourriel ci-après LCAP) ; *Code des postes et des communications électroniques*, France, version consolidée au 31 juillet 2020.

[66] GOUVERNEMENT DU CANADA, *La Loi canadienne anti-pourriel*, 2020, en ligne : <https://www.fightspam.gc.ca/eic/site/030.nsf/fra/accueil>

[67] « Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. […] » art. L-34-5, al. 1, *Code des postes et des communications électroniques*, préc., note 65.

[68] Edouard GEFFRAY et Alexandre GUÉRIN-FRANÇOIS, *Com. Code de la protection des données personnelles*, Dalloz, art. L 34-5.

[69] 2002/58/CE du 12 juillet 2002

[70] art. L-34-5, al. 2, *Code des postes et des communications électroniques*, préc., note 65.

Au Canada, la LCAP est une mouture récente dont les premières dispositions sont entrées en vigueur en 2014 pour contrer les pratiques marketing abusives[71]. Elle vise principalement les courriels non sollicités (pourriels) ainsi que ces dérivés comme les messages textes, l'installation de logiciel non consentie, les représentations fausses et trompeuses en ligne ou la collecte de renseignements personnels obtenus en contournant illégalement les paramètres de sécurité d'un système[72]. Cette loi prohibe spécifiquement l'envoi de messages électroniques commerciaux qui invitent le consommateur à contracter ou qui offre une possibilité d'affaire quelconque[73]. La définition large retenue par le législateur pour les messages électroniques commerciaux permet d'étendre le champ d'application de la loi à toute sollicitation électronique non consentie[74]. De ce fait, la sollicitation par géorepérage tombe sous le champ de protection des lois anti-pourriels et les entreprises se doivent de mettre en place des pratiques publicitaires éthiques. L'offre publicitaire doit comprendre les renseignements permettant d'identifier l'émetteur du message, lui permettre de le contacter ainsi que de s'extraire de ces envois[75].

Au Canada, les responsabilités relatives à l'application de la loi sont divisées entre le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), le Bureau de la concurrence du Canada et le Commissariat à la protection de la vie privée du Canada[76]. Dans le cadre des pratiques de marketing abusives, le CRTC est responsable des enquêtes relatives aux questions d'envoi de messages électroniques commerciaux non sollicités[77]. Il a

[71]GOUVERNEMENT DU CANADA, *La Loi canadienne anti-pourriel*, 2020, en ligne : <https://www.fightspam.gc.ca/eic/site/030.nsf/fra/accueil>
[72] *Id.*
[73] Voir la définition de « Message électronique commercial », *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*, préc., note 65, art. 1 (2).
[74] *Id.*, art. 6 (1).
[75] *Id.*, art. 6 (2).
[76] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Responsabilités incombant au Commissariat en vertu de la LCAP*, Ottawa, 2014, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/loi-canadienne-anti-pourriel/casl_faqs_2014/>
[77]*Id.*; *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*

également le pouvoir de mener des enquêtes, mettre en place des mesures pour contrer les comportements fautifs et d'imposer des sanctions administratives pécuniaires pouvant aller jusqu'à 10 000 000$ pour une personne morale[78]. Le Bureau de la concurrence est responsable des questions de déclarations fausses ou trompeuses et des pratiques de commerce déloyales dans le marché numérique[79]. Le cas échéant, le Bureau de la concurrence s'intéresse plus particulièrement aux divulgations inappropriées comme les publicités conçues pour ne pas ressembler à un message publicitaire, les pratiques de « prix partiels » ou les conditions d'utilisations qui sont rédigées de manière illisible[80]. De son côté, le Commissariat encadre les pratiques en lien avec la protection des renseignements personnels des consommateurs et la collecte non consentie des renseignements visés incluant les adresses courriels et numéros de téléphone[81].

Un duo semblable est responsable du respect de l'article L. 34-5 en France. La CNIL et la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) s'occupent conjointement de la protection des consommateurs dans leur champ de compétence distinct. La CNIL a pour mandat d'entendre les plaintes des consommateurs et de protéger leurs données collectées à des fins de prospection alors que le bureau de la concurrence encadre les pratiques commerciales trompeuses et déloyales en ligne[82]. Par ailleurs, la DGCCRF et la CNIL ont signé un protocole de coopération au début de l'année 2019 afin de renforcer leur collaboration et de s'adapter aux nouveaux enjeux du numérique[83]. En comparaison avec les pénalités imposées par la LCAP au Canada, les sanctions imposées par la CNIL sont nettement inférieures avec une amende administrative

Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications, préc., note 65, art. 62.

[78] *Id.*, art. 20 (4) ; CONSEIL DE LA RADIODIFFUSION ET DES TÉLÉCOMMUNICATIONS CANADIENNE, *La Loi canadienne anti-pourriels*, 2020, en ligne : <https://crtc.gc.ca/fra/internet/anti.htm>

[79] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Responsabilités incombant au Commissariat en vertu de la LCAP*, préc., note 76.

[80] GOUVERNEMENT DU CANADA, *Notes pour une allocution de Matthew Boswell, sous-commissaire principal de la concurrence*, Ottawa, 2014, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03856.html>

[81] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Responsabilités incombant au Commissariat en vertu de la LCAP*, préc., note 76.

[82] E. GEFFRAY et A. GUÉRIN-FRANÇOIS, préc., note 68.

[83] CNIL, *La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles*, 31 janvier 2019, en ligne : <https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des>

qui ne peut dépasser les 15 000€ en France[84]. Toutefois, le RGPD prévoit une sanction administrative pouvant s'élever jusqu'à 20 000 000€ ou 4% du chiffre d'affaires de l'entreprise en cas de non-respect d'une injonction émise par l'autorité de contrôle[85].

De ce fait, les publicités par géorepérage tombent dans le champ d'application des lois anti-pourriels et sont surveillées par différentes entités. Elles doivent faire l'objet d'un consentement express qui se retrouve dans les conditions d'utilisation lisibles et accessibles et les données recueillies doivent respecter les fins prévues pour être envoyées au consommateur[86]. De cette manière, les consommateurs sont protégés contre la multiplication des offres publicitaires non consenties et les entreprises ont intérêt à s'assurer que le consommateur accepte de recevoir la publicité.

1.1.1.2 Analyser le comportement

La géolocalisation des consommateurs n'est pas seulement un moyen pour propulser la publicité, elle sert aussi d'outil d'analyse de comportement dans l'environnement physique. Le positionnement WIFI[87] est une technique utilisée par certains commerçants pour suivre les déplacements des consommateurs dans leur commerce. Cette forme de géolocalisation utilise la position connue des réseaux WIFI afin de déterminer la position d'un appareil dans l'environnement[88]. Ces systèmes permettent de combler les lacunes des données GPS qui sont ineffectives ou imprécises dans certains milieux comme à l'intérieur d'un bâtiment. En mesurant la force des signaux émis par les appareils mobiles vers la borne

[84] « Sous réserve qu'il n'ait pas été fait application de l'article L. 36-11 et en vue d'assurer la protection du consommateur, les manquements au présent article sont sanctionnés par une amende administrative, prononcée par l'autorité administrative chargée de la concurrence et de la consommation dans les conditions prévues au chapitre II du titre II du livre V du code de la consommation, dont le montant ne peut excéder 3 000 € pour une personne physique et 15 000 € pour une personne morale.», art. L-34-5, al. 8, *Code des postes et des communications électroniques*, préc., note 65.

[85] « Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. » *Règlement (UE) 2016/679*, préc., note 23, art. 83, 6).

[86] *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,* préc., note 65, art. 6 (1) a) et 10 (1).

[87] *Wifi Positioning System.*

[88] S. K. MIZRAHI, préc., note 62, p. 36.

WIFI la plus près, il est possible de mesurer la position d'un individu à l'intérieur avec une précision d'une dizaine de centimètres[89].

Pour ce faire, les entreprises doivent constituer une base de données qui identifie les réseaux existants grâce aux numéros d'identifiants, appelées adresses MAC[90], des bornes WIFI utilisées ainsi que l'adresse des appareils qui tentent de se connecter au réseau[91]. Chaque appareil possède un identifiant unique propre à la carte réseau[92]. Le système de positionnement WIFI peut calculer la localisation d'un appareil à partir du moment où le signal est devenu disponible et que l'appareil a tenté de se connecter au réseau. La puissance du signal permet alors de suivre la localisation de l'appareil dans l'environnement[93].

Concrètement, les commerçants peuvent alors utiliser ces systèmes pour suivre les déplacements des consommateurs sur une grande surface, évaluer les points d'intérêts ou mesurer l'achalandage de leur magasin. Le risque avec ce genre de technologies est qu'un commerçant installe plusieurs bornes dans le but de suivre systématiquement les consommateurs dans son établissement[94].

L'effet sur les droits des consommateurs varie en fonction du type de données collectées par les bornes WIFI. D'entrée de jeu, il est nécessaire de qualifier si les renseignements collectés par les bornes sont des renseignements personnels au sens du droit. La collecte de renseignements concernant l'adresse MAC constitue-t-elle un traitement de données à caractère personnel ? En principe, tout renseignement susceptible d'identifier l'individu visé par la collecte est considéré comme un renseignement personnel[95]. L'identifiant unique collecté pour géolocaliser le consommateur à l'intérieur du commerce correspond à l'adresse

---

[89] Adam CONNER-SIMONS, « Wireless tech means safer drones, smarter homes and password-free wifi », *MIT News*, 31 mars 2016, en ligne : <http://news.mit.edu/2016/wireless-tech-means-safer-drones-smarter-homes-password-free-wifi-0331> ; Arnaud BÉTRÉMIEUX, « Le WI-FI pour le positionnement et la navigation en intérieur », (2007) 111 *Revue XYZ* 27, 27.

[90] *Media Access Control.*

[91] S. K. MIZRAHI, préc., note 62, p. 36.

[92] Sans entrer dans les détails, ce code correspond à l'adresse MAC (Media Access Control) qui permet de cibler les équipements connectés à un réseau. John DAINTITH et Edmund WRIGHT, *A Dictionnary of Computing*, 6e éd., Oxford University Press, 2008, « MAC address ».

[93] S. K. MIZRAHI, préc., note 62, p. 36.

[94] *Id.*, p. 38.

[95] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 2 ; *Loi sur la protection des renseignements personnels et des documents électroniques*, préc., note 21, art. 2 ; *Règlement (UE) 2016/679*, préc., note 23, art. 4, 1).

MAC de l'appareil[96]. Cette adresse est constituée d'une série de numéros qui identifient le fabricant de l'appareil et rendent le code unique à l'appareil[97].

Un rapprochement peut être fait entre l'adresse MAC des appareils et les adresses IP des ordinateurs. Dans l'affaire *R. c. Spencer*, la Cour Suprême du Canada a reconnu que l'information liée à une adresse IP comme le nom et l'adresse du propriétaire pouvait être considérée comme un renseignement personnel en raison du lien informationnel entre les deux données[98]. En France, la Cour de cassation a également reconnu que « les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel »[99]. Le fait que l'adresse IP puisse être liée à des renseignements permettant d'identifier l'individu à la source permet de caractériser ce type de données comme étant un renseignement personnel. Dans le cadre des adresses MAC, l'information liée au code permet d'identifier le fabricant et non le propriétaire de l'appareil. De ce fait, la base de données nécessaire au positionnement WIFI ne permet pas d'identifier de manière individuelle les consommateurs. Elle permet seulement d'identifier que des appareils se trouvent dans un endroit donné. Concrètement, le code permet d'identifier qu'un appareil tente de se connecter au réseau, mais le lien entre l'appareil et son propriétaire n'est pas divulgué par le code. Toutefois, si l'adresse MAC est liée à un profil identifiant le consommateur dans la base de données, elle devra être considérée comme un renseignement personnel et sera soumise au régime juridique applicable.

---

[96] J. DAINTITH et E. WRIGHT, préc., note 92.

[97] «MAC addresses are 48- or 64-bit numbers that are divided into two parts. A unique three-byte […] identifies the device's manufacturer and must be purchased from the IEEE. The remaining three or five bytes are assigned by the manufacturer in any way it chooses, provided all instances are unique. » J. DAINTITH et E. WRIGHT, préc., note 92.

[98] [2014] 2 R.C.S 212, par. 50 « L'application de ce cadre d'analyse aux faits de la présente affaire est simple. Dans les circonstances de l'espèce, la demande de la police dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée visait en fait à établir un lien entre une personne précise (ou un nombre restreint de personnes dans le cas des services Internet partagés) et des activités en ligne précises. Ce genre de demande porte sur l'aspect informationnel du droit à la vie privée relatif à l'anonymat en cherchant à établir un lien entre le suspect et des activités entreprises en ligne, sous le couvert de l'anonymat, activités qui, comme la Cour l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en matière de vie privée : *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, par. 3; *Cole*, par. 47; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 40-45. »

[99] Civ. 1re, 3 nov. 2016, n° 15-22.595, publié au Bulletin ; AJDA 2017. 23 ; D. 2016. 2285 ; Dalloz IP/IT 2017. 120, obs. G. Péronne et E. Daoud.

1.1.2 La reconnaissance faciale et le marketing

Les technologies de reconnaissance faciale font ressortir des questions juridiques fondamentales sur des enjeux éthiques et sensibles comme le profilage racial et la surveillance de masse. La technologie étant par nature imparfaite et ses créateurs parfois biaisés, le droit à la vie privée des individus peut être violé de manière mécanique par la technologie en place. Leur utilisation par les forces de l'ordre et les instances gouvernementales n'a d'ailleurs pas su obtenir les faveurs de la population[100]. Encore une fois l'image du *big brother* s'accroche à cette technologie en raison des dérives observées dans certains pays[101].

Dans la foulée du mouvement de contestation contre la brutalité policière et le profilage racial suite au décès de George Floyd lors d'une intervention policière abusive[102], Amazon suivi de IBM et Microsoft ont pris la décision de cesser la vente d'outils de reconnaissance faciale aux institutions gouvernementales afin de contrer les dérives potentielles de l'usage de cette technologie[103]. Par ailleurs, une étude menée par des chercheurs du MIT[104] a permis de démontrer que les logiciels de reconnaissance faciale développés par trois grandes compagnies du secteur technologique[105] opéraient un biais en fonction du genre et de la

[100] Tristan PÉLOQUIN, « Reconnaissance faciale : un risque de « surveillance de masse » », *LaPresse*, 29 juin 2020, en ligne : <https://www.lapresse.ca/actualites/2020-06-29/reconnaissance-faciale-un-risque-grave-de-surveillance-de-masse.php>

[101] L'exemple du développement d'une cote sociale en Chine est flagrant. Les autorités ont mis en place un système de reconnaissance faciale partout au pays afin d'identifier les individus et de contrôler un indicateur social : la cote sociale. Cette cote diminue en fonction des mauvais comportements comme traverser la rue sans passer par l'intersection. Cette cote permet par la suite d'accéder aux services sociaux comme le transport en commun et bien plus encore. Guy ST-JACQUES et *al.*, « Noter les citoyens en Chine pour mieux les contrôler », Radio-Canada Info, 9 avril 2018, en ligne : <https://ici.radio-canada.ca/premiere/emissions/medium-large/segments/entrevue/66923/chine-note-sociale-donnees-numeriques-gouvernement-chinois>

[102] Sophie-Hélène LEBOEUF, « « Je ne peux pas respirer », a répété George Floyd une vingtaine de fois », *Radio-Canada*, 9 juillet 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1718312/je-ne-peux-pas-respirer-george-floyd-transcription-cameras-intervention-cour>

[103] Joseph PREZIOSO, « IBM ne vendra plus d'outils de reconnaissance faciale », *AFP*, 9 juin 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1710439/ibm-reconnaissance-faciale-discrimination-racisme-justice> ; Karen HAO, « The two year fight to stop Amazon from selling face recognition to the police », *MIT Technology Review*, 12 juin 2020, en ligne : <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/?truid=85d02b5a0a9c094e8d8229838e9b5953&utm_source=the_algorithm&utm_medium=email&utm_campaign=the_algorithm.unpaid.engagement&utm_content=06-12-2020>

[104] Massachusetts Institute of Technology.

[105] IBM, Microsoft et Face++.

couleur de la peau[106]. Les technologies de reconnaissance faciale étant de plus en plus utilisées, le manque d'acuité pour un groupe ciblé d'individus pose le problème de l'équité du traitement. Des cas d'accusation par erreur suite à l'usage cette technologie ont également fait la une des médias depuis le début du mouvement[107]. En réponse à ces évènements, le parti démocrate a même déposé un projet de loi qui inclus la proposition de limiter l'usage de technologies de reconnaissance faciale par les autorités policières, une première au niveau du Congrès américain de vouloir encadrer ce type de technologie[108].

Le risque d'erreur ou de confusion d'identité soulevé par les chercheurs du MIT est inhérent à ce type de technologies. En effet, ce type de système probabiliste comporte inévitablement un taux de « faux rejets » et de « fausses acceptations » faisant varier les résultats obtenus[109]. Le refus par le système de l'image adéquate de la personne génère un faux rejet menant à une erreur sur l'identité. D'un autre côté, l'acceptation par erreur du système de l'image d'un autre individu représente une fausse acceptation menant à la confusion de l'identité. Les deux formes d'erreur peuvent mener à la discrimination et à une forme de profilage racial soulevées par le public.

Néanmoins, les technologies de reconnaissance faciale offrent plusieurs avenues marketing intéressantes autant pour le consommateur que le commerçant. Elle permet aux commerçants de collecter des informations en temps réel sur les consommateurs comme l'âge, le genre, le temps passé dans un lieu, les émotions et même les menaces pour la sécurité. Ces informations peuvent être utilisées par les commerçants pour identifier la clientèle (1.1.2.1) et améliorer leurs produits et services en conséquence des observations faites, au bénéfice du

---

[106] En effet, le taux d'erreur pour identifier un homme blanc serait de 0.8% comparativement à un taux variant entre 20% à 34% pour les femmes noires. Larry HARESTY, « Study finds gender and skin-type bias in commercial artificial-intelligence systems », *MIT News*, 11 février 2018, en ligne : <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212> ; Joy ADOWAA BUOLAMWINI, *Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*, mémoire de maîtrise, Faculté des Médias, Sciences et Arts, Massachusetts Institute of Technology, 2017, p. 74.

[107] AFP, « Un homme arrêté à tort à cause de la technologie de reconnaissance faciale », *LaPresse*, 24 juin 2020, en ligne : <https://www.lapresse.ca/international/etats-unis/2020-06-24/un-homme-arrete-a-tort-a-cause-de-la-technologie-de-reconnaissance-faciale?utm_source=facebook&utm_medium=social&utm_campaign=algofb>

[108] K. HAO, préc., note 103.

[109] Julie GAUTHIER, *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée*, mémoire de maîtrise, Faculté de droit, Université de Montréal, 2015, p. 51.

consommateur alors que celui-ci voit son processus d'achat simplifié. L'usage de données biométriques comporte toutefois son lot de risques (1.1.2.2)

1.1.2.1 L'identification et l'authentification

En pratique, la reconnaissance faciale a une fonction d'authentification ou d'identification. L'authentification permet de valider l'identité de l'individu représenté alors que l'identification permet de retrouver un individu dans un groupe en fonction de son profil[110]. Dans le second cas, l'identification suppose la création d'une base de données permettant d'effectuer la comparaison entre plusieurs personnes.

Dans le contexte publicitaire, la technologie permet de qualifier les informations démographiques de l'audience[111], de mesurer l'attention portée au message et même d'analyser les réactions et en tenir compte pour personnaliser le message[112]. À titre d'exemple, le centre commercial Place Ste-Foy de Québec a lancé un projet pilote permettant de mieux identifier et connaître les profils de la clientèle qui fréquentait certaines boutiques du centre commercial[113]. Des caméras dotées de la technologie d'analyse vidéo anonyme interprétaient les informations démographiques et même les réactions des consommateurs afin de mieux comprendre leurs habitudes de consommation[114]. La technologie a permis aux commerçants de mieux comprendre les besoins de leurs consommateurs, d'adapter l'offre de produits en conséquence, reconfigurer l'espace de leur boutique et même proposer de nouveaux services à la clientèle[115]. Comme mentionné précédemment, l'utilisation de la reconnaissance faciale à des fins commerciales n'est pas encore une pratique socialement acceptée[116].

---

[110] CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, 15 novembre 2019, p. 3, en ligne: <https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf>

[111] Voir PLACE STE-FOY, *La fonderie de l'innovation dans le commerce de détail (FICD)*, en ligne : <https://www.placestefoy.com/fr/la-fonderie-de-linnovation-dans-le-commerce-de-detail-ficd/#:~:text=LE%20PROJET%20PILOTE%20%C3%80%20PLACE%20STE%2DFOY%20UTILISAIT%2DIL%20DE,reconna%C3%AEtre%20l'identit%C3%A9%20des%20consommateurs.>

[112] POSTERSCOPE WORLDWINE, *Interactive Facial Recognition Digital OOH Billboard Campaign for GM*, Santa Monica, [video] en ligne : <https://www.youtube.com/watch?v=Kj7Dm_i-OoM>

[113] PLACE STE-FOY, préc., note 111.

[114] *Id.*

[115] *Id.*

[116] Loïc TASSÉ, « La folie de la reconnaissance faciale », *Journal de Montréal*, 23 janvier 2019, en ligne : <https://www.journaldemontreal.com/2019/01/23/la-folie-de-la-reconnaissance-faciale>

Les capacités d'authentification et de reconnaissance reposent sur l'identification des données biométriques d'un individu donné grâce aux traits uniques de son visage[117]. Basée sur une technique informatique probabiliste, la technologie crée, à partir d'une image donnée ou d'un vidéo, un gabarit représentant les traits spécifiques à la personne désignée. Afin de pouvoir procéder à une réelle reconnaissance, la technique doit s'opérer en deux temps soit la collecte initiale des informations puis la reconnaissance de ces traits via un autre médium comme la caméra vidéo[118]. Que ce soit pour identifier ou authentifier un individu, les techniques de reconnaissance faciale se basent donc sur l'estimation statistique de la correspondance entre l'image initiale et l'image captée.

Au niveau des services bancaires, la reconnaissance faciale permet l'authentification de la clientèle et assure en quelque sorte la légitimité de la transaction à effectuer. La *CaixaBank* en Espagne développe actuellement un projet de reconnaissance faciale adapté aux guichets automatiques qui compte permettre à leurs clients d'accéder à leur argent en un clin d'œil[119]. Ce système basé sur les données biométriques est d'ailleurs le premier en Europe à atteindre un niveau de sécurité équivalent à celui des codes NIP[120]. Pour certains, l'idée d'un mode de paiement basé sur la reconnaissance faciale relève directement de la science-fiction, alors qu'en réalité, elle est déjà établie dans plusieurs pays comme la Chine[121]. En Amérique, les entreprises Visa et Mastercard utilisent déjà la reconnaissance faciale via la technologie FaceID développée par Apple pour permettre aux consommateurs d'accéder à leur compte bancaire sur leurs téléphones intelligents[122]. La reconnaissance faciale a donc déjà fait ses premiers pas dans le quotidien des consommateurs occidentaux pour faciliter leurs opérations

---

[117] Caroline LEQUESNE ROTH (dir.), *La reconnaissance faciale dans l'espace public : une cartographie juridique européenne*, Fablex DL4T, Université Côte d'Azur, Nice, p. 11 ; Richard HOPKINS, « An Introduction to Biometrics and Large Scale Civilian Identification », (1999) 13 *Int'l Rev. of L. Computers & Tech.* 337 ; Robert R. JUENEMAN et R.J. ROBERTSON, « Biometrics and Digital Signature in Electronic Commerce », (1998) 38 *Jurimetrics J*. 427

[118] CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, préc., note 110.

[119] FINEXTRA, « CaixaBank to roll out facial recognition ATMs across Spain », *Finextra*, 10 juin 2020, en ligne : <https://www.finextra.com/newsarticle/35976/caixabank-to-roll-out-facial-recongition-atms-across-spain?utm_medium=newsflash&utm_source=2020-6-10&member=120460>

[120] *Id.*

[121] Moshe SELFIN, « Is the Rest of the World Ready for Facial Pay ? », *Payments Journal*, 10 mars 2020, en ligne : <https://www.paymentsjournal.com/is-the-rest-of-the-world-ready-for-facial-pay/>

[122] Quentin FORTTRELL, « Silicon Valley's final frontier for payments : 'The neoliberal takeover of the human body' », *Marketwatch*, 23 octobre 2019, en ligne : <https://www.marketwatch.com/story/the-technology-that-should-finally-make-your-wallet-obsolete-2019-09-06>

bancaires. Les consommateurs doivent avoir avec eux leur téléphone intelligent pour en faire l'usage, mais son développement rapide peut laisser croire que dans un futur proche la reconnaissance faciale sera coutume dans le secteur.

L'intérêt pour l'utilisation de données biométrique est qu'elles sont plus difficiles à frauder. Or, ces systèmes ne sont pas exempts de failles. Les données biométriques, comme toute autre information, peuvent être volées ou modifiées au même titre qu'un mot de passe. Les données biométriques sont permanentes et uniques à chaque individu augmentant de ce fait l'intérêt envers ce type de données à des fins de vol d'identité. Or, contrairement aux renseignements normalement utilisés à des fins de cybersécurité comme les mots de passe et les codes, les données biométriques ne sont pas secrètes[123]. L'enjeu avec ce type de données est qu'une fois les données corrompues elles deviennent caduques[124]. L'utilisateur dont les données ont été piratées sera confondu avec son usurpateur imposant à celui-ci de faire la preuve de son identité biologique.

1.1.2.2 La biométrie et la notion de renseignements personnels

Les enjeux soulevés par cette technologie dépendent de la finalité de l'usage des données recueillies. Une application qui utilise la reconnaissance faciale à des fins d'authentification de l'utilisateur n'engendre pas les mêmes risques qu'une caméra posée dans un espace public chargée d'identifier les individus[125]. Les données recueillies par les technologies de reconnaissance faciale font partie d'un plus grand ensemble : les données biométriques[126]. La CNIL définit les données biométriques comme étant : « […] l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.[127] » Dès lors, la question se pose à savoir si les données biométriques et les images recueillies à des fins de

[123] J. GAUTHIER, *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée*, préc., note 109, p. 53.
[124] *Id.*
[125] CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, préc., note 110.
[126] Les données biométriques se définissent comme étant un ensemble de données biologique propre à un individu permettant leur identification grâce à des modèles informatiques. Voir COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*, Ottawa, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/>
[127] CNIL, *Biométrie*, en ligne : <https://www.cnil.fr/fr/biometrie>

reconnaissances faciales sont considérées comme un renseignement personnel au sens de la loi. Le RGPD statue clairement sur ce point et définit les données biométriques comme étant des renseignements personnels[128]. Par ailleurs, le Groupe de travail article 29 sur la protection des données s'était prononcé déjà en 2003 afin de statuer que les données biométriques constituaient une donnée à caractère personnel[129].

