Université de Montréal

Les enjeux juridiques concernant les nouveaux modèles d'affaires basés sur la commercialisation des données

par Michael Chevalier

Université de Montréal, Faculté de droit

Mémoire présenté en vue de l'obtention du grade de LL.M.

en droit des technologies de l'information

31 décembre 2015

RÉSUMÉ / ABSTRACT
[The English abstract follows the French]

Cet essai est présenté en tant que mémoire de maîtrise dans le cadre du programme de droit des technologies de l'information. Ce mémoire traite de différents modèles d'affaires qui ont pour caractéristique commune de commercialiser les données dans le contexte des technologies de l'information. Les pratiques commerciales observées sont peu connues et l'un des objectifs est d'informer le lecteur quant au fonctionnement de ces pratiques. Dans le but de bien situer les enjeux, cet essai discutera d'abord des concepts théoriques de vie privée et de protection des renseignements personnels. Une fois ce survol tracé, les pratiques de « *data brokerage* », de « *cloud computing* » et des solutions « *analytics* » seront décortiquées. Au cours de cette description, les enjeux juridiques soulevés par chaque aspect de la pratique en question seront étudiés. Enfin, le dernier chapitre de cet essai sera réservé à deux enjeux, soit le rôle du consentement et la sécurité des données, qui ne relèvent pas d'une pratique commerciale spécifique, mais qui sont avant tout des conséquences directes de l'évolution des technologies de l'information.

Mot-clés : ***«Renseignements Personnels», «Vie Privée», «Commercialisation», «Information», «Analytics», «Big Data», «Data Brokerage», «Infonuagique», «Consentement», «Sécurité»***

This essay is submitted as part of a master's thesis in Information Technology Law. This thesis discusses different business models that have the common feature of commercializing data in the context of Information Technologies. One of the goals of this thesis is to inform the reader about the workings of the studied business practices, as they are not widely known. First, in order to situate the issues, this essay will consider the theoretical concepts of Privacy and Personal Information Protection. Once the review of Data Protection and Privacy has been established, this thesis will further explore Data Brokerage, Cloud Computing and Analytic Solutions as practices. Over the course of this description, the legal issues raised by each aspect of the aforementioned practices will be studied. Finally, the last chapter of the thesis will be dedicated to two issues that are not limited to the scope of a specific business practice, but are direct consequences of the evolution of Information Technologies: the role of Consent and Data Security.

Key words: "*Personal Information", "Privacy", "Commercialization", "Information", "Analytics", "Big Data", "Data Brokerage", "Cloud Computing", "Consent", "Security"*

Table des matières

Les enjeux juridiques concernant les nouveaux modèles d'affaires basés sur la commercialisation des données

Introduction

Peu de temps suffit lors de la navigation web, pour constater la présence d'une multitude d'entreprises en ligne. Alors que certaines entreprises se contentent d'une simple présence passive sur la toile, d'autres opèrent activement et génèrent des revenus à partir des interactions qu'elles entretiennent avec leur clientèle, dans le cyberespace.

En effet, la plupart des entreprises présentes en ligne n'y sont que pour la présentation ou référence, quasi obligatoire en cette aire technologique. Cet affichage de leur entreprise vise le public et pour utilité de jouer le rôle d'un bottin pages jaunes numérique. À l'inverse, un petit nombre d'entreprises se manifestent par leur activité soutenue et leurs offres de biens et services au consommateur. Alors qu'une portion de ces entreprises a une notoriété bien acquise et une visibilité dépassant une petite niche d'internautes, l'autre portion est moins visible et moins connue du public. Le point commun entre ces divers archétypes est la commercialisation de données.

La commercialisation des données est le dénominateur commun de ces différents modèles d'affaires et suppose qu'il peut y avoir une valeur ajoutée à la donnée collectée. Comme l'explique le site du gouvernement américain: « *Data become "information" when analyzed and possibly combined with other data in order to extract meaning and to provide context* »[1]. Ainsi, la transformation de donnée en information s'effectue lorsqu'elle est analysée dans le but d'obtenir une certaine signification et un contexte. Il y aurait donc une distinction à faire entre l'information qui n'est pas traitée et celle qui l'est.

Cette distinction est significative et engendrera un éventail d'enjeux différent conséquemment à la qualification de donnée ou d'information. Les implications relatives à la qualification se manifesteront notamment sur le plan des risques associés à la pratique commerciale, mais aussi, parfois, dans le domaine des enjeux légaux concernant la collecte,

[1] DATA.GOV, « Glossary of Terms », en ligne : <http://www.data.gov/glossary> (page consultée le 25 novembre 2015).

manipulation et divulgation d'informations personnelles. À cet effet, l'auteur Shubha GHOSH souligne que la distinction entre les données « *raw* » et celles traitées peut être un élément essentiel quant à l'étendue des droits légaux portant sur la protection des données[2]. D'ailleurs, nous observerons que la qualification ainsi que les effets qui en découlent varient selon la tradition juridique observée.

Au cœur de chacune des pratiques qui sera sous étude résidera cette idée de commercialisation de l'information. Pour bien illustrer cela, on peut concevoir l'information comme un bien marchand. Ce bien marchand suppose production d'information par une source ou un sujet, une consommation par les destinataires de l'information brute raffinée, mais évoque aussi un aspect propriétaire de l'information et les droits mercantiles ou de protection des données personnelles s'y rattachant[3].

Comme toute marchandise, la commercialisation des données évolue au sein d'un marché. Ce marché globalisé ne se limite pas aux frontières nationales puisqu'il est intrinsèquement lié au cyberespace. De par sa nature, la commercialisation des données est constamment confrontée à une multitude d'ordres juridiques.

On constate notamment une mutation des rationalités de l'encadrement de ce marché. N'en déplaise à plusieurs, la protection des données personnelles, et incidemment la commercialisation des données, semblent avoir passé d'une rationalité conçue autour des droits fondamentaux à une rationalité économique basée sur l'évaluation du risque[4]. Ce changement progressif coïncide notamment avec l'apparition de modèles d'affaires, que nous étudierons, reposant sur la mise en marché de l'information. Ainsi, l'information joue un rôle plus actif dans la création de plus-value pour les entreprises. Comme nous l'observerons, les données sont un type d'actif de plus en plus prisé par les entreprises qui orientent leurs stratégies commerciales en fonction de l'information et de l'utilisation qu'on compte en faire.

Ce marché orbite donc autour de la donnée, mais aussi de la donnée pouvant contenir un renseignement personnel. Certes, il est possible d'attribuer un prix à une information, mais

[2] Shubha GHOSH, « Commercializing Data », (2011-2012) 3 *Elon L. Rev*. 195, à la page 197.
[3] *Id.*, aux pages 201 et 202.
[4] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, « The Value of Personal Information – Evidence from Empirical Economic Studies », (2012) 88-4 *Digiworld Economic Journal* 41, à la page 43.

il semble particulièrement difficile d'en énoncer la valeur puisque celle-ci dépend notamment de sa nature, mais aussi de son contexte[5]. En effet, les auteurs ne s'entendent pas sur la façon dont on devrait calculer cette valeur[6]. Pour illustrer, les individus estiment la valeur d'une information de géolocalisation plus élevée qu'une information de base permettant leur identification [7] . Cette instabilité de valeur de l'information est due à la nature fondamentalement contextuelle de l'information.

En effet, la valeur qu'on attribuera à une information variera en fonction du contexte économique, social ou politique dans lequel on se trouve. En ce sens, il semblerait exister un écart de valeur selon le type d'information récolté. Par conséquent, la catégorisation des différents genres d'information permettrait de mettre l'emphase sur la différence de valeur entre les catégories d'information et leur apparence objective d'intrusivité dans la vie privée des individus. À titre d'exemple, on peut considérer qu'une donnée concernant l'état de santé ait plus de valeur qu'une donnée concernant le nom et prénom du même individu, puisqu'elle moins sujette à être divulguée et partagée. À l'inverse, la valeur attribuable à une information peut également être subjective en ce que chaque personne n'a pas la même évaluation de ce qui compose cette sphère intime de la vie privée. Ainsi, une personne atteint d'une maladie, mais qui cherche à sensibiliser la population sur les difficultés associées à sa condition, peut évaluer autrement le degré d'intimité ou de confidentialité que l'on devrait attribuer à cet état de santé.

Ainsi, l'élément central du marché de l'information et de la protection des renseignements personnels est, d'une certaine façon, volatil puisqu'il varie autant en fonction du contexte objectif, que de l'individu concerné. Malgré cette intangibilité, on ne peut réfuter que l'information est le moteur économique de notre ère numérique. Certains auteurs décrivent l'importance actuelle des données comme étant l'actif principal des marchés modernes et que l'information peut être considérée comme étant « *the new oil of the internet*

---

[5] Jeevan JAISINGH et al., « Privacy and Pricing Personal Information », (2008) 187-3 *European Journal of Operational Research* 857, à la page 868.
[6] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, aux pages 47 à 53. ; Voir pour exemple d'évaluation de la valeur d'un renseignement personnel : Claudio FEIJOO, José Luis GOMEZ-BARROSO et Peter VOIGT, « Exploring the Economic Value of Personal Information from Financial Statements », (2014) 34 *International Journal of Information Management* 248.
[7] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, à la page 52.

and the new currency of the digital world »[8]. Parmi ces nouvelles machines carburant à l'information, on peut identifier les géants des médias sociaux qui exercent une influence profonde sur notre société[9]. Ces entreprises sont l'illustration par excellence d'un modèle d'affaires efficace centré sur la commercialisation de renseignements pouvant être personnels.

Par souci de précision, un modèle d'affaire « *is a statement of how a firm will make money and sustain its profit stream over time* »[10]. Ce plan d'affaire déterminant les sources de revenu doit être réfléchi et adapté au contexte, sans quoi l'entreprise diminue ses chances de réussite économique[11]. D'ailleurs, TEECE explique que les modèles d'affaires doivent être évolutifs et s'adapter aux changements des marchés et des cadres réglementaires et légaux entourant la pratique[12]. Un exemple intéressant de cette nécessité d'adaptation est illustré par Eric CLEMONS, qui explique comment l'Internet est un nouveau média beaucoup plus libre et puissant que les médias traditionnels et que, par conséquent, il n'est pas avisé de se limiter aux modèles d'affaires traditionnels tels ceux reposant sur la publicité[13]. Cet essai a notamment pour objectif de décrire le contexte juridique économique dans lequel évoluent les nouveaux modèles d'affaires.

Ainsi, avant d'aborder les différents modèles d'affaires établis et les enjeux qu'ils impliquent, nous étudierons le cadre théorique de la vie privée de la protection des données. En effet, la protection des données, en tant que concept juridique, fait l'objet d'approches variant en fonction des effets recherchés par l'adoption de normes juridiques. À cet égard, il sera également intéressant d'étudier la relation entre la protection des données personnelles et la protection de la vie privée.

---

[8] Claudio FEIJOO, José Luis GOMEZ-BARROSO et Peter VOIGT, « Exploring the Economic Value of Personal Information from Financial Statements », (2014) 34 *International Journal of Information Management* 248, à la page 248, citant M. KUNEVA, *Keynote speech at the Roundtable on Online Data Collection, Targeting and Profiling*, Reference: SPEECH/09/156, Bruxelles, 2009.

[9] George F., HURLBURT, « Web 2.0 Social Media: A Commercialization Conundrum », (2012) 14-6 *ITPro* 6, à la page 6.

[10] David W. STEWART, et Qin ZHAO, « Internet Marketing, Business Models, and Public Policy », (2000) 19-2 *Journal of Public Policy & Marketing* 287, à la page 290.

[11] David J. TEECE, « Business Models, Business Strategy and Innovation », (2010) 43 *Long Range Planning* 172, à la page 174.

[12] *Id*., à la page 177.

[13] Eric K., CLEMONS, « Business Models for Monetizing Internet Applications and Web Sites : Experience, Theory, and Predictions », (2009) 26-2 *Journal of Management Information Systems* 15.

Enfin, après avoir tracé ce cadre conceptuel, il sera possible d'identifier les différents enjeux pouvant se manifester et comment ils peuvent être abordés. Ces enjeux découleront tous de la manipulation de l'information, soit la collecte, le traitement, la conservation ou la communication.

Principalement, cette étude a pour objet de décrire, sous un angle légal, les nouvelles pratiques d'affaires basées sur la commercialisation de l'information. Pour se faire, il faut d'abord identifier les différents modèles d'affaires, pour ensuite pouvoir analyser les interactions qu'ils entretiennent avec l'information. Enfin, nous utiliserons certains cadres conceptuels pour observer comment peuvent se manifester les différents problèmes, risques et enjeux lors de la collecte, l'utilisation et la conservation de l'information.

1- Protection des données et vie privée

L'éventail des pratiques commerciales que nous aborderons dans cet essai nécessite d'être observé sous plusieurs approches afin de pouvoir pleinement appréhender les enjeux que ces pratiques soulèvent. L'un des facteurs ayant un impact significatif sur les modèles d'affaires basés sur la commercialisation de l'information est celui du régime de protection des données utilisé par une juridiction.

Ainsi, nous observerons que les différentes conceptions de la protection des données permettent de délimiter le cadre dans lequel évoluent les nouveaux modèles d'affaires commercialisant l'information. D'abord, puisqu'ils sont intimement liés, nous comparerons les concepts de vie privée et de protection des données. Cette comparaison nous permettra de mettre en valeur l'évolution historique suivant l'avancement des technologies, mais aussi de représenter deux grandes cultures juridiques pouvant parfois soutenir des discours fort différents en ce qui concerne la protection des données personnelles.

Nous observerons ensuite les différentes approches pour conceptualiser la protection de la vie privée et des renseignements personnels. Nous commencerons par observer l'approche la plus large et englobante qui vise à considérer ces concepts comme étant des droits fondamentaux. Ensuite nous verrons comment il est possible de transposer les concepts de vie privée et de protection des renseignements personnels en l'attribution de droits subjectifs. Enfin, nous verrons que la vie privée et la protection des données sont des intérêts protégés nécessitant une intervention du droit.

Cette description des différentes approches à la protection des données personnelles nous permettra d'avoir un aperçu général et conceptuel de la réglementation entourant la collecte, le traitement et la divulgation des données personnelles. Grâce à cet aperçu théorique et la description des pratiques commerciales, nous serons en mesure de relever les nouveaux enjeux associés à la commercialisation des données personnelles.

1.1- Distinction entre le concept de vie privée et la protection des données

Conceptualisation de la vie privée

Pour commencer, il est impératif de dresser les contours du concept de vie privée, ou de *privacy* auquel nous référons. Cette distinction conceptuelle est importante pour interpréter les pratiques de commercialisation de l'information, car ces dernières reposent sur la collectent, l'utilisation et la conservation d'informations, qui parfois seront qualifiées de renseignements personnels. Bien souvent, les renseignements personnels sont perçus comme étant une composante de la vie privée. Or, comme nous le verrons, la protection des renseignements personnels n'est pas nécessairement un enjeu de vie privée. Enfin, à des fins de qualification, nous partirons du présupposé que faute de pouvoir se qualifier en tant que principe ou institution du droit, la « *privacy* » est un concept, une construction de l'homme, pour représenter une idée abstraite en droit[14].

Cette notion juridique ne comporte pas de définition exhaustive délimitant sa portée et son étendu. D'ailleurs, plusieurs auteurs s'entendent pour dire qu'il s'agit d'un concept flou et difficile à circonscrire[15]. C'est donc en raison de sa nature que la vie privée a été conceptualisée de plusieurs façons à travers le temps et les juridictions.

En ce qui concerne le droit américain, on situe l'avènement de l'idée de la « *privacy* », à la publication d'un article par Samuel WARREN et Louis BRANDEIS intitulé « *The Right to Privacy* »[16]. Selon cette première conception de la vie privée, la « *privacy* » était envisagée comme un concept principalement spatial, créant ainsi une dichotomie fondée sur la

---

[14] Jean-Louis HALPÉRIN, « L'essor de la "privacy" et l'usage des concepts juridiques », (2005) 61-3 *Droit et Société* 765, à la page 775.

[15] Abdelmadjid ABDELKAMEL, *Facebook et les dispositifs de traçabilité vus sous l'angle du droit canadien*, mémoire de maîtrise en droit des technologies de l'information, Montréal, Université de Montréal, 2013, à la page 90, citant James Q. WHITMAN, « The Two Western Cultures of Privacy: Dignity Versus Liberty », (2004) 113-6 *The Yale Law Journal*, p. 1153, en ligne: <http://www.yalelawjournal.org/the-yale-law-journal/article/the-twowestern- cultures-of-privacy:-dignity-versus-liberty/> (page consultée le 15 janvier 2013); Jean-Louis HALPÉRIN, préc. note 14; François RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Paris, Librairie Générale de Droit et de Jurisprudence,1990; Daniel J. SOLOVE, « A Taxonomy of Privacy », (2005-2006), 154 *U. Pa. L. Rev*. 477.

[16] Samuel D. WARREN et Louis D. BRANDEIS, « The Right to Privacy », (1890) 4-5 *Harvard Law Review*193, pp.193-220, en ligne : <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf> (page consultée le 10 novembre 2015).

distinction entre l'espace public et privé[17]. On réfère à cette notion comme étant « *The right to be let alone* ». Les auteurs constatent d'ailleurs que face aux nouvelles technologies permettant de prendre en photo les individus, il était nécessaire de protéger par le droit un espace physique, intime et impénétrable pour permettre l'échange et la manifestation des convictions et réflexions intimes de chacun[18].

Dans le même ordre d'idées, certains ont conceptualisé la vie privée en fonction de l'accessibilité. Plus précisément, on le représentait comme étant une protection du secret, de l'anonymat et de la solitude[19]. Ainsi, cette conception est un peu plus large que le « *right to be let alone* », car elle ne se confine pas aux limites spatiales pour définir une protection de certains éléments intimes de la vie d'un individu. Comme l'expliquent les auteurs ROUVROY et POULLET :

> «*They* [individuals] *need some secrecy, anonymity and solitude, withdrawal and concealment in order to reflect on their own preferences and attitudes, or, in other words, to reflexivly make revise choices in life, as well as to develop meaningful relationships with others* »[20].

Autrement dit, la « *privacy* » couvre certains aspects irréductibles et nécessaires au développement authentique des individus dans une société. D'autres auteurs vont pour leur part, aborder la vie privée comme étant un moyen de contrôler ces informations intimes qui nous concernent[21].

Sur un plan plus fondamental, certains auteurs reconnaitront la « *privacy* » comme servant à la protection de l'individualité et de la dignité humaine[22]. Cette conception englobe la protection des choix qui définissent la personne (mariage, orientation sexuelle, procréation, relations familiales)[23].

---

[17] Jean-Louis HALPÉRIN, préc. note 14, à la page 776.
[18] Antoinette ROUVROY et Yves POULLET, « The Right to Informational Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy », dans *Reinventing Data Protection*, Springer, 2009, à la page 62.
[19] Yana WELINDER, « A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks », (2012-2013) 26 *Harv. J. L. & Tech.* 165, à la page 181.
[20] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 63.
[21] Yana WELINDER, préc. note 19, à la page 181.; Charles FRIED, « Privacy »,(1968) 77 *Yale L. J.* 475, à la page 482; Scott REMPELL, « Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas », (2006) 18 *Fla. J. Int'l L.* 807, à la page 812.
[22] Yana WELINDER, préc. note 19, à la page 182.
[23] *Id.*; Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 64.

Deux cultures manifestes

Patrick O'CALLAGHAN regroupe ces différentes conceptions de la vie privée sous deux écoles de pensée, l'école réductionniste et l'école percevant la vie privée comme étant un droit conceptuellement distinct et entier[24].

La première réfère à la recherche des éléments se situant au noyau du concept, les fondations de la vie privée. Selon les auteurs adoptant cette approche, la vie privée serait un regroupement désordonné de droits qui rencontrerait d'autres regroupements de droits[25]. Cette affirmation suggère que la vie privée ne serait pas un droit en soi, mais plutôt un rassemblement d'intérêts protégés par le droit. À cet effet, O'CALLAGHAN explique que selon l'approche réductionniste suggérée par THOMSON : « *the vague and indeterminate right of privacy need not to enter the legal lexicon because privacy interests, in cases where they represent truly fundamental interests, are accorded sufficient protection by other clusters of rights* »[26]. Ainsi, on peut voir le concept de vie privée comme étant un ensemble d'intérêts protégés par le droit.

La deuxième école de pensée, pour sa part, circonscrit la vie privée comme étant un droit entier et distinct. Par opposition aux réductionnistes, les académiques adhérant à cette conception observent qu'une réduction conceptuelle aux éléments centraux de la vie privée élimine par le fait même des éléments d'ordre moral[27]. Cette conception se baserait sur l'inviolabilité de la personnalité des individus et supposerait l'indépendance, la dignité et l'intégrité de la personnalité comme fondement[28]. Dans le même sens, HALPÉRIN argumente que la vie privée est un rempart édifié par le droit protecteur des aspirations contemporaines d'autonomie et d'individualité du citoyen contre les ingérences publiques[29]. Ainsi, la vie privée peut être considérée comme une liberté fondamentale.

---

[24] Patrick O'CALLAGHAN, *Refining Privacy in Tort Law*, Springer, 2013, à la page 8.
[25] *Id.*, à la page 9.
[26] *Id.*, citant J.J. THOMSON, «The Right to Privacy», (1975) 4-4 *Philosophy and Public Affairs* 294, pp.294-314.
[27] Patrick O'CALLAGHAN, préc. note 24, à la page 10.
[28] *Id.*, à la page 10.
[29] Jean-Louis HALPÉRIN, préc. note 14, à la page 779.; Voir aussi François RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Paris, Librairie Générale de Droit et de Jurisprudence, 1990, aux pages 167 et ss.

Enfin, comme l'explique RIGAUX : « *Le concept même de privacy est lui-même l'émanation du rapport que la culture d'une société déterminée institue entre la zone d'intimité méritant la protection et la nature des relations sociales, publiques ou privées* »[30]. On constate alors pourquoi il existe plus d'une façon d'entrevoir la portée et l'étendue de la vie privée, ces dernières étant dépendantes de l'importance culturelle attribuée aux facteurs permettant de déterminer la zone d'intimité méritant une protection.

Cette citation est d'autant plus intéressante, car elle rappelle ces deux traditions juridiques concernant la protection des données personnelles. Toutefois, nous croyons qu'il est d'abord nécessaire de distinguer la protection de la vie privée de la protection des données personnelles.

La protection des données

La protection des données personnelles est souvent définie comme étant un embranchement dans le grand concept de vie privée. Ce sous-ensemble aurait ainsi pour objectif de garantir une protection et d'attribuer une certaine capacité de contrôler les renseignements personnels nous concernant, autant dans leur collecte, leur traitement, leur conservation, que leur divulgation[31]. Par conséquent, la protection des données est souvent représentée comme étant un moyen de préserver la vie privée[32].

On peut également définir la protection des données personnelles comme étant une expression voulant englober les situations ayant regard au traitement des données personnelles[33]. Ainsi, selon cette vision, la protection des données permettrait la réconciliation d'enjeux fondamentaux, mais conflictuels, comme la vie privée, la liberté d'expression, etc.[34].

---

[30] François RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Paris, Librairie Générale de Droit et de Jurisprudence, 1990, à la page 694.
[31] Isabel VICENTE, *La convergence de la sécurité informatique et de la protection des renseignements personnels: Vers une nouvelle approche juridique*, mémoire de maîtrise en droit des technologies de l'information, Montréal, Université de Montréal, 2003, à la page 9.
[32] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, Fiche d'information, Québec, CAI, 2013 à la page 2.
[33] Serge GUTWIRTH et Paul. DE HERT, « Data Protection in the Case Law of Strasbourg and Luxemburg : Constitutionalisation in Action », dans *Reinventing Data Protection*, Springer, 2009, à la page 3.
[34] *Id.*

Les objectifs de la protection des données personnelles sont généralement la protection du citoyen contre la collecte, la conservation et la dissémination injustifiée de détails personnels[35]. Les modalités de cette protection varient en fonction de la conceptualisation et de l'importance accordée à certains principes, par les différentes juridictions. Donc, la protection des données est la formulation des conditions de légitimité du traitement de l'information, ainsi que la prohibition de traitement de certains types d'informations pouvant être considérés sensibles[36].

Plus précisément, on remarque que la protection des données, ou « *information privacy* »[37], permet un contrôle sur le moment, la finalité et l'étendue des communications contenant des informations personnelles[38]. Ces éléments essentiels des lois portant sur la protection des données personnelles se présentent généralement sous la forme de « *Fair Information Principles* » portant sur la transparence, l'exactitude, la rectification, la collection, la divulgation, l'utilisation et la sécurité des données[39].

Comme pour la protection de la vie privée, on constate des différences au sein des régimes de protection des données personnelles, basées sur les différentes traditions juridiques et culturelles. Dans un article datant de 2011, les professeurs SOLOVE et SCHWARTZ identifient deux approches émanant de ces différences culturelles : l'approche réductionniste américaine et l'approche expansionniste européenne[40]. Ils constatent que les lois américaines ont tendance à faire reposer l'ouverture des régimes de protection des données personnelles sur une définition limitative du terme « renseignement personnel »[41]. En effet, pour se qualifier comme un renseignement personnel, le renseignement doit concerner un individu identifié.

---

[35] Serge GUTWIRTH et Paul DE HERT, préc. note 33, à la page 4.
[36] *Id.*
[37] Alan WESTIN, « Privacy and Freedom », (1968) 25 *Washington and Lee Law Review* 166.
[38] Scott REMPELL, « Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas », (2006) 18 *Fla. J. Int'l L.* 807, à la page 812.
[39] *Id.*, à la page 813.; ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* Working Party on Information Security and Privacy (WPISP), 2013, en ligne : http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (page consultée le 23 décembre 2013).
[40] Paul M. SCHWARTZ et Daniel J. SOLOVE, « The PII Problem : Privacy and a New Concept of Personally Identifiable Information »,(2011) 86 *New York University Law Review* 1814, à la page 1872.
[41] *Id.*

Cette approche est d'autant plus restrictive puisqu'il n'existe pas de définition générale de données personnelles et les législations sont principalement sectorielles[42].

À l'opposé, les Européens adoptent une approche expansionniste en ce qui concerne la qualification des renseignements personnels. On peut notamment observer la directive européenne de 1995 sur la protection des données, qui inclut dans la notion de renseignement personnel, les renseignements concernant une personne identifiée ou identifiable[43]. Par conséquent, les législations européennes visent tous renseignements permettant d'identifier directement ou indirectement, en utilisant des moyens raisonnables[44].

Distinctions entre vie privée et protection des renseignements personnels

Comme le reflète ce portrait des concepts de vie privée et de protection des données personnelles, il est possible, voire commode, de réduire la protection des données personnelles à un outil de protection de la vie privée. Cette confusion peut émaner du fait que, dans la plupart des lois portant sur la protection des données personnelles, une importance considérable est apportée aux enjeux de vie privée, sans toutefois définir ce qu'on entend par « protection de la vie privée »[45]. Malgré ce manque de distinction, il n'est pas totalement erroné non plus d'admettre que la protection des données ait certains objectifs communs avec la protection de la vie privée. Certains auteurs placent cet objectif commun sur le plan de la « protection de la vie privée informationnelle »[46]. Toutefois, cet intérêt commun ne justifie pas une assimilation de ces deux concepts.

[42] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40, à la page 1872.
[43] *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.
[44] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40, à la page 1873.
[45] Lee A. BYGRAVE, « The Place of Privacy in Data Protection Law », (2001) 24-1 *University of New South Wales Law Journal* 277, 2001, à la page 278.
[46] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 67.

Les concepts de vie privée et de protection des données ne sont pas interchangeables, notamment en ce qui a trait à leur portée, leur objectif et leur contenu[47]. Comme l'expliquent les auteurs DE HERT et GUTWIRTH :

> « *While privacy obviously occupies a central place in data protection law, the characterization of data protection law as solely or even essentially concerned with safeguarding privacy is misleading. Data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualizations of privacy* »[48].

À titre d'exemple, on constate qu'il n'y a aucune ou peu de manifestations de la notion d'intimité, fréquemment reprise dans les différentes conceptualisations de la vie privée, dans les lois sur la protection des données personnelles[49]. Inversement, les principes de vie privée ne permettent pas de justifier directement les principes reconnus en matière de finalité, de collecte, de divulgation et de sécurité de l'information[50].

Ainsi, lors de l'analyse des enjeux associés aux nouveaux modèles d'affaires basés sur la commercialisation de l'information, il est nécessaire de conserver à l'esprit cette distinction entre les motifs de protection de la vie privée et les motifs de protection de renseignements personnels. Ces deux derniers concepts se recoupent sous le concept de vie privée informationnelle. D'ailleurs, aux fins de cet essai, nous réutiliserons les grandes lignes des différentes conceptions de la vie privée et nous examinerons comment la protection des données se manifeste lorsqu'elle est perçue comme une liberté fondamentale, un droit subjectif ou un intérêt protégé par le droit.