Au Canada, il n'existe aucune mention explicite des données biométriques autant dans la loi fédérale sur la protection des données[130] que celle provinciale[131]. Or, ce type de renseignement correspond aux critères qui définissent la notion de renseignements personnels, soit l'identification des personnes[132]. Par ailleurs, la position du Commissariat à la protection de la vie privée du Canada et de la Commission d'accès à l'information est claire à ce propos : les données biométriques sont des renseignements personnels[133]. La *Loi concernant le cadre juridique des technologies de l'information*[134] prévoit que la création d'une banque de données biométriques doit être divulguée à la Commission d'accès à l'information[135] et que les données doivent être collectées avec le consentement exprès de la personne visée[136]. La Cour fédérale a également eu l'occasion de se prononcer sur la question dans l'affaire *Turner c. Telus Communication Inc.* en reconnaissant que l'empreinte vocale constitue un renseignement personnel[137]. Malgré l'absence explicite de mention dans les lois canadiennes, les données biométriques et les images recueillies à des fins de reconnaissances faciales sont bel et bien protégées par le corpus juridique canadien entourant le droit à la vie privée.

---

[128] *Règlement (UE) 2016/679*, préc., note 23, art. 4, al. 14 « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques; »

[129] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », Commission européenne, Adopté le 1er août 2003, p.5.

[130] *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 21, c. 5

[131] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22.

[132] *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 21, art. 2 ; *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 2.

[133] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*, préc., note 126.

[134] RLRQ, c. C-1.1.

[135] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1, art. 45.

[136] *Id.*, art. 44, al. 1.

[137] *Turner c. Telus Communications Inc.*, 2005 CF 1601, par. 22.

En pratique, l'usage des données biométriques peut constituer une atteinte au droit à la vie privée des individus. Le degré d'atteinte varie toutefois selon l'usage qui est fait des données. Par exemple, l'utilisation de la reconnaissance faciale à des fins d'authentification comme dans le secteur bancaire constitue une moins grande atteinte que l'identification des individus par les forces de l'ordre. Étant encadré par le corpus juridique du droit à la vie privée, les technologies de reconnaissance faciale sont également soumises à la nécessité d'obtenir le consentement de l'individu à la collecte des images[138]. Cette technologie sans contact et à la capacité d'être installée partout à l'insu de tous, il est dès lors utopique de croire que le consommateur pourrait réellement manifester son consentement ou même refuser qu'on utilise son visage pour quelques fins que ce soit. L'option envisagée par les commerçants dans la plupart du temps est l'affichage pour permettre au consommateur de savoir que la technologie est utilisée. Toutefois, en cas de désaccord ou de refus, les options qui s'offrent à lui sont seulement de ne pas accéder au lieu.

Cette technologie limite donc le droit à l'anonymat de l'individu dans son environnement physique, soit le droit de circuler publiquement sans être reconnu ou que des données le concernant soit recueillies. En somme, l'utilisation de technologies de reconnaissance faciale comporte plusieurs risques pour le consommateur dont il ne peut s'extraire que par le refus d'accès aux lieux où cette technologie est utilisée. L'utilisation à des fins purement statistiques comme dans le projet de la Place Ste-Foy à Québec pose un préjudice minimal au consommateur, mais c'est lorsque les données recueillies à des fins d'identification et de profilage que le consommateur est vulnérable[139].

La collecte massive de données comportementales physiques est une réalité qui envahit peu à peu le quotidien des consommateurs. L'intégration des nouvelles technologies dans la place publique regorge d'opportunités pour les commerçants que ce soit pour propulser la publicité, analyser le comportement des consommateurs ou mesurer la réponse aux publicités. Or, le consommateur est-il réellement avantagé de ses pratiques comparativement aux retombées pour les entreprises ? L'environnement numérique dévore les données générées par les

[138] CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, préc., note 110.
[139] Cette portion est étudiée en détail dans la section 2.2.1 du présent mémoire.

consommateurs alors que son environnement physique le trahit également. L'idée de circuler sans être épié s'efface donc de jour en jour.

1.2 Les données comportementales numériques

Les activités en ligne des consommateurs sont la source première de collecte de données massives par les entreprises publicitaires et les grands joueurs économiques[140]. L'hyperconnectivé des consommateurs leur permet de suivre leurs activités en ligne, et ce, peu importe la plateforme. L'essor du commerce électronique, propulsé de manière exponentielle par la pandémie qui frappe le monde entier, a transformé internet en une source de données comportementales incontournable pour les agences marketing. Le web permet facilement aux entreprises de suivre le comportement des consommateurs et de se bâtir une base de données importante sur leurs habitudes de consommation.

L'une des pratiques les plus connues est l'utilisation de témoins (1.2.1) qui permet aux marketeurs de connaître les habitudes de navigation des consommateurs sur la toile. Certaines pratiques plus intrusives et moins transparentes se sont développées au fil des années permettant non seulement d'identifier le consommateur sur un site donné, mais aussi de le suivre sur le web. La pratique ayant gagné en popularité, les témoins sont devenus presque inévitables à toute navigation sur le web. Le consommateur se voit imposer ces fichiers témoins par les commerçants alors que les moyens pour s'en extraire deviennent de plus en plus complexes.

D'un autre côté, les consommateurs partagent également de manière volontaire une multitude de données concernant leurs intérêts, les loisirs qu'ils pratiquent et bien plus encore. L'utilisation des réseaux sociaux a transformé la manière de collecter des données (1.2.2). Grâce à ces plateformes interactives, les consommateurs communiquent non seulement entre eux, mais aussi directement et indirectement avec les entreprises par le biais des boutons « j'aime », de commentaires ou de messages privés. Les marketeurs disposent alors d'une mine d'informations afin de mieux connaître le consommateur. Pour autant, celui-ci est-il suffisamment protégé face à cette collecte massive?

[140] GAFAM.

1.2.1 Les témoins et traceurs

L'usage des témoins et traceurs est une pratique grandement répandue dans l'économie numérique. Pour le grand public, ils demeurent peu connus et incompris (1.2.1.1). Les témoins permettent de collecter une foule de donnée assurant l'efficacité de la navigation pour le consommateur. Toutefois, ces données peuvent devenir particulièrement sensibles une fois agrégées ensemble (1.2.1.2). De plus, le consentement au partage de ces renseignements demeure critiquable considérant que dans certaines juridictions il peut être impossible de les refuser (1.2.1.3). Malgré les dispositions en place qui limitent la collecte de renseignements personnels (1.2.1.4), l'usage des témoins et traceurs demeure fortement répandue.

1.2.1.1 Les témoins

Les témoins, appelés communément traceurs ou *cookies*, sont des fichiers textes invisibles déposés sur le disque dur de l'ordinateur de l'utilisateur lorsqu'il navigue sur le Web[141]. Le terme *cookie* fait référence à cet identifiant opaque qui circule entre différents logiciels afin de recueillir des informations[142]. En soi, un témoin est une information textuelle échangée entre le serveur et le client (l'utilisateur de la page web) afin de permettre au serveur de conserver l'information de la dernière activité de l'utilisateur sur le site web[143]. Par exemple, lorsqu'un consommateur effectue des achats en ligne via le site d'un commerce, le serveur du commerçant dépose un témoin sur le serveur de l'utilisateur et recueille des renseignements sur son comportement en ligne lorsqu'il navigue sur le site web. Ces renseignements concernent notamment l'adresse IP de l'ordinateur, les pages web, le temps passé sur ces pages, les publicités consultées, les articles mis dans le panier d'achats virtuels, les achats effectués, les paramètres du site comme la langue ou la région, le type de navigateur utilisé et même des données de géolocalisation[144]. Le navigateur stocke le témoin en question sur le disque dur local de l'ordinateur afin que le site web puisse récupérer l'information

[141] D. M. KRISTOL, préc., note 28, 153.
[142] *Id.*, 152.
[143] *Id.*, 153-154.
[144] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La publicité comportementale en ligne : un survol*, Ottawa, 2011, p. 1, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/02_05_d_52_ba_02/>

enregistrée ultérieurement. Ces témoins visent à assurer l'amélioration des sites web, déceler la fraude, et surtout, permettent de collecter des données pour la publicité comportementale en ligne[145]. Ils sont utiles autant pour le consommateur que le commerçant. Sans ceux-ci, les consommateurs auraient l'obligation d'entrer à nouveau tous les renseignements nécessaires à chaque visite sur le site web alors que les commerçants peuvent notamment contrôler la sécurité de leur site web. Or, la diversité des témoins s'est décuplée dans les dernières années avec les témoins tiers, témoins *flash*, super-témoins ainsi que des techniques de suivi sans témoins. Ceux-ci se sont dès lors égarés de leur fonction utilitaire pour remplir avec brio une nouvelle fonction, la fonction publicitaire.

Initialement, les témoins étaient utilisés dans un contexte binaire entre l'utilisateur et le site web. Aujourd'hui, la relation est multipartite permettant aux entreprises publicitaires de se lier aux sites web pour effectuer une collecte de données sur les activités en ligne du consommateur. Ce type de témoins, les témoins tiers, sont déposés lors de la visite sur un site web lié avec l'agence publicitaire et permettent à celle-ci de recueillir le témoin lors d'une prochaine visite du consommateur sur le site ou sur tout autre site qui collabore avec cet annonceur[146]. Le témoin tiers permet alors d'identifier le consommateur dans sa navigation sur le web en général, et non seulement pour la maintenance et l'effectivité du site web.

Certains témoins peuvent être associés à des logiciels comme dans le cas des témoins *flash*[147]. Ils reposent sur le même principe que les témoins traditionnels. Leur particularité est qu'ils ont été créés par Adobe pour permettre la lecture de fichiers multimédias (flash) en ligne[148]. Toutefois, les témoins *flash* sont plus difficiles à identifier par l'internaute et, conséquemment, plus difficiles à supprimer pour celui-ci.

---

[145] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, Ottawa, 2015, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/>

[146] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les témoins et le suivi sur le web*, Ottawa, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/temoins/02_05_d_49/>

[147] ADOBE, *Use of cookies dans similar technologies*, « Témoins », 2019, en ligne : <https://www.adobe.com/ca_fr/privacy/cookies.html>

[148] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les témoins et le suivi sur le web*, préc., note 146.

Avec le temps, une forme de témoins plus sophistiquée a également vu le jour portant le nom de super-témoins. Ceux-ci possèdent des mécanismes de stockages plus étendus qui permettent de suivre le consommateur dans la plupart de ses activités en ligne et non seulement sur un site web unique[149]. L'enjeu est qu'ils sont encore une fois très difficiles à identifier, ils sont installés à l'insu du consommateur et requièrent des outils numériques particuliers pour les retirer.

Il existe également des méthodes de suivi numérique qui s'apparentent au témoin nommé le pixel-espion. Ce sont en réalité des fichiers images invisibles qui sont placés à l'intérieur d'une page web ou d'un courriel. Une fois la page consultée, l'image est téléchargée sur le serveur de l'ordinateur afin d'enregistrer le comportement de l'utilisateur. Les témoins ont donc évolué de manière complexe et diversifiée rendant la tâche du contrôle de leurs données personnelles au consommateur laborieuse.

1.2.1.2 Les témoins et les données sensibles

Un des enjeux que pose le développement des différentes formes de témoins est qu'ils touchent à de l'information de nature très privée et spécifique. Les témoins permettent de créer des profils concernant les internautes pouvant mener facilement à la réidentification de l'usager[150]. En étant installés dans les navigateurs des internautes, les témoins recueillent des données d'une sensibilité accrue. En 2006, le moteur de recherche AOL avait partagé par erreur les requêtes sur le moteur de recherche de 20 millions d'utilisateurs ce qui a permis au New York Times de réidentifier certains d'entre eux en jumelant les mots-clés utilisés aux bases de données publiques disponibles[151]. En général, les requêtes envoyées sur les moteurs de recherche renferment des informations particulièrement sensibles qui permettent de révéler les intérêts du consommateur, mais aussi ces préoccupations et des questions d'intérêts privés. Certains mots-clés sont susceptibles de représenter des états émotionnels profonds ou des problèmes psychologiques comme « dépression/anxiété » ou « arrêt de travail » et donc, susceptible de gêner l'individu identifié. Comme le démontre l'affaire AOL,

[149] *Id.*
[150] *Règlement (UE) 2016/679*, préc., note 23, considérant 30.
[151] Michael BARBARO, « A Face Is Exposed for AOL Searcher no. 4417749 », *The New York Times*, 9 août 2006, en ligne : <https://www.nytimes.com/2006/08/09/technology/09aol.html>

la collecte des données concernant la navigation sur le web d'un individu atteint un degré de sensibilité insoupçonné.

La Cour suprême du Canada a eu l'occasion de se prononcer à plusieurs reprises quant à l'importance de la protection de la vie privée en ligne. Interprété dans un contexte de droit criminel en application de l'article 8 de la *Charte canadienne des droits et libertés*[152], l'historique de navigation ou le contenu d'un ordinateur contient des renseignements intimes et privés qui ne laissent aucun doute sur leur qualification à titre de renseignement personnel[153]. Malgré tout, il est possible d'en tirer comme conclusion que les Canadiens sont en droit de s'attendre à la protection de leur vie privée à l'égard de ce type de renseignements proportionnellement à leur sensibilité[154]. Les données que recueillent les témoins peuvent être de nature très sensible puisqu'ils concernent non seulement les données d'identification, mais conservent en quelque sorte une trace de l'historique de navigation de l'utilisateur. Par ailleurs, dans un rapport canadien sur la confiance des internautes envers le numérique, 87% des Canadiens affirmaient qu'ils étaient inquiets que les entreprises auxquelles ils partagent leurs renseignements personnels acceptent de les partager à une tierce partie sans leur consentement[155].

À ce propos, le Commissariat à la protection de la vie privée du Canada a conclu, en interprétant de manière large la notion de renseignements personnels dans le contexte de la publicité comportementale en ligne, que les renseignements recueillis par les témoins peuvent constituer un renseignement personnel au regard de la LPRPDE[156]. En raison du mode d'exploitation des témoins tiers et les autres formes dérivées de témoins, les autorités

---

[152] « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » *Charte canadienne des droits et libertés*, préc., note 19, art. 8.
[153] *R. c. Spenser*, préc., note 98,
[154] *R c. Morelli*, préc., note 98, *R. c. Cole*, préc., note 98, par. 2.
[155] AUTORITÉ CANADIENNE POUR LES ENREGISTREMENTS INTERNET, *Les canadiens méritent un meilleur internet*, Ottawa, 2019, p. 6, en ligne : <https://www.cira.ca/fr/resources/letat-de-linternet/rapport/les-canadiens-meritent-un-meilleur-internet>
[156] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé du rapport d'enquête en vertu de la LPRPDE no. 2003-162*, Ottawa, 2003, p. 5, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-162/> (29 mars 2020) ; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé du rapport d'enquête en vertu de la LPRPDE no. 2005-319*, Ottawa, 2005, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-319/> (29 mars 2020) ; *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 21.

en matière de vie privée se questionnent quant à la qualité du consentement au partage de renseignements personnels à ces tiers inconnus du consommateur[157]. Autant dans le système juridique français que canadien, le consentement doit pourtant être donné à des fins spécifiques[158]. Le consommateur devrait savoir quels renseignements seront partagés et à qui.

1.2.1.3 Le consentement au dépôt de cookies et traceurs

Les témoins et traceurs se sont développés autour du modèle de consentement implicite, dit *opt-out*, prenant pour acquis le consentement du consommateur en lui laissant l'opportunité de le retirer s'il le désire. Concrètement, plusieurs sites web consultés affichent des bandeaux informant les consommateurs qu'un témoin est installé sur le site web et que la navigation sur le site équivaut au consentement à l'installation de ceux-ci. Le consommateur se voit imposé cette méthode de suivi sans pouvoir leur refuser l'accès à ses informations. À ce propos, le droit civil québécois est pourtant très clair: le silence ne vaut pas l'acceptation[159]. Cette méthode a d'ailleurs été jugée par la Cour de justice de l'Union Européenne comme étant contraire à l'exigence d'une manifestation de volonté imposée par la définition du consentement prévu dans le RGPD[160]. Depuis l'adoption de la directive « vie privée et communication électronique » de 2002[161], ce modèle de consentement a dû être remplacé au sein de l'Union Européenne par un consentement explicite, aussi appelé *opt-in*, où le consommateur doit adopter un comportement actif et accepter que le cookie soit installé[162]. En comparaison aux sites web québécois, les consommateurs français peuvent choisir quels renseignements seront partagés.

---

[157] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les témoins et le suivi sur le web*, préc., note 146.
[158] *Loi sur la protection des renseignements personnels et des documents électroniques*, préc., note 21, Principe 4.3 ; *Règlement (UE) 2016/679*, préc., note 23.
[159] *Code civil du Québec*, LQ 1991, c. 64, art. 1394, al. 1.
[160] *Bundesverband der Verbraucherzentralen und Verbraucherverbände*, CJUE, gr. ch., 1er oct. 2019, aff. C-673/17 : JCP E, n° 41, 10 Octobre 2019, act. 652
[161] *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*, OJ L 105, 13.4.2006, p. 54–6
[162] François COUPEZ et Géraldine PÉRONNE, « Consentement aux cookies : quelle est la bonne recette ? » *D. IP/IT* 2020.189 ; S. K. MIZRAHI, préc., note 62, p. 91.

Avant l'adoption du RGPD, la *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* imposait une obligation générale d'information concernant le traitement des renseignements stockés «dans le terminal de communications électroniques», aujourd'hui reconnus comme étant les *cookies* et traceurs[163]. Ces dispositions sont issues de l'ordonnance du 24 août 2011[164] transposant ainsi la directive 2009/136/CE « paquet télécoms » du 25 novembre 2009[165]. Cette disposition prévoit que le consommateur doit avoir été préalablement informé de l'installation et l'utilisation de cookies et traceurs et avoir donné son consentement à la collecte des informations visées.

De son côté, le Commissariat à la protection de la vie privée du Canada considère toutefois le modèle de consentement implicite acceptable sous certaines conditions[166]. Les consommateurs doivent être informés de la pratique de façon claire et transparente et ce, préalablement à la collecte. Ils doivent pouvoir renoncer à l'installation de témoins et le refus doit pouvoir être immédiat et durable. Les renseignements recueillis doivent être limités à ceux nécessaires et ceux-ci doivent être détruits dans un délai raisonnable[167]. La position de la Cour de justice de l'Union Européenne et la directive de 2002 est plus que respectable considérant que le modèle de consentement *opt-out* transfère au consommateur la responsabilité de comprendre ce qui est fait de ses données et de retirer son consentement s'il le désire alors qu'en réalité, une partie significative des usagés ne comprennent pas les rouages d'internet. Par ailleurs, l'approche *opt-in* répond aux exigences de consentement énoncées par les différents régimes juridiques permettant au consommateur une certaine liberté de choix.

---

[163] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* J.O. 7 janvier 1978, art. 32-II.

[164] *Ord. nº 2011-1012 du 24 août 2011,* art. 37

[165] *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs,* OJ L 337, 18.12.2009, p. 11–36

[166] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, préc., note 145.

[167] *Id.*

L'usage des différentes sortes de témoins soulève des questions juridiques par rapport au respect de plusieurs droits liés au droit à la vie privée, dont le droit à l'anonymat[168] et à l'intimité[169]. Pour le professeur Alan F. Westin, le droit à l'anonymat représente la possibilité pour le consommateur de représenter publiquement ses idées sans en être identifié comme étant l'auteur[170]. Avec les témoins et traceurs, les consommateurs ont perdu la capacité de naviguer sur le web sans que leurs activités soient suivies par une myriade d'outils technologiques partageant à plusieurs leur moment privé. La représentation de leur identité numérique est automatiquement reliée à leur profil par les entreprises publicitaires ne leur permettant pas de conserver l'anonymat sur leurs activités en ligne. Un certain rapprochement peut être fait avec les propos du professeur Westin considérant que le consommateur ne peut s'exposer publiquement sur le web sans être profilé par une entreprise.

1.1.2.4 La limitation à la collecte des renseignements

Le caractère opaque de l'environnement des témoins est problématique puisqu'il leur a permis d'évoluer avec une certaine démesure. Le nombre de témoins installés lors de la navigation dépasse largement la notion de caractère raisonnable de la collecte établi par les différents régimes juridiques encadrant la protection des données personnelles[171]. Une page web peut utiliser plus d'une dizaine de témoins, même jusqu'à une centaine dans certains cas, pour collecter différentes informations[172]. Par ailleurs, au Québec il peut s'avérer difficile de refuser l'installation d'un traceur. Par exemple, l'entreprise H&M affiche le message suivant : « *H&M utilise des témoins pour améliorer votre expérience de magasinage. Si vous continuez à utiliser nos services, nous supposerons que vous consentez à l'utilisation de ces témoins. Envie d'en savoir plus sur les témoins et comment vous pouvez les refuser*. » et renvoie le consommateur à la politique de confidentialité de l'entreprise, sans offrir au consommateur un moyen de refuser les témoins. Il ne s'agit que d'un exemple parmi

---

[168] « L'anonymat en tant que facette du droit à la vie privée revêt cependant une importance particulière dans le contexte de l'utilisation d'Internet. » *R. c. Spenser*, préc., note 98, par. 41.
[169] *Cooperberg c. Buckam*, [1958] C.S. 427; *Robbins c. Canadian Broadcasting Co.,* [1958] C.S. 152.
[170] Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967, p. 32.
[171] *Loi sur la protection des renseignements personnels et des documents électroniques,* préc., note 21, art. 5 (3) ; *Règlement (UE) 2016/679*, préc., note 23.
[172] Kelsey CAMPBELL-DOLLAGHAN, « Here's how GDPR is already changing web design », *Fast Company*, 30 août 2018, en ligne : <https://www.fastcompany.com/90229646/heres-how-gdpr-is-already-changing-web-design>

tant d'autres de l'absence réelle de contrôle que possède le consommateur sur ses informations lorsqu'il navigue sur le web. Pour d'autres, il est impossible de refuser l'installation de témoins ou d'utiliser le site web sans consentir aux témoins alors que cette pratique est illicite[173].

Pour pallier ces pratiques, certains navigateurs comme Chrome et Safari ont mis en place des mécanismes de navigation privée afin de limiter la propagation de témoins sur le web. Or, une action collective a été intenté devant la Cour californienne contre les géants américains *Google* et *Alphabet Inc*. au début du mois de juin 2020 en raison de la collecte de données sur le comportement des consommateurs en ligne, même s'ils naviguent en mode privé[174]. Ce mode permet en théorie de limiter le nombre de témoins installés pour éviter le suivi des internautes et de les supprimer une fois la navigation terminée[175]. Le moteur de recherche est accusé de collecter des données concernant l'historique de navigation ainsi que les activités en ligne malgré les mesures prises par les consommateurs pour conserver l'anonymat de leur présence en ligne[176]. En soi, cette dénonciation met de l'avant le fait que le consommateur n'a qu'une illusion de contrôle sur ses données.

Cette fausse croyance véhiculée par les géants du web pourrait être assimilée par le consommateur comme une publicité trompeuse. La *Loi sur la protection des consommateurs* interdit les publicités qui donnent une fausse impression en ce qui concerne le produit ou le service[177]. La « fausse impression » s'apprécie en fonction de l'impression générale que la publicité laisse au consommateur, dans le sens littéral des termes[178]. La notion de publicité doit être interprétée dans un sens large pour inclure toute représentation qui a pour but de promouvoir un produit ou service[179]. Dans le cas échéant, le service de navigation privée

[173] Mathieu BOURGEOIS et Marion MOINE, « La délibération 2019-093 du 4 juillet 2019 sur les cookies et autres traceurs - Une préface à la révolution e-privacy ! », JCP E, n° 38, 19 Septembre 2019, act. 595
[174] *Chasom Brown et al.* v. *Google LLC/Alphabet Inc.,* 20-3664 (Dist. Ct. Cal 2020), par. 3.
[175] *Id.*, par. 33.
[176] *Id.*, par. 3.
[177] *Loi sur la protection du consommateur*, préc., note 37, art. 219 « Aucun commerçant, fabricant ou publicitaire ne peut, par quelque moyen que ce soit, faire une représentation fausse ou trompeuse à un consommateur.»; N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 458.
[178] *Loi sur la protection du consommateur*, préc., note 37, art. 218 ; *R. c. Imperial Tobacco Products Ltd.,* (1971) 4 C.C.C. (2d) 423
[179] « Le mot « annonce » dans cette Loi a un sens très large. Il comprend toute représentation par quelque moyen que ce soit dans le but de promouvoir directement ou indirectement la vente ou l'acquisition de toute drogue,

annoncé par le moteur de recherche n'est pas conforme à ce qui est offert aux consommateurs. Les consommateurs croient naviguer de manière confidentielle alors qu'en réalité certaines formes de témoins sont utilisés pour recueillir des données. La publicité trompeuse à également un impact négatif sur le marché en affectant la confiance du consommateur envers les commerçants[180]. Toutefois, le recours qui s'offre au consommateur en vertu du droit de la consommation se limite à la nullité du contrat[181] qui n'est guère intéressant dans le cadre d'un service gratuit comme celui offert par les moteurs de recherches. C'est entre autres pour ces raisons que le droit de la consommation bénéficierait d'une réforme pour encadrer les enjeux qu'apporte l'économie numérique.

L'Europe s'est d'ailleurs lancée dans une guerre contre les cookies en 2009 avec l'adoption de la directive *e-privacy*[182]. Son effet le plus notable a été l'apparition de boîte « pop-up » requérant le consentement de l'internaute à l'installation des témoins[183]. L'adoption de RGPD en 2016 a été une arme de plus à l'artillerie européenne contre les témoins tiers reconnaissant spécifiquement à son considérant 30 que les témoins sont des renseignements personnels susceptibles d'être utilisés à des fins de profilage et d'identification clarifiant l'application de la directive à ceux-ci[184]. Cette guerre afflige déjà les témoins tiers en Europe qui ont vu une baisse de 22% sur les tribunes de nouvelles depuis l'adoption du RGPD[185].

---

aliment, cosmétique ou appareil médical. » N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 458.

[180] *Id.*, p. 480.

[181] *Loi sur la protection du consommateur*, préc., note 37, art. 8

[182] *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n o 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (Texte présentant de l'intérêt pour l'EEE),* OJ L 337, 18.12.2009, p. 11–36

[183] Richie KOCH, « Cookies, the GDPR, and the ePrivacy Directive », *GDPR.EU*, en ligne : <https://gdpr.eu/cookies/>

[184] « Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes. » *Règlement (UE) 2016/679*, préc., note 23, considérant 30 ; R. KOCH, préc., note 183.

[185] Tim LIMBERT, Lucas GRAVES et Rasmus KLEIS NIELSEN, « Third-party cookie down by 22% on Europe news sites since GDPR », *Reuters Institute – University of Oxford*, 2018, en ligne : <https://reutersinstitute.politics.ox.ac.uk/risj-review/third-party-cookies-down-22-europes-news-sites-gdpr?mod=djemCMOToday>

L'évolution de la pratique en marge du respect du droit à la vie privée du consommateur démontre la difficulté à laquelle le régime juridique du droit à la protection des renseignements personnels est confronté.

Les différentes formes de témoins préoccupent autant les autorités de protection des renseignements personnels que les entreprises privées comme les moteurs de recherche *Google Chrome* et *Firefox*. Certains navigateurs ont pris l'initiative d'éliminer les témoins tiers pour assurer une meilleure gouvernance des données au niveau publicitaire. Google Chrome a d'ailleurs lancé le programme *Privacy Sandbox* qui permet aux entreprises de partager de la publicité ciblée en limitant le profilage des consommateurs[186]. Par ailleurs, les internautes possèdent différents moyens de contrer ou de surveiller l'usage des témoins et traceurs comme la vidange de sa mémoire cache ou l'installation de divers logiciels qui permettent de bloquer les témoins tiers[187]. Or, le manque d'expérience du consommateur dans le contexte des technologies limite leurs capacités à contrôler réellement leurs données personnelles.

C'est face à cette impossibilité de naviguer dans l'intimité que le consommateur est désavantagé dans sa relation avec le commerçant. Le principe juridique à la base du droit à la vie privée élaboré par le professeur Westin et consacré par la Cour suprême dans l'arrêt *Dyment* selon lequel les individus devraient être libres de choisir quelle proportion d'eux-mêmes ils souhaitent partager en ligne est bafoué par ces fichiers textes invisibles[188]. Le consentement du consommateur à la collecte étant difficilement accessible, le régime juridique du droit à la protection des renseignements personnels atteint sa limite dans son rôle de protection du consommateur.

[186] AFP, « Google éliminera progressivement les témoins tiers d'ici deux ans », *Radio-Canada*, 14 janvier 2020, en ligne : < https://ici.radio-canada.ca/nouvelle/1473506/google-chrome-cookies-temoins-bloquer-deux-ans>
[187] Dennis ANON, « How cookies track you around the web and how to stop them », *Privacy.net*, 24 février 2018, en ligne : <https://privacy.net/stop-cookies-tracking/>
[188] *R. c. Dyment*, [1988] 2 R.C.S. 417, par. 17 ; A. F. WESTIN, préc., note 170, p. 33.

1.2.3 Le marketing et les réseaux sociaux

L'écoute des médias sociaux est une technique de suivi comportemental en ligne qui permet pour les marketeurs de mieux comprendre les intérêts des consommateurs[189]. Les médias traditionnels comme la télévision et la radio ont cédé le pas à ces nouveaux géants du web comme Facebook, Twitter, Instagram et bien d'autres. Selon les plus récents sondages, au Québec, 83% de la population adulte utilise un réseau social à des fins personnelles[190]. Pour les entreprises, les réseaux sociaux permettent d'avoir un contact direct avec la clientèle et de créer une interaction avec celle-ci[191]. Les consommateurs étant plus engagés sur ce type de médias, les entreprises ont avantage à avoir une présence sur ces plateformes et utiliser les données qu'ils peuvent recueillir pour orienter leurs campagnes publicitaires[192].

Ce virage technologique a aussi apporté beaucoup de changements dans le comportement des consommateurs et de nouveaux enjeux ont émergé. La notion de vie privée a pris un nouveau détour alors que les gens partagent dorénavant leur localisation, leurs photos personnelles ou toute autre information relative à leur quotidien sur ces plateformes web. Le partage des renseignements, destiné au membre de leur réseau (1.2.3.2), est également collecté par les géants numériques pour être revendu à des fins publicitaires (1.2.3.1).

1.2.3.1 La monétisation des données des consommateurs

Facebook est un exemple marquant de la transformation des réseaux sociaux en vache à lait publicitaire. À ses tout débuts en 2004, le site a été mis en place pour les finissants de Harvard afin qu'ils puissent se créer un profil formant une sorte d'album de finissant virtuel[193]. Déjà vingt-quatre heures après sa fondation, le réseau social facultaire comprenait 1200 membres et sa croissance s'est poursuivie très rapidement pour devenir le réseau social

---

[189] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, préc., note 145.

[190] CENTRE FACILITANT LA RECHERCHE ET L'INNOVATION DANS LES ORGANISATIONS, *L'usage des médias sociaux au Québec*, NETendance 2018, vol. 9, no. 5, Québec, p. 6, en ligne : <https://cefrio.qc.ca/media/2023/netendances-2018_medias-sociaux.pdf>

[191] *Id. :* Un adulte sur trois au Québec a publié un commentaire, soit positif au négatif, par rapport à une entreprise sur les réseaux sociaux.

[192] *Id. :* En 2018, plus d'une personne sur deux a cliqué sur une publicité affichée sur les réseaux sociaux qui a conclu 34% des fois à une transaction.

[193] Sarah PHILIPS, « A brief history of facebook », *The Guardian*, 25 juillet 2007, en ligne : <https://www.theguardian.com/technology/2007/jul/25/media.newmedia>

qu'il est aujourd'hui[194]. Quelques mois plus tard, la plupart des étudiants des grandes universités américaines avaient un profil sur le site qui a finalement été ouvert au grand public en 2006[195]. Aujourd'hui, Facebook est un des sites les plus visités au monde et permet notamment aux utilisateurs de communiquer, partager du contenu, créer des groupes et suivre différentes entreprises. Par ailleurs, un premier record a été réalisé le 24 août 2015 alors qu'un milliard d'utilisateurs à travers le monde ont utilisé le site iconique durant la journée et un second record a été établi en 2017 alors que Facebook franchit la barre des 2 milliards d'utilisateurs[196]. En moyenne, chaque minute, les internautes commentent 510 000 fois, ils publient 136 000 photos et rédigent 293 000 statuts sur la plateforme[197]. Ces informations ont une valeur inestimable sur le marché publicitaire et le succès financier de l'entreprise le démontre bien[198]. Or, la gratuité des services n'est pas considérée par tous comme étant suffisante à la collecte et la revente à grande échelle des données des internautes.

Devant ses revenus monstres, Facebook multiplie l'offre de produits et de services offerts gratuitement aux membres de la communauté. La question se pose à savoir si les services offerts par les réseaux sociaux sont réellement gratuits. Un acte à titre gratuit se définit comme étant un « [a]cte juridique par lequel une personne, dans une intention libérale, avantage quelqu'un en lui procurant ses services ou en disposant en sa faveur d'un bien ou d'un droit, sans contrepartie. »[199] Le droit civil québécois prévoit qu'un contrat à titre gratuit est « […] celui par lequel l'une des parties s'oblige envers l'autre pour le bénéfice de celle-

---

[194] *Id.*

[195] *Id.*

[196] JDN, « Nombre d'utilisateur Facebook dans le monde », *JDN*, 4 mai 2020, en ligne : <https://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/#:~:text=dans%20le%20monde-,Au%20premier%20trimestre%202020%2C%20Facebook%20revendiquait%202%2C6%20milliards%20d,A...>

[197] JDM, « Facebook en 20 chiffres très révélateurs », *Journal de Montréal*, 12 avril 2018, en ligne : <https://www.journaldemontreal.com/2018/04/12/facebook-en-20-chiffres>

[198] La capitalisation de l'entreprise étant basée sur les revenus publicitaires, Facebook a été en mesure de bâtir un modèle d'affaire qui transforme les données brutes en profits net. En octobre 2019, l'entreprise de Silicon Valley enregistrait un chiffre d'affaire de 49,62 milliards de dollars US et un bénéfice de 11,14 milliards grâce à un nombre moyen mensuel de 2,45 milliards utilisateurs actifs. Rudy VIARD, *Les chiffres de Facebook*, Webmarketing Conseil, 2020, en ligne : <https://www.webmarketing-conseil.fr/chiffres-de-facebook/>

[199] Hubert REID, *Dictionnaire de droit québécois et canadien*, 5e éd. révisée, Montréal, Wilson & Lafleur, 2016, « acte à titre gratuit », en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=acte%20%C3%A0%20titre%20gratuit&t=edictionnaire&sort=relevancy&m=detailed>

ci, sans retirer d'avantage en retour. »[200] Pourtant, au 4e trimestre de l'année 2018, Facebook a déclaré un revenu moyen de 34,86 dollars US par utilisateur[201]. Les réseaux sociaux répondent donc difficilement au critère volontariste et libérale de la gratuité[202]. Le contrat conclu entre les parties ne serait donc pas un contrat à titre gratuit, mais plutôt un contrat d'adhésion[203].

En France, la *Commission des clauses abusives* affirme que les données utilisées par les réseaux sociaux constituent une rémunération au sens du *Code de la consommation*[204]. Les clauses de gratuité des réseaux sociaux sont susceptibles de créer un déséquilibre entre les droits et les obligations des parties au détriment du consommateur en laissant croire à celui-ci qu'il ne fournit aucune contrepartie alors que le traitement de ses renseignements personnels à une valeur[205]. La Cour d'appel de Paris a également considéré que «[…] si le service proposé est gratuit pour l'utilisateur, la société Facebook Inc. retire des bénéfices importants de l'exploitation de son activité, via notamment les applications payantes, les ressources publicitaires et autres, de sorte que sa qualité de professionnel ne saurait être sérieusement contestée ; qu'il n'est pas plus contestable que le contrat souscrit est un contrat d'adhésion sans aucune latitude autre que l'acceptation ou le refus »[206]. La gratuité des services offerts par l'entreprise n'est donc pas sans contreparties de la part du consommateur.

Le Bureau de la concurrence du Canada s'est également penché sur la question de la gratuité des services offerts par l'entreprise en contrepartie de la collecte de massive de données. Le

---

[200] *Code civil du Québec*, préc., note 159, art. 1381 al. 2 « Le contrat à titre gratuit est celui par lequel l'une des parties s'oblige envers l'autre pour le bénéfice de celle-ci, sans retirer d'avantage en retour. »
[201] *Commissaire de la concurrence c. Facebook*, CT 2020-004, p. 2.
[202] Maurice TANCELIN, *Des obligations en droit mixte au Québec*, 7e éd., Montréal, Wilson & Lafleur, no. 96.
[203] *Code civil du Québec*, préc., note 159, art. 1379 « Le contrat est d'adhésion lorsque les stipulations essentielles qu'il comporte ont été imposées par l'une des parties ou rédigées par elle, pour son compte ou suivant ses instructions, et qu'elles ne pouvaient être librement discutées. »
[204] *Recommandation n°2014-02 relative aux contrats proposés par les fournisseurs de services de réseaux sociaux*, 07.11.2014, III-A. Clauses de gratuité
[205] *Id.*
[206] CA Paris, pôle 2, ch. 2, 12 févr. 2016, n° 15/08624, *Facebook Inc. c/ M. X.*, D. 2016. 422; Dalloz IP/IT 2016. 214, obs. S. André et C. Lallemand; RTD civ. 2016. 310, obs. L. Usunier BRDA 2016, n° 6, inf. 25 ; JCP E 2016. 1309, L. Marion ; CCC 2016. Repère 3, obs. C. Caron ; CCC 2016. Comm. 132, obs. S. Bernheim-Desvaux ; CCE 2016. Comm. 33, note G. Loiseau ; CCE 2016. Étude 12, obs. F. Mailhé ; RLDA 2016/114, n° 5888 ; RLDI 2016/124, n° 3944 ; Légipresse 2016, n° 337, p. 232, note A. Chéron. Confirmation de TGI Paris, ord. 5 mars 2015, n° 12/12401, Légipresse 2015. 205 et les obs. ; CCC 2015. Comm. 51, note G. Loiseau ; CCE 2016. Chron. 1, obs. M.-E. Ancel ; Gaz. Pal. 30 mai 2015, p. 18, note S. Prieur ; RLDI 2015/114, n° 3725, obs. J. de Romanet ; RLDI 2015/115, n° 3735, note M. Moritz.

Commissaire a jugé que, par son manque de transparence quant à la revente de données à des fins publicitaires, les indications face à la confidentialité des informations étaient fausses ou trompeuses au sens de l'article 74.01 (1) de la *Loi sur la concurrence*[207]. Cette disposition civile prévue interdit que soit donnée aux consommateurs une indication fausse ou trompeuse concernant un point important en fonction de l'impression générale que l'indication donne en son sens littéral[208]. Le Commissaire a conclu que Facebook n'a pas respecté les engagements indiqués dans sa politique de confidentialité et a partagé des renseignements personnels avec des entreprises tierces laissant une impression générale de confidentialité contraire aux indications retrouvées sur le site[209]. Facebook aurait profité de cette impression de confidentialité pour promouvoir ces intérêts commerciaux au détriment des consommateurs.

La Cour fédérale de justice allemande (Bundesgerichtshof) a également rendu un jugement dans le même sens le 23 juin 2020 dernier face à l'offre d'un service gratuit par Facebook en contrepartie de l'acceptation des conditions d'utilisation qui permettent à l'entreprise un traitement étendu des données personnelles des utilisateurs[210]. La Cour sanctionne la collecte de données en dehors du site web Facebook sur des plateformes tierces comme Instagram et WhatsApp et sur les sites web qui offre la fonction « j'aime »[211]. La Cour considère que l'utilisation des données recueillies sur des sites tiers est contraire aux dispositions d'abus de position dominante prévu par la *Loi allemande contre les restrictions à la concurrence*[212] et le RGPD[213].

---

[207] LRC 1985, c. C-34 ; *Commissaire de la concurrence c. Facebook*, préc., note 201, p. 2.
[208] *Id.*, art. 74.03(5).
[209] *Commissaire de la concurrence c. Facebook*, préc., note 201, p. 2.
[210]Florian CAZERES, « La justice allemande restreint la collecte de données par Facebook », *LaPresse*, 23 juin 2020, en ligne : <https://www.lapresse.ca/affaires/techno/2020-06-23/la-justice-allemande-restreint-la-collecte-des-donnees-par-facebook> ; COUR FÉDÉRALE DE JUSTICE, *La Cour fédérale de justice confirme provisoirement l'allégation d'abus de position dominante par Facebook*, KVR 69/19, décision du 23 juin 2020, N ° 080/2020, en ligne : <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=11449328> [COMMUNIQUÉ DE PRESSE]; *Facebook c. Bundeskartellamt*, KVR 69/19, décision du 23 juin 2020, N ° 080/2020, en ligne : <https://www.bundesgerichtshof.de/SharedDocs/Termine/DE/Termine/KVR69-19.html?nn=11449328>
[211] *Infra*, p. 43.
[212] *Loi allemande contre les restrictions à la concurrence*, (QWB) art. 19, al. 1
[213] Voir *OLG Düsseldorf*, décision du 26 août 2019 - VI-Kart 1/19 (V) ; *Règlement (UE) 2016/679*, préc., note 23, art. 4, 6, 7, 9.

L'argument de la gratuité des services offerts mis de l'avant par les géants économique tend à s'effondrer alors que le droit se saisit de la question[214]. Les données des consommateurs ont une valeur inestimable sur le marché et les consommateurs peinent à le réaliser. Un encadrement spécifique ou, du moins, clarifié de ces nouvelles formes de contrat entre les entreprises et les réseaux sociaux pourrait bénéficier aux parties et rétablir l'équilibre contractuel entre le consommateur et le commerçant.

1.2.3.2 L'utilisation des données à des fins publicitaires

Ce n'est d'ailleurs pas la première fois que les GAFAM doivent répondre de leurs actes en raison de son ingérence des données personnelles. Au printemps 2018, l'affaire *Cambridge Analytica* a éclaté au grand jour révélant que les données personnelles de potentiellement plusieurs millions d'utilisateurs Facebook avaient été détournées par une firme d'analyse de données afin d'orienter la campagne présidentielle américaine de 2016[215]. La firme a développé l'application « This is your digital life » permettant de faire la collecte d'information des utilisateurs via un test de personnalité. L'application permettait de recueillir les informations du participant comme son profil, ses préférences et celles de leurs amis Facebook ce qui a permis à la firme de créer une base de données gigantesque touchant plusieurs millions d'utilisateurs. L'application opérait une collecte à grande échelle en prenant pour acquis que le consentement d'un utilisateur valait également pour le partage des informations de ses amis, violant délibérément le principe de consentement prévu par la loi. La campagne présidentielle de Trump a recouru aux données recueillies pour faire du ciblage comportemental dans certains territoires afin d'orienter les élections en ce sens. Depuis, plusieurs mesures de protection ont été mises en place par le réseau social, mais l'affaire *Cambridge Analytica* démontre bien le rôle majeur que les médias sociaux peuvent avoir

[214] La CNIL a d'ailleurs sanctionné Google avec une amende de 50 millions d'euro pour son manque de transparence quant à sa politique de confidentialité et l'absence de consentement valable à l'égard du traitement des données à des fins publicitaires. Cette décision marque un tournant en Europe pour l'encadrement de la publicité ciblée remettant en question le modèle d'affaires basé sur la gratuité des géants économique. Nathalie METALLINOS, « Les leçons à tirer de la sanction de Google par la CNIL (2e partie : Renforcement des exigences de transparence et de consentement) », (2019) 6 *Communication commerce électronique / LexisNexis* SA 43.

[215] Matthew ROSENBERG, Nicholas CONFESSORE et Carole CADWALLADR, « How Trump Consultants Exploited The Facebook Data of Millions », *The New York Times*, 17 mars 2018, en ligne : <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

pour les campagnes marketing et la sensibilité de la question de l'utilisation des données des internautes.

De manière plus spécifique, les réseaux sociaux permettent aux consommateurs de se créer des profils à leur image afin de garder le contact avec leurs proches, partager du contenu sous plusieurs formes (vidéos, images, textes), accéder à une variété de sources d'informations et interagir avec les entreprises[216]. La plupart du temps, le profil des utilisateurs est composé d'une image permettant de les identifier, leur nom ou pseudonyme, leur date de naissance et certaines sections permettent de décrire des intérêts personnels, le niveau d'éducation, les expériences professionnelles et plus encore. Ces données sont accessibles aux autres membres de la communauté soit de manière publique ou restreinte aux membres du réseau de l'utilisateur selon ses préférences de confidentialité. Les utilisateurs connectent entre eux grâce au réseau avec des liens « d'amitié » qui permettent d'avoir accès au profil d'un autre utilisateur, envoyer des messages privés ou même publier du contenu sur sa page.

Grâce à ces liens d'amitié, il est également possible de reconnaître les personnes faisant partie du cercle privé de l'internaute aussi appelé, dans le jargon, le graphique social. Ce graphique permet de comprendre les liens sociaux entre les différents individus et entreprises en fonction de l'information partagée mutuellement[217]. Le graphique social soulève des questions relatives à la protection des données du graphique qui sont inférées par rapport aux liens sociaux entre les parties. De ces questions émerge le principe de vie privée groupale qui se base sur le principe qu'identifier une propriété possédée par des individus particuliers signifie créer un groupe et le groupe devient en soit une information par les corrélations qu'il renferme[218]. Ce regroupement d'individus n'est pas volontaire, mais bien un effet collatéral

---

[216] Le dernier rapport NETendance 2018 du Centre facilitant la recherche et l'innovation dans les organisations démontre que la présence québécoise sur les médias sociaux est en pleine croissance, et ce, pour tous les groupes d'âges. Plus de 80% des adultes québécois ont utilisé les réseaux sociaux durant l'année de référence et 65% d'entre eux se sont connecté au moins une fois par jour. Il s'agit d'une hausse de 13 et 16 points par rapport à l'année 2016. Voir : CENTRE FACILITANT LA RECHERCHE ET L'INNOVATION DANS LES ORGANISATIONS, *L'usage des médias sociaux au Québec*, préc. note 190, p. 6 à 8.

[217] L'expression graphique social vient de la traduction de *social graph* qui représente les liens sociaux observables entre différentes entités. Sangeet Paul CHOUDARY, « The rise of social graphs for businesses », *HBR*, 2 février 2015, en ligne : <https://hbr.org/2015/02/the-rise-of-social-graphs-for-businesses>

[218] Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT (ed.), *Group Privacy: New Challenges of Data technology, vol. 126,* Springer International Publishing, 2016, Chap. 11, p. 61-62

des algorithmes qui catégorisent certains individus comportant des traits spécifiques[219]. Dès lors, le profil d'un individu sur un réseau social peut révéler des informations par rapport à un autre en raison de ses liens sociaux. D'un point de vue juridique, ce principe est inexistant dans le vocabulaire légal laissant le cadre juridique encadrer les données en silo, soit selon chaque individu. Or, pour les entreprises, ces liens permettent de proposer des offres personnalisées selon ce qui est préféré dans un groupe quelconque. À titre d'exemple, l'entreprise Trip Advisor utilise les informations reliées au graphique social pour faire des recommandations personnalisées selon les préférences de vos proches. Dans sa suggestion de restaurants, d'hôtels et autres services, l'entreprise met de l'avant les commentaires ou critiques des proches de l'individu en fonction de son profil Facebook[220].

L'usage de ces différentes plateformes permet de révéler d'autres informations relatives à la vie privée des utilisateurs comme leur réseau de contacts, les membres de leur famille, leurs préférences via les « j'aime » ou les pages qu'ils suivent. Ces informations, une fois groupées, permettent de révéler énormément d'informations sur le mode de vie et le quotidien d'un individu donné et permettent aux entreprises tierces d'obtenir beaucoup d'informations sur le comportement des consommateurs. La collecte de données comportementales dépasse même les frontières des réseaux sociaux avec l'offre de bouton « j'aime » sur d'autres sites web. Grâce à ces boutons, Facebook peut suivre le comportement des consommateurs hors de son réseau lorsqu'ils sont sur des sites tiers. Les pages contenant la fonction « j'aime » reliée à Facebook permettent au site de déposer un témoin tiers dans le navigateur du consommateur[221] et de lui présenter des publicités ciblées en fonction des sites visités[222]. Comme la plupart des témoins, ils ont également une fonction d'identification de l'utilisateur et de sécurité pour assurer le bon fonctionnement du site. Or la fonction publicitaire est indissociable de leur usage alors que cette fonction devrait pouvoir être exclue.

[219] *Id.*, p. 14
[220] S. P. CHOUDARY, préc., note 217.
[221] *Supra*, p. 34.
[222] « [L]es cookies nous permettent de présenter des publicités à des personnes qui ont déjà consulté le site web d'une entreprise ou acheté ses produits ou utilisé ses apps, et pour recommander des produits et des services sur la base de cette activité. Les cookies nous permettent de limiter le nombre de fois que vous voyez une publicité, pour que la même publicité ne s'affiche pas encore et encore. » FACEBOOK, *Cookies et autres technologies de stockage*, 2018, en ligne : <https://www.facebook.com/policies/cookies/>

L'enjeu majeur soulevé par les réseaux sociaux est que les données sont publiées à des fins sociales et communautaires alors que les utilisateurs veulent partager leur quotidien avec leurs proches. La collecte est donc effectuée à des fins pour lesquelles le consommateur n'a pas explicitement consenti. Le consentement s'opère lors de l'acceptation du flot de conditions d'utilisation qui sont reconnues partout dans le monde comme étant extrêmement longues et comportant un vocabulaire complexe[223]. Le consommateur se retrouve prisonnier entre son désir de joindre la communauté numérique et conserver son anonymat en ligne. Les réseaux sociaux ont leur prix : la valeur publicitaire des consommateurs.

George Orwell ne s'était pas trompé en prédisant dans son ouvrage *1984* publié 70 ans plus tôt que les marketeurs surveilleraient les allées et venues des consommateurs, autant dans le monde réel que le monde virtuel[224]. L'enjeu principal qu'amène le *big data* est que les données recueillies, même triviales, ont le potentiel de révéler beaucoup d'informations sur le consommateur une fois corrélé avec les autres informations présentes dans son profil client[225]. L'utilisation des données massives confirme les propos d'Aristote : « le tout est plus grand que la somme des parties. »[226] Cette connaissance de pointe sur les caractéristiques des consommateurs devient une arme puissante pour les entreprises publicitaires, alors que les droits des consommateurs sont mis de côté avec comme argument clé : la gratuité des services. L'utilisation intelligente des données comportementales est devenue une source de capitalisation massive pour les géants économiques de ce monde, au prix du droit des consommateurs.

[223] Aleecia M. MCDONALD et Lorrie Faith CRANOR, 4-3 « The cost of reading privacy policies », (2001) *Journal of Law and Policy* 545, 545.
[224] Daniel GERVAIS, « Chronique bibliographique : Commerce électronique », 33-3 *RGD* 489, 491 ; G. ORWELL, préc., note 6.
[225] Teresa SCASSA et Michael DETURBIDE, *Electronic Commerce and Internet Law in Canada*, 2e éd., Toronto, CCH Canadian Limited, 2012, p. 123-124.
[226] *Supra*, p. 14.

Chapitre 2 – L'utilisation intelligente des données du consommateur

« It is of the highest importance in the art of detection to be able to recognize, out of a number of facts, which are incidental and which vital. »[227]

Sherlock Holmes

L'intelligence artificielle apparaît comme une réponse aux enjeux posés par les données massives qui nécessitent l'extraction d'informations à partir d'une quantité astronomique de données. En réalité, les deux sciences sont intimement liées puisque les données massives permettent de nourrir les algorithmes de l'intelligence artificielle afin d'améliorer leurs capacités d'apprentissage[228]. Le concept reste toutefois très abstrait et est devenu sujet à multiples interprétations. L'idée d'une machine capable de penser à l'image de l'homme s'est majoritairement développée suite à la publication des travaux d'Alan Turing, *Computing Machinery and Intelligence,* au début des années 1950[229]. Ce dernier avait comme vision que les ordinateurs pouvaient avoir la capacité de fonctionner de manière autonome les rapprochant du comportement humain. Ce rapprochement a suscité de vives critiques au sein de la communauté scientifique qui défend encore aujourd'hui que l'intelligence est une caractéristique propre à l'homme et que la machine est restreinte à répéter les commandements[230].