1.2- La protection des données comme droit fondamental

Comme pour la protection de la vie privée, certains auteurs ont qualifié la protection des données comme étant une liberté fondamentale. Pour expliquer sa conception de liberté fondamentale, le professeur HALPÉRIN distingue les droits et les privilèges ou libertés : « *les droits (« rights ») exercés sur une autre personne, ainsi liée par un devoir (« duty »), et les privilèges ou libertés détenus sur soi-même, entraînant seulement une absence de droit pour*

[47] Serge GUTWIRTH et Paul DE HERT, préc. note 33, à la page 9.
[48] Serge GUTWIRTH et Paul DE HERT, préc. note 33, à la page 10.
[49] *Id.*
[50] *Id.*

autrui »[51]. Ainsi, une liberté pourrait donc se définir par la négative et s'illustrer par l'absence de droit d'autrui sur certains aspects de la vie du citoyen.

Prenons, par exemple, l'Europe qui édicte dans la Charte des droits fondamentaux de l'Union européenne que : « *toute personne a droit à la protection des données à caractère personnel la concernant* »[52]. Cette provision, prévue à l'article 8 sous le chapitre des libertés, prévoit également que les données doivent être traitées loyalement, en fonction de fins spécifiques, avec le consentement du sujet de l'information et que ce dernier est bénéficiaire de droits subjectifs pour assurer l'exactitude de l'information[53]. Notons aussi que la protection des données personnelles est placée sur un pied d'égalité avec la protection de la vie privée qui se retrouve à l'article 7 de la même charte.

L'objectif principal de cette constitutionnalisation de la protection des données personnelles est de protéger les données contre les interférences arbitraires des institutions et des organes au sein de l'Union européenne[54]. Cette concrétisation de droit fondamental s'inscrit dans un mouvement amorcé dès le début des années 1980 qui reconnaissait que le traitement automatisé de l'information créait un débalancement de l'équilibre des pouvoirs entre les détenteurs de l'information et les sujets[55]. Toutefois, on remarque qu'il se produit un changement de rationalité en ce qui concerne les fondements justifiant la protection des données personnelles. En effet, les arguments pour la protection des données ont passé d'une optique axée sur les droits de l'homme et leur protection contre l'abus de pouvoir du gouvernement vers une rationalité plus économique prenant en considération des enjeux relevant du marché[56].

---

[51] Jean-Louis HALPÉRIN, préc. note 14, à la page 779.
[52] *Charte des droits fondamentaux de l'Union Européenne*, 2000/C, Journal officiel des Communautés européennes, 364/01, 2000.
[53] *Id*.
[54] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, à la page 42.
[55] *Id*.; Voir aussi ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* Working Party on Information Security and Privacy (WPISP), 2013, en ligne : http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (page consultée le 23 décembre 2013).
[56] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, à la page 43.

Approcher le concept de protection des données comme étant une liberté fondamentale engendre des répercussions quant à son interprétation. Puisqu'il s'agit d'une garantie fondamentale des droits de l'homme, elle permet d'invalider des lois édictées allant contre ses dictats, mais elle sera aussi confrontée à d'autres libertés concurrentes. Ainsi, la protection des données pourrait être confrontée à la liberté d'expression et il sera alors nécessaire d'évaluer le contexte pour accorder prépondérance à l'une des deux libertés.

1.3- La protection des données comme droit subjectif

Comme nous l'avons mentionné plus tôt, il est également possible de retrouver des manifestations de la protection des données sous forme d'attribution de droits subjectifs aux individus. Rappelons-le, on distingue un droit subjectif par son pouvoir déterminé permettant la protection d'intérêts principalement moraux. Bien souvent, ce sera sous la forme de droits tels l'accès et la rectification des informations que la protection des données se manifestera.

On remarque que la rationalité derrière la mise en place des régimes de protection des données actuels est une rationalité visant à protéger la vie privée des individus dans un contexte où les technologies de l'information permettent un traitement des données automatisé et de plus en plus efficace, soulevant des enjeux qui n'étaient pas envisagés par les législations précédentes[57]. Ainsi, l'objectif principal de ces régimes est de rétablir l'équilibre de pouvoir entre les entités détenant l'information et les sujets de l'information, en leur conférant un certain contrôle sur les modalités du traitement de ces informations.

C'est l'évolution des technologies de l'information qui est considérée comme le point de départ de ce déséquilibre entre les détenteurs de l'information et ses sujets. D'abord, les technologies permettent dorénavant de conserver les données sans limite et contrainte significative. Les possibilités de traitement et les analyses qui en découleront sont donc limitées à la créativité de ceux qui les détiennent et ces données peuvent être conservées et archivées, quasi éternellement[58]. Ces capacités de traitement accrues sont généralement à

[57] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 68.
[58] *Id*.

l'avantage des grosses entreprises et des gouvernements qui possèdent les moyens de collecter, analyser et conserver des masses de données considérables[59].

Face à ces nouveaux enjeux, on a vu naître des régimes de protection des données conçus pour rétablir ce déséquilibre de l'information. Ainsi, alors que la protection se retrouvait auparavant limitée aux données sensibles, on voit un certain élargissement de la couverture de la protection des données, que ce soit par la nomination expresse de certains types de renseignements ou par l'adoption d'une définition générale des données personnelles[60].

Couplé à l'accroissement de la portée de la protection des données personnelles, on observe une attribution de nouveaux droits aux sujets des données[61]. Ces droits subjectifs sont notamment basés sur les différentes pratiques recommandées par l'OCDE[62].

Parmi ces pratiques, on retrouve les principes reconnus de limitation de la collecte d'information, de qualité de l'information, de spécification des finalités, de limitation de l'utilisation aux finalités, de mesures de sécurité adéquates, d'imputabilité, de transparence et de participation du sujet[63].

Notons que ce sont sur ces principes, aussi connus sous le nom de « *Fair Information Princples (FIPs)* », que les législations nationales vont se baser pour justifier les différents droits subjectifs attribués aux individus[64]. En effet, l'objectif central des textes de l'OCDE est de refléter les dialogues entre les pays membres et, par le fait même, permettre un rapprochement des différents points de vue. L'importance jouée par ces lignes directrices est donc significative en raison de la nature transfrontalière de l'information à l'ère numérique.

---

[59] Omer TENE et Jules POLONETSKY, « Big Data for All: Privacy and User Control in the Age of Analytics », (2012-2013) 11 *Nw. J. Tech. & Intell. Prop.*, 239, à la page 254.
[60] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 69.
[61] *Id*.
[62] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* Working Party on Information Security and Privacy (WPISP), 2013, en ligne : http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (page consultée le 23 décembre 2013).
[63] *Id*.
[64] Philippa LAWSON and Mary O'DONOGHUE, « Approaches to Consent in Canadian Data Protection Law », chapitre 2 dans KERR, I.R., V.M. STEEVES et C. LUCOCK*, Lessons from the Identity Trail*, Oxford University Press, 2009, à la page 24, en ligne : <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_02.pdf> (page consultée le 25 novembre 2015).

Ces principes sont notamment transposés dans la directive européenne concernant la protection des données à caractère personnel[65]. Cette directive récupère les « *FIP*s » et s'assure que ces principes se transposent en obligations légales à travers l'Union Européenne[66]. Ces principes sont également repris par d'autre juridiction, comme le Canada, qui adopte des lois visant la protection de la vie privée et garantissant l'accès et la rectification des renseignements personnels[67].

Comme nous l'avons mentionné, il existe divers courants de pensée quant à la portée que devrait avoir la protection des données personnelles. Plus précisément, on remarque qu'en Europe, il y a une tendance à adopter une définition expansionniste du concept de données personnelles. Dans les directives, la notion de données personnelles réfère aux informations reliées à une personne physique identifiée ou identifiable[68]. Ainsi, avec un régime qui nécessite la qualification de renseignements personnels pour attribuer des droits subjectifs, on retrouve une propension à couvrir plus de renseignements si on adopte l'approche expansionniste.

Parmi les droits subjectifs que l'on confère généralement, le droit d'accès est définitivement l'un des plus importants. Relevant des principes de transparence et de participation individuelle, ce droit confère au sujet la possibilité de demander les informations à son sujet[69].

> « *The Directive's subject access rights give the data subject the unconstrained ability to confirm if data controllers are processing the requester's information and to inquire into the purpose for such processing, as well as the right to request communication of the processed data in an intelligible form* »[70].

Ainsi, les intérêts de vie privée informationnelle de l'individu sont protégés, en lui conférant un droit de regard sur l'information dont il est le sujet.

---

[65] *Directive 95/46/CE,* préc. note 43.
[66] EUROPA, « I14012 », dans *EUR-Lex*, en ligne : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Al14012 (page consultée le 25 novembre 2015).
[67] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015); *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, en ligne : <http://canlii.ca/t/69h5j> (page consultée le 25 novembre 2015).
[68] Scott REMPELL, préc. note 38, à la page 816.
[69] *Id.*, à la page 817.
[70] *Id.*

Aux États-Unis, on adopte une approche différente de l'approche européenne. L'approche américaine est souvent qualifiée d'approche sectorielle, ou « *Piecemeal Model* »[71]. Contrairement à l'Europe, les États-Unis ont choisi de ne pas adopter un régime de protection général, ils ont plutôt opté pour un régime orienté en fonction des secteurs d'activités[72]. Ainsi, plutôt que d'adopter une définition large de données personnelles, les Américains optent pour une définition plus réductionniste qui sera limitée selon un domaine particulier, déterminé[73].

Par exemple, on observe une volonté de protéger la vie privée informationnelle dans le domaine de la santé. Le corps législatif couvrant la protection des données dans ce secteur est principalement composé de la *Health Insurance Portability and Accountability Act* (HIPAA) tel qu'amendée par la *Health Information Technology for Economic and Clinical Health Act* (HITECH)[74]. Sous ces lois, on confère aux patients des droits d'accès, de correction et même des moyens pour porter plainte si ces droits visant la transparence ont été lésés[75]. Notons qu'il existe un large débat quant à l'utilité de ces lois autant pour leur manque de couverture et les vides juridiques qu'elles créent[76], que pour leur attribution imprécise de droits de propriété sur les données, tout en entravant les recherches médicales bénéfiques pour la société[77].

Aux États-Unis, on retrouve également des visées de protection dans le secteur financier. Dans ce domaine, on justifie l'attribution de droits aux consommateurs pour qu'ils puissent faire respecter leur droit à la vie privée face aux compagnies de crédit en ce qui concerne les données de leur dossier de crédit[78]. Ainsi, pour protéger les individus contre les

---

[71] Cécile DE TERWANGNE, « Is a Global Data Protection Regulatory Model Possible », dans *Reinventing Data Protection*, Springer, 2009, à la page 179.
[72] Cécile DE TERWANGNE, préc. note 71, à la page 179.
[73] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40.
[74] 45 C.F.R. §160-164, en ligne : <http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl> (page consultée le 25 novembre 2015).
[75] HHS.GOV, «Your Rights Under HIPAA», en ligne: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html> (page consultée le 25 novembre 2015); Nicolas P. TERRY, « What's Wrong With Health Privacy? », (2009) 5 *Journal of Health & Biomedical Law* 1, pp.1-32.
[76] Nicolas P. TERRY, « Protecting Patient Privacy in the Age of Big Dat a», (2012-2013) 81 *UMKC L. Rev.* 385, à la page 387.
[77] Barbara J. EVANS, « Much Ado About Data Ownership », (2011-2012) 25 *Harv. J. L. & Tech*. 69, à la page 73; Jane YAKOWITZ, « Tragedy of the Data Commons », (2011-2012) 25 *Harv. J. L. & Tech*. 1, à la page 13.
[78] 15 USC § 1681 et seq.; *FACTA*, Pub.L. 108–159; *Gramm–Leach–Bliley Act*,113 Stat. 1338.

entreprises, on leur accorde le droit d'exiger un rapport annuel sur leur dossier de crédit[79]. Notons qu'avec les années, des modifications ont été apportées aux lois américaines afin d'élargir l'ensemble des entreprises étant visées par les lois. De fait, la *Federal Trade Commission* a jugé que des entreprises, qui n'étaient pas des agences de crédit, pouvaient être visées par les lois américaines si elles traitaient d'informations portant sur le dossier de crédit des consommateurs[80].

Ces exemples illustrent donc que malgré une approche qui n'est pas générale, les États-Unis accordent tout de même des droits subjectifs aux citoyens. Ainsi, lorsqu'il est question de santé ou de protection du consommateur, certaines règles spécifiques concernant la protection des données s'appliqueront. Autrement, il n'existe pas de lois générales visant la protection des données personnelles. Bien que les lois américaines accordent des droits subjectifs aux consommateurs, il subsiste toutefois beaucoup de critiques à cet effet. On critique notamment l'inefficience du régime sectoriel américain qui entraîne inévitablement des vides juridiques, privant les individus de protections nécessaires pour défendre leur vie privée informationnelle[81]. D'un autre côté, on soutient également que l'attribution de droits subjectifs similaires au droit de propriété n'est pas nécessairement une idée qui bénéficie à l'intérêt public[82].

Ainsi, que ce soit en Europe ou en Amérique, on retrouve des dispositions prévoyant des droits subjectifs pour la protection des données des individus. Autant sous le régime général et expansionniste européen que sous le régime sectoriel réductionniste américain, on cherche à protéger la vie privée informationnelle des citoyens. Ce constat suggère d'ailleurs qu'il existe une différence entre les cultures juridiques américaine et européenne. L'auteur STRAHILEVITZ soutient que les différences en matière de protection de la vie privée informationnelle du consommateur ne sont pas dues à une différence de culture, mais plutôt à

[79] Preston N. THOMAS, « Little Brother's Big Book : The Case for a Right of Audit in Private Databases », (2009-2010) 18 *CommLaw Conspectus* 155, à la page 170.
[80] Preston N. THOMAS, préc. note 79, à la page 170; Paul N. OTTO et al., « How Data Brokers Should Handle the Privacy of Personal Information », (2007) 5-5 *IEEE Security & Privacy* 15, à la page 20.
[81] Cécile DE TERWANGNE, préc. note 71, à la page 179.
[82] Voir Barbara J. EVANS, « Much Ado About Data Ownership », (2011-2012) 25 *Harv. J. L. & Tech*. 69, qui explique comment le consentement à la collecte afin de divulguer légitimement de l'information, est une illusion. Le régime actuel de protection des données dans le domaine de la santé aux États-Unis porte déjà entrave à la recherche médicale et les tendances européennes ajoutent un fardeau trop lourd aux chercheurs.

une différence quant à la méthode d'édiction des normes[83]. Il soutient : « *We can now posit that path-dependance dynamics help drive the United States-versus-Europe divide on consumer privacy* »[84]. Ainsi, on se retrouve face à une protection américaine sectorielle et réactive, qui rattrapera les vides à l'aide de la responsabilité civile, et une protection européenne proactive[85]. L'auteur soulève un autre point intéressant lorsqu'il soutient que c'est en raison de ce régime américain, plus réactif, qu'il est plus difficile d'introduire de nouvelles lois plus englobantes en matière de protection des données aux États-Unis[86].

Ces droits subjectifs accordés aux individus créent à leur tour une série d'enjeux que devront considérer les entreprises cherchant à commercialiser l'information. En effet, que ce soit lors de la collecte, l'utilisation ou la conservation de données, il existe des dispositions prévoyant des droits subjectifs aux individus qui forceront les entités impliquées à adapter leurs modèles d'affaires au cadre juridique de la protection des données.

1.4- La protection des données comme intérêt protégé par le droit

Enfin, on peut également concevoir la protection des données comme étant un intérêt protégé par le droit. Dans un texte sur la notion de renseignement personnel aux États-Unis, le professeur SOLOVE retrace les origines de ce concept en lien avec la protection de la vie privée américaine[87]. Il associe les débuts de la vie privée à un article publié par les auteurs WARREN et BRANDEIS, qui concevaient la « *privacy* » comme étant un droit de la personnalité[88]. Selon eux, la vie privée était un concept général selon lequel chacun avait le droit à une personnalité inviolée. SOLOVE note ensuite un second tournant dans la protection de la vie privée américaine avec l'article de William PROSSER qui proposait une approche de la vie privée divisible en quatre « torts »[89]. Avec l'arrivée des systèmes automatisés de traitement de

[83] Lior Jacob STRAHILEVITZ, « Toward a Positive Theory of Privacy Law », (2012-2013) 126 *Harv. L. Rev.* 2010.
[84] *Id.*, à la page 2035.
[85] *Id*.
[86] *Id.*, explique qu'il est difficile de tuer l'inertie. Les compagnies américaines poussent pour établir des standards sociaux acceptables en matière de « *privacy* ». Malgré cela, il reconnait que le régime réactif américain permet d'isoler les vrais problèmes et ne pas attaquer inutilement l'innovation.
[87] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40.
[88] *Id.*, à la page 1819.
[89] *Id.*, citant William L. Prosser, « Privacy », (1960) 48 *Calif. L. Rev.* 383; Voir aussi Edward J. BLOUSTEIN, « Privacy as an Aspect of Human Dignity : An Answer to Dean Prosser », (1964) 39 *N.Y.U. L. Rev.* 962.

l'information, on a remarqué qu'un intérêt de vie privée nécessitait une protection accrue et on a vu apparaître des lois sectorielles prévoyant la protection des données des individus[90].

Bien qu'on reconnaisse des droits subjectifs pour protéger la vie privée informationnelle des individus, on se fie souvent au droit pour la protéger. En effet, que ce soit par l'édiction de normes ou par le recours classique de la responsabilité civile, on repose souvent sur ce mécanisme de réparation pour protéger certains enjeux de vie privée.

Cette façon d'aborder la protection des données est caractéristique des États-Unis qui, historiquement, ont eu recours à la responsabilité civile pour protéger la vie privée. D'ailleurs, on peut soulever plusieurs tendances dans la pratique américaine qui démontrent comment la protection de la vie privée informationnelle est prise en charge par le droit.

S'inscrivant également sous un angle contractuel, on retrouve l'intégration contractuelle de principes reconnus comme moyens d'assurer la protection des données. En effet, les juridictions ont tendance à exiger de plus en plus la présence manifeste de principes reconnus pour assurer l'équivalence des protections lorsque les informations circulent à l'international[91]. De cette façon, on a vu apparaître plusieurs marques de certification permettant aux entreprises de remplir les critères de conformité. On pense notamment au régime de « *Safe Harbor* » mis en place par l'Union européenne pour faciliter les échanges de données à l'international[92]. Notons que cette pratique est présentement en processus de révision depuis octobre 2015 et que les parties impliquées cherchent à revamper le modèle actuel[93]. Ce genre d'adoption de code de conduite est encouragé par les organismes de protection des données qui accordent une certaine reconnaissance à ces initiatives volontaires[94].

---

[90] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40, à la page 1823.
[91] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, No. 176, OECD Digital Economy Papers, 2011, à la page 32, en ligne : http://dx.doi.org/10.1787/5kgf09z90c31-en (page consultée le 25 novembre 2015).
[92] *Id.*, à la page 33.
[93] Vera JOUROVA, *Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties*, Justice and Home Affairs (LIBE), 26 Octobre 2015.
[94] Voir THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, *Washington*, 2012, 52 p. où l'administration du gouvernement américain explique que les initiatives du secteur privé sont prometteuses. Le gouvernement

Le droit prévoit également comme moyen de protection des données personnelles des exigences de notification en cas d'intrusion dans les systèmes informatiques contenant des renseignements personnels[95]. En effet, certaines législations ont décidé d'adopter cet outil pour faciliter la protection des données des individus lorsqu'un crime informatique a été commis. Ce genre d'exigence légale nécessite généralement qu'une entité, privée ou publique, divulgue aux personnes sur qui elle détient de l'information, qu'une faille de sécurité s'est produite et que leurs renseignements sont potentiellement à risque[96]. Ce faisant, les individus peuvent ainsi réagir et prendre connaissance du préjudice potentiel qu'ils peuvent subir et réagir conséquemment. Parfois, cette exigence de divulgation est accompagnée de sanctions en cas de non-accomplissement[97]. Évidemment, on prévoit certaines exceptions à cette divulgation obligatoire, notamment lorsqu'une divulgation empiéterait sur une enquête en cours.

Enfin, une atteinte à la vie privée informationnelle peut, de façon plus générale, être sujette à réparation en fonction des règles de responsabilité civile. En effet, les droits de la personnalité, telle la vie privée, confèrent le pouvoir d'obtenir réparation à leur titulaire lorsqu'un intérêt qui est protégé a été atteint[98]. En ce sens, les régimes de droit civil comme celui du Québec nécessitent la preuve de la faute, du préjudice et du lien causal. La seule démonstration de l'atteinte au droit n'est pas suffisante, il faut également démontrer qu'un dommage ait été subi[99].

---

accorde qu'il doit jouer un rôle pour encourager l'adoption volontaire de pratiques visant à protéger la vie privée. Par exemple, l'adoption de codes de conduite pré-approuvés par le FTC permettra une présomption en faveur de l'entreprise lorsque des intérêts protégés seront lésés.

[95] Marc LEMIEUX, « L'affaire Groupe Aldo : réflexions sur l'encadrement juridique de la cybercriminalité dans les opérations bancaires et l'industrie des paiements », *Revue du Barreau*, 2014, EYB2014RDB139, à la page 14.

[96] *Règlement concernant les mesures relatives à la notification des violations de données à caractère personnel* en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques, N° 611/2013, 23 juin 2013; SB. 1386 (2002).

[97] Paul N. OTTO et al., « How Data Brokers Should Handle the Privacy of Personal Information », (2007) 5-5 *IEEE Security & Privacy* 15, à la page 18.; Voir aussi la loi californienne SB. 1386 (2002) qui prévoit des recours pour les individus ou entreprises contre l'entité devant divulgué la « *security breach* » en cas de non-divulgation de la faille de sécurité.

[98] Pierre TRUDEL, *Le droit à la réputation, à la vie privée et à l'image*, à la page 394, en ligne : < pierretrudel.chairelrwilson.ca/cours/drt3805/rep.vieprive.pdf> (page consultée le 25 novembre 2015).

[99] Édith DELEURY et Dominique GOUBAU, «La protection des droits de la personnalité», dans *Le droit des personnes physique*, 5e éd., Cowansville, Éditions Yvon Blais, 2014, EYB2014DPP17, à la page 1.

La situation est toutefois différente aux États-Unis. Initialement, la réparation d'une atteinte à la protection des données était envisagée par les différents « *torts* » de Common Law en vie privée[100]. C'est en 1960 que le doyen William PROSSER décrit quatre différents « *torts* » pouvant circonscrire la protection de la vie privée aux États-Unis[101]. Ce texte publié par Prosser a généré beaucoup de discussions et a mené à la constitution de plusieurs conceptualisations de la vie privée[102]. Depuis, beaucoup de recours ayant pour fondement la « *contract law* » ou des lois écrites ont été reçus, sans grand succès[103]. Récemment, on constate que plusieurs recours en protection des données sont reçus par la *Federal Trade Commission* qui sanctionne les violations aux « *privacy policies* » et autres « *self-regulation codes* » adoptés par les entreprises[104].

Pour résumer, la protection des données peut se manifester comme étant un intérêt protégé par le droit. Que ce soit par le mécanisme général de la responsabilité, par la protection de renseignements particuliers ou en exigeant certains actes pour garantir une saine gestion des données, le droit intervient pour protéger les données des individus.

1.5- Conclusion

Le survol de la protection des données que nous venons de tracer permet déjà d'envisager les différents enjeux qu'une entreprise cherchant à commercialiser les renseignements personnels pourrait affronter. En effet, qu'il s'agisse d'enjeux de protection de vie privée ou de protection des renseignements personnels, chaque entité opérant dans le domaine de l'information aura à faire face à différents enjeux juridiques.

Nous avons vu que la vie privée n'est pas synonyme de protection des données. La vie privée cherche à protéger cet espace intime et irréductible qui est nécessaire au développement

[100] Edward J. BLOUSTEIN, « Privacy as an Aspect of Human Dignity : An Answer to Dean Prosser », (1964) 39 *N.Y.U. L. Rev.* 962, à la page 965.
[101] Edward J. BLOUSTEIN, préc. note 100, à la page 965.
[102] Yana WELINDER, préc. note 19, à la page 182.
[103] Daniel J. SOLOVE et Woodrow HARTZOG, « The FTC and the New Common Law of Privacy », (2014) 114 *Columbia Law Review* 583, aux pages 590 à 597.
[104] *Id*., aux pages 597 à 606.

authentique de l'homme. Il existe, à tout le moins, deux cultures manifestes cherchant à définir la portée de la vie privée.

La première est une culture qui cherche à identifier les éléments centraux qui constituent les fondements de la vie privée. Par exemple, lorsqu'on considère qu'un certain type de renseignement fait nécessairement partie de la sphère privée d'un individu devant être protégé par le droit. La deuxième est une culture plus expansionniste qui considère la vie privée comme un rempart fondamental de la personnalité contre les intrusions externes. Cette approche cherche à protéger, par le biais de la vie privée, des droits fondamentaux tels que l'autonomie et l'individualité.

Chacune des différentes conceptions de ce qu'est la vie privée illustre en fait le rapport que la culture d'une société entretien avec ce qui devrait être considéré comme méritant une protection contre les intrusions provenant des différentes relations sociales publiques.

La protection des données se distingue de la protection de la vie privée en ce qu'elle ne cherche pas nécessairement à identifier quels sont les éléments qui doivent être protégés parce qu'ils sont de nature intime, mais plutôt une protection accordée à tous les renseignements pouvant se qualifier dans la définition légale de « renseignement personnel ». Nous croyons que la protection de la vie privée et la protection des données s'entrecoupent dans le concept de vie privée informationnelle.

Enfin, nous avons détaillé différentes façon d'entrevoir la protection des données. Par exemple, la protection des données peut être utilisée pour protéger des valeurs et libertés fondamentales comme l'autonomie et la dignité humaine, pouvant être atteintes par la divulgation de certains renseignements personnels intimes. La protection des données peut également se manifester sous forme d'attribution de droits subjectifs aux sujets de l'information. On pense notamment aux droits d'accès et de rectification de l'information qui sont souvent accordés aux individus dont les renseignements sont compilés dans un dossier. La protection des données peut également permettre de protéger un intérêt par le droit. Ainsi, plusieurs juridictions ont recours au mécanisme de la responsabilité civile pour sanctionner une violation de la vie privée informationnelle d'un individu.

Dans les chapitres qui suivent, nous observerons les différentes pratiques commerciales et constaterons que chacune d'entre elles affrontent des enjeux qui leurs sont parfois exclusifs, parfois communs. Les enjeux varieront autant en fonction de la pratique commerciale qu'en fonction de la juridiction. Bien que toutes les conceptualisations étudiées soient utilisées, d'une façon ou d'une autre, par les différentes juridictions, la portée et l'interprétation de ce qu'est la vie privée et la protection des renseignements personnels sont spécifiques à chaque régime de protection de l'information. Nous tenterons de préciser comment l'adoption plus engagée d'une conceptualisation plutôt qu'un autre peut affecter les enjeux juridiques auxquels font face les entreprises commercialisant l'information.

Il y a un intérêt manifeste à étudier les pratiques actuelles de traitement de l'information en ce que cela nous permet de catégoriser les différentes pratiques en groupes partageant des caractéristiques communes. De cette observation, on voit apparaître plusieurs familles de modèles d'affaires. Notons qu'il ne s'agit pas ici de faire une revue exhaustive de tous les modèles d'affaires qui existent, mais plutôt d'analyser les différentes façons dont il est possible de traiter et commercialiser l'information.

Le dénominateur commun de tous ces modèles est l'information. Comme nous le verrons, certains modèles d'affaires utilisent l'information comme un bien ou une action, qui prend de la valeur, simplement par le cumul de l'information disponible, permettant d'offrir un produit fini à valeur ajoutée pour lequel une demande existe. Dans d'autres cas, nous verrons c'est la gestion de l'information qui permet aux entreprises d'offrir des services aux consommateurs. On pense aux services de conservation de l'information, garantissant la sécurité, la confidentialité ou encore l'accessibilité à cette information. La demande pour ce genre de service est grandissante et est symptomatique de l'évolution du contexte technologique qui facilite et rend abordable la conservation de masse d'information. Enfin, l'information peut également être perçue comme une matière première pouvant être raffinée. Les outils d'analyse basés sur des théorèmes statistiques ou mathématiques permettent, avec beaucoup d'innovation, d'utiliser et de rendre pertinente de l'information autrefois indésirable ou inutile.

2- Le « Data Brokerage »

La première pratique commerciale étudiée sera celle du « *Data Brokerage* ». Cette pratique consiste essentiellement en la revente d'informations collectées par les « *data brokers* » à d'autres entités. Pour ce faire, les entreprises exerçant dans cette industrie se vouent à une collecte massive et systématique de l'information qui est à la portée de leur main. Comme résultante, d'immenses bases de données privées sont constituées et prêtes à être minées[105].

À partir de ces gisements d'informations, les entreprises agrègent, identifient et référencent l'information pouvant contenir des renseignements personnels[106]. Ce raffinement de l'information brute permet ensuite aux entreprises d'offrir et de développer des services à partir des renseignements obtenus. L'éventail de services pouvant être offerts est large et est conséquent de la créativité de l'entreprise détenant des renseignements sur les individus. Cette réalité est notamment attribuable au développement des technologies de l'information, en ce que la technologie permet la numérisation systématique de données transactionnelles, mais est aussi attribuable à l'acceptation de ces technologies par les acteurs du marché[107].

En fait, la quantité d'information collectée ne peut être ignorée. D'ailleurs, les statistiques compilées quant à cette pratique sont frappantes. Dans un document émis par le *Federal Trade Commission* américain en mai 2014, les « *data brokers* » détiennent des renseignements sur la quasi-totalité des ménages aux États-Unis[108]. Comme le souligne l'auteur Preston THOMAS, les entreprises comme Acxiom et ChoicePoint détiennent probablement plus d'informations sur la population américaine que le gouvernement fédéral jumelé à ses services de renseignements[109].

---

[105] CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *On the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations With Whom You Have No Relationship*, Report on the Canadian Data Brokerage Industry, Ottawa, CIPIC, 2006, 39 p.
[106] IT LAW WIKI, «Big Data», en ligne : < http://itlaw.wikia.com/wiki/Big_data > (page consultée le 25 novembre 2015).
[107] Preston N. THOMAS, préc. note 79, à la page 159.
[108] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability,* 2014, à la page 46.
[109] Preston N. THOMAS, préc. note 79, à la page 160.

Un tel recensement de l'information sur une population soulève plusieurs considérations de vie privée puisqu'il collecte manifestement une foule de données pouvant être sensibles et pouvant se qualifier comme renseignements personnels. Malgré ces enjeux manifestes, le « *data brokerage* » fournit certains avantages non-négligeables pouvant bénéficier aux consommateurs. En effet, une fois l'information compilée et raffinée, les « *data brokers* » sont en mesure de vendre des renseignements à des fournisseurs de services, dont l'objectif est d'améliorer leurs services et de réduire, ultimement, les coûts pour les consommateurs, tout en favorisant l'innovation et en ajoutant des protections contre la fraude[110].

Par contre, les risques associés au « *data brokerage* » sont réels et significatifs. La collecte de masse et systématique de renseignements sur des individus soulèvent pléthore d'enjeux relevant de la protection des renseignements personnels et de la vie privée.

2.1- Une pratique économique encadrée?

Si on observe cette pratique d'un point de vue purement économique, il est compréhensible qu'une entreprise exerce la revente d'information comme source de revenu principal. Dans son rapport, la *Federal Trade Commission* évalue que les revenus générés, en 2012, par cette pratique commerciale avoisinent le demi-milliard de dollars[111]. L'information a donc une valeur substantielle pour les compagnies faisant affaire avec les « *data brokers* »[112].

Cette industrie de revente de l'information n'a pas toujours été où elle est actuellement. À cet effet, on rapporte que certaines entreprises se sont divisées pour éviter les lois posant certaines restrictions aux agences de crédit quant à la vente d'information[113]. De cette façon, les entreprises comme ChoicePoint ne se qualifiaient plus comme entreprise fournissant des

[110] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 3.
[111] *Id.*, à la page 23.
[112] Howard A. SHELANSKI, « Information, Innovation, and Competition Policy for the Internet », (2013) 161 *University of Pennsylvania Law Review* 1663, à la page 1682.
[113] Paul N. OTTO et al., « How Data Brokers Should Handle the Privacy of Personal Information », (2007) 5-5 *IEEE Security & Privacy* 15, à la page 16.

services financiers et, par le fait même, évitaient les lois plus rigoureuses s'appliquant à ces entreprises[114].

Pour les entreprises exerçant dans le domaine du « *data brokerage* », la portée des lois encadrant la protection de la vie privée est d'une importance significative. Autant la portée de la loi que les méthodes qu'elles emploient sont importantes pour déterminer les enjeux juridiques balisant la pratique de « *data brokerage* ». Pour éviter le fardeau que les lois sur la protection des renseignements personnels peuvent imposer, les entreprises peuvent d'abord chercher à ne pas collecter des renseignements qui se qualifieraient de renseignements personnels au sens de la loi. Comme nous l'avons mentionné, il existe différentes cultures juridiques qualifiant plus ou moins large la définition de ce qu'est un renseignement personnel.

Évidemment, le marché du « *data brokerage* » est réglementé. D'ailleurs, on remarque qu'une certaine préoccupation face à ce genre de pratique commence à se manifester. Alimentée par le développement des technologies de l'information et des capacités d'analyse de masses de données, l'inquiétude face au « *data brokerage* » s'est notamment manifestée aux États-Unis[115]. Pour répondre à ces inquiétudes et pour approfondir les connaissances sur ce marché relativement obscur[116], la *Federal Trade Commission* a produit en 2014 un rapport s'intitulant *Data Brokers – A Call for Transparency and Accountability*[117]. Ce rapport est unique en son genre, en ce qu'il répond au besoin criant d'information sur cette pratique peu documentée.

[114] Paul N. OTTO et al., préc. note 113, à la page 16.
[115] Preston N. THOMAS, préc. note 79, à la page 163; Paul N. OTTO et al., préc. note 113, à la page 17.
[116] Howard A. SHELANSKI, préc. note 112, à la page 1682.
[117] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108.

2.2- Sources d'obtention de l'information

Dans ce rapport, on observe d'abord le contexte entourant l'acquisition de données. On sait que ces données proviennent de trois sources distinctes, soit : les registres publics, l'information disponible au public et les informations qui ne sont pas disponibles au public[118].

Parmi les sources d'informations gouvernementales, la FTC relève que les « *data brokers* » obtiennent de l'information autant du gouvernement fédéral que des gouvernements étatiques et locaux[119]. La variété d'information pouvant y être récoltée est considérable, du *Census Bureau* au *Department of Motor Vehicles*, les « *data brokers* » ont développé plusieurs méthodes pour collecter ces informations sans avoir à les obtenir directement du gouvernement[120]. La plupart du temps, les « *data brokers* » obtiennent ces informations de registres publics, en embauchant du personnel pour compiler ces informations ou ayant des relations avec ces bureaux publics ou encore en achetant l'information à d'autres « *data brokers* »[121].

Il ne semble pas y avoir, aux États-Unis, de limites légales par rapport à la collecte de ce genre d'information, mais plutôt une limite quant au type d'utilisation qu'on en fait[122]. À l'inverse, d'autres juridictions en Europe sont régies par des principes qui visent à limiter autant la collecte que le traitement des informations. Comme pour la qualification de ce qu'est un renseignement personnel, il semble y avoir une différence culturelle entre l'Europe et les États-Unis. Alors que le premier adopte explicitement dans ses directives les *FIP*s cherchant à limiter la collecte de l'information, le second adopte une approche qui est plutôt orientée vers l'effet de la collecte.

Ensuite, une autre source alternative de données serait les informations disponibles au public. On entend par informations disponibles au public toutes les informations affichées sur

---

[118] Paul N. OTTO et al., préc. note 113, à la page 15; CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *ON the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations With Whom You Have No Relationship*, Report on the Canadian Data Brokerage Industry, Ottawa, CIPIC, 2006; IT LAW WIKI, «Data Broker», en ligne : <http://itlaw.wikia.com/wiki/Data_broker> (page consultée le 25 novembre 2015).
[119] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 11.
[120] *Id.*, à la page 12.
[121] *Id*.
[122] *Id.*, à la page 13; Paul N. OTTO et al., préc. note 113, à la page 20.

les différents réseaux, registres et médias, notamment les réseaux sociaux, qui ne proviennent pas d'un organe gouvernemental. En effet, plus de la moitié des grands « *data brokers* » américains ont affirmé obtenir des informations à partir de sources étant à la disposition du public comme les registres téléphoniques, les rapports de presses ou encore l'information personnelle publiée sur Internet[123]. On note d'ailleurs que les individus utilisant les médias sociaux sans se soucier des paramètres de configuration liés à la protection de leur vie privée sont une mine d'information pour ces revendeurs[124].

Enfin, comme troisième source, on retrouve les informations qui ne sont pas offertes au public. Dans son rapport, la FTC qualifie cette source comme une source de données commerciales [125] . À titre d'exemple, la plupart des « *data brokers* » récoltent des renseignements de transactions directement à partir des entreprises de vente au détail[126]. Les renseignements fournis peuvent autant porter sur l'achat lui-même, que sur le montant, le moment ou encore le type de paiement. Autrement, on peut aussi noter que certains « *data brokers* » obtiennent des renseignements à partir de sites nécessitant une inscription pour avoir accès au service offert. Toutefois, la majorité des données ayant une source commerciale proviennent des autres « *data brokers* » s'échangeant, entre eux-mêmes, les informations récoltées[127].

Comme on le constate, les « *data brokers* » sont essentiellement des tiers au sujet de l'information et collectent la majorité de l'information à partir de sources autres que le sujet lui-même. Il n'y a donc que très rarement une relation directe entre le sujet et le « *data broker* », soulevant la question de la pertinence du consentement au traitement des renseignements personnels que nous traiterons plus bas.

---

[123] Preston N. THOMAS, préc. note 79, aux pages 159 et ss.
[124] Martha C. WHITE, «Big Data Knows What You're Doing Right Now», *Time*, July 31st 2012, en ligne : < http://business.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/> (consultée le 25 novembre 2015).
[125] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 13.
[126] *Id*.
[127] *Id.*, à la page 14.

2.3- Méthodes de collecte

En ce qui concerne les méthodes de collecte, les « *data brokers* » utilisent des « *web crawlers* » leur permettant de collecter l'information disponible au public en ligne. Ils peuvent également se procurer de l'information imprimée pour ensuite la numériser. Enfin, certains revendeurs s'organisent pour traiter en lot, ou en continu, les informations fournies par les sources commerciales[128]. Les « *data brokers* » entrent fréquemment en relations contractuelles avec les sources d'informations pour s'assurer qu'elles ont été obtenues légalement, c'est-à-dire, avec le consentement du sujet et en s'assurant que celui-ci ait été informé que ses informations pourraient être vendues à des tiers. Toutefois, il est intéressant de constater que ces méthodes excluent presque automatiquement le sujet de tout type de relation avec les revendeurs[129]. Ceci a pour résultat que la plupart des sujets n'ont même pas connaissance de l'existence de ces revendeurs et encore moins du type de renseignements que ces derniers détiennent[130].

Cette exclusion du sujet de l'information est contraire, en quelque sorte, au principe de participation du sujet mis de l'avant par les *FIP*s de l'OCDE[131] et repris par différentes lois[132], puisque le sujet n'a pas connaissance que ses informations sont traitées. Par conséquent, il ne peut se prévaloir des droits subjectifs dont il pourrait bénéficier. Certains opposeront à cette exclusion du sujet, le consentement qu'il aura donné au traitement de son information. Toutefois, comme nous le commenterons plus bas, le consentement joue actuellement un rôle très important dans l'autorisation de la commercialisation de l'information, alors que son efficacité est au mieux médiocre. Autrement dit, le consentement au traitement de l'information donné par un sujet, à un fournisseur de service, autorisant des tiers de traiter et revendre ses renseignements personnels, ne devrait pas avoir beaucoup de poids juridique lorsque le contrat accordant le consentement en est un de consommation ou d'adhésion.

---

[128] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 17.
[129] *Id*, à la page 16.
[130] *Id*., à la page 17; THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Washington, 2012, à la page 13.
[131] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* préc. note 62.
[132] *Directive 95/46/CE,* préc. note 43.

Une fois ces informations obtenues, on pourra les décortiquer, les référencer et les analyser grâce aux outils « *analytics* », autre modèle d'affaire, permettant ainsi d'offrir une variété de services à leurs clients[133]. Ces services peuvent passer d'outils pour améliorer l'efficacité du marketing effectué par un détaillant à la recherche d'information sur un individu. Comme nous l'avons mentionné, les modèles d'affaires n'évoluent pas en vase clos et les entreprises œuvrant dans la commercialisation de l'information ont souvent recours, simultanément, aux différents modèles d'affaires présentés dans cet essai. Comme nous le verrons, la pratique de « *data brokerage* » se distingue des « *analytics* » en ce que la commercialisation de l'information s'opère par la collecte massive de données pour les revendre, alors que les « *analytics* » commercialise l'information en l'analysant et la traitant avec innovation.

2.4- Finalités de l'utilisation des données

La première utilisation concrète du « *data brokerage* » est le marketing, comprenant le marketing direct, le marketing en ligne et les « *marketing analytics* »[134]. Ce sous ensemble de services est offert aux entreprises désirant obtenir plus d'informations sur le consommateur, principalement dans l'objectif de leur suggérer un produit plus personnalisé. Pour ce faire, le client devra fournir certains renseignements concernant le consommateur pour que le « *data broker* » puisse identifier ce dernier et, par la suite, ajouter ses informations, ses profils ou ses tendances et comportements de consommation[135]. Les informations pouvant être transmises par le revendeur sont illimitées : âge, religion, valeur nette, affinité technologique, nouveaux parents, genre, affiliation politique, grandeur, utilisation des médias sociaux, revenu du ménage, véhicule, poids, ethnicité, statut civil, fumeur, joueur compulsif, informations médicales, éducation, etc.)[136].

Nous constatons que les « *data brokers* », dans le cadre de la vente de masses de données à des fins de marketing en ligne, opèrent une transaction qui échange des renseignements, parfois personnels, pour constituer des profils qui permettront au publicitaires

---

[133] THE WHITE HOUSE, *Big Data: Seizing Opportunities, Preserving Values*, Washington, 2014 à la page 43.
[134] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 23.
[135] *Id*.
[136] *Id*., à la page 24.

de mieux cibler leur clientèle. Il s'agit essentiellement de communication et vente de renseignements personnels à un tiers. La communication de renseignements personnels est un des aspects les plus fréquemment protégés par les lois sur la protection des données et de la vie privée. À titre d'exemple, les lois québécoises et canadienne concernant la protection des données et l'accès aux documents limitent toutes la possibilité de communiquer des renseignements personnels sans le consentement du sujet de l'information[137].

Plus précisément, on retrouve dans la loi québécoise une stricte interdiction d'utiliser les renseignements personnels à des fins autres que celles pour lesquelles les informations ont été collectées en premier lieu, à moins que le sujet de l'information consente à cette communication qui ne faisait pas partie des finalités initialement déterminées lors de la collecte. L'article 13 de la loi sur la protection des renseignements personnels dans le secteur privé prévoit :

> *« Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie. »*[138]

D'ailleurs, le consentement dont il est question doit également rencontrer certains critères afin d'être valide aux yeux de la loi. Il doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il doit également être limité dans le temps pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé[139]. Un exemple de bonne pratique serait Microsoft qui explicite dans sa politique sur la vie privée que les renseignements seront utilisés à des fins de communication et de publicité[140].

---

[137] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art. 7, en ligne : <http://canlii.ca/t/69jqs> (page consultée le 25 novembre 2015); *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 13, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015); *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, art. 59, en ligne : <http://canlii.ca/t/69m2d> (page consultée le 25 novembre 2015);
[138] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 13, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).
[139] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 14, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).
[140] MICROSOFT, « Microsoft Privacy Statement», en ligne : <https://privacy.microsoft.com/en-us/privacystatement/ >(page consultée le 25 novembre 2015).

Dans les faits, un « *data broker* » qui transige sur des masses de données, contenant des informations personnelles sur une pluralité d'individu, ne va pas vérifier pour chaque consentement donné s'il rencontre les critères énoncés par la loi. Comme nous l'avons expliqué, le « *Data Broker* » est un revendeur d'information et obtient ses renseignements de plusieurs sources. Dans le cas de marketing en ligne, les revendeurs d'informations peuvent obtenir leurs masses de données de divers fournisseurs de services qui, en échange de l'accès à leur service gratuit, demandent à ce que leurs utilisateurs consentent au partage de leurs renseignements de navigation à des tiers.

Alors que cette transaction puisse s'opérer avec le consentement des sujets de l'information, on soulève également la possibilité que ce type de communication soit permis sans nécessairement obtenir le consentement puisque la finalité de cette opération n'est pas nécessairement de communiquer des renseignements personnels, mais bien de tirer des conclusions anonymes à partir de masses de données contenant des renseignements personnels. Nous observerons plus en détail cette pratique dans le sous-chapitre portant sur le profilage et le « *behavioral advertising* » dans le chapitre portant sur les « *analytics* » et le « *Big Data* ».

Le deuxième type de services offerts par les entreprises de « *data brokerage* » sont les services pour mitiger les risques. Ceux-ci permettent notamment de procéder à une vérification plus rigoureuse de l'identité des clients d'une entreprise, mais aussi de se prémunir contre la fraude ou de la détecter plus rapidement[141]. À ces fins, les « *data brokers* » aident leurs clients à mettre sur pied des balises attribuant un indice de risque au consommateur. Cet indice de risque peut être basé sur les réponses à des questions personnelles ou encore si le numéro d'assurance sociale du consommateur est associé à des actes de fraudes ou à un dossier criminel[142]. Ce type de vérifications peut également se faire à partir de l'adresse courriel d'un

[141] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, aux pages 32 et ss.; THE WHITE HOUSE, *Big Data : Seizing Opportunities, Preserving Values*, préc. note 133, à la page 43.
[142] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 32.

consommateur. Ainsi, le revendeur aidera son client à retracer l'historique de transactions associé à cette adresse[143].

Encore une fois, on constate que les « *data brokers* » communiquent des renseignements personnels à des tiers. Toutefois, contrairement aux services de marketing en ligne, ce genre de service cherche à confirmer des renseignements personnels d'un individu bien identifié. Il ne subsiste aucun doute qu'il s'agit de renseignements personnels qui seront utilisés à des fins d'identification et de confirmation de certaines caractéristiques ou traits du sujet de l'information. Pour ce type d'utilisation, il est d'autant plus important que les dispositions des lois visant la protection des données s'appliquent, car il s'agit très précisément de l'utilisation de renseignements personnels à laquelle le sujet n'a probablement pas consentit.

Enfin, les « *data brokers* » offrent également des services permettant de consulter le dossier d'un individu. L'utilisation de ce type de services est variée et vise comme client autant les individus que les organisations. À titre d'exemple, l'entreprise Intelius offre un service de recherche sur les individus à partir d'un nom, d'une adresse, d'un numéro de téléphone ou encore d'un pseudonyme [144]. Moyennant des frais de 5$, le client pourra obtenir des renseignements tels le nom, l'âge, l'adresse, parenté, lieux visités connus, fournisseurs de service téléphonique et Internet. D'un autre côté, on observe des entreprises comme LexisNexis qui, misant sur la nécessité urgente d'information lors des enquêtes criminelles, offre aux forces de l'ordre, des services de localisation des suspects ou des témoins[145].

Ainsi, que ce soit à des fins d'identification, de marketing ou de repérage, on constate que l'éventail de services offerts par les « *data brokers* » est très large[146]. En fait, cet éventail n'est limité que par les informations à la disponibilité de ces entreprises et par leur créativité quant à la conception de nouveaux services. Cela explique, en partie, la collecte de masse à

---

[143] FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability*, préc. note 108, à la page 33.
[144] INTELIUS, «People Search», en ligne : <http://www.intelius.com/people-search.html> (page consultée le 25 novembre 2015).
[145] LEXISNEXIS, «Accurint® for Law Enforcement», *Risk Solutions,* en ligne : <http://www.lexisnexis.com/risk/products/government/accurint-le.aspx > (page consultée le 25 novembre 2015).
[146] LEXISNEXIS, «Product Index», *Risk Solutions*, en ligne : <http://www.lexisnexis.com/risk/products/> (page consultée le 25 novembre 2015).

laquelle ces « *data brokers* » s'adonnent. En effet, même si les informations ne sont pas nécessaires au moment de la collecte, ces entreprises collectent tout ce qu'elles peuvent, au-delà de ce qui pourrait sembler raisonnable, car la nature même de l'entreprise implique des fins indéterminées pour ces informations.

Cette collecte massive et non-limitée va directement à l'encontre du principe de limiter la collecte à ce qui est nécessaire. À titre d'exemple, la directive européenne 95/46/CE précise :

> « *considérant que tout traitement de données à caractère personnel doit […], porter sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies; que ces finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine;* »[147]

Ainsi, la constitution de bases de données massives est difficile à réconcilier avec ce principe de limitation. La raison d'être des « *data brokers* » est essentiellement contraire à ce principe, car ceux-ci ont pour objectif de collecter le plus d'information possible pour étayer les profils qu'ils détiennent sur les sujets.

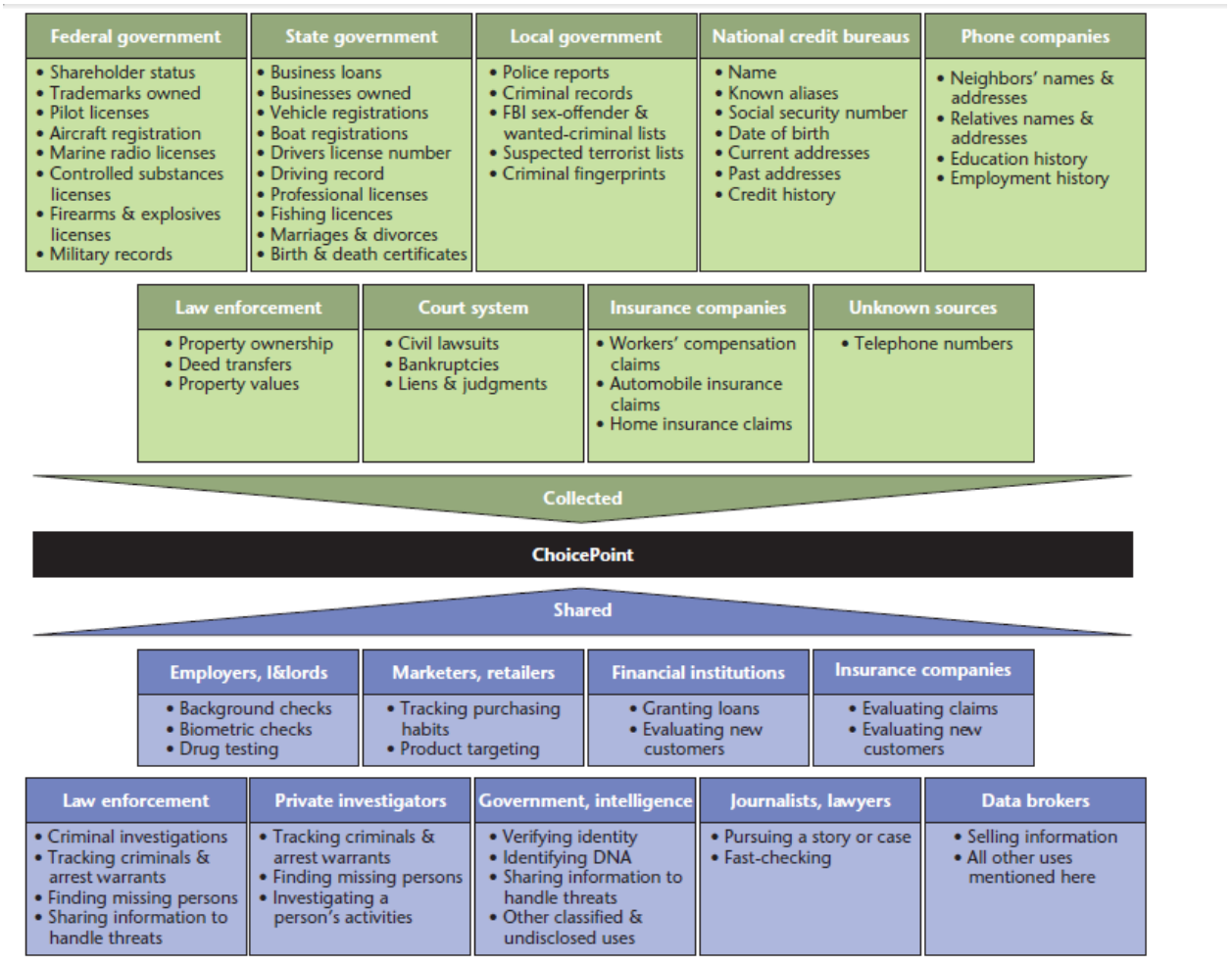
2.5- Destinataires et cheminement de l'information

Comme nous l'avons constaté, il est possible de diviser en plusieurs catégories l'ensemble des services offerts par les « *data brokers* ». De plus, au sein même de chaque catégorie, les différents services ne visent pas nécessairement le même type de clients. Parmi les clients potentiels, on retrouve notamment les employeurs, les entreprises de marketing, les institutions financières, les compagnies d'assurances, les forces de l'ordre, les investigateurs privés, les services de renseignements gouvernementaux, les journalistes, les avocats et les autres revendeurs d'information en quête de plus d'information[148].

D'ailleurs, comme le représente des auteurs dans leur article sur le « *data brokerage»*, le tableau ci-dessous représente les différentes sources d'informations et les différents services offerts selon le client[149]. Il schématise les relations entre les sources d'information, la clientèle et le revendeur d'information. Il permet par le fait même d'illustrer le parcours de

[147] *Directive 95/46/CE,* préc. note 43.
[148] Paul N. OTTO et al., préc. note 113, à la page 17.
[149] *Id*.

l'information dans la pratique de « *data brokerage* ». Ainsi, comme il appert du tableau, les « *data brokers* » collectent à partir d'une multitude de sources pour partager l'information à des destinataires ayant des motivations variées.



Source : Paul N. OTTO et al., préc. note 113, à la page 17

Ce tableau illustre avec beaucoup de simplicité la portée de la pratique commerciale de « *data brokerage* ». En prenant l'entreprise ChoicePoint comme exemple de revendeur d'information, ce schéma représente le parcours de l'information, depuis ses sources jusqu'à ses destinataires. Un élément marquant de cette représentation est que l'information revêt un caractère versatile. En effet, on peut constater que sans égard à sa provenance, une information peut être décontextualisée et utilisée de plusieurs façons. Ainsi, une information provenant d'une compagnie de téléphone peut autant servir à des fins d'investigation privée, que de journalisme, que d'évaluation financière.

Dans le même article on identifie certaines statistiques concernant la clientèle de ces services et leur proportion en ce qui concerne la source de revenu. Malgré l'âge relative de cet article, il demeure pertinent, voire d'actualité par la représentation schématique du modèle d'affaire. Ce type d'information est particulièrement intéressant, car cela nous permet de dresser un portrait plus fidèle de ce genre de pratique peu documentée.

2.6- Pratique lucrative

En terme de répartition, pour ce qui est de la compagnie ChoicePoint, on évaluait en 2005 que 38,5 % des revenus provenaient des compagnies d'assurances, 35,9 % provenaient des services offerts aux entreprises, 14 % des services offerts au gouvernement, 8,6 % des services de marketing et 3 % d'autres services[150]. Ainsi, les principaux clients des revendeurs d'information seraient les compagnies d'assurances et les compagnies privées. Il existe donc un marché qui consiste en la collecte de masse des renseignements pour ensuite l'offrir, sous forme de service, à des entreprises privées dont les fins sont indéterminées. Toutefois, notons que ces renseignements datent de 2005 et qu'il serait intéressant de constater l'évolution de cette répartition en fonction du développement récent des technologies de l'information et de leur capacité d'analyse.

Bien qu'il ne soit pas une source de revenue majoritaire, le gouvernement joue un rôle tout de même significatif en tant que client d'entreprise revendant de l'information. Une conceptualisation de la protection des données personnelles comme étant un droit fondamental aurait un impact direct sur les actions que pourraient poser un gouvernement. Advenant une constitutionnalisation de principes visant la protection des données personnelles, comme en Europe[151], un gouvernement serait tenu de respecter ce principe dans les gestes qu'il pose, mais aussi dans les lois qu'il édicte.

[150] Paul N. OTTO et al., préc. note 113, à la page 16.
[151] *Charte des droits fondamentaux de l'Union Européenne*, préc. note 52.

2.7- Enjeu – Asymétrie de l'information

Un autre des constats les plus récurrents est celui du manque d'accès à l'information et à l'exclusion des utilisateurs quant aux renseignements sur les publicités qui leur sont soumises. On peut qualifier cet enjeu du problème de « l'asymétrie de l'information ». Encore une fois, les technologies de l'information accentuent l'avantage que les entreprises ont sur les consommateurs en les munissant d'outils sophistiqués occasionnant un débalancement informationnel. Bien souvent, on constatera que les gouvernements interviennent par l'édiction de lois visant une certaine protection, pour rétablir un équilibre légal dans une relation contractuelle où les deux parties ne sont pas égales. Or, dans un contexte de commerce électronique, l'entreprise détient une quantité considérable d'information sur l'utilisateur qui navigue sur ses sites web. Ces informations peuvent notamment se transposer en publicités ciblées, efficaces et viennent accentuer le débalancement de pouvoir entre les entreprises et les individus[152].

L'asymétrie de l'information implique donc que les individus se retrouvent désavantagés face à ces entreprises et aucune mesure n'existe pour rétablir un équilibre adéquat. Avec les modèles d'affaires basés sur la publicité comportementale, le problème principal est lié au fait qu'il n'existe pas d'obligation de partage d'information entre les publicitaires et les utilisateurs. Par leurs renseignements de navigation, les utilisateurs créent une certaine valeur ajoutée pour les entreprises ayant recours au profilage. Par exemple, on remarque que cette richesse créée par les sujets de l'information est monopolisée par les publicitaires qui possèdent de gigantesques masses de données et aucun partage avec les individus n'est fait. Cette nouvelle utilité et valeur associées à l'information sont ensuite exploitées par les entreprises se spécialisant dans la revente d'information qui collectent massivement l'information dans le seul but de la revendre à des organismes cherchant à la commercialiser.