À ce jour, il n'existe pas de définition universellement reconnue du concept d'intelligence artificielle. La plus utilisée est celle selon laquelle l'intelligence artificielle est un « ensemble des mécanismes permettant à un agent de percevoir, de raisonner et d'agir »[231]. L'OCDE définit les systèmes d'intelligence artificielle comme étant « […] un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des

[227] Arthur CONAN DOYLE, *The Memoirs of Sherlock Holmes*, dans « The Reigate Square », États-Unis, Harpers & Brothers, 1894.
[228]Heejun LEE et Chang-Hoan CHO, « Digital advertising: present and futur prospect », (2019) 39-3 *International Journal of Advertising* 332, 335.
[229] Alan TURING, « Computing machinery and intelligence », (1950) 59 *MIND* 433.
[230] Luc JULIA, *L'intelligence artificielle n'existe pas*, Pars, Éditions First, 2019.
[231] Patrick Henry WINSTON, *Artificial Intelligence*, 3e éd., Massachusetts, Addison-Wesley, 1992; Stuard J. RUSSEL et Peter NORVING, *Artificial Intelligence: A Modern Approach*, 3e éd., New-Jersey, Pearson, 2002.

environnements réels ou virtuels. »[232] Cette vision s'apparente à celle généralement reconnue dans la société actuelle.

D'un point de vue marketing, l'intelligence artificielle permet d'analyser et de prédire les comportements des consommateurs. Cette meilleure interprétation du comportement du consommateur permet aux entreprises de choisir la bonne cible (2.1) pour orienter leurs campagnes et, ainsi, maximiser leurs revenus. Une fois le consommateur adéquatement ciblé, il est possible de personnaliser (2.2) l'offre publicitaire ou même de produits en fonction des préférences identifiées des consommateurs. L'intelligence artificielle permet alors de préciser et d'optimiser les pratiques marketing. Or, ces innovations se font principalement à l'avantage des entreprises alors que l'intelligence artificielle devient une sorte d'outils de manipulation du marché qui rend la publicité plus pertinente certes, mais aussi plus intrusive.

Ces pratiques qui jumèlent la force de l'intelligence artificielle à la puissance des données massives permettent aux entreprises d'exploiter l'état de vulnérabilité du consommateur. Or, ces pratiques font l'objet d'un encadrement juridique quelconque, mais est-il suffisant?

2.1 Le ciblage publicitaire

Le marché étant une arène concurrentielle féroce, les entreprises doivent réussir à se démarquer dans leur offre de produits et services en créant de la valeur pour le consommateur final[233]. Afin de mettre en place des campagnes publicitaires efficaces, les responsables marketing doivent être en mesure de segmenter et cibler adéquatement le marché. De cette manière, il est possible d'ajuster la communication, le produit et même les canaux de distribution en fonction des habitudes et préférences des consommateurs.

Par ailleurs, toute action marketing doit être engagée en respect du public cible pour assurer une réponse positive de la part du consommateur. Il est de nos jours possible de créer des profils précis sur les consommateurs (2.2.1). Une fois créés, ces profils permettent de mieux identifier les besoins des consommateurs ciblés. Or, le profilage dépasse la création de

[232] OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, Paris, 2019, p. 26
[233] Dhruv GREWAL et *al*., *Marketing*, 2e éd., Montréal, McGraw-Hill Education, Chenelière Éducation, 2015, p. iii.

personas[234] traditionnels et offre une image précise du consommateur aux entreprises. Cette pratique qui s'opère dans l'ombre bénéficierait de faire preuve d'une plus grande transparence pour assurer le respect des droits des consommateurs.

Certaines entreprises ont recours à des pratiques encore plus complexes d'aide à la décision en établissant des cotes (*scores*) sur les habitudes de consommation (2.2.2). Ces données prédictives permettent aux entreprises de chiffrer le comportement potentiel du consommateur. La qualité des cotes repose toutefois sur l'exactitude des données utilisées. Or l'accès à ce type de renseignements devrait-il être permis ou plutôt conservé à titre de secret d'affaires ? Encore une fois, les droits des consommateurs s'opposent aux intérêts des entreprises.

2.1.1 Le profilage

La myriade de données recueillies en suivant le consommateur dans son quotidien lors de ces activités en ligne ou hors ligne permet aux entreprises de créer des profils types afin d'améliorer le ciblage comportemental. La création de *personas* (personnages fictifs) en marketing est une pratique bien connue afin d'humaniser l'image du client potentiel de l'entreprise. Or, l'émergence de logiciels de gestion de la relation client (CRM)[235] qui emmagasinent les données sur la clientèle permet de créer des profils précis sur les consommateurs afin de personnaliser au maximum l'offre de produits et services[236]. Le CRM correspond à une base de données informatiques consacrée à la gestion de la relation client[237]. Les outils de communication des campagnes marketing peuvent être connectés aux CRM afin de gérer les interactions avec la clientèle et assurer la fidélisation des consommateurs. Jumelées à l'intelligence artificielle, les données massives se précisent afin de cibler de manière presque absolue les consommateurs potentiels[238].

---

[234] *Infra*, p. 52.
[235] *Customer Relationship Management* (CRM).
[236] Voir micromarketing, *infra* p. 69 ; COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, Québec, 2011, p. 2, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FI_profilage.pdf>
[237] B. BATHELOT, « CRM », *Définitions Marketing*, 13 novembre 2018, en ligne : <https://www.definitions-marketing.com/definition/crm/>
[238] Sophie LACOURS, « Intelligence artificielle : les solutions algorithmiques permettent de définir plus précisément les profils clients », *Juris Tourisme* 2019.220.13, p. 14.

Le profilage est soumis au régime juridique du droit à la protection des renseignements personnels et fait l'objet d'une protection spécifique au sein du RGPD (2.1.1.1.). Au Québec, la pratique ne fait pas l'objet de disposition spécifique pour l'instant, mais elle peut être assimilée à la création de dossier (2.1.1.2.). De ce fait, la question se pose à savoir si le consommateur devrait avoir accès aux renseignements colligés par les entreprises (2.1.1.3.)

2.1.1.1 L'encadrement du profilage

D'un point de vue juridique, la création de profils ou le profilage est un concept à caractère large et diffus. Celui-ci est souvent entendu au sens du profilage racial qui repose sur le principe qu'une action ou une décision soit prise en fonction de la couleur de la peau, l'origine ethnique ou la religion[239]. Toutefois, la définition retenue dans le cadre du présent texte fait référence au principe de collecte et de traitement automatisé des données afin d'analyser ou prédire des informations spécifiques à un consommateur[240].

Différentes versions de la définition de profilage cohabitent dans l'univers juridique. En Europe, le Groupe de travail sur l'article 29 l'entrevoit comme étant lié au caractère prédictif de ces nouvelles technologies alors que le RGPD ne l'implique pas systématiquement[241]. Dans la recommandation *2010(13) sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage du Conseil de l'Europe*[242], le profilage se base sur trois critères successifs soit la collecte de données, le traitement automatisé des données pour identifier les corrélations et l'usage de ces corrélations à des fins prédictives[243]. Au Québec, le *Projet de loi 64 modernisant des dispositions législatives en matière de protection des renseignements personnels* prévoit ajouter une définition de profilage à la LPRPSP qui dispose que : « [l]e profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou

[239] H. REID, préc., note 199.
[240] *Règlement (UE) 2016/679*, préc., note 23, art. 4, § 4.
[241] Nathalie MARTIAL-BRAZ, « RGPD – Le profilage : fiche pratique », CCE 2018.4.15, p. 1.
[242] CONSEIL DE L'EUROPE, *la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, Recommandation CM/Rec(2010)13 et exposé des motifs, Strasbourg, Éditions du Conseil de l'Europe, 2011, p. 9, en ligne : <https://rm.coe.int/16807096c4>
[243] N. MARTIAL-BRAZ, préc., note 241, p. 1.

du comportement de cette personne. »[244] La collecte et l'identification des corrélations permettent de former à elle seules des profils personnalisés des consommateurs comme la vision élargie du profilage développé dans le RGPD et le projet de loi 64 sans que l'intervention de modèle prédictif soit nécessaire[245].

Le RGPD prévoit spécifiquement à son article 22 une protection pour la prise de décision automatisée qui comprend les pratiques de profilage. Or, le profilage sans processus de décision automatisée est-il soumis à l'application de cet article ? La lecture rapide du texte peut induire en erreur puisque, malgré la définition de profilage retenue par le RGPD, seules les pratiques qui reposent sur un traitement automatisé de l'information et qui créent un effet juridique pour l'individu tombent dans le champ de protection de cette disposition[246]. Dans le cas échéant, le profilage à des fins marketing ne fait pas nécessairement l'objet de décision automatisée ou ne crée pas d'effets juridiques susceptibles d'affecter le consommateur de manière significative. De ce fait, le consommateur est protégé par les dispositions classiques encadrant le traitement des données.

Les renseignements visés par la création de profils dans les logiciels CRM ou tout autre logiciel peuvent être de différente nature. Qu'ils concernent sur la situation économique du consommateur, son statut matrimonial, son état de santé, sa localisation, ses préférences ou centres d'intérêts, les logiciels sont susceptibles de collecter ou d'inférer différentes informations leur permettant de mieux connaître le profil cible de leurs consommateurs.

La nature du profilage implique un traitement des données ainsi que le rapprochement des données recueillies afin d'identifier des corrélations pertinentes sur le comportement de l'individu visé. De ce fait, la pratique est soumise l'application du cadre juridique entourant la protection des renseignements personnels. Le Commissariat à la protection de la vie privée du Canada s'est prononcé à ce propos et prévoit que :

> Par conséquent, dans le contexte de la [publicité comportementale en ligne], compte tenu du fait que le but derrière la collecte de renseignements est de créer

[244] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi no. 64, préc., note 32, art. 99.
[245] L'utilisation des données à des fins prédictives relève plutôt de la pratique du *scoring*. Voir Infra 2.2.1, p. 60; N. MARTIAL-BRAZ, préc., note 241, p. 2.
[246] *Règlement (UE) 2016/679*, préc., note 23, art. 22, § 1-2.

> des profils de personnes qui, à leur tour, permettent d'offrir des publicités ciblées; compte tenu des moyens puissants disponibles pour recueillir et analyser les bits de données disparates et la possibilité sérieuse d'identifier les personnes concernées, et compte tenu du caractère potentiellement très personnalisé de la publicité en résultant, on peut raisonnablement penser que les renseignements en cause dans la publicité comportementale touchent à la protection de renseignements personnels et, dans les circonstances, ils doivent être considérés comme «identifiables». Même si une telle évaluation devrait être effectuée au cas par cas, il n'est pas déraisonnable de considérer cette information comme des « renseignements personnels » de prime abord.[247]

Le Commissariat adopte cette position souple pour éviter de rendre un jugement anticipé[248]. Considérant le caractère variable des données collectées et l'usage qui peut en être fait, le Commissariat juge que chaque cause doit être interprétée au cas par cas, mais il offre tout de même une orientation générale sur la question à savoir que les données collectées à des fins de profilage peuvent être soumises au régime du droit à la protection des renseignements personnels.

Le fait que les renseignements recueillis soient considérés comme des renseignements personnels au sens du RGPD et de la LPRPDE ouvre la voie à de nouvelles questions juridiques. Le consommateur devrait-il avoir un droit d'accès à ces renseignements, le droit de faire rectifier son dossier ou le droit à l'oubli ?

2.1.1.2 La création de dossiers

Le droit européen définit clairement le profilage[249]. À l'inverse, au Québec, la notion est pour l'instant[250] le fruit de l'interprétation du droit civil et du droit à la protection des renseignements personnels. L'opération de créer un profil à des fins publicitaires se rapproche à la notion de création de dossiers, soit le fait de rassembler différentes informations concernant un individu donné afin de l'utiliser ultérieurement à des fins marketing. À ce propos, le droit civil québécois dispose que « [t]oute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. »[251] Par

[247] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, préc., note 145.
[248] *Id.*, p. 1.
[249] *Règlement (UE) 2016/679*, préc., note 23, art. 4 § 4.
[250] *Supra*, p. 56.
[251] *Code civil du Québec*, préc., note 159, art. 37.

ailleurs, l'entreprise doit avoir obtenu le consentement du consommateur afin de collecter les renseignements utiles à l'objet du dossier[252]. Selon le principe 4.3.3 de la LPRPDE[253], une entreprise ne peut pas exiger le consentement d'un consommateur à la collecte, l'utilisation ou la communication de renseignements qui ne sont pas nécessaires pour réaliser les fins légitimes prévues[254]. La collecte correspond-elle à un intérêt légitime pour constituer un dossier ou une fin raisonnable à la collecte des renseignements visés? Le Commissariat à la protection de la vie privée du Canada a conclu suite à l'examen des différents modèles d'affaires des entreprises publicitaires que la collecte de renseignements personnels à des fins de publicité comportementale en ligne pouvait constituer une fin raisonnable au sens de l'article 5(3) de la LPRPDE[255]. Cette disposition retrouve son équivalent dans la LPRPSP qui prévoit que seuls les renseignements nécessaires doivent être collectés[256] et que l'entreprise qui effectue la collecte doit avoir un intérêt sérieux et légitime de le faire[257], comme il est prévu dans le *Code civil du Québec*[258]. De ce fait, les entreprises ont le droit de créer des profils sur les consommateurs, mais ceux-ci possèdent un certain droit de regard sur le dossier créé, même si parfois celui-ci existe à son insu[259].

[252] *Id.* « Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation. »
[253] *Loi sur la protection des renseignements personnels et des documents électroniques*, préc., note 21, Principe 4.3.3.
[254] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, préc., note 145, p. 5.
[255] *Loi sur la protection des renseignements personnels et des documents électroniques*, préc., note 21, art. 5 (3) : « L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »
[256] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 5
[257] *Id.*, art. 4
[258] *Code civil du Québec*, préc., note 159, art. 37.
[259] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, préc., note 236.

2.1.1.3 Le droit d'accès et à la rectification

Le RGPD[260] et le Contrôleur Européen de la Protection des Données[261] (CEPD) prévoient que la personne concernée par le traitement de ces données a le droit d'être informée de l'existence d'un profil à son égard. Par ailleurs, le droit civil québécois dispose que :

> Sous réserve des autres dispositions de la loi, toute personne peut, gratuitement, consulter et faire rectifier un dossier qu'une autre personne détient sur elle soit pour prendre une décision à son égard, soit pour informer un tiers; elle peut aussi le faire reproduire, moyennant des frais raisonnables. Les renseignements contenus dans le dossier doivent être accessibles dans une transcription intelligible.[262]

De la même manière, la LPRPSP prévoit que toute personne qui constitue un dossier sur une autre doit l'en informer de l'objet du dossier, l'utilisation qui sera faite des renseignements et l'endroit où son dossier sera détenu et son droit d'accès et de rectification[263]. Le projet de loi 64 prévoit un complément à cette disposition concernant le profilage et dispose qu'en plus des renseignements nommés précédemment, l'entreprise qui utilise une technologie permettant d'effectuer un profilage devra informer le consommateur du recours à cette technologie ainsi que des moyens disponibles pour en désactiver les fonctions[264].

À ce jour, la pratique du profilage reste une notion plutôt abstraite. Pourtant, toute entreprise qui utilise un CRM ou qui constitue une base de données sur les consommateurs est soumise à ce régime juridique et doit garantir un droit d'accès aux consommateurs à leurs renseignements personnels[265]. Pour ce faire, le consommateur doit faire une demande écrite à l'entreprise visée[266]. Malgré le mécanisme juridique en place, il peut être laborieux pour le consommateur de s'y retrouver dans les politiques de confidentialités des différentes entreprises ou même de savoir où provient la publicité et avec quelle entreprise

[260] *Règlement (UE) 2016/679*, préc., note 23, art. 13-14.
[261] CEPD, WP 251 rév. 01, pp. 27-29
[262] *Code civil du Québec*, préc., note 159, art. 38.
[263] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 8.
[264] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi no. 64, préc., note 32, art. 99.
[265] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 27, al. 1. : « Toute personne qui exploite une entreprise et détient un dossier sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication des renseignements personnels la concernant. » ; *Code civil du Québec*, préc., note 159, art. 39.
[266] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 30.

communiquer. Le droit est peut paraître clair en théorie sur la question, or les mécanismes présents pour le consommateur le sont moins.

Plusieurs informations recueillies dans les profils des consommateurs sont susceptibles d'intéresser celui-ci afin d'en assurer l'exactitude ou même d'en demander l'effacement[267]. Ce droit d'accès n'est toutefois pas absolu et peut faire l'objet de limitation en fonction du type d'information demandée.

2.1.2 La création de cotes (*scoring)*

Tous les consommateurs n'ont pas la même valeur d'un point de vue marketing[268]. Certains clients sont plus réceptifs à la publicité et rapportent plus de revenus que d'autres. Le mariage entre les données massives, l'apprentissage machine et l'analyse statistique donne naissance à une pratique intéressante : le *scoring* ou la création de cotes. Cette pratique consiste à associer une cote à un consommateur dans une base de données en fonction du niveau d'intérêt pour les offres publicitaires[269]. La plupart des entreprises utilisent ce genre de codes pour représenter les données des consommateurs recueillies à partir de différentes sources comme les programmes de fidélisation. Cette pratique repose sur une analyse prédictive des renseignements concernant les profils des consommateurs[270]. Elle permet entre autres de rentabiliser les actions marketing en priorisant les campagnes sur les consommateurs ayant un meilleur potentiel d'achat.

À titre d'exemple, l'entreprise Target a semé la controverse alors qu'elle avait sollicité une adolescente pour lui offrir des produits de maternité. Le père, choqué par le comportement de l'entreprise, a porté plainte alors qu'il était en réalité le dernier à savoir que sa fille était bel et bien enceinte de plusieurs mois[271]. L'entreprise avait élaboré une cote de maternité en

---

[267] Droit à l'oubli : « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, […] » *Règlement (UE) 2016/679*, préc., note 23, art. 17

[268] Stephane CONTREPOIS, « Scoring client : définition et avantages », *MyFeelBack*, 4 juillet 2019, en ligne : <https://www.myfeelback.com/fr/blog/scoring-client-avantages>

[269] *Id.*

[270] *Supra*, p. 54

[271] Charles DUHIGG, « How Companies Learn Your Secrets », *The New York Times*, 16 février 2012, en ligne : <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>

fonction des habitudes de consommation des consommateurs leur permettant de déterminer avec une précision choquante si une consommatrice était enceinte et à quel trimestre de grossesse elle se situait[272]. Target utilisait les cotes pour orienter les promotions offertes aux consommatrices en fonction de l'état de leur grossesse.

Ce type de méthode génère des résultats globaux qui donnent une réponse générique dont le résultat est imprévisible[273]. Un certain rapprochement peut être fait avec les méthodes de calcul des cotes de crédit par les agences. Le pointage de crédit est basé sur une formule mathématique qui utilise les informations contenues dans le dossier de crédit du consommateur pour calculer le risque auquel celui-ci correspond[274]. Les méthodes de calculs des cotes sont inconnues du public et sont la propriété des agences de crédit[275]. Contrairement aux agences de crédit, les méthodes pour calculer les différentes cotes concernant les consommateurs peuvent varier d'une entreprise à l'autre en fonction des différents critères utilisés et leur pondération[276]. Les cotes établies se rapprochent du profilage étudié précédemment et seraient susceptibles d'intéresser le consommateur pour en assurer l'exactitude.

La statistique à elle seule est peu susceptible de révéler des informations qui pourraient permettre d'identifier un individu donné. Il s'agit en réalité d'une information concernant les données recueillies. Le caractère probabiliste du résultat obtenu transforme l'état de l'information. De ce fait, la donnée devient le résultat d'un processus interne de l'entreprise qui mérite une protection au titre de secret d'affaires ou peut-elle faire l'objet d'une demande accès de la part des consommateurs (2.1.2.1)? Sans un accès au renseignement, il peut être

---

[272] « One Target employee I spoke to provide a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. What's more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny's habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store. And they know that if they reward her with a printed receipt that entitles her to a free cup of Starbucks coffee, she'll use it when she comes back again. »

[273] Augustin HURET et Jean-Michel HUET, « L'intelligence artificielle au service du marketing », (2012) 146-3 *L'Expansion Management Review* 18, 19.

[274] OPTION CONSOMMATEURS, *Les nouveaux services offerts par les agences de crédit : utilisation légitime des renseignements personnels?,* Rapport de recherche présenté au Commissariat à la protection de la vie privée, avril 2014, p. 15.

[275] *Id.*

[276] S. CONTREPOIS, préc., note 268.

difficile pour les entreprises de contrôler l'exactitude des données et éviter les biais algorithmiques (2.1.2.2)

2.1.2.1 Le droit d'accès et le secret d'affaires

Les cotes obtenues sont le résultat des choix internes de l'entreprise concernant la pondération des données recueillies par rapport aux informations recherchées. Or, ces informations ont-elles le potentiel d'être protégées comme un droit de propriété intellectuelle au titre de secret d'affaires? De manière générale, pour être considérée comme un secret d'affaires, la confidentialité des renseignements doit leur conférer une valeur commerciale, les renseignements doivent être connus d'un groupe restreint de personnes et faire l'objet de mesure raisonnable de protection à l'interne[277]. Le *scoring* est une technique qui permet de maximiser les actions marketing en prédisant le comportement potentiel des consommateurs. L'entreprise ayant développé une méthode lui permettant d'évaluer adéquatement ces renseignements possède un avantage concurrentiel notable et a l'intérêt de conserver ses renseignements au titre de secret d'affaires.

En théorie, plusieurs types de renseignements peuvent être considérés comme un secret d'affaires[278]. Il peut s'agir de renseignements techniques, de programmes d'ordinateur, de liste de fournisseurs, d'algorithmes et même de stratégies publicitaires[279]. Il peut également s'agir d'une combinaison d'élément qui, une fois réunie, génère un avantage concurrentiel pour l'entreprise qui les détient[280]. Une analyse *a contrario* permet de voir l'impact de la qualification des cotes créées au titre de secret d'affaires ou comme renseignement personnel. Par exemple, en appliquant le droit à la portabilité prévu par le RGPD qui permet à toute

[277] OMPI, *Secrets d'affaires*, en ligne : <https://www.wipo.int/tradesecrets/fr/> ; OMC, *Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce*, art. 39, al. 2 « Les personnes physiques et morales auront la possibilité d'empêcher que des renseignements licitement sous leur contrôle ne soient divulgués à des tiers ou acquis ou utilisés par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes, sous réserve que ces renseignements: a) soient secrets en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, ils ne sont pas généralement connus de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles; b) aient une valeur commerciale parce qu'ils sont secrets; et c) aient fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrets. »; *Cie H.J. Heinz du Canada Ltée c. Canada*, 2003 CFPI 250, par. 29

[278] OMPI, *Secrets d'affaires*, préc., note 277.

[279] *Id.*

[280] *Id.*

personne qui fait l'objet d'un traitement de demander à ce que ces renseignements personnels soient transférés à une entreprise tierce aux cotes produites par les entreprises[281], ce transfert d'information pourrait être préjudiciable pour l'entreprise et lui faire perdre son avantage concurrentiel. De ce fait, il est raisonnable de croire que les cotes obtenues et la méthode pour y arriver devraient être protégées comme un secret d'affaires.

Au Canada, les secrets d'affaires ne sont pas protégés au même titre que les autres droits de propriété comme les brevets[282], les marques de commerce[283] ou le droit d'auteur[284] qui relèvent d'un régime juridique spécifique. La protection conférée varie en fonction du système juridique et de l'évolution de la jurisprudence en la matière[285]. Leur protection puise sa source dans le droit civil et la common law, se fondant notamment sur les droits contractuels et extracontractuels[286]. Comme mentionné précédemment, pour être considérés comme un secret d'affaires les renseignements doivent faire l'objet d'une protection raisonnable de la part de l'entreprise pour être en mesure d'établir le bris de confidentialité.

En Europe, la *Directive n° 2016/943/UE du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites*[287], transposée en droit français par la *loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires*[288] prévoit un régime juridique spécifique au secret d'affaires et le positionne comme étant un véritable droit de propriété intellectuelle. Pour avoir accès à la protection, les renseignements visés doivent répondre à

[281] *Règlement (UE) 2016/679*, préc., note 23, art. 20.
[282] *Loi sur les brevets*, LRC 1985, c. P-4.
[283] *Loi sur les marques de commerce*, LRC 1985, c. T-13.
[284] *Loi sur le droit d'auteur,* LRC 1985, c. C-42.
[285] OMPI, *Secrets d'affaires*, préc., note 277.
[286] *Lac Minerals Ltd. c. International Corona Resources Ltd*., [1989] 2 R.C.S. 574 *(common law)*: L'obtention de renseignements confidentiels dans le cadre de rapports de confiance crée l'obligation de ne pas utiliser ces renseignements pour une autre fin que celle en vue de laquelle ces renseignements ont été donnés. Le critère applicable pour décider s'il y a eu abus de confiance consiste à établir la présence de trois éléments: (1) le caractère confidentiel des renseignements confiés; (2) leur communication à titre confidentiel; et (3) leur emploi abusif par la personne à laquelle ils ont été communiquées. Au Québec, il est également possible de s'appuyer sur l'obligation de bonne foi prévu aux articles 6 et 7 du *Code civil du Québec*, préc., note 159.
[287] *Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites*, O.J., L 157, 15.6.2016, p. 1–18
[288] *Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires*, J.O. 31 juillet 2018

certains critères : ne pas être aisément accessible ou familier ; la protection au titre de secret d'affaires confère une valeur commerciale aux renseignements visés et ceux-ci doivent faire l'objet de mesures de protection raisonnables[289]. Ces critères reprennent essentiellement ceux développés par l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) notamment utilisée en droit canadien[290]. Dès lors, les renseignements visés par les scores répondent également aux critères élaborés par la loi française et peuvent faire l'objet d'une protection face aux demandes d'accès de renseignements personnels.

S'il est clair autant en France qu'au Québec que les renseignements en lien avec les cotes créées par les entreprises méritent une protection au titre de secret d'affaires, leur valeur réelle au niveau concurrentiel dépend grandement de la qualité des informations recueillies et l'acuité des technologies utilisées. Le consommateur peut donc faire l'objet de décisions automatisées grâce à ces cotes sans pouvoir avoir accès aux renseignements le concernant.

2.1.2.2 Exactitude des données et biais algorithmique

Le mode de fonctionnement de l'intelligence artificielle impose comme prémisse que pour obtenir un extrant de qualité, l'intrant doit l'être également. Les algorithmes se nourrissent des données massives recueillies dont la forme et la provenance varient grandement. Or, les facteurs d'erreur lors de la collecte sont multiples et peuvent provenir de la technologie elle-même, des administrateurs de la technologie ou des consommateurs.