Pour illustrer l'enjeu d'asymétrie de l'information, il faut se rappeler que l'objectif des « *data brokers* » est de commercialiser les renseignements personnels. Ainsi, l'information est

[152] Serge GUTWIRTH et Mireille HILDEBRANDT, « Some Caveats on Profiling» dans *Data Protection in a Profiled World*, Springer, 2010, aux pages 3 et 4, en ligne : <http://www.springer.com/law/book/978-90-481-8864-2> (page consultée le 25 novembre 2015).

une matière brute que les « *data brokers* » collectent et revendent à des entreprises cherchant à raffiner cette information brute, grâce aux outils « *analytics* » (que nous étudions plus bas). À leur tour, les entreprises raffinant l'information revendront un produit basé sur les renseignements personnels, au sujet lui-même. L'enjeu d'asymétrie de l'information fait donc référence à toute l'information qui est utilisée et communiquée en arrière-scène et à laquelle le sujet de l'information n'a pas accès, ou même connaissance de son existence.

Ainsi, l'asymétrie de l'information cause un débalancement de pouvoir informationnel dans les pratiques de « *data brokerage* ». Ces entreprises qui ont pour seul objectif de collecter la plus grande quantité d'information afin de la revendre, constituent des bases de données massives portant sur les individus. D'ailleurs, on remarque que les sujets sont rarement informés qu'un dossier les concernant existe. Ainsi, on se retrouve face à une situation où de l'information quant à un sujet est agrégée, pour y donner une plus-value et ensuite revendue à d'autres entités qui vont éventuellement prendre des décisions fondées sur l'information contenue dans ces dossiers, et ce, sans que le sujet n'ait la possibilité de rectifier l'information, voire sans qu'il n'ait connaissance de son existence.

Pour pallier à cette asymétrie de l'information, on peut offrir aux sujets de l'information des munitions, sous forme de droits subjectifs, permettant de prendre connaissance de cette information. Prenons par exemple la *Loi sur la protection des renseignements personnels dans le secteur privé* qui édicte à son article 27 que :

> *« 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.*
>
> *Lorsque le requérant est une personne handicapée, des mesures d'accommodement raisonnables doivent être prises, sur demande, pour lui permettre d'exercer le droit d'accès prévu par la présente section*.»[153]

Encore selon l'idée qu'il est possible d'assurer la protection des données personnelles selon l'interprétation qu'on donne à ce concept, on constate qu'il est possible de contrer l'asymétrie de l'information par d'autres moyens. Par exemple, une perspective considérant la protection des données personnelles sous l'angle d'un droit fondamental, interprétera que les

[153] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 27, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).

asymétries de l'information engendrées par les modèles d'affaires basés sur la commercialisation de renseignements personnels ont un impact sur l'autodétermination informationnelle des individus[154]. De la même façon que pour les décisions automatisées que nous discuterons, l'autonomie décisionnelle associée au contrôle de l'information et qui est protégée par les libertés fondamentales est atteinte par les technologies de l'information qui permettent aux compagnies et aux entreprises de prendre des décisions par rapport aux individus sans que ceux-ci ne connaissent l'existence ou les modalités du traitement de leur information[155].

> « *These developments had of course direct impact on the autonomy of the data subjects: vast collections and intensive processing of data enable data controllers […] to take decisions about individual subjects on the basis of these collected and processed personal information without allowing for any possibility for the data subjects to know exactly which data would be used, for which purposes, for which duration and overall without control of the necessity of these processing […]* »[156].

Pour ces raisons, certains régimes de protection des données ont dénoté la nécessité d'établir des organismes ayant la compétence d'assurer la protection des données et de réinstaurer un certain équilibre dans les pouvoirs associés au contrôle de l'information[157]. Le rôle de ces organismes réglementaires n'est pas envisagé comme un rôle de régulateur du marché, mais plutôt en tant que champion de la protection d'un droit fondamental particulier. Ainsi, ces organismes ont une approche plus politique qu'économique quant aux enjeux associés à la protection des données[158].

Ces organismes, champions de la protection des renseignements personnels et de la vie privée, sont des organismes mis sur pied par et ayant pour principal objectif d'assurer l'application et le respect des lois portant sur la vie privée et les renseignements personnels. Au Québec, on pense notamment à la Commission d'Accès à l'Information (CAI), constituée par la *Loi sur l'accès aux documents des organismes publics et sur la protection des*

[154] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 68.
[155] Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 68,
[156] *Id*.
[157] *Id.*
[158] Jan BERKVENS, «Role of Trade Associations : Data Protection as a Negotiable Issue», dans *Reinventing Data Protection*, Springer, 2009, pp. 125-129.

renseignements personnels[159], qui a pour objectif de superviser les lois concernant l'accès à l'information et à la protection des renseignements personnels [160].

Ces mêmes organismes de protection seront souvent les gardiens gérant l'attribution de droits subjectifs aux individus. Aussi, on observera que certains régimes offrent des droits visant à améliorer la transparence des opérations liées à la constitution des gisements d'information par l'entremise de droits visant l'accès et la rectification de l'information. Ainsi, on tient pour acquis que certaines entités ont la possibilité de constituer des bases de données massives pouvant porter atteinte à la vie privée des sujets de l'information. Par conséquent et pour assurer une protection adéquate de la vie privée informationnelle des individus, on doit leur permettre de prendre connaissance de l'information les concernant, mais aussi de corriger lesdites informations ou d'en exiger le retrait lorsque des décisions peuvent être prises à partir de celles-ci. L'attribution de droits subjectifs permet donc de venir balancer le déséquilibre qui existait en raison de l'asymétrie de l'information. Ainsi, conceptualiser la protection des données par l'attribution de droits subjectifs permettra d'encadrer certains enjeux par l'attribution de droit tels des droits d'accès et de rectification.

Cette attribution de droits est fortement utile dans un contexte où la pratique de « *data brokerage* » est caractérisé par l'absence, dans la plupart des cas[161], de connaissance de la collecte d'information concernant le sujet de cette dernière. Par conséquent, l'attribution de droits subjectifs associés à la transparence joue un rôle crucial contre l'asymétrie de l'information en équipant l'individu de certains pouvoirs lui permettant de prendre connaissance de l'information qui le concerne.

2.8- Impact de l'attribution de droits subjectifs en fonction de la tradition juridique

D'ailleurs, l'impact qu'auront ces mesures attributives variera selon les différentes traditions juridiques en matière de protection des renseignements personnels. En effet, on

[159] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, en ligne : <http://canlii.ca/t/69h5j> (page consultée le 25 novembre 2015).
[160] *Id.*
[161] Dans certains cas comme Facebook, les entreprises offrant un service gratuit au consommateur obtiendront le consentement de l'individu pour la vente de données de navigation, pouvant constituer un profil, aux tiers. Toutefois, il s'agira souvent d'un consentement implicite et l'acceptation par défaut de cookies permettant de suivre les individus qui constituera la méthode de constitution de leur profil de navigation.

constate que l'adoption de lois, visant la protection des données personnelles, qui comprennent une définition large de la notion de renseignement personnel affectera la couverture des droits subjectifs en augmentant la portée des obligations de transparence sur une plus grande quantité d'information. À l'inverse, l'adoption de lois qui limitent la notion de renseignements personnels limitent, par le fait même les droits d'accès et de rectification à une définition restrictive de renseignements personnels.

Par exemple, on remarque dans les régimes similaires à celui des États-Unis une certaine motivation de la protection des données en fonction du fardeau économique que cela imposerait aux entreprises[162]. En effet, on remarque que ces régimes prévoient l'attribution de droits subjectifs, mais seulement dans certains secteurs où l'on considère l'information sensible ou manifestement identifiable[163].

Dans le même sens, on rappelle que la simple existence d'un avantage économique ne constitue pas une justification pour une intervention de l'État et qu'il serait nécessaire de démontrer qu'il existe un risque économique ou de vie privée pour justifier cette intervention[164]. Comme l'expliquent les auteurs TENE et POLONETSKY, avant d'entraver des nouveaux modèles d'affaires à première vue légitimes, il serait nécessaire d'établir que la société les considère comme étant une pratique nuisible[165].

Ainsi, on constate que peu importe où l'on se situe, les régimes balancent, chacun à leur façon, ce déséquilibre évident de pouvoir associé au contrôle de l'information[166]. Que ce soit sur le plan des libertés fondamentales ou des droits subjectifs, on encourage l'adoption de mesures venant rééquilibrer les forces en jeu. Toutefois, on note également une certaine réticence, aux États-Unis, à établir des lois qui imposeraient un fardeau indu aux entités qui utilisent l'information de façon acceptable.

---

[162] Omer TENE et Jules POLONETSKY, préc. note 59, aux pages 260 et 261.
[163] Voir supra notes 74 à 78.
[164] Ryan CALO, « Digital Market Manipulation », (2014) 82 *GEO. Wash. L. Rev*. 995, à la page 28.
[165] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 261.
[166] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40, à la page 1854.

2.9- Conclusion

La pratique du « *Data Brokerage* » est le premier modèle d'affaires que nous avons étudié. Elle consiste à l'acquisition de masses d'information, du plus de sources possible, pour éventuellement les revendre sous forme de différents services.

Au moment de la rédaction de ce mémoire, très peu d'articles discutaient en profondeur du « *Data Brokerage* ». Pourtant, la revente d'information est massive et génère des revenus significatifs. Malgré un manque d'encadrement, on constate que les lois sur la protection des données et protection de la vie privée peuvent avoir un impact sur cette pratique.

Nous avons vu que les entreprises qui opèrent dans l'industrie du « *Data Brokerage* » obtiennent des masses de données de trois sources distinctes : les registres publics, l'information disponible au public comme des renseignements publiés sur les réseaux sociaux et de l'information qui n'es pas disponible au public, par exemple, des données acquises d'un détaillant sur sa clientèle.

La collecte d'information se fait autant par l'acquisition de données imprimées, par contrats avec des vendeurs commerciaux et par la collecte systématique des informations sur internet par l'entremise de « *web crawlers* ». Ces revendeurs d'information obtiennent le consentement de leurs sources, mais ne cherchent pas nécessairement à obtenir le consentement du sujet de l'information.

Toute cette information est utilisée de plusieurs façons. Elle peut être revendue à des agences de marketing qui chercheront à établir des corrélations entre les consommateurs et leurs produits. Elle peut également être revendue à des entités qui cherchent certains renseignements spécifiques afin de minimiser leurs risques. Par exemple, une entreprise pourrait s'enquérir des différentes transactions financières opérées par un individu afin de déterminer s'il s'agit d'un fraudeur. Enfin, l'information peut également servir à vérifier l'identité d'un individu et d'obtenir de l'information quant à ses coordonnées. Cette collecte massive, contenant souvent des renseignements personnels, s'effectue sans le consentement du

sujet de l'information et ne se limite aucunement à des finalités spécifiques qui devraient être explicitées si l'on suivait les dictats des « *Fair Information Principles* ».

Nous avons vus que parmi les clients potentiels des « *data brokers* », on retrouve des employeurs, des entreprises de marketings, des institutions financières, des compagnies d'assurances, des forces de l'ordre, des investigateurs privées, des journalistes, des avocats, des services de renseignements gouvernementaux et d'autres revendeurs d'information.

Cette collecte et communication de masse renforce le problème d'asymétrie de l'information qui existe entre les entreprises et les consommateurs. Cette asymétrie réfère au pouvoir informationnel qu'une partie à sur l'autre et désavantage les individus qui n'ont pas cette information entre les mains.

Pour pallier à cette asymétrie, plusieurs juridictions ont mis sur place des organismes gouvernementaux champions de la protection des renseignements personnels et de la vie privée. Généralement ces organismes veillent à l'application et le respect des lois protégeant la vie privée et les données personnelles des citoyens. D'ailleurs, un des moyens les plus efficaces pour rétablir cette balance de pouvoir liée à l'information est de garantir un droit subjectif d'accès et de rectification aux individus.

Pour résumer, les entreprises de « *data brokerage* » exercent de la collection de masses de données. Ces données sont collectées sans discrimination et sont stockées dans le but de développer des services grâce aux capacités d' « *analytics* ». Ces services sont offerts à une gamme de clients ayant des objectifs variés. La pratique commerciale de « *data brokerage* » implique donc toute une panoplie d'acteurs, autant pour ses sources d'informations que lors de la revente. Toutefois, on constate l'exclusion d'un acteur, qui pourtant, joue un rôle central dans cette industrie de l'information, le sujet de l'information. Cette exclusion, que plusieurs constatent, est déplorable, car ce sont ces sujets qui sont à risque de dommages potentiels, que ce soit par discrimination, faille de sécurité ou invasion indue de leur vie privée.

Cette pratique de « *data brokerage* » est relativement nouvelle et peu de textes concernant les enjeux juridiques entourant cette pratique ont été publiés. L'objet de cet essai vise à mettre en lumière les éléments constitutifs de cette pratique, mais aussi de commencer à

comprendre les différentes méthodes de protection des renseignements personnels et comment ces méthodes peuvent affecter une pratique de commercialisation des renseignements personnels comme le *« data brokerage ».*

3- Cloud Computing

La deuxième pratique commerciale que nous étudierons sera celle du « *cloud computing* ». Cette pratique vaste consiste à mettre à la disposition du client un service opérable en ligne. Comme nous le verrons, les fournisseurs de services Cloud ont plusieurs modèles de services qui ne visent pas les mêmes clients et objectifs. En fonction de chacun de ces modèles, les enjeux et les caractéristiques essentielles de leur fonctionnement varient.

D'ailleurs, cette pratique a évolué significativement au cours des dernières années[167]. On constate plusieurs changements fondamentaux au sein de la pratique qui ont pour conséquence de lever de nouveaux enjeux.

3.1- Augmentation de circulation

D'abord, on constate une mutation d'échelle de grandeur de circulation des données[168]. Auparavant, les déplacements d'informations étaient unidirectionnels, il n'avait qu'une seule source et un destinataire. Dorénavant, on remarque une tendance nette à des déplacements multidirectionnels qui s'effectuent à différents paliers du traitement de l'information[169]. Cette augmentation de déplacements informationnels optimise, mais complexifie la structure selon laquelle l'information est conservée, traitée et communiquée. Pour les entreprises détenant une expertise interne et une architecture appropriée, cette complexité ne représente pas un défi aussi significatif que pour les entreprises qui traitent, communiquent et conservent de l'information de façon accessoire à leurs opérations principales.

Pour pallier à ce déficit d'expertise ou structurel, les entreprises reposent dorénavant de plus en plus sur les services Cloud afin de déléguer le fardeau opérationnel que nécessite un traitement et une conservation appropriée des données. En effet, les services Cloud permettent de réduire les couts, en déléguant le traitement et la conservation de l'information, qui seraient autrement destinés à se munir d'une expertise et d'une architecture technologique appropriée.

---

[167] Paul M. SCHWARTZ, *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*, Berkeley, The Privacy Projects, 2009.
[168] *Id.*, à la page 10.
[169] *Id.*, à la page 12.

Cette réalité rappelle notamment cette plainte soumise au *Federal Trade Commission* et ayant été réglée en 2014[170]. Dans cette décision, on explique que l'entreprise GMR, qui pratique la transcription médicale, déléguait certaines étapes du traitement de l'information médicale à un tiers dans une autre juridiction[171]. Ce sous-traitant aurait ensuite, par inadvertance, divulgué des renseignements médicaux, faute d'avoir des mesures de sécurité similaires à celles exigées par le contrat entre GMR et son client.

La décision GMR en est le témoin, la pratique de « *Cloud Computing* » a évolué par rapport aux méthodes de traitement de l'information. Alors que le traitement était traditionnellement prévisible, administratif et au sein d'une même entité ayant un contrôle sur l'information, le traitement s'inscrit dorénavant dans une série de procédés ayant pour objectifs des résultats commerciaux[172]. Cette complexification et cette croissance en termes de masse d'information circulant sur les réseaux poussent les entreprises à déléguer à des tiers la manipulation de données pouvant contenir des renseignements personnels. Comme nous le verrons, cette délégation entraîne des risques juridiques en ce qui concerne la protection des données des sujets de l'information.

Enfin, on constate également que corrélativement à cette augmentation du niveau de circulation de renseignements, il y a eu une amélioration au niveau de la prise en considération des enjeux de vie privée et de sécurité lors de l'administration des services Cloud[173].

3.2- Externalisation

Concrètement, utiliser le Cloud signifie avoir accès à un service, une plateforme ou une infrastructure à distance, dans le but d'externaliser le traitement de l'information. Cette externalisation a pour effet de garantir une accessibilité accrue, mais aussi une gestion plus

[170] *GMR Transcription Services, Inc., In the Matter of*, Federal Trade Commission, August 21st 2014.
[171] Daniel J. SOLOVE et Woodrow HARTZOG, « The FTC and Privacy and Security Duties for the Cloud », (2014) 13 *BNA Privacy & Security Law Repor*t 577, à la page 2.
[172] Paul M. SCHWARTZ, *Managing Global Data Privacy : Cross-Border Information Flows in a Networked Environment*, préc. note 167, à la page 16.
[173] *Id.*, à la page 24.

adéquate, plus experte, des ressources et du traitement de l'information[174]. Pour illustrer le concept de service Cloud, on peut se servir de l'analogie du courriel :

> «*Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer; you access it through an internet connection, and you can access it anywhere*» [175]

Ainsi, sans avoir de logiciel installé et sans traitement d'information local, il est possible d'accéder à des informations et des services à distance.

Dans le même ordre d'idées, Maureen K. OHLHAUSEN, commissaire au *Federal Trade Commission*, explique que le « *Cloud Computing* » ne se résume pas qu'à la circulation internationale de l'information. C'est également un service permettant à des partenaires économiques, géographiquement éloignés, de travailler simultanément sur le même produit[176]. Citant Paul SCHWARTZ, elle explique que le « *Cloud Computing* » offre une flexibilité considérable aux entreprises et joue un rôle significatif pour la création de nouveaux modèles d'affaires[177]. Pour résumer, « *Cloud computing is the core technology that is enabling a wide range of location-agnostic business models and consumer services* »[178].

Cette externalisation pousse les entreprises à se munir d'outils pour assurer une gouvernance adéquate l'information. En effet, afin d'éviter d'être tenu responsable pour avoir faille à un devoir ou une obligation visant la protection des données, les entreprises adoptent des meilleures pratiques quant à la gestion des données[179]. Ces meilleures pratiques visent à établir des politiques, des standards et des stratégies concernant la qualité de l'information, la vie privée, conformité légale et d'architecture technologique, le tout dans le but de minimiser

---

[174] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, Gaithersburg, U.S. Department of Commerce, 2012, à la page 2-1.
[175] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, *The Basics of Cloud Computing*, Pittsburgh, Carnegie Mellon University, 2011, à la page 1.
[176] Maureen K. OHLHAUSEN, *Remarks of Commissionner Maureen K. Ohlhausen – Forum Global*, Cloud Computing Conference, Washington DC, 2014, à la page 3.
[177] *Id*.
[178] *Id*.
[179] ORACLE, « Enterprise Information Management : Best Practices in Data Governance », *White Paper*, en ligne : <http://www.oracle.com/technetwork/articles/entarch/oea-best-practices-data-gov-400760.pdf> (page consultée le 25 novembre 2015).

les risques associés à cet externalisation du traitement et d'assurer un suivi et un contrôle sur les déplacements de l'information[180].

3.3- Délocalisation internationale

Les services Cloud ont pour objectif de délocaliser le traitement des données pour faciliter ou encore optimiser les opérations du client et du consommateur. À cet effet, on note que cette délocalisation s'effectue souvent à l'échelle internationale[181]. D'ailleurs, il est possible de distinguer les différents services Cloud en fonction de leur accessibilité, mais aussi en fonction du modèle de service offert[182].

Ainsi, en délocalisant les opérations à l'international, les solutions de « *Cloud Computing* » amènent un nouveau type de responsabilité pour les entités détenant des renseignements personnels sur des individus. Les entreprises ayant recours au *« Cloud Computing »* et qui communiquent des renseignements dans d'autres juridictions doivent maintenant s'assurer que le destinataire conservant ou traitant l'information confidentielle, personnelle, sera tenu aux mêmes obligations légales[183].

À titre d'exemple, on retrouve dans les lois québécoises des dispositions à l'effet qu'une entreprise ou organisme public doit, avant de communiquer à l'extérieur du Québec des renseignements personnels, s'assurer que les sujets des renseignements personnels bénéficieront d'une protection à tout le moins équivalente à celle prévue au Québec[184]. Autrement dit, la loi intervient et protège les sujets des renseignements personnels en prévoyant que l'entité ayant communiqué les renseignements personnels à l'étranger sera tenue responsable si elle n'a pas faite de vérification diligente.

---

[180] ORACLE, préc. note 179.
[181] Paul M. SCHWARTZ, *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*, préc. note 167, à la page 11.
[182] Grace LEWIS, *Basics About Cloud Computing*, Pittsburgh, Software Engineering Institute, Carnegie Mellon University, 2010, à la page 2.
[183] Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec*, Secrétariat du Conseil du Trésor, 2014, à la page 113.
[184] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, art. 70.1, en ligne : <http://canlii.ca/t/69h5j> (page consultée le 25 novembre 2015); *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 17 en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).

Comme nous l'avons mentionné, la protection des renseignements personnels peut se manifestée sous la forme d'intérêts protégés par le droit. Autant par les lois québécoises que nous venons de mentionner, que par les initiatives similaires au « *Safe Harbor* » européen-américain, on constate que les juridictions adoptent des moyens pour protéger localement les intérêts de vie privée et de protection des renseignements de leurs ressortissants des enjeux technologiques globaux qui accompagnent quasi-automatiquement les services de « *Cloud Computing* ».

3.4- Différents modèles

Également connue sous l'expression « *deployment models* », l'accessibilité permet de distinguer les différents services Cloud[185]. Ces modèles de déploiement peuvent être divisés en quatre catégories : les modèles privés, publics, communautaires ou hybrides[186]. Ces différents modèles impactent les caractéristiques de contrôle et de visibilité que les entreprises qui acquièrent le service Cloud délèguent à l'entreprise offrant le service Cloud[187].

Le modèle privé implique que le service Cloud est utilisé par une seule organisation. Ce service sera géré par l'organisation, un tiers ou une combinaison de ceux-ci[188]. L'accès à ce Cloud privé sera limité au groupe désigné par l'organisation[189]. Enfin, notons qu'il existe une distinction à faire en ce qui a trait à la localisation des installations physiques puisqu'il est possible d'externaliser le Cloud à un tiers résidant dans une autre juridiction[190]. En d'autres termes, le modèle privé est une externalisation d'une ou plusieurs fonctions liées au traitement de l'information. L'accès à ce nuage sera généralement destiné aux utilisateurs de

---

[185] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST Definition of Cloud Computing*, Special Publication 800-145, Gaithersburg, U.S. Department of Commerce, 2011, à la page 4;
[186] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Introduction to Cloud Computing*, Fiche d'information, Gatineau, CPVPC, à la page 2, en ligne : < https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf > (page consulté le 25 novembre 2015).
[187] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 4-3.
[188] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST Definition of Cloud Computing*, préc. note 185, à la page 3; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Introduction to Cloud Computing*, préc. note 186, à la page 2.
[189] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, préc. note 175, à la page 2.
[190] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 4-7.

l'organisation qui externalise ses opérations et qui aurait autrement eu accès à ces fonctions à l'interne.

De la même façon qu'un Cloud privé, le Cloud communautaire est un service visant un groupe restreint d'organisations (deux ou plus) ayant les mêmes besoins en matière de service Cloud[191]. Pareillement, la gestion pourra être externalisée ou administrée localement, en fonction des besoins et ressources de la communauté.

Bien que le nombre de parties impliqués dans un modèle privé ou communautaire soit relativement limité, il est nécessaire d'établir un schéma organisationnel clair afin de bien évaluer qu'elles sont les responsabilités qui sont attribuables aux parties impliquées. À titre d'exemple, si l'entreprise qui externalise ses fonctions liées au traitement de l'information fait affaires avec un tiers pour conserver de l'information confidentielle ou des renseignements personnels, il faudra s'assurer d'obtenir les autorisations nécessaires de la part des individus fournissant l'information ou étant sujet de l'information. De plus, il est de bonne pratique d'obtenir, par le biais d'une convention avec le sous-traitant, une garantie que ce sous-traitant sera responsable au même titre que l'entreprise qui externalise ses fonctions liés au traitement de l'information.

Pour sa part, le Cloud public sera nécessairement contrôlé, opéré et administré par une entreprise tierce à l'utilisateur visé par le service[192]. L'accès au Cloud public sera ouvert à tout utilisateur ou consommateur, inscrit ou abonné au service, muni d'une connexion internet pour accéder au nuage[193]. Enfin, le Cloud hybride est une structuration plus complexe regroupant deux des modèles mentionnés (privé, public, communautaire), ou plus[194].

Les services Cloud public et hybride doivent, comme le modèle privé ou communautaire, s'assurer d'obtenir les autorisations nécessaires à la lumière du nombre d'intervenants pour fournir l'ensemble du service Cloud. Toutefois, les services publics

[191] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Introduction to Cloud Computing*, préc. note 186, à la page 2.
[192] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST Definition of Cloud Computing*, préc. note 185, à la page 7.
[193] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, préc. note 175, à la page 2.
[194] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174.

doivent également répondre à un autre ordre de complexité provenant du fait que le service Cloud est offert au grand public. On pense notamment aux questions liées à l'accessibilité au service, la responsabilité en cas de défaut technique, la communication de renseignements personnels et confidentiels à des tiers autorisés, et enfin l'obtention d'un consentement libre et éclairé pour un contrat qui sera probablement d'adhésion et de consommation.

3.5- Différents Services

Parallèlement à ces modèles de services, il existe trois différents services offerts par les fournisseurs de Cloud : le « *Software as a Service* » (SaaS), le « *Platform as a Service* » (PaaS) et le « *Infrastructure as a Service* » (IaaS)[195]. La principale distinction entre ces services est le niveau de contrôle accordé au consommateur[196]. Cette distinction est importante, car elle permet de départager les parts de responsabilités entre le fournisseur de service et les utilisateurs[197]. Il est donc nécessaire d'identifier le type de service Cloud avant de s'avancer sur les responsabilités des différents acteurs[198].

On peut décrire le service de « *Software as a Service* » (SaaS) comme étant un logiciel déployé en tant que service hôte accessible par l'Internet[199]. Plus communément, on peut également référer à ce type de service comme étant un service web. De façon générale, le « *Cloud Computing* » repose sur la location de ressources informatiques[200]. Dans ce modèle d'affaires, les entreprises louent l'accès à une application et la majorité du traitement de l'information est fait sur le serveur Cloud du fournisseur[201]. Ainsi, les utilisateurs n'ont qu'un contrôle limité sur l'information qui se retrouve sur le Cloud, alors que le fournisseur a un

[195] CISCO, *Cloud : What an Enterprise Must Know*, White Paper, San Jose, Cisco, 2011, à la page 1; CISCO, *Networking and Cloud: An Era of Change*, White Paper, San Jose, Cisco, 2011, à la page 1.
[196] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, préc. note 175, à la page 2.
[197] *Id*.
[198] Pour plus de détails sur les obligations généralement associées au « *Cloud Computing* » voir : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174.
[199] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 5-1.
[200] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 5-1.
[201] *Id*., à la page 5-2.

contrôle administratif sur cette dernière et un contrôle total sur le système d'opération et sur le matériel physique[202].

Ensuite, le service de « *Platform as a Service* » (PaaS) s'exécute à un niveau plus élevé que le SaaS. Le fournisseur de service PaaS offre à ses clients les outils et les composantes nécessaires pour le développement et pour opérer efficacement des applications par Internet[203]. Les consommateurs de PaaS ont donc un contrôle plus avancé, car ils disposent d'outils pour développer eux-mêmes les applications traitant l'information[204].

Enfin, le service de « *Infrastructure as a Service* » (IaaS) pourrait être décrit comme étant le service offrant le plus de contrôle au consommateur. En effet, le fournisseur de service IaaS ne contrôle que les composantes matérielles nécessaires au fonctionnement du service[205]. Grâce à la création de machines virtuelles, le consommateur a donc à sa disposition une machine configurable selon ses désirs[206].

Comme nous le voyons, il existe une grande variété de combinaisons selon le mode de déploiement et du service offert, dans l'objectif de personnaliser en fonction de ses besoins, un service Cloud. Ainsi, le consommateur de service Cloud pourra choisir à la lumière des avantages et désavantages de chaque modèle d'affaires[207]. Ces modèles permettront ensuite aux consommateurs de bénéficier de systèmes permettant le stockage « de l'information et/ou d'applications en ligne, de manière à permettre à un utilisateur d'y accéder à partir de n'importe quel dispositif »[208]. Néanmoins, cette nouvelle technologie donne naissance à certaines considérations d'ordre juridique, qui ne peuvent être ignorées[209].

---

[202] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 5-3.
[203] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, préc. note 175, à la page 3.
[204] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 6-4.
[205] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, préc. note 175, à la page 3.
[206] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174, à la page 7-6.
[207] Pour plus de détails sur les avantages et désavantages de chaque modèles voir : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations,* préc. note 174.
[208] Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, préc. note 183, à la page 6.
[209] *Id*.

3.6- Risques associés aux différents services?

Une offre de services en « *Cloud Computing* » comporte également des enjeux pouvant relever de lois autres que des lois visant à protéger les données personnelles et la vie privée. On pense notamment à la loi québécoise, *Loi concernant le cadre juridique des technologies de l'information*[210], qui établit certains devoirs légaux. Citons, par exemple, l'accessibilité, l'intégrité et la confidentialité de l'information.

L'accessibilité des documents suppose que les documents détenus par une entité doivent être « *accessibles dans les délais convenables pour les personnes autorisées à en disposer dès qu'elles le désirent* »[211]. Cette obligation d'accessibilité à l'information n'est pas limitée aux renseignements personnels, elle concerne tout document auquel un individu à un droit d'accès. Ainsi, au Québec, les entreprises recourant au « *Cloud Computing* » ont un devoir de rendre disponible tout document qui se retrouve en leur possession et auquel un individu a le droit d'accéder. Par ce mécanisme de la responsabilité, le droit vient protéger l'intérêt que les individus ont à accéder à leurs documents.

L'intégrité des documents technologiques est un second exemple d'obligation ne relevant pas directement de la protection de la vie privée ou des renseignements personnels. Lorsqu'elle conserve des documents pour ses utilisateurs, l'entreprise offrant des services de « *Cloud Computing* » doit maintenir l'intégrité du document, c'est-à-dire, adopter des moyens pour assurer que l'information d'un document n'est pas altérée et qu'elle est maintenue dans son intégralité, l'information contenue dans le document est stable et son support garantie une certaine pérennité[212].

Enfin, la conservation de documentation suppose le respect de l'obligation de confidentialité des documents technologiques. Cette confidentialité concerne manifestement les renseignements personnels, mais s'étend à tout autre document de nature confidentielle[213].

---

[210] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, en ligne : <http://canlii.ca/t/q5zn> (page consultée le 25 novembre 2015).
[211] Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, préc. note 183, à la page 85.
[212] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, art. 6, en ligne : <http://canlii.ca/t/q5zn> (page consultée le 25 novembre 2015).
[213] Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, préc. note 183, à la page 96.

En effet, la notion de renseignement confidentiel est plus large que celle de renseignement personnel. Au Québec, la loi impose que :

> « *[l]a personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.* »[214]

Pour résumer, l'obligation de confidentialité suppose un contrôle des droits d'accès servant à assurer que seuls les individus autorisés puissent accéder un document.

En plus de ces obligations légales d'accessibilité, d'intégrité et de conservation, les entreprises recourant à un modèle d'affaire ou structurel basé sur les services Cloud doivent également respecter les diverses lois visant la protection de la vie privée, et incidemment, des renseignements personnels pouvant être contenues dans les données. À titre d'exemple, la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit les circonstances selon lesquelles il sera autorisé ou interdit de collecter des renseignements personnels[215]. Cette loi prévoit également les règles concernant la communication de ces informations aux tiers et les droits d'accès étant conférés aux sujets de l'information[216].

Les entreprises faisant défaut de se conformer aux dispositions de cette loi sont également passibles d'une amende. En effet, une loi est aussi efficace que l'effet dissuasif ou incitatif qu'elle peut avoir sur les acteurs qu'elle vise à réglementer. Pour cette raison, une loi cherchant à établir un standard ou une norme à laquelle des acteurs privés doivent se conformer, cherchera généralement à prévoir des dispositions pénales pouvant sanctionner certains acteurs récalcitrants. *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit des pénalités qui varient entre 1 000 $ et 100 000 $, en fonction de la gravité de l'infraction et de s'il s'agit d'une récidive ou d'une première offense[217].

---

[214] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, art. 25, en ligne : <http://canlii.ca/t/q5zn> (page consultée le 25 novembre 2015).
[215] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 4 à 9, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).
[216] *Id*., art. 10 à 41.
[217] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 4 à 9, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).

Évidemment ce type de responsabilité statutaire s'ajoute à toute responsabilité contractuelle et extracontractuelle s'appliquant aux entreprises utilisant les services Cloud, selon le cas.

3.7- Conclusion

Dans cette section nous avons remarqué qu'il y avait un constat à l'effet que les services Cloud étaient de plus en plus courants et nécessaires aux entreprises. Ils servent à optimiser leurs services et à demeurer compétitif. Cette nécessité de recourir à ces services provient du fait que la technologie évolue, se complexifie et nécessite une sophistication accrue. Pour cette raison, les entreprises ont souvent besoin de déléguer certaines fonctions du traitement de l'information à des tiers.

Les modèles de services Cloud sont variés et nombreux. En fait, chaque façon d'externaliser un service ou une fonction comble un besoin spécifique pour l'entreprise. Parmi ces besoins on retrouve notamment l'obtention d'une expertise nécessaire, la réduction des coûts et l'accès à une architecture technologique fiable. Ainsi, plusieurs modèles se sont créées : privés, publics communautaires et hybrides. D'ailleurs les services varient également en fonction du contenu du service. Par exemple, certains modèles offrent « *Software as a Service* », « *Platform as a Service* » ou « *Infrastructure as a Service* ». La pratique de « *Cloud Computing* » est définitivement très large et se découpe en plusieurs embranchements, chacun ayant ses propres caractéristiques.

Nous avons vu que cette pratique implique certaines responsabilités quant aux garanties offertes aux utilisateurs de services Cloud et à aux standards de surveillance et contrôle de la sous-traitance. Ces obligations légales que nous avons survolées sont d'autant plus nécessaires puisque le « *Cloud Computing* » est, dans sa nature même, une décentralisation, parfois internationale, des opérations d'une entreprise dans un contexte global.

Nous avons également vu que les services Cloud devaient également jongler avec des enjeux relevant de lois autres que celles visant à protéger la vie privée. Par exemple, la loi québécoise, *Loi concernant le cadre juridique des technologies de l'information,*

responsabilise les fournisseurs de services quant à l'accessibilité, l'intégrité et la confidentialité de l'information.

En plus de ces diverses responsabilités, les services Cloud doivent respecter les lois sur la protection des renseignements personnels. Ces lois fournissent généralement des balises quant à la collecte, la conservation, le traitement et la communication des renseignements personnels. De plus, nous avons souligné que ces lois prévoient des dispositions pénales afin de dissuader et inciter les différents acteurs à respecter la loi.

Pour résumer, le « *Cloud Computing* » est une pratique commerciale qui repose essentiellement sur le stockage et l'accessibilité à l'information à distance. Ces nouvelles capacités sont toutes issues du développement des technologies de l'information. Autant la rentabilisation des procédés, que leur complexité croissante, font en sorte que de plus en plus d'entreprises ont recours à des services tiers pour externaliser la collecte, le traitement ou la conservation des données.

4- Les outils « *analytics* » ou « *Big Data* »

Les avancées technologiques ont permis à l'homme d'enregistrer des masses d'informations sur des supports efficaces. La gestion de l'information se révèle de moins en moins couteuse et par conséquent, la possibilité de collecter, de traiter et de conserver des renseignements n'a jamais paru aussi simple. Les entreprises et les individus se retrouvent donc face à d'énormes gisements de données qui nécessiteraient plus d'une vie pour qu'un seul individu les analyse. C'est à cette réalité que réfère le phénomène de « *Big Data* » : l'être humain collecte et conserve des renseignements qu'il lui aurait été impossible de traiter dans leur totalité s'ils avaient été sur support papier. Toutefois, malgré cette quantité effarante d'information, le « *Big Data* » permet aux individus de traiter efficacement celle-ci afin de la transformer en connaissance utilisable.

4.1- Qu'est-ce que le Big Data?

Le phénomène du « *Big Data* » réfère à cette aptitude à massivement collecter, traiter, conserver des données. Ces différentes utilisations s'exécutent massivement et permettent de déduire de la connaissance à partir de masses de données. On définit d'ailleurs ce phénomène comme référant à trois concepts de manipulation des données :

> « *[F]irst, it refers to technology that maximizes computational power and algorithmic accuracy; second, it describes types of analysis that draw on a range of tools to clean and compare data, and third, it promotes a certain mythology – the belief that large data sets generate results with greater truth, objectivity, and accuracy* »[218].

Ainsi, il est possible de concevoir le « *Big Data* » comme étant l'utilisation des nouvelles technologies, sans pareil dans l'univers papier, dans le but de permettre un traitement efficace des données et dans l'espoir d'arriver à des conclusions réelles et objectives, invisibles à l'œil humain.

Au sein de cette définition de « *Big Data* », on réfère, entre autres, aux outils qui permettent le traitement efficace de l'information. Ces outils sont en fait le concept d' « *analytics* » auquel nous avons référé plus tôt. Paul SCHWARTZ explique d'ailleurs que cet outil «*refers to the use of information technology to harness statistics, algorithms, and other tools of mathematics to improve decision-making. A wide variety of organizations use*

[218] Kate CRAWFORD et Jason SCHULTZ, « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms », (2013) 55 *B.C.L. Rev.* 93, à la page 5.

analytics to convert data to actionable knowledge»[219]. Donc, on comprend que ces procédés statistiques, algorithmiques ou mathématiques, permettent aux entreprises et aux individus de créer une certaine richesse à partir des nombreuses informations collectées.

Toute cette connaissance, si facilement acquise, n'est pas sans revers. Les technologies permettent effectivement de générer de la connaissance à partir de données. Toutefois, comme le soulignent les auteurs GUTWIRTH et HILDEBRANDT, cette façon de traiter l'information constitue une rupture avec l'approche analytique traditionnelle, notamment au niveau de la recherche de corrélations entre un comportement et la raison de celui-ci[220].

En effet, les auteurs constatent que traditionnellement, la connaissance précède la collecte de l'information. La connaissance aurait d'abord été formulée par des hypothèses, qui seraient ensuite confirmées ou invalidées à partir des données qui seront récoltées. À l'inverse, l'approche actuelle, permise par les technologies de l'information, consiste à observer les gisements d'information pour détecter les corrélations, sans avoir à formuler une quelconque hypothèse[221]. On observe un comportement, des tendances, pour ensuite formuler des hypothèses quant à leur raison d'être. Ainsi, le traitement automatisé de l'information retire la recherche de fondements sous-jacents à une corrélation et ne permet que de tirer des conclusions superficielles sur les individus. Bien que cette façon de faire rompt avec la tradition, cela ne veut pas dire pour autant que le « *Big Data* » ne peut s'avérer utile.

4.2- Profils et renseignements personnels

Dans le domaine de la publicité, les outils « *analytics* » permettront de conclure qu'un individu se classe dans une catégorie, un profil, qui est caractérisé par un type de comportement. Ce comportement type sera utilisé pour mieux cibler le consommateur par la publicité. Toutefois, comme l'expliquaient GUTWIRTH et HILDEBRANDT peu de réflexion portera sur les raisons justifiant le comportement, puisqu'elle se concentre principalement sur

[219] Paul M. SCHWARTZ, *Data Protection Law and the Ethical Use of Analytics*, Berkeley, The Centre for Information Policy Leadership, 2010, à la page 2.
[220] Serge GUTWIRTH et Mireille HILDEBRANDT, préc. note 152, à la page 1.
[221] *Id*, à la page 2.

l'identification de comportement[222].Les entreprises faisant de la publicité comportementale s'organisent pour regrouper et classifier des comportements en différentes catégories grâce au traitement probabiliste de l'information qu'elles récoltent[223]. Ces diverses catégories sont des profils.

On reconnait d'ailleurs que le profilage est de plus en plus présent dans l'industrie de la publicité en ligne[224]. Contrairement à ce qui était traditionnellement possible, la technique de profilage est relativement simple et peu couteuse. En effet, les réseaux électroniques sont constamment en expansion, la quantité d'information récoltée augmente, mais surtout, s'accumule[225]. Cette accumulation d'information existe en raison de la facilité de la collecte et de la conservation des données, mais est accentuée par la vente et l'échange de ces bases de données.

Dans le domaine de la publicité, les profils se baseront généralement sur des données agrégées des transactions, des déplacements et des intérêts des individus[226]. Ce suivi était traditionnellement effectué par l'entremise de cookies qu'un site web plaçait sur l'ordinateur lors de la consultation. Par contre, on constate que les techniques évoluent constamment et qu'elles deviennent de plus en plus sophistiquées[227]. Par voie de conséquences, les dossiers digitaux constitués sont également plus précis.

Ces profils digitaux sont donc conçus à partir des renseignements des individus. Dans le domaine de la publicité en ligne, les renseignements collectés pour cibler le consommateur sont variés. Les méthodes de collecte le sont également. Ainsi, il s'en vient à se poser la question de savoir si les renseignements collectés sont des renseignements personnels au sens de la loi. Encore, est-ce que les profils constitués à partir de ces renseignements peuvent être qualifiés de renseignements personnels. Selon le régime juridique, la qualification de

[222] Les auteurs GUTWIRTH et HILDEBRANDT expliquent que ce procédé permet certainement de rendre visible à l'oeil humain, ce qui lui était invisible, mais en retour, rend invisible ce qui ne peut être analysé par les machines.
[223] Serge GUTWIRTH et Mireille HILDEBRANDT, préc. note 152, à la page 1.
[224] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Advice Paper on Essential Elements of a Definition and a Provision on Profiling Within the EU General Data Protection Regulation,* Advice Paper, Bruxelles, 2013, à la page 3.
[225] Serge GUTWIRTH et Mireille HILDEBRANDT, préc. note 152, à la page 1.
[226] Chris EVANS, « It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age », (2012) 13 *Minn. J.L. Sci. & Tech*. 867, à la page 879.
[227] *Id*., à la page 880.

renseignement personnel sera portée à varier et il n'y a pas de standard international permettant de simplifier la question. Notons que la Commission d'Accès à l'Information s'interroge justement sur la possibilité d'encadrer le profilage et le traitement massif de mégadonnées[228].

4.3- Anonymisation des renseignements personnels et profilage

Malgré le fait que la qualification de renseignement personnel ait été débattue de long en large, il demeure beaucoup d'incertitude. Toutefois, « *Big Data is coming, like it or not. We have an opportunity to shape it, to ensure it operates for us, not on us* »[229]. Dans le but d'atteindre un niveau raisonnable de certitude, certains ont cherché la solution / éviter le problème en tentant d'anonymiser les renseignements personnels afin d'obtenir des profils anonymes.

Sur le plan juridique, le profilage comporte certains enjeux lorsque les données collectées, traitées et conservées, sont qualifiées de renseignements personnels. Conséquemment, les modèles d'affaires reposant sur les « *analytics* » soulèvent la question à savoir si l'anonymisation constitue une solution technique, à un enjeu juridique. Comme nous l'avons expliqué, le profilage ne cherche pas nécessairement à identifier un individu, mais plutôt à le catégoriser en fonction des renseignements collectés. Le produit de la classification est donc, en quelque sorte rendu anonyme. Toutefois, le débat à savoir si les données anonymisées doivent être soumises à l'application des lois sur la protection des renseignements personnels persiste.

Dans le domaine de la publicité en ligne, il existe un risque que certains auteurs qualifient de « *Incremental Effect* »[230]. Ce risque est intimement lié au contexte technologique actuel. Il réfère notamment à l'accroissement constant d'information en ligne. Les informations contenues dans une base de données relient parfois des renseignements anonymes à des renseignements personnels pouvant notamment identifier des individus. Plus

---

[228] Vincent GAUTRAIS, « Rapport auprès de la Commission d'accès à l'information (CAI) », *Gautrais.com*, en ligne :<https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/ > (page consultée le 15 décembre 2015).
[229] Paul OHM, « The Underwhelming Benefits of Big Data », (2012) 161 *U. Pa. L. Rev*. 339, à la page 346.
[230] Omer TENE et Jules POLONETSKY, préc. note 59.

on possède une grande quantité d'information, plus il est facile de relier des renseignements anonymes à d'autres renseignements considérés anonymes, pour ensuite les attacher à un individu. Alors que dans l'univers papier, des renseignements pris isolément demeuraient isolés en ce qu'il serait trop laborieux de traiter manuellement une base de données aussi énorme que le web, le contexte technologique actuel permet au risque d'« *incremental effect* » de se matérialiser. Ainsi, même un renseignement isolé peut être collecté, conservé, pour ensuite être recroisé avec d'autres renseignements et, éventuellement, être relié à un individu identifiable.

L'auteur Paul OHM redoute que cet « *incremental effect* » mène à une base de données des ruines[231]. Il explique qu'un renseignement anonyme, une fois rattaché à un individu identifiable, faciliterait le rattachement et l'identification subséquente d'autres renseignements théoriquement anonymes. Plus il existera d'informations sur l'individu, plus il sera facile de le relier à ses activités anonymes. L'exemple le plus souvent cité est celui de l'étude exercée par les chercheurs NARAYANAN et SHMATIKOV[232]. Dans cette recherche, ils ont démontré qu'il était possible de réidentifier des commentaires anonymes du site IMDB[233] à partir des commentaires et des notes laissées sur Netflix[234]. Ainsi, après avoir procédé à ce référencement croisé, il était possible d'affirmer que l'utilisateur *étudiant7382* était en fait, Michael Chevalier. Par conséquent, chaque renseignement que l'on retrouvera divulgué sous le pseudonyme anonyme de *étudiant7382* ne sera plus anonyme, mais attribuable à l'individu Michael Chevalier.

Par conséquent, les lois utilisant une définition large du concept de renseignement personnel se retrouveraient à couvrir un large éventail de données menant à l'identification indirecte des individus. De plus, comme plusieurs lois européennes, le texte de la Loi fédérale sur la protection des renseignements personnels définit les renseignements personnels de la façon suivante : « *Les renseignements, quels que soient leur forme et leur support, concernant*

---

[231] Paul OHM, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », (2010) 57 *UCLA Law Review* 1701, à la page 1705.
[232] Arvind NARAYANAN et Vitaly SHMATIKOV, « Robust De-anonymization of Large Sparse Datasets », (2008) *Proc. 29th IEEE Symp. on Security & Privacy* 111.
[233] INTERNET MOVIE DATABASE (IMDB), en ligne : < http://www.imdb.com/> (page consultée le 10 avril 2014).
[234] NETFLIX, en ligne : < http://www.netflix.com/> (page consultée le 10 avril 2014).

un individu identifiable »[235]. Suivant la logique du risque d'« *incremental effect* » et à la lumière du texte de la loi, la quasi-totalité des renseignements publiés sous un pseudonyme pourrait éventuellement être qualifiée de renseignements personnels et se voir imposer les critères de protection édictés par la loi. Puisque Netflix serait en mesure, à partir de sa base de données privée, d'identifier un pseudonyme, ce pseudonyme, ainsi que les renseignements qui lui sont associés seraient alors des renseignements personnels puisqu'ils se rapportent à un indvidu identifiable. Ainsi, le même renseignement, en fonction de l'individu, pourra devenir un renseignement personnel. Il semble donc y avoir une certaine incongruité au niveau de cet enjeu et par rapport à son encadrement légal. Pis encore, l'adoption d'une définition large ou restrictive des renseignements personnels influerait également sur la qualification du renseignement.

Ce risque incrémental persiste pour les modèles d'affaires commercialisant les renseignements personnels pour des tiers publicitaires, puisque ces-derniers accumulent des bases de données de renseignements qui, à première vue, ne permettent pas d'identifier des individus. Toutefois, advenant cette base de données des ruines telle que décrite par OHM, ces renseignements pourraient être sujets aux lois de protection des renseignements personnels.

En ce sens, Paul OHM critique la dé-identification et constate une perte de confiance envers l'anonymisation, surtout après des études comme celle impliquant Netflix et IMDB[236]. À l'inverse, d'autres auteurs expliquent que les risques qui ont mené à la perte de confiance envers l'anonymisation ont été mal interprétés et sont théoriques[237], et font la remarque que les avantages de l'anonymisation supplantent les désavantages techniques qu'on lui associe[238].

C'est à cette étape qu'il est possible de constater un choc des différentes conceptions de ce qu'est la protection des données. À la lumière de ce risque d' « *incremental effect* », les régimes qui conçoivent la protection des données comme étant un droit fondamental et qui adoptent une définition large de ce qu'est un renseignement personnel ont pour conséquence de rendre l'outil d'anonymisation inutile, puisque tous ces renseignements mèneraient

[235] *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, art. 2.
[236] Paul OHM, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », préc. note 231; Paul OHM, « The Underwhelming Benefits of Big Data », préc. note 229.
[237] Jane YAKOWITZ, « Tragedy of the Data Commons », (2011-2012) 25 *Harv. J. L. & Tech.* 1.
[238] *Id.*; Paul M. SCHWARTZ, « Information Privacy in the Cloud *»,* (2013) 161 *U.PA. L. Rev.* 1623.

éventuellement à permettre l'identification d'un individu. Sous une telle approche, l'anonymat est placé en opposition à l'identification et agit comme critère de qualification de renseignement personnel. À l'inverse, une approche où la protection des données est un intérêt protégé par le droit, l'anonymisation est présentée comme étant un outil protégeant, ou maximisant, la protection de la vie privée informationnelle.

À titre d'exemple, il existe un projet de loi américain visant à promouvoir la transparence dans l'utilisation commerciale de renseignements personnels[239]. Ce projet date de 2011 et n'a pas été adopté. Un aspect intéressant de ce projet de loi américain est prévu à la section 501. On y édicte que rien dans l'acte ne peut empêcher une entreprise de collecter, d'utiliser et de divulguer des renseignements sensibles si ces derniers sont anonymisés. Cette exemption est toutefois sujette à certains critères, mais il n'en demeure pas moins que cette disposition aurait créé un effet considérable sur le rôle de l'anonymisation des renseignements personnels comme solution aux enjeux de vie privée informationnelle.

On comprend que les enjeux comme l'anonymisation sont des outils qui semblent de prime à bord utiles, mais qui soulèvent plusieurs questions quant à leur efficacité. Cette hésitation à adopter ces outils découle des multitudes conceptualisation de ce que constituent la vie privée et la protection des données.

D'ailleurs, certains textes recommandent une redéfinition complète du concept de vie privée. En effet, on explique que le changement de contexte technologique est si percutant qu'on ne peut transposer des principes élaborés à une époque où on ne pouvait concevoir la possibilité d'utiliser le « *Big Data* » comme un outil décisionnel au sein d'une entreprise. Pour illustrer ses propos, un auteur explique que la distinction entre les renseignements identifiables et non identifiables crée une course inefficiente pour la détermination de la protection de l'individu concerné[240]. Il suggère comme remplacement un régime qui serait basé sur le risque

[239] H.R. 611 - 112th Congress (2011).
[240] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 258.

de préjudice et qui prendrait en compte divers facteurs qui intégreraient les FIPs, de façon efficace et à ne pas entraver l'innovation de l'industrie[241].

On se retrouve donc devant plusieurs possibilités de rôles que peut jouer l'anonymisation au sein des régimes de protection des renseignements personnels. D'un côté on constate une tendance à discuter de la portée des définitions de renseignements personnels pouvant couvrir les renseignements anonymisés selon le contexte, et d'un autre côté, on note une tendance à minimiser ce risque théorique et à faciliter un traitement de l'information qui prend en considération les enjeux de vie privée, mais aussi les réalités économiques et pratiques des entités traitant ces informations.

Malgré ce débat quant au rôle que doit jouer l'anonymisation dans la protection des renseignements personnels, il semble y avoir un consensus quant à l'interdiction de réidentifier des banques de données ayant été anonymisées[242]. Comme l'explique Paul OHM, les enjeux reliés à l'anonymisation sont trop élevés pour permettre d'accepter la réidentification, même sans préjudice apparent :

> *«Entropy formalizes the accretion problem. We should worry about reidentification attacks that fall short of connecting anonymized data to actual identities, and we should worry about reidentification attacks that do not reveal sensitive information. Even learning a little benign information about a supposedly anonymized target reduces entropy and brings an evil adversary closer to his prey»*[243].

En conclusion, l'anonymisation des données se présente donc comme un enjeu significatif en ce qui concerne la protection des données. Selon le type de régime de protection des données, l'anonymisation jouera un rôle différent et cela pourrait éventuellement avoir un impact sur les services basés sur la commercialisation de l'information qui collectent et traitent massivement des informations pour les divulguer sous une forme anonyme. Considérant que les modèles d'affaires basés sur la commercialisation des renseignements progressent de plus en plus en rapidement, il sera nécessaire d'établir des balises légales

---

[241] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 258; Paul OHM, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », préc. note 231, à la page 1765.
[242] Paul OHM, « Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization », préc. note 231, à la page 1746.; Jane YAKOWITZ, préc. note 237, à la page 49.
[243] Paul OHM, « Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization », préc. note 231, à la page 1749.

concernant le rôle que doit jouer l'anonymisation dans la protection des données. Cet enjeu est d'autant plus critique puisque l'anonymisation peut s'avérer comme outil efficace malgré les risques de dé-identification qui existent.

Avec égards au potentiel de l'anonymisation des renseignements, il faut toutefois s'interroger à savoir si une telle opération technique est nécessaire pour tous les types de profils constitués. En effet, la qualification de renseignement personnel pourrait varier en fonction des différentes méthodes de profilage.

4.4- Méthodes de profilage

Pour tracer les profils, les sites web utilisent principalement des cookies. On estime d'ailleurs que plus de 90 % des sites web ont recours à cette pratique[244]. Expliqué simplement, le cookie est un document texte placé sur l'ordinateur de l'utilisateur qui stocke les renseignements de navigation de l'utilisateur. Lorsque l'utilisateur retournera sur le site en question, le cookie sera récolté et, par le fait même, les renseignements de navigation de la dernière visite. Il offre donc la possibilité de retracer la navigation d'un utilisateur sur une période prolongée et même sur un grand éventail de sites web[245].

Il existe différents types de cookies. On retrouve notamment les cookies de session, les cookies persistants, les cookies internes, les cookies des tiers et les supercookies[246]. Le cookie de session est un cookie éphémère qui expire lorsque l'utilisateur éteint son navigateur. Chaque visite sur le site engendrera donc la création d'un nouveau cookie. Ce faisant, le cookie de session ne trace pas sur de longues périodes de temps et n'est pas invasif sur le plan de la collecte de renseignements par le site web.

Par opposition, les cookies persistants ne s'effacent pas lorsque l'utilisateur ferme son navigateur. Ils demeurent sur le disque dur et seront chargés lors de la connexion subséquente au site émetteur du cookie. Chaque cookie étant unique à l'utilisateur associé, le cookie permet au site web de reconnaître l'individu et de rappeler les informations qu'il avait insérées lors de

[244] Abdelmadjid ABDELKAMEL, *Facebook et les dispositifs de traçabilité vus sous l'angle du droit canadien*, mémoire de maîtrise en droit des technologies de l'information, Montréal, Université de Montréal, 2013, à la page 19.
[245] *Id*.
[246] *Id*., à la page 20.

sa première visite. Autant les paramètres (langues, préférences) que les noms d'utilisateurs et mots de passe pourront alors être sauvegardés.

Enfin, on distingue également les cookies quant à l'entité qui les place sur le disque dur. Cette distinction réfère aux cookies internes et de tiers. On dira qu'un cookie est interne (« *first party cookie* ») lorsqu'il proviendra du site web visité[247]. Les entreprises ayant recours à ces cookies visent généralement à offrir des services spécialisés en fonction des habitudes de navigation de leurs utilisateurs. Plus précisément, les entreprises peuvent constituer des profils à partir de ces données de navigation pour ensuite vendre des espaces publicitaires à des tiers en fonction de ces profils. À titre d'exemple, Facebook ne vend pas les renseignements collectés aux tiers, mais vend des espaces publicitaires en fonction du profil ou caractéristiques d'un individu[248].

À l'inverse, on qualifiera le cookie comme provenant d'un tiers (« *third-party cookie* ») lorsqu'il proviendra d'une source différente du site web visité[249]. Bien souvent, les espaces publicitaires sur les sites web visités sont administrés par un tiers publicitaire. Ces derniers achètent ces espaces pour faire la promotion de différents produits. Ainsi, le tiers publicitaire place un cookie sur le disque dur de l'utilisateur. Pour chaque site que l'individu visitera, où le publicitaire est affilié, le cookie permettra de tracer les habitudes de navigation sur ces différents sites web. Ces informations serviront ensuite à suggérer de la publicité en fonction des habitudes de l'utilisateur. Pour illustrer cette pratique, il suffit de penser au moteur de recherche Google. Depuis l'acquisition du publicitaire Doubleclick par Google en 2008, on estime qu'environ 70 % des publicités que l'on observe sur le web sont administrées par Google[250]. Ainsi, les profils constitués à partir de ces habitudes de navigation doivent être particulièrement précis et exacts.

---

[247] Abdelmadjid ABDELKAMEL, préc. note 244, à la page 22.
[248] FACEBOOK, « Facebook's Privacy Policy - Full Version », en ligne : <https://www.facebook.com/note.php?note_id=%20322194465300> (page consultée le 10 avril 2014).
[249] Abdelmadjid ABDELKAMEL, préc. note 244, à la page 22.
[250] SEARCH ENGINE WATCH, « Google + DoubleClick = 69% of Online Advertising Market », en ligne : <http://searchenginewatch.com/article/2054513/Google-DoubleClick-69-of-Online-Advertising-Market> (page consultée le 10 avril 2014).