Le paramétrage des algorithmes et la quantité de données analysée peuvent être responsables des erreurs produites. Contrairement au cerveau humain, les algorithmes n'opèrent pas de distinction basée sur l'instinct et apprennent grâce à la masse de données agrégées. Un manque de données d'une catégorie quelconque peut créer des distorsions dans l'apprentissage de l'algorithme. Par exemple, Amazon a développé un algorithme afin d'analyser les nombreux dossiers de candidatures reçus par l'entreprise[291]. Étant basé sur les

[289] C. com., art. L. 151-1 s., art. R. 152-1 s.

[290]L'OMPI représente en guichet mondial en matière de propriété intellectuelle et permet d'assurer la coopération entre les états membres. Voir OMPI, *Au sein de l'OMPI*, en ligne : <https://www.wipo.int/about-wipo/fr/>

[291] Jeffrey DASTIN, « Insight - Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters*, 9 octobre 2018, en ligne : <https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH>

candidatures précédentes qui étaient majoritairement formées d'hommes, l'algorithme a développé une forme de misogynie en priorisant les candidatures masculines au détriment des femmes[292]. Les algorithmes sont une construction de l'homme qui reflète les valeurs des individus impliqués dans le développement des algorithmes, mais aussi les valeurs de la société empreintes dans les données historiques collectées et utilisées[293]. Ces biais créent des formes de discriminations qui peuvent être empreintes d'idéologie en fonction des statistiques recensée par l'algorithme.

Les biais peuvent également résulter de l'action délibérée des personnes impliquées dans le processus d'entraînement des algorithmes. Le robot conversationnel Tay de Microsoft a été victime de cette forme de biais et s'est mis à proférer des propos racistes sur les réseaux sociaux lors de sa mise en marche[294]. L'entrainement avec des propos haineux et des discours teintés par des commentaires racistes produit le résultat observé. Toutefois, les causes possibles de biais sont toutefois difficiles à établir puisqu'elles sont le fruit des apprentissages de l'algorithme. La Commission européenne propose dans son *Projet de livre blanc sur l'intelligence artificielle* une approche fondée sur la personne la plus à même de répondre de l'erreur[295]. Dans le cas des cotes générées par les entreprises, la responsabilité de l'erreur doit incomber à l'entreprise.

Le comportement des consommateurs peut devenir une source d'erreur pour les algorithmes. Plusieurs ménages partagent entre eux les appareils électroniques semant la confusion lors de la collecte de données[296]. L'inférence effectuée sur les habitudes de consommation est alors flouée puisque la collecte ne relève plus d'un seul individu, mais de plusieurs dont le genre, l'âge, la situation économique et plusieurs autres facteurs peuvent varier. Par ailleurs, un changement dans les habitudes de consommation des consommateurs comme une récession ou la pandémie actuelle peut bouleverser les facteurs prédictifs de l'intelligence

[292] *Id.*
[293] CNIL, *Comment permettre à l'homme de garder la main?,* Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, 2017, p. 31, en ligne : <https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de>
[294] *Id.*, p. 32.
[295] COMMISSION EUROPÉENNE, *Livre blanc sur l'intelligence artificielle*, COM (2020) 65, Bruxelles, 19 février 2020, p. 12.
[296] Sol TANGUAY, « Le ciblage publicitaire en ligne », dans Claude LAFOND et Vincent GAUTRAIS (dir.), *Consommateur numérique : une protection à la hauteur de la confiance?*, Montréal, Éditions Yvon Blais, 2016, p. 167.

artificielle et, conséquemment, la publicité offerte. Lorsque la pandémie a frappé le monde entier en début d'année 2020, les consommateurs se sont mis à acheter des produits qu'ils n'avaient jamais achetés auparavant comme les masques N95 ou du papier toilette en grande quantité. En quelques semaines, les entreprises de commerce en ligne ont vu un changement drastique dans les habitudes de consommation à un point tel que les algorithmes peinaient à réaliser leurs fonctions de base comme la détection de la fraude, la gestion des inventaires et même les suggestions publicitaires[297]. Ces changements rapides ont eu un impact sur les campagnes marketing qui ont dû réorienter leurs discours vers les pratiques permises. Les publicités encourageant les activités de groupes ou des slogans à connotation négative en temps de pandémie comme « devenez viral » ont dû être banni[298].

Malgré les formes de biais probables, les entreprises ont l'obligation d'assurer l'exactitude des données recueillies et traitées pour assurer le traitement équitable des consommateurs[299]. Il s'agit d'une obligation de moyen qui impose à l'entreprise de mettre en place les mesures techniques et organisationnelles appropriées pour assurer que les dossiers qu'elle possède sur les consommateurs soient à jour[300]. Toutefois, le *scoring* relève du processus d'apprentissage machine qui extrait l'essence de l'information recueillie pour générer une cote. Le processus reste relativement opaque imposant à l'entreprise d'assurer la qualité de ces données en

[297] Will DOUGLAS HEAVEN, « Our weird behavior during pandemic is messing with IA models », *MIT Technology Review*, 11 mai 2020, en ligne : <https://www.technologyreview.com/2020/05/11/1001563/covid-pandemic-broken-ai-machine-learning-amazon-retail-fraud-humans-in-the-loop/>

[298] *Id.*

[299] « Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risques d'erreur soit réduit au minimum, et sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur la l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet. La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques. » [nos soulignés] *Règlement (UE) 2016/679*, préc., note 23, considérant 71.

[300] « Toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée. » *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 11.

amont, lorsqu'il fait du profilage[301] pour assurer qu'en aval les scores générés soient adéquats.

Si les consommateurs n'ont pas tous la même valeur aux yeux des entreprises, l'utilisation intelligente de leurs données représente un avantage concurrentiel en or. Sélectionner la bonne cible permet de personnaliser l'offre de manière optimale, mais à quel moment la personnalisation devient-elle abusive ?

2.2 La personnalisation abusive

Selon les statistiques récentes, plus de la moitié (63%) des consommateurs s'attendent à avoir une offre de produits ou services personnalisée selon leurs préférences et 54% d'entre eux accepteraient de partager leurs informations personnelles pour recevoir ce type d'offres[302]. Pourtant, le marketing ciblé continue de créer le malaise auprès des consommateurs laissant un gout amer lorsque la publicité présentée semble être un calque des activités des consommateurs[303].

L'émergence de nouvelles technologies comme l'intelligence artificielle a transformé le marketing traditionnel par une pratique individualisée. Les médias de masse ont laissé place à la communication « one-to-one » afin d'optimiser l'effet des campagnes publicitaires. Le micromarketing (2.2.1) est alors né de l'exploitation de la masse de données regroupées dans les profils des consommateurs. De cette manière, les marketeurs peuvent personnaliser leurs différentes offres spécifiquement pour chaque consommateur. Cette pratique, bien qu'optimale est toutefois très intrusive pour le consommateur.

Par ailleurs, l'exploitation des données des consommateurs permet non seulement de lui faire des offres personnalisées, mais aussi d'adapter le prix des produits en fonction de sa sensibilité au prix. Cette pratique, mieux connue sous le nom de discrimination tarifaire (2.2.2), permet aux entreprises d'optimiser leurs revenus en fonction de la capacité du consommateur à payer.

---

[301] *Infra*, p. 68.
[302] REDPOINT, *Adressing the Gaps in Customer Experience*, The Harris Poll, Massachussetts, États-Unis, 2019, p. 6.
[303] S. TANGUAY, préc., note 296, p. 169.

Ces nouvelles méthodes soulèvent la question à savoir à partir de quel moment la personnalisation devient-elle une pratique abusive pour le consommateur? La personnalisation de l'offre et des prix des produits dépasse la simple relation d'affaires pour se transformer en exploitation de l'état de vulnérabilité psychologique et économique du consommateur. Le résultat des abus de la collecte se concrétise par une utilisation tout aussi abusive des données des consommateurs, encore une fois, à leur détriment.

2.2.1 Le micromarketing

Le micromarketing s'opère grâce à la forte segmentation d'un marché formant ainsi un marché de niche afin d'offrir aux consommateurs des publicités uniques et personnalisées à leurs besoins[304]. Pour le consommateur, le micromarketing permet d'assurer la pertinence des campagnes publicitaires. Il peut s'agir, par exemple, d'offres ou de promotions spécifiques aux consommateurs les plus loyaux ou aux clients insatisfaits désireux de délaisser l'entreprise. Dans certains cas, il est même possible de modifier les produits et services selon des critères prédéfinis comme le lieu de résidence du consommateur, son titre professionnel ou tout autre critère pertinent.

Au Québec, l'application SAQ Inspire de la Société des alcools du Québec[305] représente un exemple intéressant de micromarketing. L'application mobile collecte les renseignements sur le type d'alcool acheté et personnalise les promotions selon les préférences des consommateurs en proposant des offres exclusives[306]. Ces offres vont varier d'un consommateur à l'autre en fonction de leurs habitudes d'achat. Il est possible d'observer que les campagnes marketings tendent à se développer vers cette pratique plus individualiste afin de maximiser l'engagement des consommateurs.

Du côté européen, l'entreprise France Télévision vient de signer un partenariat avec le fournisseur de télécommunication Orange afin d'offrir des publicités ciblées télévisées sur 7 millions de décodeurs en fonction du profil des consommateurs chez Orange[307]. De cette

[304] D. GREWAL et *al*., préc., note 233, p. 249.
[305] Au Québec, la vente et la distribution de boissons alcoolisées est assurée et contrôlé par l'État via la SAQ.
[306] SAQ, *Profitez d'une expérience plus personnalisée*, en ligne : <https://www.saq.com/fr/saqinspire>
[307] Lionel BONNAVENTURE, « France Télévision prépare ces publicités ciblées avec Orange », *AFP*, 23 juillet 2019, en ligne : <https://apple.news/AnmvK1DSgQTWUZL3yR1qQIQ>

manière, la publicité sera adaptée à chaque décodeur en fonction des préférences des ménages. Ses publicités sur mesure ont pour objectif de limiter la navigation d'une chaîne à l'autre durant les pauses publicitaires. Par ailleurs, un rapport sur le marché de la télévision ciblée prévoit que les recettes publicitaires pourraient s'élever entre 120 et 220 millions d'euros d'ici 2023 ouvrant la voie à cette nouvelle forme de marketing ciblé[308]. Toutefois, en vertu du décret n°92-280 du 27 mars 1992, les messages publicitaires doivent être diffusés de manière simultanée à l'ensemble du territoire limitant actuellement la possibilité de développer cette forme de micromarketing[309]. Le Ministère de la culture travaille activement à faire évoluer cette disposition législative afin de renforcer le dynamisme économique du secteur et permettre le développement de nouvelle technologie de ce genre[310]. Le Ministère défend que l'assouplissement des règles publicitaires pourrait permettre aux chaînes télévisées de concurrencer les autres formes de médias numériques. Le partenariat entre France Télévision et Orange est fort intéressant d'un point de vue marketing, toutefois des modifications législatives sont toujours nécessaires afin de mettre de projet en œuvre.

Le micromarketing correspond toutefois à un usage secondaire des données. Cette forme de recyclage de l'information est souvent critiquée par la communauté juridique qui défend que les données ne sont pas utilisées selon l'usage qui est prévu (2.2.1.1). Toutefois, les entreprises peuvent avoir recours à certaines pratiques techniques pour dépersonnaliser les renseignements utilisés et conserver que des données qui ne concernent pas des individus identifiables (2.2.1.2). L'anonymisation et la pseudonymisation assure une meilleure protection des données des consommateurs, toutefois le consommateur demeure vulnérable face à cette pratique extrêmement ciblée (2.2.1.3).

2.2.1.1 Le principe de nécessité de l'usage des données

Les dispositions en matière de protection des renseignements personnels prévoient que les entreprises peuvent collecter que les renseignements nécessaires à l'objet de la

[308] *Id.*
[309] *Décret n°92-280 du 27 mars 1992 pris pour l'application des articles 27 et 33 de la loi n° 86-1067 du 30 septembre 1986 et fixant les principes généraux définissant les obligations des éditeurs de services en matière de publicité, de parrainage et de télé-achat*, France, en ligne : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000346165>, art. 13.
[310] MINISTÈRE DE LA CULTURE, *Consultation publique sur l'assouplissement des règles relatives à la publicité télévisée*, Décembre 2019, 10 p.

prestation[311]. La Commission d'accès rappelle que le critère de nécessité prévue par le LPRPSP doit être interprété de manière stricte :

> Compte tenu du caractère fondamental que le *Code civil du Québec* et la *Charte des droits et libertés de la personne* donnent au droit au respect de la vie privée, le mot « nécessaire » doit être interprété de façon restrictive. C'est donc dans son sens d'« indispensable », d'« essentiel » ou de « primordial » qu'il doit être retenu. N'est donc pas « nécessaire », au sens de l'article 5 L.p.r.p.s.p. (et par ricochet aux fins de l'article 37 C.c.Q.) ce qui est simplement commode, utile, avantageux ou expédient : est nécessaire ce qui est indispensable, essentiel et dont la présence « rend seule possible une fin ou un effet », pour reprendre les mots du Petit Robert. Nous sommes donc d'accord avec ce qu'affirme à ce propos la Commission d'accès à l'information lorsque, dans un contexte différent du nôtre, elle en arrive elle aussi à la conclusion que le mot « nécessaire », aux fins de l'article 5 L.p.r.p.s.p., doit recevoir une interprétation restrictive : […][312]

Cette collecte doit avoir été préalablement consentie par le consommateur pour les fins expressément mentionnées. Le critère de nécessité s'étend également à la durée de conservation des données[313]. Les renseignements recueillis doivent être conservés seulement pour leur durée utile.

En pratique, les entreprises détiennent déjà la plupart des données nécessaires dans leur base de données client[314]. Il ne s'agit donc pas d'une collecte de données, mais plutôt d'une utilisation secondaire des données collectées à des fins publicitaires. À ce propos, la LPRPSP prévoit que « [l]'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement. »[315] Le projet de loi 64 prévoit mettre fin à cette possibilité en imposant aux entreprises de recueillir seulement les renseignements nécessaires aux fins déterminées lors

[311] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 5. ; *Règlement (UE) 2016/679*, préc., note 23, art. 5 c).
[312] *Syndicat des employées et employés professionnels et de bureau, section locale 57* et *Caisse populaire St-Stanislas de Montréal*, (T.A.), 98-09766, Kirkland, 1998 ; *M.L. c. Gatineau (Ville de)*, 2010 QCCAI 68, par. 79.
[313] *Règlement (UE) 2016/679*, préc., note 23, considérant 39.
[314] Supra, (profilage) p. 54.
[315] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 12.

de la collecte[316]. De son côté, le RGPD exclut spécifiquement l'utilisation ultérieure des données pour d'autres fins que pour constituer des archives, faire des recherches scientifiques ou historiques ou à des fins statistiques[317]. La seule issue pour les publicitaires reste d'obtenir le consentement du consommateur pour l'utilisation de leurs données à des fins publicitaires, mais est-ce juridiquement possible ? La définition même du consentement prévoit que celui-ci doit être spécifique et donné à une fin prédéfinie pour une durée limitée à celle utile en fonction de la finalité du traitement[318]. Le projet de loi 64 prévoit même que le consentement devra être recueilli à chacune des fins pour lesquelles les données sont susceptibles d'être utilisées[319].

Dès lors, le droit s'oppose de manière frontale aux pratiques marketing. Les entreprises publicitaires ont besoin de conserver les données des consommateurs en grande quantité et idéalement sur une longue période afin de pouvoir créer une base de données utile. Comme il a été précédemment étudié, les algorithmes ont besoin de beaucoup d'information pour assurer un résultat intéressant et aussi éviter les sources de biais[320]. En vertu du droit à la protection des renseignements personnels, les entreprises ne peuvent pas conserver et collecter de manière large des renseignements sur les consommateurs ni les conserver sur une longue période. Une des solutions qui s'offre à eux est de s'assurer que les renseignements conservés ne soient pas des renseignements personnels au sens de la loi soit en transformant les données de manière à ce qu'elles deviennent anonymes ou en leur associant un pseudonyme.

2.2.1.2 Anonymisation et pseudonymes

La clé de voute pour la plupart des entreprises qui collectent des données en grande quantité est de s'assurer que les renseignements ne permettent pas d'identifier l'individu à la

[316] « La personne qui recueille des renseignements personnels sur autrui ne doit recueillir que les renseignements nécessaires aux fins déterminées avant la collecte. ». *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi no. 64, préc., note 32, art. 97.
[317] *Règlement (UE) 2016/679*, préc., note 23, art. 5 b).
[318] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 22, art. 14.
[319] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi no. 64, préc., note 32, art. 102.
[320] *Supra*, (biais algorithmique), p. 65.

source des données. Il existe différentes techniques pour rompre le lien entre l'individu et ses données comme l'anonymisation et la pseudonymisation[321].

L'anonymisation est une méthode qui consiste, en théorie, à rendre techniquement impossible la réidentification de la personne visée, et ce, de manière irréversible[322]. De cette manière, il est possible pour l'entreprise d'exploiter les données anonymisées sans porter atteinte aux droits des consommateurs et de les conserver au-delà de la durée de conservation nécessaire[323]. Le droit applicable en matière de protection des renseignements personnels ne couvre plus les données anonymisées puisqu'il n'existe théoriquement aucune possibilité de réidentifier les personnes concernées.

Considérant la puissance des technologies et la masse de données existante, l'anonymisation est-elle une utopie ? Les autorités de protection des données en Europe ont défini trois critères permettant de valider que les données sont bel et bien anonymes soit l'individualisation, la corrélation et l'inférence[324]. Dans un premier temps, il doit être impossible d'isoler un individu dans la base de données. En second, il ne doit pas être possible de relier entre elles des données distinctes et, troisièmement, il ne doit pas être possible de déduire de nouvelles informations à partir des données anonymisées. Toutefois, la recherche a pu démontrer au fil des années que l'anonymisation des données est illusoire. Des chercheurs de l'université de Louvain ont démontrés qu'il était possible de réidentifier 99.98% de la population américaine de n'importe quelle base de données anonymisées avec seulement quinze critères démographiques[325]. Ce genre de résultats démontre que l'usage de données anonymisées n'est pas juridiquement viable du point de vue de la protection des données des consommateurs. Par ailleurs, cette méthode, très réductrice de la qualité des données n'est

---

[321] COMMISSION DE CONTRÔLE DES INFORMATIONS NORMATIVES, *Fiches pratiques : anonymisation ou pseudonymisation*, en ligne : <https://www.ccin.mc/fr/fiches-pratiques/anonymisation-ou-pseudonymisation>

[322] *Id.*

[323] CNIL, *L'anonymisation de données personnelles*, 19 mai 2020, en ligne : <https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles>

[324] *Id.*

[325] Luc ROCHER, Julien M. HENDRICKX, Yves-Alexandre DE MONTJOYE, « Estimating the success of re-identifications in incomplete datasets using generative models », (2019) 3069 *Nature communications* 10, 2.

pas d'un grand intérêt pour les entreprises publicitaires. La réalisation de corrélations et d'inférence sur les données constitue les pratiques les plus intéressantes pour les marketeurs.

De ce fait, de nombreuses entreprises vont utiliser la pseudonymisation comme méthode pour protéger les données. Le RGPD définit la pseudonymisation comme étant :

> […] le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;[326]

A contrario, la pseudonymisation n'a pas le caractère irréversible de l'anonymisation. Elle permet seulement de réduire le risque d'identification des personnes. Concrètement, la pseudonymisation consiste à remplacer les données qui permettent l'identification par des codes ou des données plus élargies. L'équilibre entre la quantité d'information nécessaire pour avoir une base de données utile et la minimisation des données disponibles peut être précaire. Le laboratoire de protection de la vie privée de Harvard a développé une technique sur le critère K-Anonymity.[327] Cette méthode calcule le risque statistique le plus faible de réidentification en fonction de la réduction de la précision de l'information. Par exemple, l'âge peut être remplacé par un groupe d'âge, et le lieu de naissance par une région ou un territoire afin de conserver des informations sur les consommateurs tout en réduisant le degré précision.

La pseudonymisation des données apporte son lot d'avantages pour les entreprises. Étant plus sécuritaire, elle peut améliorer la confiance des individus à partager leurs informations personnelles et permettre la mise en place de bases de données plus élargies. La rupture du lien entre l'internaute et ses activités collectées peut lui permettre d'assurer minimalement la protection de sa vie privée[328]. Or, qu'en est-il pour les publicitaires ? Ce dessein pour les renseignements collectés est intéressant au niveau juridique, mais pas viable au niveau des

[326] *Règlement (UE) 2016/679*, préc., note 23, art. 4 § 5.
[327] Latanya SWEENEY et le Data Privacy Lab de Harvard, « K-Anonymity: A model for protecting privacy» (2002) 10:5 *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 557
[328] *R. c. Spenser*, préc., note 98, par. 46.

affaires marketing. Les données collectées doivent permettre aux publicitaires de créer des profils sur les consommateurs pour que la collecte soit utile. Le retour vers l'équilibre doit être établi entre les intérêts des commerçants et le respect des droits de consommateurs pour assurer une évolution viable de la pratique.

2.2.1.3 La notion de consommateur moyen en micromarketing

De manière générale, les entreprises et les consommateurs apprécient recevoir une publicité adaptée à leurs besoins[329]. Or, ces pratiques peuvent rapidement devenir agressives ou intrusives pour le consommateur et finir par créer une forme d'insatisfaction. Une approche trop personnalisée a tendance à créer un effet d'évitement chez le consommateur[330]. Avec le temps, de nombreuses recherches ont démontré que le ciblage publicitaire était considéré par les consommateurs comme une intrusion dans leur vie privée[331]. Il existe une corrélation négative entre la perception du consommateur et ces préoccupations face à la protection de leur vie privée. En effet, les consommateurs ayant une opinion positive d'une publicité donnée auraient moins d'inquiétude par rapport à la protection de leur vie privée[332]. La confiance est une notion qui varie dans le temps et la multiplication des scandales en matière de vol de données et d'utilisation à des fins non consentie encourage cette méfiance face à la publicité ciblée.

La connaissance et la compréhension des nouvelles technologies jouent un rôle important dans la perception du risque pour les consommateurs. Il existe une pluralité de mécanisme permettant de protéger le consommateur, autant technique que juridique, mais il serait faux de croire que le consommateur est adéquatement protégé. L'idée que le consommateur est en mesure de comprendre et d'utiliser les outils de protection à sa disposition est illusoire. Le professeur de droit américain Paul Ohm prévient dans ces recherches que le droit ne doit pas protéger les internautes aguerris[333], mais plutôt le consommateur moyen à l'image du

[329] Christian LATOUR, « Le marketing direct (le marketing relationnel)… ce qu'il faut savoir », *HRI Mag*, 18 février 2018, en ligne : <https://www.hrimag.com/Le-marketing-direct-marketing-relationnel-ce-qu-il-faut-savoir> ; S. TANGUAY, préc., note 296, p. 168.
[330] S. TANGUAY, préc., note 296, p. 166.
[331] *Id.*, p. 169 ; Sangdow ALNADI, Maged ALI et Kholoud ALKAYID, « The effectiveness of online advertising via the behavioral targeting mecanism », (2014) 5-1 *The Business and Management Review* 23, 28.
[332] *Id.*, 28.
[333] Paul OHM, « The Myth of the Superuser : Fear, Risk and Harm Online », (2008) 41 *UC Davis L. Review* 1327; Éloïse GRATTON, « Publicité ciblée et défis en matière de protection des renseignements personnels »,

consommateur illustré dans l'affaire *Richard c. Times*[334]. Si en matière de publicité trompeuse la Cour suprême juge que le consommateur doit être assimilé au consommateur moyen avec un faible degré de discernement pour les subtilités des représentations commerciales, qu'en est-il du statut du consommateur face aux nouvelles technologies? L'individu visé par le micromarketing n'est-il pas d'autant plus crédule et vulnérable[335] ?

La Cour adopte cette vision du consommateur en respect de « […] la volonté législative de protéger les personnes vulnérables contre les dangers de certaines méthodes publicitaires.»[336] Le professeur Claude Masse prônait également la vision du consommateur crédule et inexpérimenté dans l'interprétation du droit[337]. La définition du terme crédule réduit toutefois le consommateur moyen à un individu naïf susceptible de croire trop facilement[338]. Le professeur Lacoursière soulève le point dans son analyse de la décisions *Times* que l'objectif du législateur n'est pas de protéger le consommateur crédule[339], mais plutôt d'apprécier la publicité au regard du consommateur vulnérable et inexpérimenté par rapport au commerçant[340]. Par ailleurs, dans le cadre des nouvelles technologies, ce n'est pas nécessairement la naïveté du consommateur qui le rend vulnérable, mais plutôt son manque de connaissance et son incompréhension des technologies. L'objet du micromarketing étant

---

dans Claude LAFOND et Vincent GAUTRAIS (dir.), *Consommateur numérique : une protection à la hauteur de la confiance?*, Montréal, Éditions Yvon Blais, 2016, p. 211.

[334] *Richard c. Times*, préc., note 38, par. 72.

[335] « Les qualificatifs « crédule et inexpérimenté » expriment donc la conception du consommateur moyen qu'adopte la *L.p.c.* Cette description du consommateur moyen respecte la volonté législative de protéger les personnes vulnérables contre les dangers de certaines méthodes publicitaires. Le terme « crédule » reconnaît que le consommateur moyen est disposé à faire confiance à un commerçant sur la base de l'impression générale que la publicité qu'il reçoit lui donne. Cependant, il ne suggère pas que le consommateur moyen est incapable de comprendre le sens littéral des termes employés dans une publicité, pourvu que la facture générale de celle-ci ne vienne pas brouiller l'intelligibilité des termes employés. » [nos soulignés] *Richard c. Times*, préc., note 38, par. 72. ; *R v. Imperial Tobacco Products Ltd*, [1971] 5 WWR 409); *Riendeau c Brault & Martineau inc*, 2007 QCCS 4603, par. 149
1448 au para 27.

[336] *Id.*

[337] La vision du consommateur crédule et inexpérimenté en droit de la consommation s'est développée en analyse de l'article 218 et 219 de la L.p.c. concernant les pratiques de publicité trompeuse. Ce critère permet de dégager l'impression générale de la représentation publicitaire pour le consommateur. M. LACOURSIÈRE, préc., note 40, 498 et s.; Claude MASSE, *Loi sur la protection du consommateur : analyse et commentaires*, Cowansville, Yvon Blais, 1999, p. 828.

[338] LAROUSSE, préc., note 8, « crédule »

[339] « En effet, associer un consommateur moyen à une personne crédule constitue une démarche paternaliste qui déresponsabilise le consommateur, ce qui va à l'encontre de l'esprit de la Lpc et des principes du droit de la consommation. » M. LACOURSIÈRE, préc., note 40, 502.