Enfin, le supercookie réfère à la pratique d'enregistrer les pages web et les renseignements de l'utilisateur dans le «cache» de l'ordinateur[251]. Ce faisant, il est plus difficile de se débarrasser complètement de ces cookies, car même après avoir effacé le registre des cookies, ces supercookies demeurent sur l'ordinateur. On comprend toutefois que cette pratique a pour objectif de réduire le chargement des pages web et n'est pas nécessairement utilisée dans le domaine de la publicité en ligne.

On comprend donc que le type de renseignements collectés est partiellement conséquent du type de cookie utilisé. En effet, un cookie tiers qui s'insère dans le « cache » de l'ordinateur et analyse les données d'un internaute, individualisé, à travers différents sites web, collecte des renseignements beaucoup plus précis et susceptibles d'être qualifiés de renseignements personnels qu'un simple cookie de session qui n'analyse que le comportement d'une session donnée.

4.5- La finalité des profils – nouveaux modèles d'affaires

Les outils « *analytics* » permettent donc de traiter une quantité considérable d'information, pouvant notamment être générée par les cookies, pour la traduire en renseignements pertinents et en connaissances. Toutefois, ce savoir accumulé ne vise pas nécessairement à établir l'identité d'un individu, mais plutôt à constituer des profils types dans lesquels il sera possible de classifier les consommateurs. Grâce à ces profils, le publicitaire sera en mesure de modifier la nature de la publicité qui sera présentée à un consommateur catégorisé[252]. Telle est l'essence de la publicité comportementale, l'adaptation de la publicité à son destinataire, afin de maximiser son efficacité. Autrement dit, il s'agit d'un modèle d'affaire qui se base sur le profilage des individus pour leur suggérer une publicité qui leur sera plus pertinente.

D'ailleurs, ce type de modèle d'affaire est fortement répandu en ligne. Les entreprises offrant un service sont financées par les revenus provenant de la vente d'espace publicitaire. De plus, comme nous l'avons vu, la valeur de cet espace a accrue par sa capacité à cibler efficacement les internautes qui recevront la publicité en question. Par conséquent, il est

[251] Abdelmadjid ABDELKAMEL, préc. note 244, à la page 23.
[252] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 249.

désormais possible d'offrir des services en ligne, abordables, voire gratuits, sans avoir à recourir nécessairement à la formule d'utilisateur payeur.

Le pendant de cet éventail gratuit est tout aussi manifeste. Les utilisateurs passent d'un statut de consommateurs de services à un statut de produit pour les entreprises de marketing. Comme l'explique cet adage : « *if you're not paying for it, you're not the customer; you're the product* »[253], alors que les services sont au bénéfice des utilisateurs, ils sont également au détriment de leurs renseignements de navigation.

4.6- Exemple d'utilisation des cookies - Facebook

À titre d'exemple de la pratique de profilage, nous utiliserons la politique de vie privée de Facebook pour lister les renseignements qui seront collectés[254]. D'abord, Facebook recueille une grande quantité d'informations, souvent personnelles, dans le cadre de l'utilisation de leur service social. Ils collectent notamment des renseignements tels que l'adresse de résidence, les numéros de téléphone, le pays habité et la date de naissance, la religion, l'orientation sexuelle, le contenu des messages, les données transactionnelles et les informations sur les amis. Ensuite, la compagnie collecte également l'activité sur le site, les renseignements concernant les appareils utilisés pour se connecter, y compris les adresses IP et les renseignements fournis par les cookies. Enfin, Facebook recevra certaines informations communiquées par les tiers à partir des modules sociaux sur les autres sites et les interactions des utilisateurs avec la publicité.

Facebook décrit également comment ils comptent utiliser ces renseignements. En ce qui concerne la publicité ciblée «*personalized advertising*», l'entreprise explique qu'elle ne communique pas les renseignements sans le consentement de l'utilisateur. Il permet aux publicitaires de choisir les caractéristiques des utilisateurs qui visionneront leur publicité. En fonction des intérêts identifiés et de renseignements personnels non identifiables, le réseau social définira l'auditoire adéquat pour une publicité donnée. Les utilisateurs sont également

---

[253] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 255.; HARVARD LAW, « Meme patrol: "When something online is free, you're not the customer, you're the product." », *Harvard Law Blogs*, en ligne :, <http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/> (page consultée le 10 avril 2014).

[254] FACEBOOK, « Facebook's Privacy Policy - Full Version », en ligne : <https://www.facebook.com/note.php?note_id=%20322194465300> (page consultée le 10 avril 2014).

avertis par la politique d'utilisation, qu'à partir du moment où ils cliquent sur la publicité, le tiers a la possibilité de placer un cookie sur l'ordinateur et ainsi tracer lui-même les actions de l'individu.

4.7- Mutation de l'information en connaissance – Profilage

En transformant l'information récoltée en connaissances, les « *analytics* » offrent aux entreprises l'opportunité de prendre de meilleures décisions quant à leurs produits et services[255]. Dans le domaine de la publicité, les « *analytics* » permettent aux entreprises de prendre connaissance des intentions du consommateur et ainsi d'exécuter leurs stratégies de marketing plus efficacement et de mesurer et optimiser l'impact de leurs interactions avec les consommateurs[256].

Toutefois, comme l'explique Eli PARISER à une conférence TedX, bien que ces outils soient pratiques, commodes, voire nécessaires, ils isolent en quelque sorte l'utilisateur à son insu :

> «*As web companies strive to tailor their services (including news and search results) to our personal tastes, there's a dangerous unintended consequence: We get trapped in a "filter bubble" and don't get exposed to information that could challenge or broaden our worldview.* »[257].

La décision que prend un système informatique à l'égard d'un individu a des conséquences sur ce-dernier. L'individu, ne participant pas activement à la prise de décision se voit imposé un choix, fait par une machine, qui aura vraisemblablement un impact sur les activités qu'il comptait mener.

Le profilage peut notamment être utilisé dans le domaine de la publicité ciblée, où l'on repose considérablement sur la classification type des individus pour leur distribuer de la publicité pertinente. Avec la publicité comportementale, l'individu n'a pas de pouvoir décisionnel quant à la catégorie de profil qui lui sera attribuée. Cette dernière sera attribuée en fonction de son comportement, ses messages et son historique de navigation. Comme

---

[255] Paul M. SCHWARTZ, *Data Protection Law and the Ethical Use of Analytics*, préc. note 219 à la page 5.
[256] WINTERBERRY GROUP, *The New Rules of the Road: Marketing Data Governance in the Era of "Big Data"*, Winterberry Group White Paper, 2013, à la page 6.
[257] Eli PARISER, « Eli Pariser: Beware online "filter bubbles" » *TedX*, en ligne : <http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-397884> (page consultée le 10 avril 2014).

l'explique PARISER, une décision automatisée, prise en fonction d'un algorithme élaboré, déterminera le contenu qui apparaîtra à l'écran de l'individu, créant effectivement une bulle quant au contenu autour de cet individu[258].

L'absence de contrôle sur cette bulle ainsi créée constitue un problème auquel il semble nécessaire de remédier. Dans une telle situation, l'individu est d'abord le sujet des renseignements collectés, mais aussi le destinataire de la publicité qui sera adaptée en fonction des renseignements qu'il aura communiqué. À cet égard, le sujet et destinataire devrait avoir, à tout le moins, un certain contrôle sur les aspects déterminants de l'attribution de son profil. Il serait donc avisé de l'informer de l'existence de la publicité ciblée, mais il serait également important de l'instruire sur les facteurs qui ont mené à la publicité en question, plutôt qu'une autre.

Pour ces raisons, on constate que différentes juridictions attribuent des droits subjectifs aux individus pour renverser ces effets collatéraux engendrés par les nouvelles technologies de l'information. En effet, on confère souvent des droits, basés sur le principe de transparence du traitement de l'information, qui permettront notamment aux individus d'accéder à leurs renseignements personnels, mais aussi de les rectifier en cas d'erreurs. Ainsi, il est possible de prendre connaissance des motifs qui ont mené à une prise de décision automatisée, mais aussi de corriger les données sur lesquels ces motifs se basent[259].

4.8- Mutation de l'information en connaissance – Décisions automatisées

Dans d'autres domaines que celui de la publicité, le « *Big Data* » permet notamment la prise de décision automatisée. Cette capacité est associée à l'utilisation des outils « *analytics* » et permet aux systèmes informatiques de prendre la décision la plus adéquate selon les circonstances, le tout, en fonction d'analyses empiriques. Comme nous l'avons vu, les décisions automatisées sont une des nombreuses possibilités qui nous sont offertes par les

[258] Eli PARISER, « Eli Pariser: Beware online "filter bubbles" » *TedX*, en ligne : <http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-397884> (page consultée le 10 avril 2014).

[259] À titre d'exemple, la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 8 <http://canlii.ca/t/pp6c> (consultée le 25 novembre 2015), impose à son article 8 qu'une entité formant un dossier sur une personne doivent communiquer les motifs de la collecte, mais aussi informer la personne des droit d'accès et de rectification.

technologies de l'information. Les entreprises peuvent orienter leur modèle d'affaires de façon à bénéficier du traitement de l'information qui est à leur disposition.

Pour arriver à une décision automatisée, les systèmes informatiques doivent être alimentés d'une quantité considérable d'information. En effet, c'est par l'accumulation massive de l'information, mais surtout par l'analyse des masses de données ainsi constituées, qu'il est dorénavant possible de déceler des tendances et prendre des décisions en fonctions de ces dernières. C'est donc dire que les outils « *analytics* » nous permettent d'analyser rapidement des gisements de données si grands que l'on identifie des tendances avec tant de précisions qu'elles permettent, en quelque sorte, de prédire le comportement humain, voire l'avenir et que les systèmes informatiques agissent et prennent une décision en fonction des prédictions.

Ces décisions automatisées peuvent aussi apparaître sous la forme d'analyses prédictives. De la même façon que le profilage afin d'émettre du contenu ciblé, les analyses prédictives mènent à une prise de décision ayant un impact relatif sur l'individu. Toutefois, un enjeu significatif des analyses prédictives est la prise de décisions discriminatoires. Cet enjeu est récurrent à travers la littérature. En effet, un des espoirs du phénomène de « *Big Data* » est celui de prédire l'avenir à partir des masses d'informations récoltées. De ces gisements d'informations, il serait possible de déceler des tendances se rapprochant constamment plus de la vérité. Malencontreusement, ces analyses peuvent également mener à des décisions qui seront discriminatoires.

4.9- Risques associés au profilage et décisions automatisées

Comme les autres pratiques, les analyses prédictives peuvent jouer un rôle efficace et pertinent pour la société, mais ces bienfaits sont vite rattrapés par d'autres enjeux sociaux, comme la protection des renseignements personnels ou la discrimination. Il suffit de se rappeler de cette situation où un père s'est insurgé contre la compagnie Target, car cette dernière distribuait des publicités de produits pour bébé, à sa fille mineure[260]. Alors que Target n'avait probablement récolté aucun renseignement sensible concernant l'état de santé de la

[260] Charles DUHIGG, « How Companies Learn Your Secrets », *The New York Times*, en ligne : <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=&_r=0> (page consultée le 25 novembre 2015).

jeune fille, l'analyse prédictive leur avait permis de déterminer qu'elle était enceinte. Ce faisant, ils ont divulgué des renseignements de nature éminemment sensible, sa grossesse, sans le consentement de la jeune fille, à un tiers. « *Predictive analysis is useful for law enforcement, national security, credit screening, insurance, and employment. It raises ethical dilemmas* »[261]. Il existe donc une certaine ligne éthique, ou même morale, facilement franchissable lors de ces analyses prédictives. D'un côté, une entreprise peut vouloir offrir des produits mieux adaptés aux besoins de leur clientèle, alors que de l'autre côté, elle divulgue par le fait même des renseignements personnels à l'égard de ses clients sans que ceux-ci aient pu évaluer le processus décisionnel menant à leur catégorisation dans certains profils.

À titre d'exemple, la *Loi sur la protection des renseignements personnels dans le secteur privé* stipule à son article 13 que :

> «*Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie.*»[262]

Ainsi, la divulgation d'un renseignement personnel ne peut être faite sans obtenir le consentement de la personne concernée. Or, les analyses prédictives et les décisions automatisées doivent inclure une sorte de mécanisme permettant soit d'obtenir le consentement, ou encore d'identifier adéquatement le destinataire du renseignement personnel.

Dans d'autres cas, on redoute que la prise de certaines décisions automatisées ait des répercussions discriminatoires. Certains auteurs y réfèrent par le terme « *redlining* »[263]. Selon Wikipédia, le « *redlining* » référerait à la pratique de charger plus cher ou de refuser un service à des individus en fonction d'un dénominateur commun, souvent la race ou le lieu de résidence[264]. Plusieurs craignent que le profilage à des fins publicitaires serve indirectement à

---

[261] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 253.
[262] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 13 en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).
[263] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 253.
[264] WIKIPEDIA, «Redlining», en ligne : <http://en.wikipedia.org/wiki/Redlining> (page consultée le 10 avril 2014).

hausser les prix pour les individus ayant les poches plus profondes. D'ailleurs, ce type de pratique est souvent jugé illégal et discriminatoire[265].

Ensuite, l'utilisation indue de la publicité ciblée peut amener des questions d'éthique. Lorsqu'on parle de « *Big Data* », d'« *analytics* » et de profilage, les questions d'éthique sont souvent soulevées, car le traitement automatisé de l'information exclut presque automatiquement le traitement informatique d'un concept aussi flou que celui de l'éthique. Ces enjeux éthiques sont particulièrement pertinents dans le cas des données personnelles médicales et des campagnes politiques.

Il est communément accepté que les renseignements médicaux constituent des données sensibles. D'ailleurs, la plupart des entreprises qui s'adonnent à la personnalisation de la publicité annoncent qu'elles ne collecteront pas ou adopteront des standards plus élevés pour le traitement de renseignements sensibles comme des données médicales[266]. Il demeure tout de même certains risques quant à l'abus d'individus plus vulnérables. En publicité, il existe un concept simple : ce qui passionne permet d'isoler, de cibler et de vendre un produit. Ce principe se transpose tout aussi facilement lorsqu'on parle de maladie, car elle aussi isole et permet de vendre des produits à des personnes vulnérables[267]. Toutefois, profité des personnes vulnérables est reconnu comme n'étant pas conforme aux règles de l'industrie de la publicité en ligne[268].

En 2015, le Commissariat à la Protection de la Vie Privée du Canada a publié un rapport documentant la pratique de publicité ciblée[269]. On y rapport justement que l'utilisation d'un mécanisme « *opt-out* » pour envoyer de la publicité ciblée contenant de l'information sensible est inacceptable. On constate toutefois que certaines entreprises ciblent les consommateurs en fonction de données sensibles. Le Commissariat a remarqué que les

---

[265] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 253.; Kate CRAWFORD et Jason SCHULTZ, préc. note 218, à la page 8.
[266] Voir les sept principes d'autoréglementation concernant le « *online behavioral advertising* » développés par des associations de publicitaires : DIGITAL ADVERTISING ALLIANCE, «Self-Regulatory Principles Overview», en ligne : <http://www.aboutads.info/obaprinciples> (page consultée le 25 novembre 2015).
[267] Nicolas P. TERRY, préc. note 76, à la page 392.
[268] DIGITAL ADVERTISING ALLIANCE, «Self-Regulatory Principles Overview», en ligne : <http://www.aboutads.info/obaprinciples> (page consultée le 25 novembre 2015).
[269] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Online Behavioural Advertising (OBA)*, Follow Up Research Project, Gatineau, CPVPC, 2015, à la page 8.

entreprises ayant été contactées ont immédiatement cessé et ont amélioré leur procédures pour cibler les consommateurs vulnérables. Malgré cela, le rapport souligne que : « *the present results show that retargeting is taking place for other sensitive topics, both by Google and by others* » [270].

Encore dans le domaine de la publicité comportementale, on se préoccupe de l'application des méthodes d'analyses du « *Big Data* » afin de mieux individualiser les électeurs et de prédire leur intention de vote. En effet, il existe une pratique cherchant à identifier des électeurs potentiels, pour leur envoyer de la publicité afin de consolider leur vote. Une fois que l'électeur potentiel est identifié, de la publicité politique lui sera envoyée et elle lui sera personnalisée, dans l'objectif d'obtenir son vote. Bien que l'utilisation des technologies de l'information apporte un aspect novateur à cette pratique, ce système de profilage politique n'est pas récent, les banques de données privées concernant les électeurs existent depuis bien longtemps[271]. Toutefois, l'application des méthodes de publicité ciblée au contexte politique soulève des questions d'autonomie de l'individu et de protection du droit de vote.

Ces considérations quant à l'autonomie décisionnelle se manifestent d'ailleurs lorsqu'on étudie les enjeux entourant les systèmes de transport intelligents[272]. On y remarque notamment une certaine préoccupation quant à l'impact de la délégation de certaines capacités humaines vers la technologie et l'importance du processus décisionnel du conducteur. Dans son article *Privacy in Autonomus Vehicles*, Dorothy GLANCY explique comment les voitures intelligentes posent un risque sérieux à un aspect fondamental de la vie privée des individus. C'est par l'accumulation de données sur le conducteur et son environnement que les véhicules automatisés prennent des décisions et réduisent l'autonomie décisionnelle du conducteur[273].

Cette autodétermination décisionnelle à laquelle nous référons repose sur des principes de libertés fondamentales qui sont fermement enchâssés dans une conceptualisation de la

[270] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Online Behavioural Advertising (OBA)*, Follow Up Research Project, Gatineau, CPVPC, 2015, à la page 9.
[271] Chris EVANS, préc. note 226, à la page 884.
[272] Dorothy J. GLANCY, «Privacy in Autonomous Vehicles», (2012) 52 *Santa Clara L. Rev*. 1171, 71p.
[273] *Id*.

protection des données qui repose sur la dignité humaine[274]. En effet, l'autodétermination décisionnelle est un des multiples aspects de la vie privée. D'ailleurs, elle vient recouper la protection des renseignements en ce qu'elle exige un certain contrôle sur les informations qui sont communiquées et par un contrôle de la transparence des décisions déléguées à la technologie.

Pour résumer, les décisions automatisées peuvent donc être envisagées en fonction des différentes conceptions de ce qu'est la protection des données. Cette protection de l'individu intervient, car le développement des technologies nous force à étudier le rapport entre le processus décisionnel, les individus et une technologie sur laquelle ceux-ci n'ont aucun contrôle. Avec l'amélioration et le progrès constant dans le domaine technologique, il sera de plus en commun d'observer certaines critiques quant aux questions d'autonomie puisque la technologie est dorénavant en mesure de prendre des décisions par elle-même.

4.10- Conclusion

Dans cette section, nous avons établi que le « *Big Data* » est l'utilisation des nouvelles technologies dans le but de permettre un traitement massif des données et d'arriver à des conclusions réelles et objectives. Les outils d' « *analytics* » sont des procédés statistiques, algorithmiques et mathématiques, utilisés pour tirer des conclusions à partir des données agrégées.

Nous avons que le « *Big Data* » est utilisé dans le domaine de la publicité en ligne. On utilise l'information à notre disposition pour constituer un profil, une classe ou une catégorie qui permet de caractériser un individu selon son comportement. Cette classification a pour objet de mieux cibler le consommateur en lui offrant des publicités sur mesures. Les profils digitaux utilisés sont conçus à partir des renseignements des individus ciblés. Ces renseignements se qualifient parfois comme renseignements personnels, par exemple, des renseignements quant à une transaction particulière.

---

[274] Yves POULLET, M. DINANT et al., *Rapport sur l'Application des principes de protection des Données aux Réseaux Mondiaux de Télécommunication : L'autodétermination Informationnelle à l'Ère de l'Internet*, Comité Consultatif de la Convention pour la Protection des Personnes à l'égard du Traitement Automatisé des Données à Caractère Personnel, pour le Conseil de l'Europe, 2004, à la page 25.

Alors que des renseignements personnels sont utilisés pour constituer les profils, les profils eux-mêmes ne sont pas un renseignement personnel, car il est anonyme et définie une classe d'individu, plutôt qu'un individu particulier. Pour cette raison, nous avons étudié la question de l'anonymisation des renseignements personnels, son utilité et les risques pouvant miner l'utilité de l'anonymisation tels que l'« *incremental effect* » et les définitions législatives de ce que constitue un renseignement personnel.

De plus, les entreprises ayant recours aux « *analytics* » doivent considérer d'autres enjeux qui les guettent selon les différentes méthodes de profilage utilisées. En effet, nous avons décrit les différentes façons par lesquelles une entité peut collecter de l'information. On discute notamment des cookies de session, des cookies persistants, des cookies internes, des cookies de tiers et des super cookies. Chacun de ces cookies opère différemment et ils varient en fonction de leur niveau d'intrusivité dans la vie privée du sujet de l'information.

Un des modèles les plus courants d'utilisation des cookies et des profils est le modèle d'affaires qui se base sur le profilage des individus pour leur suggérer une publicité, incluse dans un service gratuit, qui leur sera pertinente.

Les profils sont également utilisés afin de faire des déductions quant au comportement des individus. Dorénavant, les entreprises sont en mesure d'identifier un comportement type selon les profils et d'optimiser les circonstances qui mène à ce comportement, par exemple, l'achat d'un bien selon le temps passé dans un magasin.

Le « *Big Data* » est également utilisé dans des contextes autres que celui de la publicité en ligne. On discute notamment du rôle du *«Big Data »* dans la prise de décisions automatisées basée sur les renseignements entrant dans un algorithme. Plusieurs critiques ont été formulées contre ce type d'utilisation des « *analytics* ». En effet, plusieurs auteurs commentent qu'il s'agit en fait d'une utilisation des renseignements personnels qui affectent certaines valeurs fondamentales comme la dignité et l'autodétermination. Ces auteurs suggèrent également que les lois sur la protection des données devraient protéger ces valeurs fondamentales et encadrer ces pratiques liées au « *Big Data* ».

Quoi qu'il en soit, l'utilisation du « *Big Data* » et des « *analytics* » est controversée. On pourrait souligner que ces outils sont indispensables pour ne pas se perdre dans l'immensité du web. En effet, compte tenu de la nature du web et de la quantité infinie du contenu qu'on peut y trouver, effectuer une recherche sans reposer sur les capacités des outils « *analytics* » serait une tâche lourde, redondante et insurmontable. Sans ces outils, retrouver une page en fonction de son contenu serait l'équivalent de rechercher une aiguille dans une botte de foin.

En fait, les outils « *analytics* » servent à beaucoup plus que la simple indexation du web. Ces outils permettent d'analyser, synthétiser, comprendre et d'interpréter les masses données qui sont à la portée de nos mains. Toutefois, il faut demeurer conscient que certains risques accompagnent cette capacité de traitement. En effet, en collectant, traitant l'information, pour éventuellement la synthétiser et la divulguer, les entreprises recourant aux « *analytics* » doivent se conformer aux lois protégeant la vie privée et les renseignements personnels. Pour déterminer si les données qu'elles collectent sont des renseignements personnels, elles peuvent observer les méthodes utilisées pour collecter les renseignements, les types de renseignements, les moyens utilisés pour anonymiser l'information et les finalités auxquelles les données sont destinées.

5- Enjeux communs aux différents modèles d'affaires

Au cours de cette recherche, nous avons constaté que certains enjeux étaient communs à tous les modèles d'affaires commercialisant l'information. Pour chaque pratique, on pouvait retrouver une certaine considération, ou encore une absence de considération envers le rôle du consentement à la collecte, le traitement et la divulgation des informations et à la sécurité des données. En fait, ces questions ne sont pas des enjeux communs aux divers modèles d'affaires, mais plutôt des enjeux transcendants les modèles d'affaires et d'avantage intrinsèques aux technologies de l'information.

En effet, sans égards aux modèles d'affaires, le consentement est un élément déterminant lors de l'évaluation des enjeux juridiques concernant une entreprise. Que ce soit par la détermination que l'obtention du consentement est nécessaire, facultative, voire inutile, les entreprises doivent considérer la possibilité qu'il soit nécessaire d'obtenir le consentement du sujet de l'information afin de traite, collecter, conserver ou communiquer une information et quelles en sont les conséquences légales.

Les lois québécoises et canadiennes sur la protection des renseignements réfèrent au consentement comme condition quasi sine qua non de validité. On pense notamment à la loi fédérale qui discute de validité du consentement, collecte, utilisation et communication d'information sans le consentement de l'intéressé[275]. On pense également à la loi provinciale qui impose le consentement à la collecte et à la communication de renseignements personnels[276].

Ces dispositions portant sur le consentement sont centrales aux différents modèles d'affaires qui commercialisent des données pouvant contenir des renseignements personnels. Considérant les masses de données qui sont collectées, conservées, communiquées et traitées et la plus-value qu'apportent des renseignements personnels agrégés, il est plus que probable que chacun des modèles d'affaires étudiés soient, dans une certaine mesure, sujets aux dispositions d'une loi sur la protection des données qui impose l'obtention du consentement.

---

[275] *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, art. 7 en ligne : <http://canlii.ca/t/69jnp> (page consultée le 25 novembre 2015).

[276] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 10 et ss., en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).

Pour cette raison, nous observerons le rôle du consentement, ses modalités, son efficacité, ses manifestations et ses critiques.

Pareillement, la sécurité des données est un enjeu qui concerne tous les modèles qui commercialisent des données personnelles. À partir du moment où l'on collecte et conserve des masses de données, une entreprise aura à s'assurer qu'elle respecte les lois portant sur la sécurité et la confidentialité des renseignements personnels.

Or, chacun des différents modèles d'affaires observés opère sur la plus-value qu'entraînent la collecte, le traitement, la communication et la conservation de masses de données. Ces masses de renseignements ont une valeur et sont sujettes à être accédées sans autorisation, pour des finalités autres que celles pour lesquelles les renseignements ont été initialement collectés. D'ailleurs, comme nous l'avons expliqué, ces masses de données contiennent probablement une foule de données personnelles étant protégées par les diverses loi visant la protection des renseignements personnels et la vie privée.

Avec cette réalité en tête, la plupart des lois prévoient des dispositions engageant la responsabilité des entreprises qui manipulent les renseignements personnels d'autrui. Par exemple, la loi québécoise sur la protection des renseignements personnels dans le secteur privé prévoit que :

> « *Toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.* » [277]

Ainsi, nous croyons que l'enjeu de sécurité est un enjeu qui s'impose à tous les différents modèles d'affaires qui commercialisent de l'information pouvant contenir des renseignements personnels. Nous étudierons comment la sécurité se manifeste lors de l'évaluation des risques pour les différents modèles d'affaires étudiés et de son importance croissante.

---

[277] [277] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, art. 10, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015).

5.1- Consentement

Que ce soit lors de la vente de masses de données par un « *Data Broker* », par la délégation ou l'externalisation d'une partie significative des opérations ou de la structure pour l'analyse des données ou par l'analyse de masses de données, le consentement est un enjeu auquel les entreprises commercialisant les données personnelles doivent porter beaucoup d'attention. Nous constatons que la première question que toute entreprise informationnelle doit se poser est à savoir si le consentement doit être obtenu par le sujet de l'information.

Le « *Data Broker* » cherchera à déterminer si les sujets ont déjà fourni un consentement au tiers vendant une masse d'information, ou s'il s'agit d'information disponible au public. Les entreprises offrant des services Cloud chercheront à obtenir un consentement contractuel des utilisateurs pour conserver les données. Ce consentement pourra à la fois porter sur l'autorisation de conserver et manipuler l'information, mais aussi de s'assurer que l'utilisateur consente à ce que ses informations soient sujette à un cadre réglementaire provenant d'une autre juridiction, selon l'endroit où seront entreposées les données. Pour sa part, les entreprises s'adonnant au « *Big Data* » chercheront soit à obtenir le consentement des sujets pour traiter leurs informations et constituer des profils ou à déterminer si le consentement est nécessaire puisque les informations générées seront anonymisées.

Bien souvent, l'obtention du consentement pour collecter, traiter, communiquer ou conserver de l'information sera nécessaire à partir du moment que des renseignements personnels seront manipulés.

La nécessité d'obtenir le consentement est l'un des moyens fréquemment utilisés par les législations pour protéger les données personnelles. Bien que cette condition, souvent légale, puisse importuner certaines entités désirant collecter le plus de renseignements possible, des études démontrent d'ailleurs que l'adoption de lois favorisant la protection de la vie privée n'est pas nécessairement une embuche supplémentaire aux entreprises désirant commercialiser l'information[278]. En effet, l'adoption de politiques exigeant le consentement

[278] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, à la page 54.

favorise le développement des marchés de l'information puisque cela crée un climat de confiance au sein duquel les individus se sentent plus confiants à participer[279].

Le consentement peut prendre plusieurs formes et être sujet à une multitude de modalités selon les juridictions. Par exemple, il est possible de distinguer le consentement de type « *opt-in* » et « *opt-out* ». Le consentement « *opt-out* » repose sur l'accomplissement de critères préétablis afin de présumer le consentement de l'individu[280]. À l'inverse, le consentement « *opt-in* » exige que l'individu manifeste un consentement exprès avant que la collecte des données ne soit entreprise.

D'ailleurs, plusieurs débats subsistent quant au type idéal de consentement requis par les législations. Certains allèguent d'ailleurs que le régime de consentement « *opt-in* » est défaillant et impose des obligations irréalistes envers les individus et les entreprises[281]. Dans le même sens, on accuse le consentement de poser entrave à l'innovation[282]. Certains vont même jusqu'à suggérer l'adoption de « *Commonly Accepted Practices* » qui permettraient de ne pas demander le consentement avant de collecter les renseignements pour certaines fins précises[283].

D'un autre côté, on soutient que le consentement « *opt-in* » est une pratique recommandée et reconnue comme faisant partie des « *best practice* »[284]. On exclut le consentement « *opt-out* » comme solution valide puisqu'on considère que l'objectif principal du consentement est de s'assurer que le consommateur est informé de la collecte et de l'utilisation de ses informations et que la formule « *opt-in* » seule permet de remplir cet objectif[285]. De surcroît, on accuse la formule « *opt-out* » d'être en partie responsable des

[279] Moritz GODEL, Annabel LITCHFIELD et Iris MANTOVANI, préc. note 4, à la page 54.
[280] Pour exemple, voir projet de loi américain H.R. 611 - 112th Congress (2011) prévoyant qu'à partir du moment où une entreprise informe le consommateur que ses données sont collectées et qu'elle lui procure un moyen raisonnable d'exercer son droit d'« *opt-out* », le consentement du consommateur sera présumé.
[281] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 260.
[282] Yana WELINDER, préc. note 19, à la page 188.
[283] FEDERAL TRADE COMMISSION (FTC), *Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report, 2012, à la page 38.
[284] Preston N. THOMAS, préc. note 79, à la page 175.; Anita L. ALLEN, « Privacy Law : Positive Theory and Normative Practice », (2012-2013) 126 *Harv. L. Rev. F.* 241, à la page 249.
[285] Preston N. THOMAS, préc. note 79, à la page 175.

inégalités du savoir informationnel entre les entreprises et les consommateurs (asymétrie de l'information)[286].

De façon plus générale, le consentement est un outil utilisé par le droit pour moduler la protection des données. En plus d'être central à ce sujet, le consentement fait, depuis longtemps déjà, partie des éléments fondamentaux de la théorie des contrats[287]. En ce qui nous concerne, le consentement sert principalement d'outil pour assurer une meilleure protection de la vie privée informationnelle. Comme le soulignent les auteurs canadiens LAWSON et O'DONOGHUE, le consentement ne peut pas servir à justifier des atteintes à la vie privée des sujets de l'information, puisque celui-ci s'inscrit dans un ensemble d'outils juridiques visant à protéger la vie privée[288]. D'ailleurs, on s'aperçoit que pour être valide, le consentement est fréquemment sujet à certains critères concernant sa formulation, mais aussi des modalités qui l'entourent[289].

De façon générale et malgré ses objectifs bienveillants, l'utilité et l'efficacité du consentement n'ont pas été épargnées par la critique. En effet, on peut relever des critiques portant sur la validité du consentement qui soulèvent l'aspect imprécis de ce dernier dans un contexte où le sujet n'est pas informé et fait face à une industrie profitant d'un quasi-monopole et d'une asymétrie dans les pouvoirs liés à l'information[290]. De plus, on souligne que, puisque plusieurs lois prévoient des exceptions au consentement, ce dernier offre peu de contrôle effectif sur l'information[291]. Enfin, on constate également que le consentement n'est pas à lui seul suffisant[292]. Suivant une logique plus pratique que théorique, le consentement est exigé au moment initial, lors de la première collecte et ne peut pas prévoir les traitements

[286] Preston N. THOMAS, préc. note 79, à la page 176.
[287] *Id.*, à la page 175.
[288] Philippa LAWSON and Mary O'DONOGHUE, préc. note 64, à la page 41.
[289] Voir par exemple Philippa LAWSON and Mary O'DONOGHUE, préc. note 64, concernant la possibilité de retrait du consentement et la nécessité que le consentement soit manifeste et éclairé. Cette nécessité de consentement expresse sous-entend la possibilité d'un individu de pouvoir manifester son absence de consentement.
[290] Lee A. BYGRAVE et Dag Wiese SCHARTUM, «Consent, Proportionality and Collective Power», dans *Reinventing Data Protection*, Springer, 2009, à la page 160.
[291] Philippa LAWSON and Mary O'DONOGHUE, préc. note 64, à la page 32.
[292] *Id.*, à la page 41; Antoinette ROUVROY et Yves POULLET, préc. note 18, à la page 72.

subséquents de l'information. Pour ces raisons, le consentement ne peut pas être le seul outil permettant de protéger les données des individus[293].

Le consentement, un outil juridique

Le consentement en tant qu'outil juridique joue un rôle significatif sur les pratiques commerciales reposant sur la commercialisation de l'information. En effet, les enjeux et répercussions varient en fonction de l'approche adoptée et de l'importance qu'on y accorde. Les modalités du consentement et ses critères de validité soulèvent des questions d'ordre de protection du consommateur, mais comprend aussi des enjeux économiques.

Alors qu'il est communément accepté que le consentement de type « *opt-in* » est une meilleure pratique, voire une nécessité dans les juridictions européennes, il n'en demeure pas moins que le consentement de type « *opt-out* » est accepté et utilisé aux États-Unis. En effet, alors que l'on reconnait une nécessité de récolter un consentement éclairé et accompagné de possibilités de retrait ou de modification, on reconnait aussi que les entreprises devraient être en mesure de présumer dans certaines situations[294].

Cette tendance est particulièrement manifeste aux États-Unis où la protection des données personnelles est principalement sectorielle. Ce genre de cadre juridique accorde une très forte importance aux pratiques commerciales et encourage l'adoption de mesures volontaires pour encadrer adéquatement les enjeux comme le consentement. On retrace même ce souci de ne pas entraver le cours des affaires dans certains textes gouvernementaux[295]. Principalement, on tend à favoriser les codes de conduite qui encouragent les pratiques permettant l'obtention d'un consentement informé. Ce faisant, les intérêts des individus sont pris en considération, et cela sans imposer indûment les entreprises d'obligations exagérées[296].

Par ailleurs, il ne faut pas oublier que bien souvent, la nécessité d'obtenir le consentement pour collecter, traiter ou divulguer certaines informations est souvent liée à la

[293] Preston N. THOMAS, préc. note 79, à la page 176.
[294] THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Washington, 2012, à la page 17.
[295] INTERNET POLICY TASKFORCE, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, U.S. Department of Commerce, 2010, à la page 29.
[296] *Id.*

notion légale de ce que constitue un renseignement personnel. Par conséquent, la nécessité d'obtenir le consentement est dépendante du type de définition que l'on adopte pour guider le régime de protection des renseignements personnels. Sans entrer dans le débat de ce qui constitue un renseignement personnel et ce qui n'en est pas un, il est facile de constater qu'une différence de portée des lois s'effectue en fonction de l'adoption de définitions larges comme en Europe, et l'adoption de définitions limitatives se référant uniquement aux types de renseignements énumérés par la loi comme aux États-Unis[297].

Importance du consentement

Le consentement est d'autant plus crucial puisqu'il constitue souvent la première étape menant à la commercialisation de l'information[298]. Comme nous l'avons vu, plusieurs pratiques commerciales reposent sur l'obtention de renseignements pouvant être personnels et, par conséquent, seront sujettes à l'application des lois visant à encadrer les pratiques affectant la vie privée informationnelle. On pense notamment à la pratique de publicité comportementale ou « *behavioral advertising* ». En effet, un régime de consentement de type « *opt-out* » ou « *opt-in* » va avoir un impact direct sur les pratiques publicitaires en ligne puisque l'affichage d'une publicité personnalisée nécessite une certaine collecte d'informations. Ainsi, on verra le type de renseignements récoltés limité par les régimes de protection des renseignements personnels.

Les différentes modalités du consentement permettent d'illustrer la distinction entre les différentes conceptions de protection des données et comment se transposent ces conceptions dans les lois. Par exemple, on remarque que la protection des données et la définition de renseignement personnel reçoivent une interprétation large dans les régimes où la protection des données a une assise dans les libertés constitutionnelles fondamentales, comme en Europe. Ce type d'approche amène le consentement à jouer un rôle plus important, soit de pré requis à l'obtention d'une plus grande variété d'information.

À l'inverse, on constate que dans les régimes où on se limite à une définition de renseignement personnel qui prescrit expressément certains renseignements comme étant

[297] Paul M. SCHWARTZ et Daniel J. SOLOVE, préc. note 40, à la page 1829.
[298] Michael A. FROOMKIN, « The Death of Privacy? », (2000) 52 *Stan. L. Rev.* 1461, à la page 1502.

personnels, les entreprises auront tendance à récolter une plus grande variété de renseignements que sous les régimes où on adopte une définition large de ce que constitue un renseignement personnel. Pour contrebalancer le rôle que jouerait le consentement au moment de la collecte, ces régimes assureront la protection des données par l'utilisation de mécanismes tels des modalités de signification obligatoires et de mise à la disposition des individus de formules d'« *opt-out* » pour retirer leur consentement présumé à la collecte de leur renseignement[299].

Nécessité d'obtenir le consentement – publicité en ligne

Les modèles d'affaires basés sur la publicité comportementale ont également soulevé de nouveaux enjeux dans les régimes où l'on refuse la présomption de consentement. En effet, certaines questions sont soulevées en ce qui concerne la validité du consentement pour la constitution de profils à des fins publicitaires.

Au Canada, nous avons répertorié deux décisions du Commissariat à la protection vie privée concernant la publicité ciblée en ligne et traitant du rôle du consentement. Les deux décisions concernent des sites de réseaux sociaux ayant enfreint des principes de la loi fédérale sur la protection des renseignements personnels[300].

La première décision étudie le réseau social Facebook[301]. Dans cette décision, le Commissariat soulève quelques points pertinents concernant la publicité ciblée. Elle précise notamment que, contrairement aux modèles d'affaires traditionnels, la collecte de renseignements personnels à des fins de profilage publicitaire est une finalité principale aux entreprises comme Facebook[302]. Il serait donc légitime pour un réseau social gratuit d'exiger un consentement pour la publicité ciblée. Subséquemment, elle explique que la communication des profils agrégés, aux publicitaires, est une utilisation de renseignements

[299] Philippa LAWSON and Mary O'DONOGHUE, préc. note 64, à la page 42.
[300] *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, en ligne : <http://canlii.ca/t/69jnp> (page consultée le 25 novembre 2015).
[301] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc.*, Gatineau, CPVPC, 2009, en ligne : < https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.asp> (page consultée le 25 novembre 2015).
[302] *Id.*, au paragraphe 131.

personnels au sens de la loi fédérale[303]. En ce sens, l'entreprise accède aux renseignements personnels, les collecte, les agrège et renvoie des publicités en fonction de ce qu'elle a récolté[304]. Finalement, la commissaire rappelle l'importance des principes de protection des renseignements personnels et que par conséquent, il est impératif que les entreprises de réseaux sociaux se dotent de politiques claires et transparentes axées sur la compréhension de l'utilisateur qui faciliteraient la compréhension du rôle que jouent les publicités dans un modèle d'affaire comme Facebook. On favorise, de cette façon, l'éducation et la compréhension du consommateur, le menant ainsi vers un consentement éclairé.

Cette décision concernant Facebook est une illustration du rôle que peut jouer, et de l'importance qu'on peut accorder au consentement de l'utilisateur à la collecte, utilisation et conservation de ses données. En résumant, la commissaire soumet qu'il est légitime d'exiger un consentement, mais que ce dernier doit, le plus possible, être clair et transparent pour s'assurer que le consommateur ait connaissance et consente à ce que ses renseignements soient utilisés.

La deuxième décision implique des mineurs et un réseau social exigeant la publicité ciblée pour s'inscrire gratuitement au site web. La commissaire conclue :

> *« [qu'] envoyer des publicités aux utilisateurs en fonction des données de leur profil, même si l'information est transmise aux annonceurs sous forme agrégée [est] considérée comme une utilisation de renseignements personnels aux termes de la Loi »*[305].

Cette affirmation entérine ainsi la décision Facebook de 2009 et confirme que, au Canada, la communication de profils constitués à partir de renseignements personnels constitue une utilisation de renseignements personnels et doit donc être visée par le consentement pour que la communication de ce profil soit valide en vertu des lois assurant la protection des renseignements personnels.

---

[303] *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21, en ligne : <http://canlii.ca/t/69jnp> (page consultée le 25 novembre 2015).

[304] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc.*, préc. note 301, au paragraphe 132.

[305] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels*, Gatineau, CPVPC, 2012, au paragraphe 49, en ligne : <https://www.priv.gc.ca/cf-dc/2012/2012_001_0229_f.asp> (page consultée le 25 novembre 2015).

Par ailleurs, la décision « *Nexopia* » souligne qu'exiger le consentement à des fins de profilage pour publicité est valable dans le contexte d'un service gratuit[306]. La communication de renseignements agrégés (profils) est acceptée si l'entreprise a pris le soin d'expliquer à l'utilisateur comment ses renseignements seront utilisés. La commissaire nuance toutefois en expliquant qu'elle ne serait pas du même avis s'il s'agissait de cookies externes (tiers)[307]. Elle explique qu'imposer comme condition d'inscription *sine qua non* que l'utilisateur accepte que les tiers posent des cookies sur leur ordinateur n'est pas acceptable. Elle suggère notamment qu'un individu ait la possibilité de refuser les cookies tiers[308]. La commissaire opère cette distinction, car l'identité du tiers est généralement inconnue.

Ainsi, dans un contexte de publicité comportementale, le consentement joue un double rôle. Il exerce d'abord une fonction de protection de l'intérêt du consommateur, soit l'exigence que son consentement soit obtenu pour que ces informations soient traitées. Ensuite, le consentement vient jouer le rôle d'un outil, permettant de porter à la connaissance du consommateur que ses informations sont collectées. Le consentement est donc un intérêt manifestement protégé par le droit canadien, qui peut éventuellement permettre de baliser les différentes pratiques de commercialisation de l'information.

De façon semblable, le Groupe de l'Article 29 explique qu'il sera éventuellement nécessaire de revisiter la notion de profilage pour synchroniser les réalités pratiques de collecte d'information et le consentement que doivent fournir les utilisateurs. Le Groupe suggère notamment l'élargissement de la notion actuelle de profilage. Cette nouvelle définition assimilerait la mise sur pied de profils, à l'utilisation et à la création de renseignements personnels par les « *data controller* »[309].

---

[306] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels*, Gatineau, CPVPC, 2012, au paragraphe 49, en ligne : <https://www.priv.gc.ca/cf-dc/2012/2012_001_0229_f.asp> (page consultée le 25 novembre 2015)

[307] *Id.*, aux paragraphes 51 et ss.

[308] *Id.*, au paragraphe 55.

[309] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Advice Paper on Essential Elements of a Definition and a Provision on Profiling Within the EU General Data Protection Regulation*, Advice Paper, Bruxelles, 2013, à la page 3.

Ainsi, bien qu'un profil ne constitue pas un renseignement personnel, *per se*, mais plutôt une catégorisation, on reconnaîtra que cette catégorisation est un renseignement personnel nécessitant le consentement des utilisateurs. De cette interprétation, on comprend que les entreprises utilisant la publicité ciblée auront le devoir d'informer les utilisateurs des informations qui sont générées à partir de leurs renseignements afin d'être en mesure d'obtenir un consentement éclairé. Le Groupe suggère également que cette notion de profilage à des fins publicitaires soit balancée selon les effets sur les intérêts, les droits et les libertés de l'utilisateur.

On réalise que le consentement est un réel enjeu pour les modèles d'affaires commercialisant l'information par l'entremise de publicité comportementale. Les différentes conceptions de protection des données influencent les définitions et la portée que l'on attribue à la notion de renseignement personnel, qui à son tour, influence les caractéristiques du consentement et les modalités permettant de le baliser.

Absence de consentement – Data brokerage

Dans d'autres situations, comme celle du « *data brokerage* », on verra que le consentement joue un rôle plus secondaire, mais soulève des enjeux menant à remettre en question des principes reconnus comme celui de limiter la collecte et le traitement de l'information à des fins spécifiques ayant fait l'objet d'un consentement éclairé.

Comme nous l'avons mentionné, la pratique de « *data brokerage* » s'opère souvent sans que le sujet de l'information ait connaissance qu'une collecte, un traitement ou une divulgation a eu lieu à son sujet. Les revendeurs d'information achètent des gisements de données à d'autres revendeurs, à des entreprises ayant une relation contractuelle avec le sujet ou encore collectent l'information à partir de sources publiques disponibles. Sans relation contractuelle, les marchands d'information n'ont pas de consentement exprès de la part du sujet.

La situation où le « *data broker* » est un tiers au contrat entre le sujet et l'entreprise offrant un service moyennant la vente de renseignements personnels rappelle les enjeux

soulevés par les critiques concernant le consentement limité à des fins déterminées[310]. À ce sujet, plusieurs ont questionné la validité du consentement lorsque les fins n'étaient pas déterminées. Ainsi, plusieurs questionnent la validité du consentement d'un sujet ayant accepté de partager ses renseignements avec un commerçant qui précisait dans le contrat que ces renseignements allaient être revendus à des tiers.

Dans le même sens, il existe un « *Fair Information Principle* » à l'effet que les utilisations subséquentes doivent être limitées à la portée du consentement[311]. D'ailleurs, ce principe est intégré au sein du régime de protection des données européen qui prévoit que les données ne peuvent être traitées ultérieurement et de façon incompatible aux fins déterminées[312]. Cette prise en considération impérative des finalités légitimes est confinée au sein du spectre du consentement et nous renvoie donc à une réflexion sur la pertinence du consentement comme base de légitimité de la collecte et du traitement de l'information[313].

Comme nous le voyons, l'arrivée des modèles d'affaires commercialisant les masses de données, tel le « *data brokerage* » viennent remettre en question la pertinence, ou plutôt l'efficacité, de protéger le consentement par le droit. Cet outil de tradition ne confère plus les garanties qu'il offrait autrefois, en raison du développement rapide des technologies qui nous force à revoir les objectifs que visaient ces outils et s'il est possible de garantir ces objectifs d'une autre façon.

En effet, la suffisance du consentement est contestée autant sur le plan de la qualité du consentement, que sur son utilité et son efficacité en pratique. La qualité du consentement est notamment critiquée, car il est difficile d'évaluer la valeur de perte de vie privée associée à la divulgation de certains renseignements[314]. On qualifie généralement cette réalité de « *privacy myopia* », voulant que par manque d'information à leur disposition, les individus aillent trop

---

[310] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* préc. note 62, à la page 20.
[311] Omer TENE et Jules POLONETSKY, préc. note 59, à la page 26.
[312] *Charte des droits fondamentaux de l'Union Européenne*, préc. note 52, art. 6 (1) b).
[313] Yves POULLET, M. Dinant et al., *Rapport sur l'Application des principes de protection des Données aux Réseaux Mondiaux de Télécommunication : L'autodétermination Informationnelle à l'Ère de l'Internet*, préc. note 274, à la page 41.
[314] Michael A. FROOMKIN, préc. note 298, à la page 1503.

souvent céder, pour trop peu, leur vie privée informationnelle[315]. Cette myopie veut qu'il soit difficile, voire impossible, d'évaluer pleinement l'intrusivité des profils constitués à notre sujet et les préjudices pouvant en découler[316]. Selon cette optique, que l'on se retrouve sous un régime où le renseignement personnel est un bien marchand protégé par le droit ou sous un régime considérant la protection des renseignements personnels comme étant un enjeu fondamental relevant de la dignité humaine, le consentement de l'individu est futile puisqu'il existe une tendance à consentir à la collecte et au traitement pour peu en contrepartie[317].

Consentement comme entrave à l'innovation

Enfin, le consentement est aussi considéré comme étant une entrave additionnelle à l'innovation. On considère que les lois portant sur la protection des données personnelles et prévoyant des mesures comme la nécessité de consentement causent la perte d'un bien commun au bénéfice des intérêts privés[318]. L'auteure Jane YAKOWITZ explique qu'un accès général, à des fins de recherche, devrait être accordé selon certaines conditions pour ne pas entraver l'innovation et rajoute que les lois voulant protéger la vie privée vont parfois jusqu'à brimer d'autres libertés[319]. Certains suggèrent le développement d'une doctrine plus étoffée pour l'utilisation publique des données à des fins de recherche[320]. Ce mouvement en faveur de l'utilisation de données personnelles pour des fins de recherche s'inquiète principalement du ralentissement à l'innovation que les lois sur la protection de la vie privée peuvent causer. Ce mouvement, caractéristique de la tradition américaine, argumente que la protection de la vie privée ne doit pas créer un environnement litigieux, mais plutôt de préserver l'innovation. On cite : « *Any protection of online privacy ought to take into account the flexible features of the Internet that invite innovation* »[321]. Ainsi, une pratique exigeant le consentement et la

[315] Michael A. FROOMKIN, préc. note 298, à la page 1502.
[316] *Id.*, à la page 1503.
[317] *Id.*, à la page 1504.
[318] Jane YAKOWITZ, préc. note 237.
[319] *Id*., aux pages 13 et ss.; Voir aussi Richard LANGELIER, « La protection de la vie privée par la Commission d'accès à l'information : quelle vie privée? Quelle protection? En fonction de quels intérêts? », dans *Développements récents en droit de l'accès à l'information*, Service de la formation permanente du Barreau du Québec, 2005, EYB2005DEV1090, 51 p.
[320] Barbara J. EVANS, « Much Ado About Data Ownership », (2011-2012) 25 *Harv. J. L. & Tech*. 69, à la page 119.
[321] Yana WELINDER, préc. note 19, à la page 179.

signification de collecte et de traitement, parfois trop sévère, limite involontairement l'habilité des entreprises à innover en échange d'une prévisibilité légale limitée[322].

Au final, on constate que le consentement joue un rôle mécanique et processuel, puisqu'au lieu de représenter une manifestation de volonté, il représente un préalable au traitement de l'information[323]. Ce consentement semble, la plupart du temps, un artéfact légal fondé sur de nobles principes, mais qui peine à trouver les moyens pour remplir ces objectifs. C'est pourquoi il est nécessaire d'envisager le consentement comme un critère légal pertinent, mais insuffisant pour accomplir une protection des renseignements personnels adéquate qui prend en considération les différents enjeux économiques entourant le marché de l'information.

5.2- Sécurité

Le principe de mesures de sécurité adéquates est un enjeu que l'on a vu apparaître dès les premiers régimes de protection des données. Ce principe veut que les données personnelles soient protégées par des mesures de sécurité raisonnables contre les risques de pertes, d'accès, de destruction, d'utilisation, de modification et de communication non autorisés des données[324]. Cet enjeu, notamment repris par les lignes directrices de l'OCDE en matière de protection des données face à l'automatisation du traitement de l'information, met de l'avant un concept, une obligation, de sécurité informationnelle[325].

Rappelons que la sécurité de l'information se distingue de la protection des renseignements personnels ou de la vie privée en ce qu'il constitue plutôt un outil permettant la protection de ces intérêts. En effet, comme le relate Isabel VICENTE dans son mémoire : « *la protection des renseignements personnels renvoie au contrôle personnel sur les données concernant un individu, tandis que la notion de sécurité renvoie au contrôle organisationnel*

[322] Nicklas LUNDBLAD et Betsy MASIELLO, « Opt-In Dystopias », (2010) 7-1 *SCRIPTed* 155, à la page 160.
[323] Lee A. BYGRAVE et Dag Wiese SCHARTUM, « Consent, Proportionality and Collective Power », préc. note 290, à la page 161.
[324] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* préc. note 62.
[325] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, préc. note 91, à la page 23.

des informations personnelles »[326]. Ce contrôle organisationnel couvre généralement les aspects de confidentialité, d'intégrité et de disponibilité de l'information[327]. Par conséquent, la sécurité informationnelle cherche à limiter la circulation de l'information à ceux ayant un droit d'accès et cherche à maximiser la préservation de la valeur, l'authenticité de l'information et la capacité d'accéder à l'information aux systèmes d'information en temps voulu[328].

Avec le développement constant des technologies, on voit croître corrélativement l'importance de la sécurité informationnelle dans la gestion de l'information. Cet intérêt faisant l'objet de protections juridiques se révèle significatif dans les modèles d'affaires où la conservation de l'information joue un rôle de premier plan. Plus précisément, on pense aux pratiques de « *cloud computing* » ou de « *data brokerage* » qui, chacune à leur façon, utilise principalement la conservation de l'information pour rentabiliser leurs opérations.

Comme nous l'avons vu, la pratique de « *cloud computing* » repose essentiellement sur la délégation du traitement de l'information à des entités tierces offrant une expertise ou simplement l'utilisation d'installations permettant un allègement des prérequis techniques associés au traitement de l'information. Cette délégation comporte nécessairement un enjeu, d'abord technique, mais ayant aussi des conséquences juridiques pour les entités n'assurant pas une protection adéquate aux individus.

Pour sa part, le « *data brokerage* » est une pratique qui vise à récolter des masses de données pour constituer des profils concernant les individus. Comme certains incidents l'ont déjà démontré, une mauvaise sécurité entourant ces bases de données peut mener à des conséquences catastrophiques, autant pour les sujets de l'information que l'entité la contrôlant.

Ainsi, certains enjeux de sécurité peuvent se manifester sous les aspects d'intégrité et de disponibilité de l'information. À cet égard, nous avons observé les différents modèles d'affaires de « *cloud computing* » reposant sur la délégation du traitement de l'information. Cette délégation peut se faire à différents niveaux de l'architecture technologique des systèmes

[326] Isabel VICENTE, préc. note 31, aux pages 13 et 14.
[327] Jean-Marc DINANT, « The Concepts of Identity and Identifiablity : Legal and Technical Deadlocks for Protecting Human Beings in the Information Society? », dans *Reinventing Data Protection*, Springer, 2009, à la page 111.
[328] Isabel VICENTE, préc. note 31, à la page 16.

d'information. En effet, en fonction du modèle utilisé, et aussi en fonction de la décentralisation interne ou externe du système informatique, les devoirs de sécurité associés à l'intégrité et la disponibilité seront attribuables à différents acteurs.

Principalement, les enjeux de sécurité se manifestent quant à la confidentialité des renseignements. On pense notamment au cas récent de l'entreprise GMR qui illustre parfaitement cet enjeu de sécurité[329]. Dans cette affaire, l'entreprise qui avait délégué le traitement des informations dont elle assurait la transcription médicale a été trouvée responsable de ne pas avoir surveillé et de ne pas avoir assuré des balises de sécurité suffisantes par le sous-traitant. Par conséquent, certaines données personnelles qui devaient être confidentielles ont été divulguées par le sous-traitant qui n'était pas tenu contractuellement d'offrir les mêmes garanties de sécurité que l'entreprise GMR. Le manque de diligence lors de son choix de sous-traitant, l'absence de garantie de protection suffisante dans leur contrat de sous-traitance et l'absence de vérification quant au traitement adéquat de l'information ont tous été des motifs pour reconnaître l'entreprise GMR responsable de ne pas avoir garanti la sécurité des renseignements personnels de ses clients.

Dans le même ordre d'idée, des entreprises telles que ChoicePoint ont été reconnues responsables d'avoir manqué à leurs obligations de sécurité, suite à une intrusion dans leur système informatique[330]. Après ces évènements, beaucoup de discussions ont eu lieu quant à la portée des obligations et la responsabilité de l'entreprise dans ces évènements. En effet, lorsque des entreprises qui se spécialisent dans la revente d'information et la constitution de profils d'individus à l'aide des gisements de données qu'ils possèdent, perdent le contrôle de l'information, peu de temps suffit pour que plusieurs questions quant aux enjeux de sécurité soient soulevées. La centralisation de telles masses de données fait paraître ces entreprises de « *data brokerage* » comme des cibles de choix pour les pirates en quête d'accès non autorisé. Par conséquent, on tente d'évaluer la portée des obligations en matière de sécurité compte tenu de ce manifeste.

[329] *GMR Transcription Services, Inc., In the Matter of*, préc. note 170.
[330] Paul N. OTTO et al., préc. note 113, à la page 18.

Les brèches de sécurité sont bien souvent, sans égards à la source de la faille, attribuables au contrôleur de données. On considère alors qu'il est de la responsabilité du « *data controller* » de s'assurer que le principe des mesures de sécurité adéquates est respecté, afin de protéger les données personnelles[331]. Ainsi, que la brèche ait été accidentelle ou forcée, les entreprises doivent déployer beaucoup de moyens pour identifier, mais aussi pour empêcher la récurrence des évènements. Le principe de notification en cas de brèche de sécurité est un moyen de protection utilisé par le droit, car celui-ci informe les individus des risques potentiels auxquels ils sont exposés et force la main des entreprises qui ont peu de motivation à divulguer de tels évènements.