[340] N. L'HEUREUX et M. LACOURSIÈRE, *Droit de la consommation*, préc., note 34, p. 25-26.

d'atteindre de manière la plus efficace le consommateur, le consommateur moyen est plus vulnérable face à la forte personnalisation des pratiques marketing.

2.2.2 La discrimination tarifaire

L'objectif premier du marketing est sans aucun doute la création de valeur[341]. Cette valeur a toutefois un prix qui, dans certains cas, peut varier d'un consommateur à l'autre. En effet, la notion fait référence aux différentes stratégies de prix que les entreprises adoptent afin de vendre un produit identique dont le prix change d'un consommateur à l'autre[342].

Au Canada, la discrimination tarifaire a longtemps été encadrée par le droit de la concurrence au titre de pratique anticoncurrentielle[343]. Depuis la réforme de 2009[344], la discrimination par les prix est envisagée sous les dispositions de l'abus de position dominante[345]. Cette notion impose l'identification de trois éléments distincts et cumulatifs soit l'existence d'un pouvoir de marché, que ce pouvoir ait un caractère substantiel et qu'il ait un effet d'empêchement ou de réduction de la concurrence[346]. Le gouvernement canadien considère toutefois que les dispositions relatives à l'abus de position dominante sont suffisantes pour protéger les consommateurs face aux effets de la discrimination tarifaire[347].

---

[341] D. GREWAL et *al*., préc., note 233, p. iii.

[342] Akiva A MILLER, « What Do We Worry about When We Worry about Price Discrimination: The Law and Ethics of Using Personal Information for Pricing », (2014) 19-1 *J Tech L & Policy* 41, 44.

[343] *Loi sur la concurrence*, préc., note 207, art. 50 (1) [ancien] abrogé par la *Loi d'exécution du budget de 2009*, LC 2009, c. 2 « **50 (1)** Commet un acte criminel et encourt un emprisonnement maximal de deux ans toute personne qui, exploitant une entreprise, selon le cas : **a)** est partie intéressée ou contribue, ou aide, à une vente qui est, à sa connaissance, directement ou indirectement, discriminatoire à l'endroit de concurrents d'un acheteur d'articles de cette personne en ce qu'un escompte, un rabais, une remise, une concession de prix ou un autre avantage est accordé à l'acheteur au-delà et en sus de tout escompte, rabais, remise, concession de prix ou autre avantage accessible à ces concurrents au moment où les articles sont vendus à cet acheteur, à l'égard d'une vente d'articles de qualité et de quantité similaires; **b)** se livre à une politique de vente de produits, dans quelque région du Canada, à des prix inférieurs à ceux qu'elle exige ailleurs au Canada, cette politique ayant pour effet ou tendance de réduire sensiblement la concurrence ou d'éliminer dans une large mesure un concurrent dans cette partie du Canada ou étant destinée à avoir un semblable effet; **c)** se livre à une politique de vente de produits à des prix déraisonnablement bas, cette politique ayant pour effet ou tendance de sensiblement réduire la concurrence ou éliminer un concurrent, ou étant destinée à avoir un semblable effet. »

[344] *Loi d'exécution du budget de 2009*, préc., note 343; Karounga DIAWARA, « La réforme du droit des ententes anticoncurrentielles : aperçut du domaine du nouveau régime hybride à double volet », (2010) 1-3 *Bulletin de droit économique* 23, 23.

[345] *Loi sur la concurrence*, préc., note 207, art. 78-79.

[346] Karounga DIAWARA, *Droit de la concurrence*, Cowansville, Éditions Yvon Blais, 2015, p. 263 ; *Canada (Commissaire de la concurrence) c. Toronto Real Estate Board*, 2014 CAF 29, par. 10.

[347] OCDE, *Compte rendu de la table ronde sur la discrimination par les prix*, 126e réunion du Comité de la concurrence, 29 et 30 novembre 2016, p.5, en ligne :

La discrimination tarifaire pose de tout nouveaux enjeux à savoir l'effet sur le consommateur de la manipulation des prix des biens et services. Pour les entreprises, la discrimination tarifaire assure une forme d'efficience alors que le consommateur est économiquement désavantagé[348]. Le commerçant bénéficie d'une meilleure position du fait qu'il possède la connaissance qu'apportent les données massives et un pouvoir économique supérieur à celui du consommateur. Cette réalité renforce l'hypothèse défendue selon laquelle l'utilisation des nouvelles technologies en marketing cause préjudice au consommateur en déséquilibrant la relation entre les parties[349]. Les données des consommateurs sont utilisées afin d'évaluer quel prix maximal le produit ou service peut atteindre pour maximiser les gains des commerçants. À ce propos, l'auteur Ryan Calo développe dans son article *Digital Market Manipulation* que :

> Even if we do not believe the economic harm story at the level of the market, the mechanism of harm at the level of the consumer is rather clear: the consumer is shedding information that, without her knowledge or against her wishes, will be used to charge her as much as possible, to sell her a product or service she does not need or needs less of, or to convince her in a way that she would find objectionable were she aware of the practice.[350]

Vu sous cet angle, le consommateur crée son propre préjudice en partageant ces données notamment grâce aux nombreux programmes de fidélité (2.2.2.1). Les entreprises sont en mesure de mieux segmenter le marché pour discriminer en fonction des différents critères pertinents (2.2.2.2) La notion d'équilibre contractuel est plus que jamais présente alors que la puissance économique de l'un permet l'exploitation et accentue la vulnérabilité économique de l'autre. Cette forme de discrimination a également ces répercutions sur le jeu de la concurrence entre les entreprises dans le marché (2.2.2.3).

2.2.2.1 La fidélisation et la maximisation des prix

La collecte massive de données permet aux entreprises d'en connaître davantage sur la propension du consommateur à investir pour un produit désiré. En effet, pour offrir un prix

<http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M(2016)2/ANN3/FINAL&docLanguage=Fr>

[348] R. CALO, préc., note 35, 1030.

[349] *Supra*. p. 12.

[350] R. CALO, préc., note 35, 1030.

individualisé, les entreprises doivent être en mesure d'identifier les consommateurs et d'en apprendre davantage sur leurs préférences notamment grâce au profilage[351]. Le succès de leur politique de prix repose sur la capacité de l'entreprise d'exploiter l'information qu'il possède sur un consommateur donné[352]. De cette manière, il est possible d'adapter le prix des produits en conséquence soit en offrant des promotions basées sur le profil du consommateur.

Une des techniques les plus reconnues de discrimination tarifaire est l'utilisation de l'historique d'achat du consommateur pour ajuster les prix[353]. Grâce aux différents programmes de fidélités, les entreprises obtiennent de manière consensuelle une grande quantité d'information sur le consommateur et ont accès à un canal de communication direct leur permettant d'envoyer des offres personnalisées. L'exemple de la SAQ présenté précédemment est encore une fois pertinent. Les consommateurs ont accès à un profil personnalisé afin de suivre leur historique d'achat, le nombre de points accumulé, la valeur en argent des points accumulés, recevoir des offres personnalisées et même acheter en ligne, et ce, à même leur téléphone cellulaire. L'intérêt pour le consommateur n'est plus simplement d'acheter des produits alcoolisés, mais il est susceptible d'évoluer vers la maximisation des points obtenus sur les achats en orientant le comportement du consommateur vers les produits qui offrent plus de points.

La SAQ étant une société d'État, l'objectif de rétention des consommateurs est quasiment absent considérant qu'elle possède un monopole sur la distribution et la vente des vins et spiritueux au Québec. Les cartes de fidélités pour les entreprises en forte concurrence en raison de la faible différentiation des biens comme les épiceries peuvent bénéficier d'un avantage concurrentiel majeur avec la mise en place d'un programme de fidélité intéressant. En général, ces programmes ont pour ambition de fidéliser le consommateur ainsi que de les inciter à orienter leurs achats dans le magasin visé en offrant des rabais exclusifs. De cette manière, le consommateur a un intérêt économique à faire ces courses au même endroit. De leur côté, les entreprises rivalisent avec les compétiteurs qui offrent des produits similaires en créant de la valeur pour le consommateur. Dans cette relation d'affaires, les entreprises

[351] *Supra*, p. 52
[352] A. A MILLER, préc., note 342, 56.
[353] *Id.*, 59.

perdent une part de leur marge de profits en offrant des réductions sur les produits alors que les consommateurs génèrent un gain[354]. Le gain économique pour l'entreprise est atteint si la mise en place d'un programme de fidélité permet de fidéliser le consommateur et résulte en un plus grand volume de vente.

Au regard du droit de la concurrence, l'offre de rabais fidélité peut s'apparenter à une entente d'exclusivité déguisée. Dans l'affaire *Hoffman-La Roche,* la Cour de justice des Communautés européennes a scindé les pratiques d'application de rabais fidélité illicite aux rabais licites appliqués à la quantité de produits achetés :

> En effet, les engagements d'approvisionnement exclusif de cette nature, avec ou sans la contrepartie de rabais ou l'octroi de rabais fidélité en vue d'inciter l'acheteur a s'approvisionner exclusivement auprès de l'entreprise en position dominante sont incompatible avec l'objectif d'une concurrence non faussée dans le marché commun parce qu'ils ne reposent pas sur une prestation économique justifiant cette charge ou cet avantage, mais tendent à enlever à l'acheteur, ou à restreindre dans son chef, la possibilité de choix en ce qui concerne ses sources d'approvisionnement et à barrer l'accès du marché au producteurs. [355]

L'octroi d'un rabais fidélité doit avoir pour objectif de fidéliser la clientèle et non d'évincer ou réduire la concurrence. Ces pratiques exclusives peuvent avoir comme effet de réduire l'offre de produits pour le consommateur final[356].

En théorie, il existe un revers à la personnalisation tarifaire. Si certains consommateurs sont enclins à payer plus cher pour un produit, d'autres pourraient obtenir un meilleur prix en raison du faible intérêt pour le même produit[357]. En pratique, l'intérêt pour la discrimination tarifaire repose sur la maximisation des profits pour les entreprises. Par exemple, il peut être beaucoup moins coûteux pour une entreprise d'effectuer de l'analyse de données à cette fin plutôt qu'investir dans une campagne de marketing ciblée[358]. D'un point de vue économique, elle est considérée comme étant viable pour le marché puisqu'elle augmente l'efficience économique en répartissant le prix selon l'offre et la demande[359]. Malgré ce parti pris par les

[354] A. A MILLER, préc., note 342, 64.
[355] CJCE 13 févr. 1979, aff. 85/76, Rec. CJCE 461.
[356] Comm. CE 13 mai 2009, n° COMP/C-37.990.
[357] R. CALO, préc., note 35, 1030.
[358] Andrew ODLYZKO, « Privacy, Economics, and Price Discrimination on the Internet », dans *Economics of information security*, Boston, Springer, 2004, p. 187, à la p. 189.
[359] *Id.*, p. 187.

économistes, la discrimination tarifaire est souvent perçue de manière très négative par le public. Il est possible d'observer cette perception avec l'émergence d'une foule de ressources permettant de comparer les prix des différents sites pour permettre au consommateur de retrouver leur position économique avantageuse.

2.2.2.2 Segmentation et discrimination économique

Les consommateurs et les entreprises sont naturellement en opposition en ce qui concerne la tarification. Le jeu de prix est un élément essentiel de la négociation entre les parties, puisque chacun cherche à y tirer un avantage. Le consommateur souhaite bénéficier de la meilleure offre en fonction de ses critères et l'entreprise souhaite maximiser sa marge de profits. Analysée au premier degré, la discrimination tarifaire impose à l'entreprise d'être en mesure d'identifier de manière presque absolue le consommateur pour évaluer sa sensibilité au prix[360]. Cette pratique très invasive est de plus en plus complexe à mettre en place en raison des différentes mesures établies par le droit à la protection des renseignements personnels comme l'anonymisation et la pseudonymisation des bases de données[361]. Une des stratégies plus courantes de discrimination tarifaire est de segmenter le marché par groupe selon des traits caractéristiques donnés pertinents à l'établissement d'un prix optimal[362]. Par exemple, les rabais pour personnes âgées ou la tarification spéciale offerte aux jeunes enfants fait partie de ce type de tarification.

Pour les entreprises, il est clair qu'il existe un fort intérêt à discriminer en fonction des prix, même si cette pratique est critiquable[363]. Le secteur des transports est très propice à cette forme de discrimination grâce à la mise en place d'un système de tarification qui offre une large gamme de prix pour essentiellement le même service. Les entreprises sont en concurrence directe pour offrir le même trajet entraînant une abondance de catégories de tarifs[364]. La concurrence étant féroce, les entreprises tentent de capitaliser en ciblant les points névralgiques sur lesquels le consommateur n'est pas prêt à faire de compromis. Par exemple,

[360] A. A MILLER, préc., note 342, 56.
[361] *Supra*, p. 69.
[362] A. A MILLER, préc., note 342, 56.
[363] A. ODLYZKO, préc., note 358, p. 187.
[364] Stéphanie GIAUME et Sarah GUILLOU, « L'impact de la concertation sur la discrimination par les prix dans le transport aérien européen », (2005) 109 *Revue d'Économie Industrielle* 53, 53.

le prix d'un siège adjacent dans un avion peut rapporter à l'entreprise entre 200$ et 2000$ supplémentaire en fonction des conditions de vente des billets[365]. Des économistes ont démontré que la discrimination tarifaire dans un environnement concurrentiel amenait une plus grande dispersion des prix que dans un environnement monopolistique ou oligopolistique[366]. Par ailleurs, plus l'entreprise possède d'information sur le consommateur, plus il est facile pour celle-ci de limiter les possibilités de revente. Dans le cas du secteur de l'aviation, l'attribution des billets d'avion à un consommateur spécifique et la vérification de son identité à la douane permettent à l'entreprise de contrôler leur pratique et d'éviter la revente. De cette manière, le consommateur paye réellement pour le prix qu'il aurait dû payer.

La segmentation du marché peut également permettre aux entreprises de tarifer en fonction du type d'acheteur et des secteurs d'activités. Par exemple, à une certaine époque, l'entreprise Dell offrait sur son site web son plus récent ordinateur portable à un prix 3% inférieur aux entreprises œuvrant dans le secteur de la santé et 10% moins cher aux services gouvernementaux comparativement aux petites entreprises[367]. Les économistes défendent que cette pratique rend le marché plus efficient en plus de lui permettre de réaliser des profits sur des acteurs ayant un plus grand pouvoir économique. De cette manière, les entreprises peuvent offrir au consommateur des produits à meilleur prix. Ce genre de tarification se base toutefois sur un vieil argument économique qui assume que la discrimination tarifaire permet d'assurer une meilleure allocation des ressources.

Cette idée s'oppose au principe juridique d'égalité qui veut que dans un contexte équivalent les conditions soient égales[368]. L'égalité de traitement est un droit fondamental consacré par les articles 20 et 21 de la *Charte des droits fondamentaux de l'Union européenne* qui prévoit que toutes les personnes sont égales en droit[369]. De ce fait, des situations comparables

[365] A. ODLYZKO, préc., note 358, p. 189.
[366] S. GIAUME et S. GUILLOU, préc., note 364, 54. ; Severin BORENSTEIN, « Price Discrimination in Free-Entry Market », (1985) 16 *Rand Journal of Economics* 380 ; Lars A. STOLE, « Nonlinear Pricing and Oligopoly », (1995) 4 *Journal of Economics and Management* 529 ; Tommaso M. VALLENTI, « Price Discrimination and Price Dispersion in a Duopoly », (2000) 54 *Research in Economics* 351.
[367] A. ODLYZKO, préc., note 358, p. 189.
[368] Irène LUC, « La discrimination tarifaire : approche juridique », D 2015.299.
[369] *Charte des droits fondamentaux de l'Union européenne*, OJ C 326, 26.10.2012, p. 391–407

devraient être traités de la même manière, à moins que le traitement différent soit objectivement justifié[370].

2.2.2.3 Le jeu de la concurrence et la protection du consommateur

La discrimination tarifaire est susceptible de faire intervenir le droit de la concurrence en raison de son impact sur le marché. En pratique, une entreprise peut adapter sa politique de prix en fonction du consommateur qu'elle souhaite atteindre de manière tout à fait licite[371]. L'objet du droit de la concurrence est d'encadrer les entreprises dans le but de favoriser la concurrence dans le marché et stimuler l'efficience économique tout en assurant aux consommateurs des prix compétitifs[372]. De ce fait, toute pratique qui a un effet négatif sur le prix des produits serait considérée comme étant restrictive de la concurrence. Par ailleurs, la définition de consommateur en droit de la concurrence est relativement proche de celle élaborée par la Cour suprême en droit de la consommation[373]. Le consommateur est considéré comme étant une personne dénuée de pouvoir économique qui acquiert un bien sur le marché indifféremment de son statut social professionnel[374]. Le consommateur est encore vu comme étant la partie vulnérable dans le rapport contractuel. Le droit de la concurrence les protège en quelque sorte de ces pratiques, mais est-ce suffisant ?

Le Bureau de la concurrence du Canada s'est prononcé à plusieurs reprises sur le caractère nocif de la discrimination tarifaire pour les consommateurs et l'économie en général[375]. Dans un mémoire rendu en appui au CRTC concernant un cas de discrimination par les prix dans

---

[370] Affaire C-550/07 P - *Akzo Nobel Chemicals Ltd et Akcros Chemicals Ltd contre Commission européenne*
[371] I. LUC, préc., note 368.
[372] *Loi sur la concurrence*, préc., note 207, art. 1.1 : « La présente loi a pour objet 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. » [nos soulignés]
[373] *Richard c. Times*, préc., note 38, par. 72.
[374] K. DIAWARA, préc., note 346, p. 65.
[375] Voir BUREAU DE LA CONCURRENCE, *L'Intervention du Bureau de la concurrence : Avis de consultation télécom CRTC 2016-192*, 29 juin 2016, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04108.html> ; BUREAU DE LA CONCURRENCE, *Mémoire au comité d'examen de la Loi sur les transports au Canada*, 27 février 2015, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04040.html> ; BUREAU DE LA CONCURRENCE, *Mémoire présenté au Groupe d'étude sur les politiques en matière de concurrence*, 11 janvier 2008, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/02555.html>

le secteur des fournisseurs de service internet (FSI), le Commissaire de la concurrence a conclu que cette forme de tarification pouvait nuire à la concurrence, l'innovation et provoquer une hausse des prix pour les consommateurs finaux[376]. Par ailleurs, il prévoit que la discrimination par les prix peut aussi reposer sur la gratuité[377]. La notion de de prix doit être appréciée en fonction de l'avantage conféré à un groupe d'individu privilégié en comparaison au groupe désavantagé[378]. Toutefois, la discrimination par les prix n'est pas suffisante pour assumer qu'il peut y avoir un effet anticoncurrentiel sur le marché[379].

En droit français, la discrimination tarifaire était autrefois considérée comme une pratique restrictive de la concurrence en vertu de l'ancien article L. 442-6 1° du *Code de commerce*[380]. Abrogée par la loi du 4 août 2008[381], cette disposition permet aujourd'hui de définir de manière large la discrimination tarifaire, soit le fait pour une entreprise « de pratiquer ou d'obtenir à l'égard d'un partenaire des prix différents, sans justification par des contreparties réelles, de ceux négociés par d'autres. »[382] La disposition a été conçue à l'origine pour limiter les effets pervers de l'abus de la puissance d'achat de certains acteurs réduisant la concurrence entre fournisseurs[383]. Ces pratiques pouvaient avoir comme effet d'augmenter le prix final pour le consommateur, mais jamais il n'a été question dans l'application de cette disposition de la relation entre le commerçant et le consommateur. Le droit de la concurrence encadre spécifiquement les relations entre les acteurs du marché laissant au consommateur les dispositions de droit civil et du droit de la consommation comme recours.

Au Canada, il existe un mécanisme d'accès pour les particuliers au Tribunal de la Concurrence qui ne concerne que certaines pratiques[384]. Avant la réforme de 2002, seul le

---

376 BUREAU DE LA CONCURRENCE, *L'Intervention du Bureau de la concurrence : Avis de consultation télécom CRTC 2016-192*, préc., note 375, par. 7.
377 *Id*., par. 9 à 12.
378 *Id.*
379 BUREAU DE LA CONCURRENCE, *Table ronde sur le monopole et le pouvoir de l'acheteur*, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/02995.html>
380 « La discrimination est le fait pour une entreprise de pratiquer ou d'obtenir à l'égard d'un partenaire économique des prix, des délais de paiement, des conditions de vente, ou d'achat différents, sans justification par des contreparties réelles, de ceux négociés avec des concurrents du partenaire, créant de ce fait un désavantage ou un avantage dans la concurrence pour ce dernier ». C. com., art. L. 442-6, 1° ; Com. 29 janv. 2008, n° 07-13.778, Bull. civ. IV, n° 20. D. 2008. 541, obs. E. Chevrier ; *ibid*. 2009. 2888, obs. D. Ferrier.
381 *Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie*, J.O. 5 août 2008, art. 22.
382 I. LUC, préc., note 368.
383 *Id.*
384 K. DIAWARA, préc., note 346, p. 173 ; *Loi sur la concurrence*, préc., note 207, art. 103.1.

Commissaire pouvait saisir le Tribunal de la concurrence. Depuis, les consommateurs peuvent le saisir si elles sont « directement et sensiblement gênés par les activités d'une autre partie privée »[385]. Toutefois, le refus de vendre[386], le maintien de prix[387] et les pratiques d'exclusivité, de ventes liées et de limitation du marché[388] sont les seules questions susceptibles d'examen par le Tribunal. L'interprétation du critère de l'atteinte directe et sensible[389] impose presque à l'auteur de la demande d'avoir été ruiné par la pratique visée pour considérer l'atteinte comme étant sensible[390]. En cas de discrimination tarifaire, l'atteinte pour le consommateur peut être notable, mais pas nécessairement sensible au sens des critères établis par le tribunal.

L'objectif du droit de la concurrence est d'encadrer les entreprises dans le marché concurrentiel et non d'assurer la protection du consommateur[391]. Assumer que la discrimination tarifaire est encadrée par le droit de la concurrence et assure la protection du consommateur est inadéquat. La discrimination tarifaire navigue de manière obscure entre les pratiques commerciales déloyales et les pratiques anticoncurrentielles.

L'utilisation intelligente des données permet aux entreprises de bénéficier d'un avantage concurrentiel intéressant sur le marché. La connaissance demeure la clé du succès en affaires. Toutefois, l'exploitation de ces connaissances se fait au détriment des droits des consommateurs qui se retrouvent lésés et avec très peu de recours.

Le ciblage et la personnalisation abusive posent un enjeu autant éthique que juridique. Le préjudice majeur que peut entraîner la pratique n'est pas nécessairement situé au niveau de la violation des droits des consommateurs, mais plutôt dans l'exploitation de son état de vulnérabilité. Réduire la publicité à une pratique individuelle s'insère dans une voie qui concerne l'éthique et la responsabilité sociale des entreprises. Il existe différents mécanismes non contraignants qui encouragent les bonnes pratiques publicitaires comme le *Code*

[385] *Id.*
[386] *Id.*, art. 75.
[387] *Id.*, art. 76.
[388] *Id.*, art. 77.
[389] Le terme sensible est vu au sens de substantielle.
[390] K. DIAWARA, préc., note 346, p. 177 ; *Barcode Systems Inc c. Symbol Technologies Canada ULC*, 2004 CAF 339.
[391] K. DIAWARA, préc., note 346, p. 17.

canadien des normes de la publicité adopté en 1963[392]. Ces mécanismes sont toutefois silencieux quant à l'encadrement des nouvelles technologies dans le secteur de la publicité. Il existe toutefois un intérêt et une certaine urgence de se positionner, tant au niveau du droit qu'au niveau de la société, sur la question de la personnalisation abusive. Comme le prévoit le livre blanc sur l'intelligence artificielle[393], ce genre de technologie devrait être utilisé pour maximiser le bienêtre de l'être humain, l'utilisation de l'intelligence artificielle en marketing tend à s'éloigner de ces louables ambitions. Considérant que les intérêts des consommateurs rencontrent difficilement ceux des entreprises[394], l'intervention du droit de la consommation serait opportune pour assurer une protection adéquate des consommateurs.

[392] NORMES DE LA PUBLICITÉ, *Code canadien des normes de la publicité*, en ligne : <https://adstandards.ca/fr/code-canadien/code-en-ligne/>
[393] COMMISSION EUROPÉENNE, préc., note 295.
[394] R. CALO, préc., note 35, 1023.

Conclusion

La publicité a dépassé l'univers télévisuel traditionnel pour s'étendre sur le web, les téléphones intelligents ou même entre deux morceaux de musique. Grâce aux nouvelles technologies, l'environnement médiatique ne possède plus de limites de temps ou d'espace[395]. Maintenant que le consommateur peut être ciblé à n'importe quel endroit au moment opportun. L'omniprésence de la publicité et son caractère intrusif dans le quotidien des consommateurs sont susceptibles de créer un inconfort chez certains individus. Le dernier rapport *Consumer Trust in Digital Marketing* de l'agence internationale *GroupM* démontre que malgré l'opinion positive des consommateurs envers les nouvelles technologies, le marketing numérique conserve une mauvaise réputation[396]. Les statistiques parlent d'elles-mêmes : 60% des répondants affirment que la technologie améliore leur qualité de vie alors que moins de 20% ont une opinion positive de la publicité en ligne[397]. Les consommateurs seraient dès lors plus enclins à tolérer l'usage de leurs données à des fins sociales, mais plus exigeant quant à l'usage de leur donnée à des fins commerciales[398].

Le père fondateur du World Wide Web que l'on connaît aujourd'hui, Tim Berner Lee, a lancé le projet *Contract for the Web* au Sommet de Lisbonne de 2018 afin d'établir une liste de principe permettant aux gouvernements, aux compagnies et aux citoyens de collaborer pour assurer un environnement numérique meilleur[399]. Les enjeux prioritaires du projet concernent l'accès à internet, mais aussi la navigation sécuritaire et transparente pour les internautes[400]. L'objectif est de responsabiliser et de mobiliser les différents acteurs du web pour assurer qu'il poursuive sa croissance dans le respect des fondamentaux des droits humains dans le numérique[401]. On y retrouve d'ailleurs dans la liste d'entreprises supporteur des géants

---

[395] H. LEE et C-H. CHO, préc., note 228, 333.

[396] Les statistiques établies par l'agence se basent sur un sondage réalisé auprès de 13 900 personnes de 18 à 49 ans avec un revenu moyen a élevé étendu sur 4 continents. GROUPM, *Consumer trust in digital marketing*, New-York, 2020, p. 17, en ligne : <https://www.groupm.com/news/new-groupm-research-examines-consumer-trust-digital-marketing>

[397] *Id.*, p. 9.

[398] *Id.*, p. 4.

[399]CONTRACT FOR THE WEB, *Building the contract for the web*, en ligne : < https://contractfortheweb.org/process/> ; CONTRACT FOR THE WEB, *Join us and figth #ForTheWeb*, 5 novembre 2018, en ligne : < https://contractfortheweb.org/2018/11/05/join-us-and-fight-fortheweb/>

[400] *Id.*

[401] CONTRACT FOR THE WEB, *It took all of us to build the web that we have. It will take all of us to secure its future*, en ligne **:** < https://contractfortheweb.org/about/>

comme Google, Facebook, Amazon, Twitter et Microsoft[402]. Indirectement, la publicité et le marketing sur le web sont les secteurs les plus touchés par ce besoin d'encadrer la protection des données d'internautes.

D'un point de vue économique, l'utilisation des données en marketing permet aux entreprises d'atteindre une efficience opérationnelle inégalée au niveau marketing. Or, le succès de l'opération repose sur la confiance des individus à partager leurs données. En 2019, les investissements en marketing digital étaient estimés mondialement à près 333.25 milliards de dollars US, représentant une hausse significative de 17,6%[403]. La popularité grandissante du marketing numérique rappelle qu'autant les entreprises que les consommateurs peuvent bénéficier d'un cadre juridique adéquat concernant l'utilisation des technologies en marketing.

Au niveau juridique, la CNIL et le CPVPC s'intéressent au ciblage publicitaire et au marketing numérique depuis déjà plusieurs années. Il y a près d'une décennie, les deux entités étaient déjà préoccupées par les risques d'atteinte à la vie privée par les différentes techniques de publicité ciblée[404]. Encore aujourd'hui, ces enjeux sont toujours d'actualité, et ce, de manière encore plus sophistiquée avec le développement des nouvelles technologies comme la géolocalisation ou la reconnaissance faciale. La CNIL a d'ailleurs décidé en 2019 de s'attaquer de front au ciblage publicitaire par l'élaboration d'un plan d'action pour accompagner les différents acteurs à assurer leur conformité aux règles de droit applicables[405]. Cette prise de position rappelle l'importance pour la société de la protection des consommateurs dans l'évolution de leur rapport contractuel avec les commerçants.

---

[402]CONTRACT FOR THE WEB, *Contract for the web*, Supporters, en ligne : < https://contractfortheweb.org/>
[403]H. LEE et C-H. CHO, préc., note 228, 333 ; Jasmine ENERG, « Global digital ad spending 2019 », *Emarketer*, 28 mars 2019, en ligne : < https://www.emarketer.com/content/global-digital-ad-spending-2019>.
[404] CNIL, *La publicité ciblée en ligne*, communication présentée en séance plénière le 5 févr. 2009, rapporté par M. Peyrat, en ligne, 33 p. ; CNIL, *Marketing ciblé sur internet : vos données ont de la valeur*, 26 mars 2009, en ligne : < https://www.cnil.fr/fr/marketing-cible-sur-internet-vos-donnees-ont-de-la-valeur>; 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*, Ottawa, 2011, 61 p., en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/report_201105/>
[405]CNIL, *Ciblage publicitaire en ligne : quel plan d'action de la CNIL?,* 28 juin 2019 : <https://www.cnil.fr/fr/ciblage-publicitaire-en-ligne-quel-plan-daction-de-la-cnil>

Le marketing intelligent ouvre la voie à plusieurs avancées technologiques et économiques. L'optimisation des pratiques marketing est viable autant pour le consommateur que le commerçant : le consommateur se voit offrir une publicité adaptée à ses besoins alors que les coûts marketing sont réduits à leur minimum pour le commerçant. La publicité permet également au consommateur d'avoir accès à une pluralité de services gratuitement. Toutefois, lorsque l'objectif est financier, l'appât du gain peut vicier une pratique initialement louable. Entre les mains de géants économiques, le marketing intelligent devient un outil de domination sur le marché en ciblant le consommateur lorsqu'il est le plus vulnérable pour lui offrir un produit dont il n'a probablement pas besoin[406].

Le législateur français a introduit dans le *Code de la consommation* la notion d'abus de faiblesse suite à l'ordonnance 2016-301 du 14 mars 2016. Consacrée à l'article L.121-8, la disposition prévoit que :

> Est interdit le fait d'abuser de la faiblesse ou de l'ignorance d'une personne pour lui faire souscrire, par le moyen de visites à domicile, des engagements au comptant ou à crédit sous quelque forme que ce soit, lorsque les circonstances montrent que cette personne n'était pas en mesure d'apprécier la portée des engagements qu'elle prenait ou de déceler les ruses ou artifices déployés pour la convaincre à y souscrire ou font apparaître qu'elle a été soumise à une contrainte.

L'idée de sanctionner l'exploitation du consommateur faible et ignorant est appréciable considérant que, dans le contexte des nouvelles technologies, le consommateur se retrouve dans une position particulière. Comme il a été démontré dans ce mémoire, l'utilisation des données massive et de l'intelligence artificielle affectent une pluralité de droits du consommateur et celui-ci se retrouve dans une position vulnérable face aux entreprises. Par ailleurs, la complexité des nouvelles technologies et des pratiques marketing rappelle cet état d'ignorance dans lequel le consommateur se trouve. En interprétant de manière large cette disposition, l'idée que l'exploitation d'une position dominante de la part du commerçant par rapport au consommateur devrait être sanctionnée est intéressante. Toutefois, la disposition doit être interprétée dans son contexte. Celle-ci a été prévue pour permettre au consommateur qui a consommé dans un contexte de pression déraisonnable ou de contrainte puisse se

[406] R. CALO, préc., note 35, 1030.

rétracter et annuler la transaction. Le même type de disposition se retrouve dans la *Loi sur la protection du consommateur* au Québec[407].

Néanmoins, la protection des consommateurs ne peut plus reposer sur la délégation à celui-ci du contrôle de l'usage de ces informations. Le numérique et les technologies comportent un degré de complexité qui augmente de manière exponentielle avec le temps. Il serait déraisonnable de s'attendre que le consommateur moyen puisse comprendre l'usage de ces données à des fins marketing. De plus, l'état de vulnérabilité dans lequel le consommateur se trouve en raison de la puissance des nouvelles techniques publicitaires soulève plusieurs questions éthiques souvent tu par des arguments économiques. Le caractère obligatoire de la publicité et le manque de contrôle du consommateur sur ses données personnelles sont excusés en partie par la gratuité des services offerts sur le web. Le prix à payer est celui de la publicité, mais est-il réellement juste considérant la contrepartie financière que les géants économiques sont en mesure de générer grâce à celle-ci ? La notion de disparité économique entre les parties est encore une fois présente ramenant le consommateur à sa position de faiblesse.

Par ailleurs, encadrement juridique et développement technologique ne sont pas des termes antinomiques. Le droit ne tue pas nécessairement l'innovation, mais lui permet de grandir dans un cadre dirigé assurant la protection des parties prenantes. De ce fait, pour que la technologie soit réellement synonyme de progrès pour l'humanité[408], la protection du consommateur doit être pleinement envisagée à l'ère du marketing intelligent. En soi, l'utilisation des nouvelles technologies affecte d'une multitude de façons les droits des consommateurs. Différents régimes juridiques sont en place pour encadrer la pratique et les méfaits qui peuvent en dériver. Or, c'est l'usage généralisé des technologies dans le secteur qui affecte l'équilibre contractuel entre les parties.

[407] *Loi sur la protection du consommateur*, préc., note 37, art. 8 « Le consommateur peut demander la nullité du contrat ou la réduction des obligations qui en découlent lorsque la disproportion entre les prestations respectives des parties est tellement considérable qu'elle équivaut à de l'exploitation du consommateur, ou que l'obligation du consommateur est excessive, abusive ou exorbitante. »
[408] *Supra*, p. 1.

Bibliographie

TABLE DE LA LÉGISLATION

Législation canadienne

Textes constitutionnels

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

Textes fédéraux

Loi d'exécution du budget de 2009, LC 2009, c. 2

Loi sur la concurrence, LRC 1985, ch. C-34

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

Loi sur l'accès à l'information, LRC 1985, c. A-1

Loi sur le droit d'auteur, LRC 1985, c. C-42

Loi sur les brevets, LRC 1985, c. P-4

Loi sur les marques de commerce, LRC 1985, c. T-13

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

Textes québécois

Charte des droits et libertés de la personne, LRQ, c. C-12

Code civil du Québec, LQ 1991, c. 64

Loi concernant le cadre juridique des technologies de l'information, LQ, c. C-1.1

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, projet de loi no. 64 (présentation – 12 juin 2020), 1re session, 42e légis. (Qc)

Loi sur la protection des renseignements personnels dans le secteur privé, LRQ, c. P-39.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1

Loi sur la protection du consommateur, RLRQ, c. P-40.1

Législation européenne

Textes européens

Charte des droits fondamentaux de l'Union européenne, OJ C 326, 26.10.2012, p. 391–407

Convention Européenne des droits de l'homme, 04.XI.1950, Rome

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, JO L 201, 31.7.2002, p. 37

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, OJ L 105, 13.4.2006, p. 54–6

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n o 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, J.O. L 337, 18.12.2009, p. 11–36

Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil Texte présentant de l'intérêt pour l'EEE, J.O. L 304, 22.11.2011, p. 64–88

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, OJ L 119, 4.5.2016, p. 89–131

Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, O.J., L 157, 15.6.2016, p. 1–18

Directive (UE) 2019/770 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, J.O. L 136 du 22.5.2019, p. 1–27

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), J.O. L 119 du 4.5.2016, p. 1–88

Textes français

Code civil, version consolidée au 31 juillet 2020

Code de la consommation, version consolidée au 31 juillet 2020

Code des postes et des communications électroniques, version consolidée au 31 juillet 2020

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 21.12.1976

Loi n° 2004-575 pour la confiance dans l'économie numérique, J.O. 21.06.2004

Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, J.O. 5 août 2008

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, J.O. 08.10.2016

Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, J.O. 31 juillet 2018

Législation américaine

Textes californiens

California Consumer Privacy Act of 2018, SB-1121 c. 73

TABLE DE LA JURISPRUDENCE

Jurisprudence canadienne

Jones c. Tsige, 2012 O.N.C.A. 32

Lac Minerals Ltd. c. International Corona Resources Ltd., [1989] 2 R.C.S. 574

M.L. c. Gatineau (Ville de), 2010 Q.C.C.A.I. 68

Québec (Sous-ministre du revenu) c. *Lasalle*, J.E. 97-1575 (C.Q.)

R. c. Cole, [2012] 3 R.C.S. 34

R. c. Dyment, [1988] 2 R.C.S. 417

R. c. Morelli, [2010] 1 R.C.S. 253

R. c. Pohoretsky, [1987] 1 R.C.S. 945

R. c. Spenser, [2014] 2 R.C.S. 212

R v. Imperial Tobacco Products Ltd, [1971] 5 W.W.R. 409

Reeves c. *Fasken Martineau DuMoulin*, [2001] C.A.I. 322

Reibeiro c. *Shawinigan Chemicals*, [1973] C.S. 389

Reid c. *Belzile*, [1980] Q.C.C.S. 717

Riendeau c Brault & Martineau inc, 2007 Q.C.C.S. 4603

Richard c. Times, [2012] 1 R.C.S. 265

Robbins c. *Canadian Broadcasting Corporation*, [1958] C.S. 152

Syndicat des employées et employés professionnels et de bureau, section locale 57 et *Caisse populaire St-Stanislas de Montréal*, (T.A.), 98-09766, Kirkland, 1998

The Gazette c. *Valiquette*, [1997] R.J.Q. 30

Turner c. Telus Communications Inc., 2005 C.F. 1601

Union des consommateurs c. Bell Canada, 2011 Q.C.C.S. 1118

Jurisprudence européenne

CJCE 13 févr. 1979, aff. 85/76, Rec. CJCE 461

CJUE, *VKI c. Amazon,* 3e ch., 28 juill. 2016, n° C-191/15

CJUE 5 juin 2018, aff. C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH* : *CCE* 2018, comm. 86, obs. N. Metallinos ; ibid. Étude 21, note I. Barsan ; *RDC* 2018. 555, note A. Danis-Fatôme ; *D.* 2018. 1208; ibid. 2270, obs. J. Larrieu, C. Le Stanc et P. Tréfigny; ibid. 2019. 1016, obs. S. Clavel et F. Jault-Seseke; ibid. 1673, obs. W. Maxwell et C. Zolynski

CJUE, *Fashion ID*, 29 juillet 2019, C-40/17

CJUE, *Bundesverband der Verbraucherzentralen und Verbraucherverbände eV/Planet49 GmbH*, gr. ch., 1er oct. 2019, aff. C-673/17 : *JCP E*, n° 41, 10 Octobre 2019, act. 652

Jurisprudence française

CA Paris, 12 févr. 2016, no. 201658, *Contrats conc. consom*. 2016, comm. 132, obs. S. Bernheim-Desvaux ; *Com. com. élect.* 2016, comm. 33, obs. G. Loiseau ; *RTD Civ.* 2016, p. 310, note L. Usunier ; *D.* 2016, p. 1045, obs. H. Gaudemet-Tallon et F. Jault-Seseke, Dalloz IP/IT 2016, p. 214, obs. S. André et C. Lallemand

CA Paris, 5 juil. 2019, no. 17/03974

Civ. 1re, 3 nov. 2016, n° 15-22.595, publié au Bulletin ; AJDA 2017. 23 ; D. 2016. 2285 ; Dalloz IP/IT 2017. 120, obs. G. Péronne et E. Daoud

Com. 29 janv. 2008, n° 07-13.778, Bull. civ. IV, n° 20. D. 2008. 541, obs. E. Chevrier ; *ibid*. 2009. 2888, obs. D. Ferrier

Com. CE 13 mai 2009, n° COMP/C-37.990.

CNIL, 5 déc. 2013, no. 2013-378

CNIL, 24 juin 2015, no. 2015-048

CNIL, 26 jan. 2016, no. 2016-007

CNIL, 30 oct. 2018, no. MED-2018-042

Crim. 28 jan. 2004, *Bull crim.*, no. 03-80.930

Cons. d'Ét., 9e et 10e ch., 16 oct. 2019, no. 433069

Jurisprudence américaine

Chasom Brown et al. v. *Google LLC/Alphabet Inc.*, 20-3664 (Dist. Ct. Cal 2020)

BIBLIOGRAPHIE

Monographie et ouvrages collectifs

AKINKUNMI, M., *Data Mining and Market Intelligence: Implications for Decision Making*, Californie, Morgan & Claypool, 2018

ATKINSON, R. D. et A. S. MACKAY, *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution*, New-York, The Information Technology and Innovation Foundation, 2007

BOURGEOIS, M., *Droit de la donnée*, Paris, LexisNexis, 2017

BOURGOIGNIE, T., *Éléments pour une théorie du droit de la consommation : au regard des développements du droit belge et du droit de la Communauté économique européenne*, Bruxelles, Story Scientia, 1988

BOURGOIGNIE, T., *Regards croisés sur les enjeux contemporains du droit de la consommation*, Cowansville, Éditions Yvon Blais, 2006

CARNEROLI, S., *Marketing et Internet*, Bruxelles, Larcier, 2011

CASILLAS, J. et F. J. MARTINEZ LOPEZ, *Marketing Intelligent Systems Using Soft Computing*, New-York, Springer, 2010.

CONAN DOYLE, A., *The Memoirs of Sherlock Holmes*, dans « The Reigate Square », États-Unis, Harpers & Brothers, 1894.

C. DIZON, M. A., *A socio-legal study of hacking : breaking and remaking law and technology*, New-York, Routledge, 2018

DAINTITH, J. et E. WRIGHT, *A Dictionnary of Computing*, 6e éd., Oxford University Press, 2008

DERIEUX, E., *Droit européen et international des médias*, Paris, LGDJ, 2003

DIAWARA, K., *Droit de la concurrence*, Cowansville, Éditions Yvon Blais, 2015

FABRE, R. et al., *Droit de la publicité et de la promotion des ventes*, 4e éd., Paris, Dalloz, 2014

FRISON ROCHE, M.-A., *Internet, espace d'interrégulation*, Paris, Dalloz, 2016

GREFFE F. et P.-B. GREFFE, *La publicité et la loi*, 11e éd., Paris, LexisNexis SA, 2009

GREWAL, D. et *al*., *Marketing*, 2e éd., Montréal, McGraw-Hill Education, Chenelière Éducation, 2015

GAUTHIER, J., *Le droit de la biométrie au Québec : sécurité et vie privée*, Montréal, Éditions Yvon Blais, 2015

GAUTRAIS, V., (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002

JULIA, L., *L'intelligence artificielle n'existe pas*, Paris, Éditions First, 2019

LAFOND, C. et V. GAUTRAIS (dir.), *Consommateur numérique : une protection à la hauteur de la confiance ?*, Montréal, Éditions Yvon Blais, 2016

LAFOND, P-C., (dir.), *L'équité au service du consommateur*, Cowansville, Éditions Yvon Blais, 2010

L'HEUREUX, N. et M. LACOURSIÈRE, *Droit de la consommation*, 6e éd., Cowansville, Éditions Yvon Blais, 2011

MASSE, C., *Loi sur la protection du consommateur : analyse et commentaires*, Cowansville, Yvon Blais, 1999.

MIZRAHI, S. K., *The Legal Implications of Internet Marketing: Exploiting the Digital Marketplace Within the Boundaries of the Law*, Cowansville, Éditions Yvon Blais, 2015

ORWELL, G., *1984*, Angleterre, Édition Gallimard, 1950

PATENAUDE, P., *La preuve, les techniques modernes et le respect des valeurs fondamentales : enquête, surveillance et conservation des données*, Sherbrooke, Les Éditions R.D.U.S., 1990

RAYMOND, G., *Droit de la consommation*, 5e éd., Paris, LexisNexis SA, 2019

ROSS, W. D., *Aristotle's Metaphysics*, Oxford, Clarendon Press, 1981

RUSSEL, S. J., et P. NORVING, *Artificial Intelligence: A Modern Approach*, 3e éd., New-Jersey, Pearson, 2002

SCASSA, T. et M. DETURBIDE, *Electronic Commerce and Internet Law in Canada*, 2e éd., Toronto, CCH Canadian Limited, 2012

STERN, J., *Artificial Intelligence for Marketing: Practical Applications*, New Jersey, Wiley & Sons Inc., 2017

TANCELIN, M., *Des obligations en droit mixte au Québec*, 7e éd., Montréal, Wilson & Lafleur, 2009.

TAYLOR, L., L. FLORIDI et B. VAN DER SLOOT (ed.), *Group Privacy: New Challenges of Data technology, vol. 126,* Springer International Publishing, 2016

WESTIN, A. F., *Privacy and Freedom*, New York, Atheneum, 1967

WINSTON, P. H., *Artificial Intelligence,* 3e éd., Massachusetts, Addison-Wesley, 1992

Articles de périodiques et études d'ouvrages collectifs

ALNADI, S., M., ALI et K., ALKAYID, « The effectiveness of online advertising via the behavioral targeting mecanism », (2014) 5-1 *The Business and Management Review* 23

BALL, K. et W. WEBSTER, « Big data and surveillance: Hype, commercial logic and new intimate sphere », (2020) 7-1 *Big Data and Society* 1

BARDIN, M., « L'identité numérique et le droit : esquisse d'une conciliation difficile », (2018) 80-1 *Hermès* 283

BATTAIS, L., « L'efficacité des actions de marketing direct sur les marchés de grande consommation : l'expérience BehaviorScan en France et en Allemagne », (2003) 30 *Décisions Marketing* 63

BERGER, D. D., « Balancing Consumer Privacy with Behavioral Targeting », (2010) 27-1 *Santa Clara Computer & High Technology Law Journal* 3

BERGERON V. et T. GAGNON-VAN LEEUWEN, « Géolocalisation et applications mobiles : mode d'emploi pour une géolocalisation éloignée des problèmes juridiques », dans S.F.C.B.Q., vol. 406, *Développements récents en droit de la propriété intellectuelle*, Cowansville, Éditions Yvon Blais, 2015

BORENSTEIN, S., « Price Discrimination in Free-Entry Market », (1985) 16 *Rand Journal of Economics* 380

BOURGEOIS, M. et M. MOINE, « La délibération 2019-093 du 4 juillet 2019 sur les cookies et autres traceurs - Une préface à la révolution e-privacy ! », (2019) *JCP E* 38, aff. 595.

BOURGOIGNIE, T., « Un droit de la consommation est-il encore nécessaire en 2006 ? », dans BOURGOIGNIE, T, *Regards croisés sur les enjeux contemporains du droit de la consommation*, Cowansville, Les Éditions Yvon Blais Inc., 2006

CIGNA, M-H., J-P GUAY et P. RENAUD, « La reconnaissance émotionnelle faciale: validation préliminaire de stimuli virtuels dynamiques et comparaison avec les Pictures of Facial Affect (POFA) », (2015) 45-2 *Criminologie* 237

CNIL, « Délib. n° 2019-093, 4 juill. 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou

écriture dans le terminal d'un utilisateur [notamment aux cookies et autres traceurs] [rectificatif] » (2019) *JCP E* 28, aff. 473.

CONSTANTINIDES, E. et S. J. FOUNTAIN, « Web 2.0 : Conceptual foundation and marketing issues », (2008) 9 *J Direct Data Mark Pract* 231

COUPEZ, F. et G. PÉRONNE, « Consentement aux cookies : quelle est la bonne recette ? » *D. IP/IT* 2020.189.

DE MONTJOYE, Y., et *al.,* « Unique in the Crowd: The privacy bounds of human mobility » (2013) 3 *Sci Rep* 1376

DEBET, A., « APBN enfin remis en cause par la CNIL! », (2017) 12 *Communication commerce électronique / LexisNexis SA* 43-46.

DE RICO, J-F. et D. JAAR, « Le cadre juridique des technologies de l'information », dans S.F.C.B.Q., *Congrès annuel du Barreau du Québec 2009*, Cowansville, Éditions Yvon Blais

DIAWARA, K., « La réforme du droit des ententes anticoncurentielles : apperçut du domaine du nouveau régime hybride à double volet », (2010) 1-3 *Bulletin de droit économique* 23

DION D., et A. MICHAUD-TREVINAL, « Les enjeux de la mobilité des consommateurs », (2004) 34 *Décisions Marketing* 17

DOUVILLE, T., « Bouton J'aime et responsabilité conjointe de traitement », *D. IP/IT* 2020.126

EDMUNDSON, K. E., « Global Position System Implants: Must Consumer Privacy Be Lost in order for People to Be Found? », (2005) 38 *Ind. L. Rev.* 207

EREVELLES, S., N. FUKAWA et L. SWAYNES, « Big data consumer analytics and the transformation of marketing », (2016) 69 *Journal of Business Research* 897

FILIPPI, P. D., « Repenser le droit à l'ère numérique : entre la régulation technique et la gouvernance algorithmique », dans V. GAUTRAIS et P. E. MOYSE, *Droit et Machine*, vol. 3, Éditions Thémis, 2017.

FONTAINE, M., S. JUILLET et D. FROGER, « La donnée numérique : l'or noir du XXIe siècle ? », *Les Petites Affiches*, n° 179, 2017, p. 90.

GAUTRAIS, V. et A. PORCIN, « Les 7 pêchés de la L.p.c. : actions et omissions applicables au commerce électronique », (2009) 43 *R.J.T.* 559

GEFFRAY, E. et A. GUÉRIN-FRANÇOIS, *Com. Code de la protection des données personnelles*, Dalloz, art. L 34-5.

GERVAIS, D., « Commerce électronique : chronique bibliographique », 33-3 *RGD* 489

GIAUME, S. et S., GUILLOU, « L'impact de la concertation sur la discrimination par les prix dans le transport aérien européen », (2005) 109 *Revue d'Économie Industrielle* 53

GUIMOND, A., « La notion de confiance et le droit du commerce électronique », (2008) 12-3 *LexElectronica* 1

GRATTON, É., « Publicité ciblée et défis en matière de protection des renseignements personnels », dans Claude LAFOND et Vincent GAUTRAIS (dir.), *Consommateur numérique : une protection à la hauteur de la confiance?*, Montréal, Éditions Yvon Blais, 2016, p. 177-218.

GREENWALD, G., E., MACASKILL et L., POITRAS, « Edward Snowden : the whistleblower behind the NSA surveillance revelation », *The Guardian*, 11 juin 2013, en ligne : <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

HAYES, D. R., C. SNOW et S. ALTUWAYJIRI, « Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application », (2017) 10 : 4511, *Proceedings of the Conference on Information Systems Applied Research*, 1 p.