La protection des données, par l'entremise des enjeux de sécurité, nous apparait donc principalement comme étant un intérêt protégé par le droit plutôt qu'une attribution de droit subjectif ou de protection de liberté fondamentale. En effet, on remarque que c'est par le truchement des garanties contractuelles et des protections légales offertes au consommateur que les principes de sécurité sont assurés. Notons toutefois que cette tendance à recourir à cette conception peut être attribuable au fait que le marché de commercialisation de l'information est plus développé aux États-Unis qu'en Europe, et que les États-Unis ont une approche bien différente des Européens à l'égard de certains enjeux[332]. Notons qu'il est possible de retrouver certaines suggestions doctrinales amenant des solutions de l'ordre de l'attribution de droits subjectifs pour assurer la sécurité des renseignements personnels par les entités les contrôlant[333].

La sécurité informationnelle est donc un enjeu qui est apparu dès le développement des technologies de l'information et demeure d'actualité pour toutes les pratiques commerciales technologiques. Malgré l'évolution fulgurante des possibilités dans ce domaine, cet enjeu demeure d'actualité. On peut même affirmer que cet enjeu prend de l'importance, puisque les entreprises ayant un modèle d'affaires basé sur la commercialisation des renseignements personnels accentuent les risques envers les sujets de l'information. En effet, l'accumulation de données et la délégation du traitement de l'information font en sorte que les individus sont

[331] Paul N. OTTO et al., préc. note 113, à la page 16.
[332] Lior Jacob STRAHILEVITZ, préc. note 83, à la page 2035.
[333] Preston N. THOMAS, préc. note 79, à la page 182.

exposés à des risques additionnels et que, par conséquent, ils nécessitent une meilleure protection à cet égard. Ainsi, peut-être verrons-nous se développer un intérêt accru envers cet enjeu et donc une protection plus étendue que la protection d'un intérêt par le droit.

5.3- Conclusion

Nous avons identifié deux enjeux qui étaient communs à tous les modèles d'affaires commercialisant l'information, le consentement du sujet de l'information et la sécurité des données. Ces deux modèles se doivent d'être considérés lorsqu'une entreprise manipulant des masses d'information établie son modèle d'affaires.

Le premier enjeu commun, le consentement, est un critère de validité de toute opération sur les renseignements personnels dans plusieurs juridictions. Il peut se manifester de plusieurs façons et autant faire l'objet d'un régime « *opt-in* » que « *opt-out* ». La modulation des critères de validité du consentement varie en fonction de la juridiction et de l'importance que cette dernière accorde à la protection des données personnelles. La portée du consentement varie en fonction de la définition qu'on adopte de ce qu'est un renseignement personnel.

Nous avons observé des décisions du Commissariat à la protection de la vie privée du Canada, concernant le consentement et la publicité en ligne. Dans ces décisions, on rappelle qu'il est légitime pour une compagnie d'exiger le consentement à la publicité ciblée pour avoir accès au service gratuit. En fait, on comprend que le consentement est la contrepartie pour laquelle ces services sont offerts. Sans cette autorisation à collecter et communiquer des renseignements personnels, le service n'aurait pas de revenus suffisants pour maintenir le service. Dans d'autres instances, comme dans le cas du « *Data Brokerage* », le consentement est pratiquement absent.

Dans tous les cas, plusieurs auteurs ont soulevé que la qualité et la validité du consentement à collecter, traiter et communiquer de l'information étaient discutables. De plus, l'utilité du consentement est également critiquée. Nous avons soulevé que les sujets de l'information ont trop souvent tendance à céder, pour trop peu, leur renseignements personnels. Il existe une « *privacy myopia* » quant à la valeur réelle de nos renseignements personnels.

Le second enjeu commun, la sécurité des renseignements personnels et confidentiels, est un principe fondamental qui concerne toutes les entreprises conservant des données. La sécurité informationnelle croît constamment en importance avec le développement des technologies et la transition vers le numérique de notre société. Pareillement, les pratiques comme le « *Cloud Computing* » gagnent en importance parce que les technologies permettent d'optimiser le rendement et les capacités des entreprises, mais augmentent par le fait même la complexité et la sophistication nécessaire.

Les brèches de sécurité dans les systèmes informatiques mènent à la divulgation involontaire de renseignements personnels. Cette divulgation non autorisée cause un préjudice pour le sujet de l'information qui peut aller jusqu'au vol d'identité.

Pour cette raison, plusieurs juridictions commencent à adopter des mesures visant à responsabiliser et protéger les intérêts des consommateurs, sujets de l'information. Par exemple, certaines juridictions adoptent l'idée de forcer les entreprises à divulguer qu'une faille de sécurité s'est produite et de contacter les personnes pouvant être affectée.

Considérant que la collecte, le traitement, la communication et la conservation de renseignements personnels sont plus féroces que jamais, en raison du développement des technologies de l'information, il est d'une importance significative de porter attention à ces deux enjeux qui ne cesseront de gagner en importance dans les prochaines années.

6- Conclusion

On constate donc qu'il existe plusieurs modèles d'affaires qui reposent sur la commercialisation de l'information. Chacun de ces modèles possède ses caractéristiques particulières et des finalités qui leur sont propres. Par conséquent, les enjeux que ces modèles entraînent sont également uniques à chaque situation, même si parfois certains d'entre eux se recoupent. Dans cet essai, nous avons étudié les pratiques de « *data brokerage* », de « *cloud computing* », et des outils « *analytics* ».

Nous avons d'abord observé cette pratique plus ou moins connue de « *data brokerage* ». Les « *data brokers* » sont des revendeurs d'information qui ont pour objectif d'accumuler la plus grande quantité d'information possible par le plus de sources possible. Une fois ces informations agrégées et croisées, ils les ordonnent sous forme logique dans le but d'offrir un service. Ainsi, la revente d'information est une pratique soulevant plusieurs ordres d'enjeux. D'abord, par la constitution de bases de données massives, ils s'exposent à plusieurs risques quant à la sécurité des renseignements collectés. Ensuite, par le traitement de ces informations, avec l'aide d'outils « *analytics* », la pratique de « *data brokerage* » soulève également des enjeux similaires. Enfin, la vente de ces informations soulève des enjeux d'ordre de protection des libertés fondamentales et de consentement des sujets.

Comme nous l'avons vu, la pratique de « *cloud computing* » réfère à la tendance, de plus en plus marquée, des entreprises à déléguer le traitement ou la conservation de l'information à d'autres entités pour optimiser leurs services. Cette pratique qui repose principalement sur la conservation de l'information des individus soulève des questions de responsabilité des sous-traitants, eu égard à la protection de la confidentialité des renseignements personnels, mais aussi à la préservation des garanties de sécurité en place.

Enfin, les outils « *analytics* » sont les fonctions informatiques permettant aux entreprises d'analyser efficacement des gisements de données. Ces outils sont caractéristiques au phénomène de « *Big Data* », car ils offrent la possibilité d'interpréter un nombre constamment grandissant d'information, en cette ère de développement technologique. Bien que fort utiles, ces outils soulèvent plusieurs considérations reposant sur le traitement de l'information. En effet, on remarque que le sujet des informations est fréquemment écarté du

processus menant à une décision pouvant l'affecter. Ce faisant, une disparité apparait sur le plan du pouvoir informationnel entre le sujet et les entités qui l'observent. On constate aussi un certain mouvement quant à la protection des individus contre ces décisions faites à leur sujet. Dans un autre ordre d'idées, on souhaite également encadrer cette pratique pour bénéficier des avantages qu'elle peut nous apporter. Ainsi, on a observé l'impact de concepts comme l'anonymisation et le rôle du consentement face aux nouveaux enjeux soulevés par cette pratique.

Les différentes conceptions de la protection des renseignements personnels permettent de mettre l'emphase sur certaines facettes de ces enjeux. La première remarque face à ces conceptualisations est la distinction entre le concept de protection des données et protection de la vie privée. Alors que ces concepts s'interceptent dans leurs effets sur la protection de la vie privée informationnelle, on constate qu'ils ne peuvent être considérés comme visant les mêmes objectifs ou comme étant des concepts parents qui découleraient des mêmes principes fondamentaux.

Autant que la protection des données semble être un concept généralement accepté, autant les moyens mis en place pour l'assurer sont variés. On constate que c'est en fonction des traditions juridiques et de l'importance accordée à certains intérêts que la protection des données est modulée. Par conséquent, les enjeux soulevés dans la troisième partie de cet essai n'ont pas la même importance selon l'approche adoptée. En effet, certains enjeux auront plus d'écho lorsque la conception de protection des données sera basée sur des intérêts fondamentaux plutôt que sur la protection d'un intérêt par le droit. À titre d'exemple, les enjeux associés aux décisions automatisées, prises par un ordinateur et pouvant avoir des conséquences discriminatoires soulèvent des questions d'ordre fondamental et peut se voir mieux encadré ou, du moins, appréhender, par une conception de la protection des données comme étant un droit fondamental garantissant une certaine autonomie décisionnelle quant à son information.

En somme, ce mémoire avait pour objectif d'identifier certaines pratiques commerciales émergentes, qui ont pour caractéristique principale de modèle d'affaire la commercialisation de l'information. Ces dernières font l'objet de peu d'études et sont en

constante évolution, d'où la difficulté de les circonscrire. Pour aider à tracer les nouveaux enjeux soulevés par ces pratiques, il a été nécessaire de situer les différents concepts juridiques pertinents et de comparer les différentes approches face à ces concepts. Enfin, une fois ce cadre établi, il a été possible d'identifier les enjeux pouvant se manifester, en fonction des différentes conceptions de la protection des données. Sans aucune prétention d'exhaustivité, nous croyons que cet essai regroupe plusieurs pratiques commerciales sous le dénominateur commun de la commercialisation de l'information.

Bibliographie

Législation et réglementation

Fédérale – Canada

Loi sur la protection des renseignements personnels, LRC 1985, c P-21, en ligne : <http://canlii.ca/t/69jnp> (page consultée le 25 novembre 2015).

Provinciale – Québec

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1, en ligne : <http://canlii.ca/t/pp6c> (page consultée le 25 novembre 2015)

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1, en ligne : <http://canlii.ca/t/69h5j> (page consultée le 25 novembre 2015)

États-Unis

15 USC § 1681 et seq.

45 C.F.R. §160-164

FACTA, Pub.L. 108–159

Gramm–Leach–Bliley Act,113 Stat. 1338

H.R. 611 - 112th Congress (2011)

SB. 1386 (2002)

Europe

Charte des droits fondamentaux de l'Union Européenne, 2000/C, Journal officiel des Communautés européennes, 364/01, 2000

Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du Parlement européen et du Conseil, Journal officiel n° L 281 du 23/11/1995, p. 0031 – 0050

Règlement concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques, N^{o} 611/2013, 23 juin 2013

Jurisprudence

Autres pays

GMR Transcription Services, Inc., In the Matter of, Federal Trade Commission (FTC), August 21st 2014

Doctrine

Monographies et ouvrages collectifs

ABDELKAMEL, A., *Facebook et les dispositifs de traçabilité vus sous l'angle du droit canadien*, mémoire de maîtrise en droit des technologies de l'information, Montréal, Université de Montréal, 2013.

BERKVENS, J., « Role of Trade Associations : Data Protection as a Negotiable Issue », dans *Reinventing Data Protection*, Springer, 2009, pp. 125-129

BYGRAVE, L.A. et D.W. SCHARTUM, « Consent, Proportionality and Collective Power », dans *Reinventing Data Protection*, Springer, 2009, pp. 157-173

CISCO, *Cloud : What an Enterprise Must Know*, White Paper, San Jose, Cisco, 2011

CISCO, *Networking and Cloud: An Era of Change*, White Paper, San Jose, Cisco, 2011

DE TERWANGNE, C., « Is a Global Data Protection Regulatory Model Possible », dans *Reinventing Data Protection*, Springer, 2009, pp. 175-189

DELEURY, É. et D. GOUBAU, « La protection des droits de la personnalité », dans *Le droit des personnes physique*, 5^{e} éd., Cowansville, Éditions Yvon Blais, 2014, EYB2014DPP17

DINANT, J.-M., « The Concepts of Identity and Identifiablity : Legal and Technical Deadlocks for Protecting Human Beings in the Information Society? », dans *Reinventing Data Protection*, Springer, 2009, pp. 111-122

GAUTRAIS V. et P. TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montréal, Éditions Thémis, 2010, en ligne : < http://lccjti.ca/wp-content/uploads/2012/05/livreversionfinal.pdf>

GUTWIRTH, S. et M. HILDEBRANDT, « Some Caveats on Profiling » dans *Data Protection in a Profiled World*, Springer, 2010, en ligne : <http://www.springer.com/law/book/978-90-481-8864-2>

GUTWIRTH, S. et P. DE HERT, « Data Protection in the Case Law of Strasbourg and Luxemburg : Constitutionalisation in Action », dans *Reinventing Data Protection*, Springer, 2009, pp. 3-44

HUSTINX, P., « The Role of Data Protection Authorities », dans *Reinventing Data Protection*, Springer, 2009, pp. 130-137

LAWSON, P. and M. O'DONOGHUE, « Approaches to Consent in Canadian Data Protection Law », chapitre 2 dans KERR, I.R., V.M. STEEVES et C. LUCOCK, *Lessons from the Identity Trail*, Oxford University Press, 2009, en ligne : <http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_02.pdf>

LEENES, R. et I. OOMEN, «The Role of Citizens : What Can Dutch, Flemish and English Students Teach Us About Privacy », dans *Reinventing Data Protection*, Springer, 2009, pp. 139-153

LEWIS, G., *Basics About Cloud Computing*, Pittsburgh, Software Engineering Institute, Carnegie Mellon University, 2010

O'CALLAGHAN, P., *Refining Privacy in Tort Law*, Springer, 2013

RAAB, C. et B.-J. KOOPS, « Privacy Actors, Performances and the Future of Privacy Protection », dans *Reinventing Data Protection*, Springer, 2009, pp. 207-221

RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Paris, Librairie Générale de Droit et de Jurisprudence, 1990

ROUVROY, A. et Y. POULLET, « The Right to Informational Self-Determination and the Value of Self-Development : Reassessing the Importance of Privacy for Democracy », dans *Reinventing Data Protection*, Springer, 2009, pp. 45-76

SCHWARTZ, P.M., *Data Protection Law and the Ethical Use of Analytics*, Berkeley, The Centre for Information Policy Leadership, 2010

SCHWARTZ, P.M., *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*, Berkeley, The Privacy Projects, 2009

TRUDEL, P., « Le droit à la réputation, à la vie privée et à l'image », en ligne : < pierretrudel.chairelrwilson.ca/cours/drt3805/rep.vieprive.pdf>

VERMEYS, N., J.M. GAUTHIER et S. MIZRAHI, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec*, Secrétariat du Conseil du Trésor, 2014

VICENTE, I., *La convergence de la sécurité informatique et de la protection des renseignements personnels: Vers une nouvelle approche juridique*, mémoire de maîtrise en droit des technologies de l'information, Montréal, Université de Montréal, 2003

WESTIN, A., *Privacy and Freedom*, (1968) 25 *Washington and Lee Law Review* 166

WINN, J.K., « Technical Standards as Data Protection Regulation », dans *Reinventing Data Protection*, Springer, 2009, pp. 191- 206

WINTERBERRY GROUP, *The New Rules of the Road: Marketing Data Governance in the Era of "Big Data"*, Winterberry Group White Paper, 2013

Articles de revue et études d'ouvrages collectifs

ALLEN, A.L., « Privacy Law : Positive Theory and Normative Practice », (2012-2013) 126 *Harv. L. Rev. F*. 241

ALLEN, J., « It's Three O'Clock in the Morning : Do You Know Where Your Data Is? », (2011) 28 *GPSolo* 6

BLOUSTEIN, E.J., « Privacy as an Aspect of Human Dignity : An Answer to Dean Prosser », (1964) 39 *N.Y.U. L. Rev.* 962

BYGRAVE, L.A., « The Place of Privacy in Data Protection Law », (2001) 24-1 *University of New South Wales Law Journal* 277, 2001

CALO, R.M., « Against Notice Skepticism in Privacy (And Elsewhere) », (2011-2012) 87 *Notre Dame L. Rev.* 1027

CALO, R.M., « Digital Market Manipulation », (2014) 82 *GEO. Wash. L. Rev.* 995

CALO, R.M., « People Can Be So Fake : A New Dimension to Privacy and Technology Scholarship », (2009-2010) 114 *Penn St. L. Rev.* 809

CALO, R.M., « The Boundaries of Privacy Harm », (2011) 86 *Ind. L.J.* 1131

CATE, F.H., « Government Data Mining: The Need for a Legal Framework », (2008) 43 *Harv. C.R.-C.L. L. Rev.* 435

CHASSIGNEUX, C., « La protection des données personnelles en France », (2001) 6-2 *Lex Electronica* 1, en ligne : <http://www.lex-electronica.org/articles/v6-2/chassigneux.htm>

CLEMONS, E.K., « Business Models for Monetizing Internet Applications and Web Sites : Experience, Theory, and Predictions », (2009) 26-2 *Journal of Management Information Systems* 15

CRAWFORD, K. et J. SCHULTZ, « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms », (2013) 55 *B.C.L. Rev.* 93

CUKIER, K. et V. MAYER-SCHOENBERGER, « The Rise of Big Data – How It's Changing the Way We Think About the World », (2013) 92 *Foreign Aff.* 28

DAYARATHNA, R., « Taxonomy for Information Privacy Metrics », (2011) 6 *J. Int'l Com. L. & Tech.* 194

EVANS, B.J., « Much Ado About Data Ownership », (2011-2012) 25 *Harv. J. L. & Tech.* 69

EVANS, C., « It's the Autonomy, Stupid: Political Data-Mining and Voter Privacy in the Information Age », (2012) 13 *Minn. J.L. Sci. & Tech.* 867

FEIJOO, C., J.L. GOMEZ-BARROSO et P. VOIGT, « Exploring the Economic Value of Personal Information from Financial Statements », (2014) 34 *International Journal of Information Management* 248

FERNANDO, A., J.D. SANTOS et J.A. MONTEIRO, « E-Commerce Business Models in the Context of Web 3.0 Paradigm », (2013) 3-6 *International Journal of Advanced Information Technology* 1

FRIED, C., « Privacy »,(1968) 77 *Yale L. J.* 475

FROOMKIN, M.A., « The Death of Privacy? », (2000) 52 *Stan. L. Rev.* 1461

GHOSH, S., « Commercializing Data », (2011-2012) 3 *Elon L. Rev.* 195

GHOSH, S., « Informing and Reforming the Marketplace of Ideas: The Public-Private Model for data Production and the First Amendment », (2012) 2 *Utah L. Rev.* 653

GODEL, M., A. LITCHFIELD et I. MANTOVANI, « The Value of Personal Information – Evidence from Empirical Economic Studies », (2012) 88-4 *Digiworld Economic Journal* 41

HALPÉRIN, J.-L., « L'essor de la 'privacy' et l'usage des concepts juridiques », (2005) 61-3 *Droit et Société* 765

HOPKINS, S.R. et P.R. REYNOLDS, « Redefining Privacy and Security in the Electronic Communication Age: A Lawyer's Ethical Duty in the Virtual World of the Internet », (2002-2003) 16 *Geo. J. Legal Ethics* 675

HURLBURT, G.F., « Web 2.0 Social Media : A Commercialization Conundrum », (2012) 14-6 *ITPro* 6

JACOBY, N., « Redefining the Right to be Let Alone : Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States », (2006-2007) 35 *Ga. J. Int'l & Comp. L.* 433

JAISINGH, J. et al., « Privacy and Pricing Personal Information », (2008) 187-3 *European Journal of Operational Research* 857

LANGELIER, R., « La protection de la vie privée par la Commission d'accès à l'information : quelle vie privée? Quelle protection? En fonction de quels intérêts? », dans *Développements récents en droit de l'accès à l'information*, Service de la formation permanente du Barreau du Québec, 2005, EYB2005DEV1090

LEMIEUX, M., « L'affaire Groupe Aldo : réflexions sur l'encadrement juridique de la cybercriminalité dans les opérations bancaires et l'industrie des paiements », *Revue du Barreau*, 2014, EYB2014RDB139

LUNDBLAD, N. et B. MASIELLO, « Opt-In Dystopias », (2010) 7-1 *SCRIPTed* 155

NARAYANAN, A. et V. SHMATIKOV, « Robust De-anonymization of Large Sparse Datasets », (2008) *Proc. 29th IEEE Symp. on Security & Privacy* 111

NELSON, S.D. et J.W. SIMEK, « Security in the New Decade - What Goes Around Comes Around », (2011) 28 *GPSolo* 40

NISSENBAUM, H., « A Contextual Approach to Privacy Online», (2011)140-4 *Dædalus, the Journal of the American Academy of Arts & Sciences* 32

OHM, P., « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », (2010) 57 *UCLA Law Review* 1701

OHM, P., « The Underwhelming Benefits of Big Data », (2012) 161 U. *Pa. L. Rev.* 339

OTTO, P.N. et al., « How Data Brokers Should Handle the Privacy of Personal Information », (2007) 5-5 *IEEE Security & Privacy* 15

Prosser, W.L., « Privacy », (1960) 48 *Calif. L. Rev.* 383

RAINES, J., « The Digital Accountability and Transparency Act of 2011 (DATA): Using Open Data Principles to Revamp Spending Transparency Legislation », (2012-2013) 57 *N.Y. L. Sch. L. Rev.* 313

REMPELL, S., « Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas », (2006) 18 *Fla. J. Int'l L.* 807

SCHWARTZ, P.M. et D.J. SOLOVE, « The PII Problem : Privacy and a New Concept of Personally Identifiable Information »,(2011) 86 *New York University Law Review* 1814

SCHWARTZ, P.M., « Information Privacy in the Cloud *»,* (2013) 161 *U.PA. L. Rev.* 1623

SHELANSKI, H.A., « Information, Innovation, and Competition Policy for the Internet », (2013) 161 *University of Pennsylvania Law Review* 1663

SOLOVE, D.J. et W. HARTZOG, « The FTC and Privacy and Security Duties for the Cloud », (2014) 13 *BNA Privacy & Security Law Report* 577

SOLOVE, D.J. et W. HARTZOG, « The FTC and the New Common Law of Privacy », (2014) 114 *Columbia Law Review* 583

SOLOVE, D.J., « A Taxonomy of Privacy », (2005-2006) 154 *U. Pa. L. Rev.* 477

STEWART, D.W. et Q. ZHAO, « Internet Marketing, Business Models, and Public Policy », (2000) 19-2 *Journal of Public Policy & Marketing* 287

STRAHILEVITZ, L.J., « Toward a Positive Theory of Privacy Law », (2012-2013) 126 *Harv. L. Rev.* 2010

TEECE, D.J., « Business Models, Business Strategy and Innovation », (2010) 43 *Long Range Planning* 172

TENE, O. et J. POLONETSKY, « Big Data for All: Privacy and User Control in the Age of Analytics », (2012-2013) 11 *Nw. J. Tech. & Intell. Prop*. 239

TERRY, N.P., « Protecting Patient Privacy in the Age of Big Data », (2012-2013) 81 *UMKC L. Rev.* 385

TERRY, N.P., « What's Wrong With Health Privacy? », (2009) 5 *Journal of Health & Biomedical Law* 1

THOMAS, P.N., « Little Brother's Big Book : The Case for a Right of Audit in Private Databases », (2009-2010) 18 *CommLaw Conspectus* 155

THOMSON, J.J., « The Right to Privacy », (1975) 4-4 *Philosophy and Public Affairs* 294

WARREN, S.D., et L.D. BRANDEIS, « The Right to Privacy », (1890) 4-5 *Harvard Law Review*193, pp.193-220, en ligne : <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>

WELINDER, Y., « A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks », (2012-2013) 26 *Harv. J. L. & Tech.* 165

WHITMAN, J.Q., « The Two Western Cultures of Privacy: Dignity Versus Liberty », (2004) 113-6 *The Yale Law Journal*, p. 1153, en ligne: <http://www.yalelawjournal.org/the-yale-law-journal/article/the-twowestern- cultures-of-privacy:-dignity-versus-liberty/>

YAKOWITZ, J., « Tragedy of the Data Commons », (2011-2012) 25 *Harv. J. L. & Tech.* 1

Documents gouvernementaux

CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *On the Data Trail : How Detailed Information About You Gets Into the Hands of Organizations With Whom You Have No Relationship*, Report on the Canadian Data Brokerage Industry, Ottawa, CIPIC, 2006

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Introduction to Cloud Computing*, Fiche d'information, Gatineau, CPVPC, en ligne : < https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf >

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Online Behavioural Advertising (OBA)*, Follow Up Research Project, Gatineau, CPVPC, 2015

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc.*, Gatineau, CPVPC, 2009, en ligne : < https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.asp>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de conclusions Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels*, Gatineau, CPVPC, 2012, en ligne : <https://www.priv.gc.ca/cf-dc/2012/2012_001_0229_f.asp>

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Le profilage et la publicité ciblée*, Fiche d'information, Québec, CAI, 2013

FEDERAL TRADE COMMISSION (FTC), *Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report, 2012

FEDERAL TRADE COMMISSION (FTC), *Data Brokers – A Call for Transparency and Accountability,* 2014

GOUVERNEMENT DU QUÉBEC, *Guide des responsables Web : Pratiques recommandées pour l'application du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels,* Ministère des Services Gouvernementaux*,* 2008

INTERNET POLICY TASKFORCE, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, U.S. Department of Commerce, 2010

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, Gaithersburg, U.S. Department of Commerce, 2012

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST Definition of Cloud Computing*, Special Publication 800-145, Gaithersburg, U.S. Department of Commerce, 2011

THE WHITE HOUSE, *Big Data : Seizing Opportunities, Preserving Values*, Washington, 2014

THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Washington, 2012

UNITED STATES COMPUTER EMERGENCY READINESS TEAM, *The Basics of Cloud Computing*, Pittsburgh, Carnegie Mellon University, 2011

Documents internationaux

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Advice Paper on Essential Elements of a Definition and a Provision on Profiling Within the EU General Data Protection Regulation*, Advice Paper, Bruxelles, 2013

JOUROVA V., *Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties*, Justice and Home Affairs (LIBE), 26 Octobre 2015

KUNEVA, M., *Keynote speech at the Roundtable on Online Data Collection, Targeting and Profiling*, Reference: SPEECH/09/156, Bruxelles, 2009

OHLHAUSEN, M.K., *Remarks of Commissionner Maureen K. Ohlhausen – Forum Global*, Cloud Computing Conference, Washington DC, 2014

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, No. 176, OECD Digital Economy Papers, 2011, en ligne : http://dx.doi.org/10.1787/5kgf09z90c31-en.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The OECD Privacy Framework,* Working Party on Information Security and Privacy (WPISP), 2013, en ligne : <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

POULLET, Y., M. DINANT et al., *Rapport sur l'Application des principes de protection des Données aux Réseaux Mondiaux de Télécommunication : L'autodétermination Informationnelle à l'Ère de l'Internet*, Comité Consultatif de la Convention pour la Protection des Personnes à l'égard du Traitement Automatisé des Données à Caractère Personnel, pour le Conseil de l'Europe, 2004

Sites

Charles DUHIGG, «How Companies Learn Your Secrets», *The New York Times*, en ligne : <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=&_r=0>

DATA.GOV, « Glossary of Terms », en ligne : <http://www.data.gov/glossary>

DIGITAL ADVERTISING ALLIANCE, «Self-Regulatory Principles Overview», en ligne : <http://www.aboutads.info/obaprinciples>

Eli PARISER, «Eli Pariser: Beware online "filter bubbles"» *TedX*, en ligne : <http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles#t-397884>

EUROPA, «I14012», dans *EUR-Lex*, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Al14012>

FACEBOOK, « Facebook's Privacy Policy - Full Version», en ligne : <https://www.facebook.com/note.php?note_id=%20322194465300>

GAUTRAIS, V., « Rapport auprès de la Commission d'accès à l'information (CAI) », *Gautrais.com*, en ligne : <https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/ >

HARVARD LAW, « Meme patrol: "When something online is free, you're not the customer, you're the product." », *Harvard Law Blogs*, en ligne : <http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/>

HHS.GOV, «Your Rights Under HIPAA», en ligne: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html>

INTELIUS, «People Search», en ligne : <http://www.intelius.com/people-search.html>

INTERNET MOVIE DATABASE (IMDB), en ligne : < http://www.imdb.com/>

IT LAW WIKI, «Big Data», en ligne : < http://itlaw.wikia.com/wiki/Big_data >

IT LAW WIKI, «Data Broker», en ligne : <http://itlaw.wikia.com/wiki/Data_broker>

LEXISNEXIS, «Accurint® for Law Enforcement», *Risk Solutions,* en ligne : <http://www.lexisnexis.com/risk/products/government/accurint-le.aspx >

LEXISNEXIS, «Product Index», *Risk Solutions*, en ligne : <http://www.lexisnexis.com/risk/products/>

NETFLIX, en ligne : < http://www.netflix.com/>

SEARCH ENGINE WATCH, «Google + DoubleClick = 69% of Online Advertising Market», en ligne : <http://searchenginewatch.com/article/2054513/Google-DoubleClick-69-of-Online-Advertising-Market>

WIKIPEDIA, «Redlining», en ligne : <http://en.wikipedia.org/wiki/Redlining>