HOPKINS, R., « An Introduction to Biometrics and Large Scale Civilian Identification », (1999) 13 *Int'l Rev. of L. Computers & Tech.* 337

J VAN HAL, T., « Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection » (2013) 15-3 *Vand J Ent L & Prac* 713

JACQUEMIN, H., « Le big data à l'épreuve des pratiques du marché et de la protection du consommateur », (2018) 70 *R.D.T.I* 75

JALUZOT, B., « Méthodologie du droit comparé : bilan et prospective », (2005) 57 *R. I. D. C.* 29

JOHNSON, D. et D. POST, « Law and borders – the rise of law in cyberspace » (1996) 48 *Stan. L. Rev*. 1367

JUENEMAN, R. R., et R.J. ROBERTSON, « Biometrics and Digital Signature in Electronic Commerce », (1998) 38 *Jurimetrics J*. 427

KING, N. J., « Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices », (2007) 60-2 *Federal Communications Law Journal* 239

KRISTOL, D. M., « HTTP Cookies : Standards, Privacy and Politics », (2001) 1-2 *ACM Transaction on Technology* 151

LACOURS, S., « Intelligence artificielle : les solutions algorithmiques permettent de définir plus précisément les profils clients », *Juris Tourisme* 2019.220.13

LACOURSIÈRE, M., « Richard C Time Inc : à la recherche de la définition du «consommateur moyen »! », 2012 90-2 *Revue du Barreau canadien* 493

LEE, H. et C-H. CHO, « Digital advertising : present and futur prospect », (2019) 39-3 *International Journal of Advertising* 332

LIMBERT, T., L. GRAVES et R. KLEIS NIELSEN, « Third-party cookie down by 22% on Europe news sites since GDPR », *Reuters Institute – University of Oxford*, 2018, en ligne : <https://reutersinstitute.politics.ox.ac.uk/risj-review/third-party-cookies-down-22-europes-news-sites-gdpr?mod=djemCMOToday>

LOCKWOOD, S., « Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators », (2004) 18 *Harv. J. L. & Tech.* 307

LUC, I., « La discrimination tarifaire : approche juridique », D 2015.299

MARTIAL-BRAZ, N., « RGPD – Le profilage : fiche pratique », CCE 2018.4.15

MARTINEZ LOPEZ, F. J. et J. CASILLAS, « Marketing Intelligent Systems for consumer behaviour modelling by a descriptive induction approach based on Genetic Fuzzy Systems », (2009) 38 *Industrial Marketing Management* 714

MARTINEZ LOPEZ, F. J., et J. CASILLAS, « Artificial intelligence-based systems applied in industrial marketing: An historical overview, current and future insights » (2013) 42 *Industrial Marketing Management* 489

MASSE, C., « Fondement historique de l'évolution du droit québécois de la consommation », dans Pierre-Claude Lafond (dir.), *Mélanges Claude Masse – En quête de justice et d'équité*, Cowansville, 2003

MAXIMIN, N., « Proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace », *D.* 2020.03.144

MCDONALD, A. M. et L. F. CRANOR, 4-3 « The cost of reading privacy policies », (2001) *Journal of Law and Policy* 545

METALLINOS, N., « Les leçons à tirer de la sanction de Google par la CNIL (1re partie : Pas de « guichet unique » pour Google !) », (2019) 5 *Communication Commerce électronique* 35

METALLINOS, N., « Les leçons à tirer de la sanction de Google par la CNIL (2e partie : Renforcement des exigences de transparence et de consentement) », (2019) 6 *Communication commerce électronique / LexisNexis SA* 43

METALLINOS, N., « Adoption de lignes directrices de la CNIL sur les cookies pour assurer la conformité avec les exigences de consentement posé par le RGPD », (2019), 10 *Communication commerce électronique / LexisNexis SA* 62, fasc. 940

MERRY, K. et P. BETTINGER, « Smarthphone GPS accuracy study in an urban environment », (2019) 14-7 *Plos ONE* 1

MILLER, A. A, « What Do We Worry about When We Worry about Price Discrimination: The Law and Ethics of Using Personal Information for Pricing », (2014) 19-1 *J Tech L & Policy* 41

MONNERIE, N., « Les défis de la commercialisation des données après le RGPD : aspects concurrents d'un marché en développement », (2018) 4 *Revue internationale de droit économique* 431

MOORE, B., « Autonomie ou dépendance : réflexions sur les liens unissant le droit contractuel de la consommation au droit commun », dans Pierre-Claude Lafond, *Le droit de la consommation sous influences*, Cowansville, Les Éditions Yvon Blais Inc., 2007

NIORT, J-F., « Droit, économie et libéralisme dans l'esprit du Code Napoléon », (1992) 37 *Archives de philosophie du droit* 101

ODLYZKO, A., « Privacy, Economics, and Price Discrimination on the Internet », dans *Economics of information security*, Boston, Springer, 2004

OHM, P., « The Myth of the Superuser : Fear, Risk and Harm Online », (2008) 41 *UC Davis L. Review* 1327;

OUAKRAT, A., « Le ciblage publicitaire comportemental, une perte de contrôle des éditeurs sur les données de l'audiance », (2012) 6-1 *Tic&Société* 33

REITZ, J. C., « How to Do Comparative Law », (1998) 4-46 *Amercian Journal of Comparative Law* 617

Luc ROCHER, L., J. M. HENDRICKX et Y.-A. DE MONTJOYE, « Estimating the success of re-identifications in incomplete datasets using generative models », (2019) 3069 *Nature communications* 10

SEFFAR, K. et K. BENYEKHLEF, « Commerce électronique et normativité alternative », (2006) 3-2 *U.O.L.T.J* 353

STOFFEL-MUNCK, P., « L'autonomie du droit contractuel de la consommation : d'une logique civiliste à une logique de régulation », *RTD com.* 2012

STOLE, L.A., « Nonlinear Pricing and Oligopoly », (1995) 4 *Journal of Economics and Management* 529

SWEENEY, L et Data Privacy Lab de Harvard, « K-Anonymity: A model for protecting privacy» (2002) 10:5 *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 557

TANGUAY, S., « Le ciblage publicitaire en ligne », dans Claude LAFOND et Vincent GAUTRAIS (dir.), *Consommateur numérique : une protection à la hauteur de la confiance?*, Montréal, Éditions Yvon Blais, 2016

THIBAUDEAU, L., « Le I-consommateur à la recherche de la protection adéquate », S.F.C.B.Q., vol. 380, *Colloque national sur les recours collectifs – Développements récents au Québec, au Canada et aux États-Unis*, Cowansville, Éditions Yvon Blais, 2014, p. 573

TRUDEL, P., « Quel droit et quelle régulation dans le cyberespace ? », (2000) 32-2 Sociologie et sociétés 189

TURING, A., « Computing machinery and intelligence », (1950) 59 *MIND* 433

VALLENTI, T. M., « Price Discrimination and Price Dispersion in a Duopoly », (2000) 54 *Research in Economics* 351.

WIERENGA, B., « Marketing and Artificial Intelligence: Great Opportunities, Reluctant Paterns », dans Jorge CASILLAS Francisco J. MARTINEZ LOPEZ, *Marketing Intelligent Systems Using Soft Computing*, New-York, Springer, 2010, p. 1

WU, X., *et al.*, « Data mining with the big data », (2014) 26-1 *EEE Transactions on Knowledge and Data Engineering* 97

ZIEGEL, J. S., « The Future of Canadian Consumerism », (1973) 51 *R. du B. can.* 191

Articles de journaux

AFP, « Google éliminera progressivement les témoins tiers d'ici deux ans », *Radio-Canada*, 14 janvier 2020, en ligne : < https://ici.radio-canada.ca/nouvelle/1473506/google-chrome-cookies-temoins-bloquer-deux-ans>

AFP, « Un homme arrêté à tort à cause de la technologie de reconnaissance faciale », *LaPresse*, 24 juin 2020, en ligne : <https://www.lapresse.ca/international/etats-unis/2020-06-24/un-homme-arrete-a-tort-a-cause-de-la-technologie-de-reconnaissance-faciale?utm_source=facebook&utm_medium=social&utm_campaign=algofb>

ANON, D., « How cookies track you around the web and how to stop them », *Privacy.net*, 24 février 2018, en ligne : <https://privacy.net/stop-cookies-tracking/>

BENESSAIEH, K., « Clins d'œil technologique », *LaPresse*, 31 mai 2020, en ligne : <https://www.lapresse.ca/affaires/techno/202005/30/01-5275737-clins-doeil-technologiques.php>

BENESSAIEH, K., « Navigation privée : demande d'action collective contre Google », *LaPresse*, 26 juin 2020, en ligne : <https://www.lapresse.ca/affaires/techno/2020-06-26/navigation-privee-demande-d-action-collective-contre-google>

CAMPBELL-DOLLAGHAN, K., « Here's how GDPR is already changing web design », *Fast Company*, 30 août 2018, en ligne : <https://www.fastcompany.com/90229646/heres-how-gdpr-is-already-changing-web-design>

CARR, D., « Giving user what they want », *The New York Times*, 24 février 2013, en ligne : < https://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?auth=linked-facebook>

CHOUDARY, S. P., « The rise of social graphs for businesses », *HBR*, 2 février 2015, en ligne : <https://hbr.org/2015/02/the-rise-of-social-graphs-for-businesses>

CONNER-SIMONS, A., « Wireless tech means safer drones, smarter homes and password-free wifi », *MIT News*, 31 mars 2016, en ligne : <http://news.mit.edu/2016/wireless-tech-means-safer-drones-smarter-homes-password-free-wifi-0331>

CONTREPOIS, S., « Scoring client : définition et avantages », *MyFeelBack*, 4 juillet 2019, en ligne : <https://www.myfeelback.com/fr/blog/scoring-client-avantages>

DASTIN, J., « Insight - Amazon scraps secret AI recruiting tool that showed bias against women », *Reuters*, 9 octobre 2018, en ligne : <https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH>

DEBÈS, F. et S. DUMOULIN, « La CNIL publie ses recommandations très attendues sur le ciblage publicitaire », *Les Echos*, 14 janvier 2020, en ligne : < https://www.lesechos.fr/tech-medias/hightech/la-cnil-publie-ses-recommandations-tres-attendues-sur-le-ciblage-publicitaire-1162582>

DEBÈS, F., et R., BALENIERI, « Comment Google a asphyxié les comparateurs de prix européens », *LesEchos*, 8 octobre 2018, en ligne : <https://www.lesechos.fr/tech-medias/hightech/comment-google-a-asphyxie-les-comparateurs-de-prix-europeens-140639>

DOUGLAS HEAVEN, W., « Our weird behavior during pandemic is messing with IA models », *MIT Technology Review*, 11 mai 2020, en ligne : <https://www.technologyreview.com/2020/05/11/1001563/covid-pandemic-broken-ai-machine-learning-amazon-retail-fraud-humans-in-the-loop/>

DUHIGG, C., « How Companies Learn Your Secrets », *The New York Times*, 16 fevrier 2012, en ligne : < https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>

FINEXTRA, « CaixaBank to roll out facial recognition ATMs across Spain », *Finextra*, 10 juin 2020, en ligne : <https://www.finextra.com/newsarticle/35976/caixabank-to-roll-out-facial-recongition-atms-across-spain?utm_medium=newsflash&utm_source=2020-6-10&member=120460>

FORTTRELL, Q., « Silicon Valley's final frontier for payments : 'The neoliberal takeover of the human body' », *Marketwatch*, 23 octobre 2019, en ligne : <https://www.marketwatch.com/story/the-technology-that-should-finally-make-your-wallet-obsolete-2019-09-06>

HAO, K., « The two year fight to stop Amazon from selling face recognition to the police », *MIT Technology Review*, 12 juin 2020, en ligne : <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/?truid=85d02b5a0a9c094e8d8229838e9b5953&utm_source=the_algorithm&utm_medium=email&utm_campaign=the_algorithm.unpaid.engagement&utm_content=06-12-2020>

HARESTY, L., « Study finds gender and skin-type bias in commercial artificial-intelligence systems », *MIT News*, 11 février 2018, en ligne : <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>

INFOPRESSE, « COVID-19 : l'opportunité du commerce électronique », *Infopresse*, 2 avril 2020, en ligne : <https://www.infopresse.com/article/2020/4/2/covid-19-l-opportunite-du-commerce-electronique>

KOCH, R., « Cookies, the GDPR, and the ePrivacy Directive », *GDPR.EU*, en ligne : <https://gdpr.eu/cookies/>

LATOUR, C., « Le marketing direct (le marketing relationnel)… ce qu'il faut savoir », *HRI Mag*, 18 février 2018, en ligne : <https://www.hrimag.com/Le-marketing-direct-marketing-relationnel-ce-qu-il-faut-savoir>

LEBOEUF, S-H., « « Je ne peux pas respirer », a répété George Floyd une vingtaine de fois », *Radio-Canada*, 9 juillet 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1718312/je-ne-peux-pas-respirer-george-floyd-transcription-cameras-intervention-cour>

LECOCQ S., « L'UE veut une intelligence artificielle "responsable" et maîtrisée par l'humain », *AFP*, 18 février 2020, en ligne : <https://apple.news/ABwuPukb0RA-MMwvuiNNxMA>

MALBOEUF, M-C., « Bell veut nous faire suivre en continu », *LaPresse+*, en ligne : <https://plus.lapresse.ca/screens/d2892670-94f2-4adf-b8f6-ebbd0d428f7d__7C___0.html>

PÉLOQUIN, T., « Reconnaissance faciale : la SQ pourrait acquérir une technologie controversée », *LaPresse*, 22 juin 2020, en ligne : <https://www.lapresse.ca/actualites/justice-et-faits-divers/2020-06-22/reconnaissance-faciale-la-sq-pourrait-acquerir-une-technologie-controversee>

PELOQUIN, T., « Reconnaissance faciale : « Un risque grave de surveillance de masse » », *LaPresse*, 29 juin 2020, en ligne : <https://www.lapresse.ca/actualites/2020-06-29/reconnaissance-faciale-un-risque-grave-de-surveillance-de-masse.php>

PHILIPS, S., « A brief history of facebook », *The Guardian*, 25 juillet 2007, en ligne : <https://www.theguardian.com/technology/2007/jul/25/media.newmedia>

PIQUARD, A., « La crise du coronavirus va-t-elle améliorer l'image des GAFA ? », *Le Monde*, 10 avril 2020, en ligne : <https://www.lemonde.fr/economie/article/2020/04/10/coronavirus-une-guerre-de-l-image-pour-les-geants-du-numerique_6036161_3234.html>

PREZIOSO, J., « IBM ne vendra plus d'outils de reconnaissance faciale », *AFP*, 9 juin 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1710439/ibm-reconnaissance-faciale-discrimination-racisme-justice>

RONFAUT, L., « La technologie de reconnaissance faciale est-elle raciste », *Figaro Tech & Web*, 2 juillet 2015, en ligne : <https://www.lefigaro.fr/secteur/high-tech/2015/07/02/32001-20150702ARTFIG00144-la-technologie-de-reconnaissance-faciale-est-elle-raciste.php>

ROSENBERG, M., CONFESSORE, M., et C., CADWALLADR, « How Trump Consultants Exploited The Facebook Data of Millions », *The New York Times*, 17 mars 2018, en ligne : <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

SELFIN, M., « Is the Rest of the World Ready for Facial Pay ? », *Payments Journal*, 10 mars 2020, en ligne : <https://www.paymentsjournal.com/is-the-rest-of-the-world-ready-for-facial-pay/>

ST-JACQUES, G., et *al.*, « Noter les citoyens en Chine pour mieux les contrôler », Radio-Canada Info, 9 avril 2018, en ligne : <https://ici.radio-canada.ca/premiere/emissions/medium-large/segments/entrevue/66923/chine-note-sociale-donnees-numeriques-gouvernement-chinois>

TELECOMPAPER, « JiWire licenses Wi-Fi positioning system from Skyhook », 31 mai 2007, en ligne : <http://www.telecompaper.com/news/jiwire-licenses-wifi-positioning-system-from-skyhook>

TRUDEL, P., « Cadrer la reconnaissance faciale », *Le Devoir*, 3 mars 2020, en ligne : <https://www.ledevoir.com/opinion/chroniques/574078/cadrer-la-reconnaissance-faciale>

UNTERSINGER, M., « Données personnelles : un nouveau règlement européen contraignant », *Le Monde*, 24 janvier 2018, en ligne : <https://www.lemonde.fr/pixels/article/2018/01/24/un-nouveau-reglement-contraignant_5246333_4408996.html>

WINDER, D., « Google Chrome Privacy Lawsuit: Could You get a 5000$ payout », *Forbes*, 3 juin 2020, en ligne : < https://www.forbes.com/sites/daveywinder/2020/06/03/google-

chrome-privacy-lawsuit-could-you-get-a-5000-payout-incognito-mode-class-action/#632774221485>

Rapport d'organismes et sources internet

ADOBE, *Use of cookies dans similar technologies*, 2019, en ligne : <https://www.adobe.com/ca_fr/privacy/cookies.html>

AUTORITÉ CANADIENNE POUR LES ENREGISTREMENTS INTERNET, *Attitudes des canadiens sur les enjeux relatifs à internet*, Ottawa, 2020, en ligne : <https://www.cira.ca/fr/resources/letat-de-linternet/rapport/attitudes-des-canadiens-sur-les-enjeux-relatifs-a-linternet>

AUTORITÉ CANADIENNE POUR LES ENREGISTREMENTS INTERNET, *Les canadiens méritent un meilleur internet*, Ottawa, 2019, p. 6, en ligne : <https://www.cira.ca/fr/resources/letat-de-linternet/rapport/les-canadiens-meritent-un-meilleur-internet>

BUREAU DE LA CONCURRENCE, *L'Intervention du Bureau de la concurrence : Avis de consultation télécom CRTC 2016-192*, 29 juin 2016, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04108.html>

BUREAU DE LA CONCURRENCE, *Mémoire au comité d'examen de la Loi sur les transports au Canada*, 27 février 2015, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04040.html>

BUREAU DE LA CONCURRENCE, *Mémoire présenté au Groupe d'étude sur les politiques en matière de concurrence*, 11 janvier 2008, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/02555.html>

BUREAU DE LA CONCURRENCE, *Table ronde sur le monopole et le pouvoir de l'acheteur*, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/02995.html>

CENTRE FACILITANT LA RECHERCHE ET L'INNOVATION DANS LES ORGANISATIONS, *L'usage des médias sociaux au Québec*, NETendance 2018, vol. 9, no. 5, Québec, en ligne : <https://cefrio.qc.ca/media/2023/netendances-2018_medias-sociaux.pdf>

CHUNG, R., « How much data is generated each day », *World Economic Forum*, 17 avril 2019, en ligne : < https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>

CNIL, *Biométrie*, en ligne : <https://www.cnil.fr/fr/biometrie>

CNIL, *Ciblage publicitaire en ligne : quel plan d'action de la CNIL ?*, 28 juin 2019 : <https://www.cnil.fr/fr/ciblage-publicitaire-en-ligne-quel-plan-daction-de-la-cnil>

CNIL, *Comment permettre à l'homme de garder la main ?*, Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, 2017, en ligne : <https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de>

CNIL, *Marketing ciblé sur internet : vos données ont de la valeur*, 26 mars 2009, en ligne : <https://www.cnil.fr/fr/marketing-cible-sur-internet-vos-donnees-ont-de-la-valeur>

CNIL, *L'anonymisation de données personnelles*, 19 mai 2020, en ligne : <https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles>

CNIL, *La CNIL et la DGCCRF font évoluer leur protocole de coopération pour renforcer la protection des consommateurs et de leurs données personnelles*, 31 janvier 2019, en ligne : <https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des>

CNIL, *La publicité ciblée en ligne*, communication présentée en séance plénière le 5 févr. 2009, rapporté par M. Peyrat, en ligne, 33 p. (11 octobre 2019)

CNIL, *Reconnaissance Faciale : pour un débat à la hauteur des enjeux*, 2019, 11 p., en ligne: <https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf>

COMMISARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consentement et protection de la vie privée.* Document de discussion sur les améliorations possibles au consentement sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, 2016, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/consent_201605/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée*, Ottawa, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La publicité comportementale en ligne : un survol*, Ottawa, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/02_05_d_52_ba_02/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les témoins et le suivi sur le web*, Ottawa, 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/temoins/02_05_d_49/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne*, Ottawa, 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/gl_ba_1112/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Position de principe sur la publicité comportementale en ligne*, Ottawa, 2015, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions d'enquête en vertu de la LPRPDE n #2017-002 : Wajam Internet Technologies Inc., développeur de publiciel canadien, enfreint de nombreuses dispositions de la LPRPDE (Loi sur la protection des renseignements personnels et les documents électroniques)*, Ottawa, 17 août 2017, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2017/lprpde-2017-002/>

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,* Ottawa, 2011, 61 p., en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/report_201105/>

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, Québec, 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FI_profilage.pdf>

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, Technologies et vie privée à l'heure des choix de société, Rapport quinquennal, Québec, 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf>

COMMISSION DE CONTRÔLE DES INFORMATIONS NORMATIVES, *Fiches pratiques : anonymisation ou pseudonymisation*, en ligne : <https://www.ccin.mc/fr/fiches-pratiques/anonymisation-ou-pseudonymisation>

COMMISSION DES CLAUSES ABUSIVES, *Recommandation N°14-02 : Contrats de fourniture de services de réseaux sociaux,* 07 novembre 2014, en ligne : < http://www.clauses-abusives.fr/recommandation/contrats-de-fourniture-de-services-de-reseaux-sociaux-nouveau/>

COMMISSION EUROPÉENNE, *Renforcer la confiance dans l'intelligence artificielle axé sur le facteur humain*, COM (2019) 168, Bruxelles, 8 avril 2019, 12 p.

COMMISSION EUROPÉENNE, *Livre blanc sur l'intelligence artificielle*, COM (2020) 65, Bruxelles, 19 février 2020, 31 p.

CONSEIL DE LA RADIODIFFUSION ET DES TÉLÉCOMMUNICATIONS CANADIENNE, *La Loi canadienne anti-pourriels*, 2020, en ligne : <https://crtc.gc.ca/fra/internet/anti.htm>

CONSEIL DE L'EUROPE, *La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, Recommandation CM/Rec(2010)13 et exposé des motifs, Strasbourg, Éditions du Conseil de l'Europe, 2011, p. 9, en ligne : <https://rm.coe.int/16807096c4>

CONTRACT FOR THE WEB, *Building the contract for the web*, en ligne : <https://contractfortheweb.org/process/>

CONTRACT FOR THE WEB, *Join us and figth #ForTheWeb*, 5 novembre 2018, en ligne : <https://contractfortheweb.org/2018/11/05/join-us-and-fight-fortheweb/>

CONTRACT FOR THE WEB, *It took all of us to build the web that we have. It will take all of us to secure its future*, en ligne **:** <https://contractfortheweb.org/about/>

FACEBOOK, *Cookies et autres technologies de stockage*, 2018, en ligne : <https://www.facebook.com/policies/cookies/>

GOUVERNEMENT DU CANADA, *La Loi canadienne anti-pourriel*, 2020, en ligne : <https://www.fightspam.gc.ca/eic/site/030.nsf/fra/accueil>

GOUVERNEMENT DU CANADA, *Notes pour une allocution de Matthew Boswell, sous-commissaire principal de la concurrence*, Ottawa, 2014, en ligne : <https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03856.html>

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Document de travail sur la biométrie », Commission européenne, adopté le 1er août 2003

LEQUESNE ROTH, C., (dir.), *La reconnaissance faciale dans l'espace public : une cartographie juridique européenne*, Fablex DL4T, Université Côte d'Azur, Nice, 130 p.

MINSTÈRE DE L'ÉCONOMIE ET DE L'INNOVATION, *Le neuromarketing : une tendance marketing à votre portée*, Québec, 2019, en ligne : < https://www.economie.gouv.qc.ca/bibliotheques/outils/gestion-dune-entreprise/gestion-du-marketing/le-neuromarketing-une-tendance-du-marketing-a-votre-portee/>

OCDE, *Compte rendu de la table ronde sur la discrimination par les prix*, 126e réunion du Comité de la concurrence, 29 et 30 novembre 2016, p.5, en ligne : <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M(2016)2/ANN3/FINAL&docLanguage=Fr>

OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, Paris, 2019

OCDE, *Protection de la vie privée en ligne : orientation politiques et pratiques de l'OCDE*, 2003

OMPI, *Secrets d'affaires*, en ligne : <https://www.wipo.int/tradesecrets/fr/>

OPTION CONSOMMATEUR, *Le prix de la gratuité : doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne*, Montréal, 2015, en ligne : <https://option-consommateurs.org/wp-content/uploads/2017/06/option-consommateurs-2014-2015-gratuite-rapport.pdf>

OPTION CONSOMMATEURS, *Les nouveaux services offerts par les agences de crédit : utilisation légitime des renseignements personnels?*, Rapport de recherche présenté au Commissariat à la protection de la vie privée, avril 2014

PLACE STE-FOY, *La fonderie de l'innovation dans le commerce de détail (FICD),* en ligne : <https://www.placestefoy.com/fr/la-fonderie-de-linnovation-dans-le-commerce-de-detail-ficd/#:~:text=LE%20PROJET%20PILOTE%20%C3%80%20PLACE%20STE%2DFOY%20UTILISAIT%2DIL%20DE,reconna%C3%AEtre%20l'identit%C3%A9%20des%20consommateurs.>

POSTERSCOPE WORLDWINE, *Interactive Facial Recognition Digital OOH Billboard Campaign for GM*, Santa Monica, [video] en ligne : <https://www.youtube.com/watch?v=Kj7Dm_i-OoM>

REID, H., *Dictionnaire de droit québécois et canadien*, 5e éd. révisée, Montréal, Wilson & Lafleur, 2016, « profilage racial », en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=profilage&t=edictionnaire&sort=relevancy&m=search>

REDPOINT, *Adressing the Gaps in Customer Experience,* The Harris Poll, Massachussetts, États-Unis, 2019

SAQ, *Profitez d'une expérience plus personnalisée*, en ligne : <https://www.saq.com/fr/saqinspire>

STARBUCKS, *Conditions de l'application : communications par courriel, notifications poussées et messages in-app*, 2019

STRAVA, *Suivez et analysez chaque aspect de votre activité*, en ligne : <https://www.strava.com/features?hl=fr-FR#:~:text=Strava%20est%20le%20r%C3%A9seau%20social,chacun%2C%20et%20laisser%20des%20commentaires.>

UBER, *Utilisation des informations de localisation des passagers par Uber (IOS)*, en ligne : <https://help.uber.com/fr-FR/riders/article/utilisation-des-informations-de-localisation-des-passagers-par-uber%C2%A0ios?nodeId=741744cb-125c-4efc-ab3f-4a977940ac87>

VIARD, R., *Les chiffres de Facebook*, Webmarketing Conseil, 2020, en ligne : <https://www.webmarketing-conseil.fr/chiffres-de-facebook/>

Mémoires et thèses

ADOWAA BUOLAMWINI, J., *Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*, mémoire de maîtrise, Faculté des Médias, Sciences et Arts, Massachusetts Institute of Technology, 2017

GAUTHIER, J., *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée*, mémoire de maîtrise, Faculté de droit, Université de Montréal, 2015

KABLAN, S., *Pour une évolution du droit des contrats : le contrat électronique et les agents électroniques*, thèse de doctorat, Faculté de droit, Université Laval, 2008

Annexe I

Représentation de la capacité de mémoire du système international d'unité

1 **kilooctet** (ko)	= 10^3 octets		= 1 000 octets
1 **mégaoctet** (Mo)	= 10^6 octets	= 1 000 ko	= 1 000 000 octets
1 **gigaoctet** (Go)	= 10^9 octets	= 1 000 Mo	= 1 000 000 000 octets
1 **téraoctet** (To)	= 10^{12} octets	= 1 000 Go	= 1 000 000 000 000 octets
1 **pétaoctet** (Po)	= 10^{15} octets	= 1 000 To	= 1 000 000 000 000 000 octets
1 **exaoctet** (Eo)	= 10^{18} octets	= 1 000 Po	= 1 000 000 000 000 000 000 octets
1 **zettaoctet** (Zo)	= 10^{21} octets	= 1 000 Eo	= 1 000 000 000 000 000 000 000 octets
1 **yottaoctet** (Yo)	= 10^{24} octets	= 1 000 Zo	= 1 000 000 000 000 000 000 000 000 octets