

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

DONNÉES PERSONNELLES ET COMMERCE ÉLECTRONIQUE : POUVONS-NOUS,
EN TANT QUE CONSOMMATEURS EN LIGNE, TIRER PROFIT DE NOS DONNÉES
PERSONNELLES?

TRAVAIL DIRIGÉ
PRÉSENTÉ
COMME ÉXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE (POLITIQUE INTERNATIONALE/DROIT
INTERNATIONAL)

PAR
ALEJANDRO DE LA TORRE

AVRIL 2021

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce document diplômant se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév.10-2015). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

REMERCIEMENTS

D'un point de vue académique, je tiens à exprimer toute ma reconnaissance à la directrice de mon travail dirigé, Madame Michèle Rioux. Je la remercie de m'avoir encadré et orienté dans la réalisation de ce travail. Ses conseils et surtout sa confiance en mes capacités d'analyse m'ont permis de bien exprimer mes idées et bien structurer les résultats de la recherche. Je tiens aussi à témoigner toute ma reconnaissance à Monsieur Christian Deblock, professeur du Département de science politique à l'UQAM, qui, en compagnie de Madame Rioux, ont suscité mon intérêt à choisir le sujet des données personnelles et commerce électronique grâce aux cours, aux séminaires, et à l'école d'été sur le commerce international qu'ils ont offert durant mes deux années à la maîtrise.

D'un point de vue professionnel, je tiens à remercier le Groupe Restos Dix30, notamment, Monsieur Claude Labonté pour avoir déposé sa confiance en moi les 12 dernières années. Le rôle que j'ai pris au sein de son entreprise m'a permis d'établir un équilibre de vie entre l'école et le travail de façon personnelle, professionnelle et financière. L'assiduité, l'attention au détail, la gestion du temps, la gestion du stress, le travail d'équipe et le sens d'amélioration continue sont des qualités qui m'ont permis de devenir un meilleur employé mais aussi un meilleur élève. La discipline a sans doute été mon meilleur outil de performance.

D'un point de vue personnel, je tiens à remercier tous les membres de ma famille, mes amis et spécialement ma fiancée Rose-Marie Vallée qui m'a énormément soutenu. Sans son appui moral, ce travail n'aurait pas été possible. Les moments les plus difficiles de ma vie sont arrivés durant la période de rédaction de ce travail mais la volonté de finir ce que j'ai commencé, le support émotionnel de mes chers et la discipline ont fait en sorte que ce travail représente une réussite non seulement dans l'angle académique mais aussi un accomplissement au niveau personnel.

TABLE DES MATIÈRES

REMERCIEMENTS.....	ii
RESUMÉ.....	2
INTRODUCTION	3
PROBLÉMATIQUE	6
MÉTHODOLOGIE.....	8
STRATÉGIE D'ARGUMENTATION ET STRUCTURE DU TRAVAIL.....	10
CHAPITRE I Données Personnelles : Moteur des GAFA et de Microsoft.....	12
1.1 Portrait économique des GAFA et Microsoft (2015-2019)	13
1.2 « Alexa, Pouvons-nous tirer profit de nos données personnelles? ».....	15
1.3 « Hey Siri! Mes DP, sont-elles bien protégées avec Facebook? ».....	18
1.4 Google vs Microsoft : Deux géants, un seul marché.....	20
CHAPITRE II Reconfiguration du cyberspace : est-elle possible?	23
2.1 Structure du cyberspace : Centralisation des intérêts des géants du Net.....	24
2.2 Radiographie des responsables du monopole cybernétique	27
2.3 Fonctionnement du cyberspace	30
2.4 Reconfiguration du cyberspace : vers un modèle décentralisé?.....	33
CHAPITRE III Régulation du Cyberspace : Atteinte à la vie privée.....	38
3.1 Chine vs Canada : Régulation contraignante vs Régulation responsable.....	39
3.2 États-Unis vs Canada : Régulation laxiste vs Régulation cartésienne.....	42
3.3. Europe vs Canada : Régulation proactive vs Régulation innovante.....	44
3.4 Régulation Hybride canadienne : IA à la rescousse de la vie privée.....	49
CONCLUSION.....	55
BIBLIOGRAPHIE.....	58

RESUMÉ

À l'intérieur de ce travail, nous évaluons la possibilité de voir une ristourne économique vers les internautes qui mettent leurs données personnelles à disposition des GAFAM (Google, Facebook, Amazon, Apple et Microsoft). Notre recherche se base sur une revue littéraire. C'est un sujet d'actualité qui nous affecte tous et dont l'évolution constante de la problématique est indéniable. Nous faisons face à la problématique de l'atteinte à la vie privée causée par le manque de protection des données personnelles sur le cyberspace. La technologie avance plus rapidement que la régulation le fait. Si les données ne sont pas protégées adéquatement il est impossible de penser à une marchandisation de celles-ci. L'intervention de l'État est nécessaire à des fins de régulation et de distribution des profits des données personnelles. Nous examinons d'abord le portrait économique des GAFAM afin de démontrer que les profits venant des données personnelles ne sont pas distribués aux internautes. Ensuite, nous constatons que la nature centralisatrice du cyberspace favorise le monopole de celui-ci par les GAFAM. Nous terminons avec une comparaison de la régulation des données personnelles dans le Canada, les États-Unis, l'Europe et la Chine afin de démontrer la nécessité d'uniformiser les règles de protection de la vie privée pour éviter des vols, de la fraude, mais aussi la collecte, le stockage et l'exploitation sans consensus des données personnelles.

Mots clés : données personnelles, cyberspace, GAFAM, vie privée, commerce électronique, régulation, monopole.

Six millions de Canadiens touchés par une fuite massive de données chez Capital One¹. Quatre millions de membres de Desjardins ont été touchés par une fuite de données personnelles². Ces événements sont survenus au cours de la dernière année et lancent un cri d'alarme dans la population québécoise. La confidentialité et la protection des données personnelles font la une des journaux. La crise de la COVID-19 accentue le besoin de la population à numériser plusieurs secteurs de l'économie comme le télétravail, la télémédecine et l'éducation en ligne. La pandémie montre une carence en matière de numérisation de l'économie au Canada et souligne l'importance de la technologie dans notre quotidien.

La technologie de l'information est au rendez-vous, mais à quel prix? Le traçage numérique de la population, l'avènement des caméras thermiques aux entrées de commerces et des aéroports, la géolocalisation des gens ayant été en contact avec le virus grâce au téléphone mobile en sont des exemples qui soulignent une présence envahissante de la technologie dans le quotidien. Est-ce que nos données personnelles sont bien protégées? Quel profit tire la population à divulguer toutes ces données en masse? Le constat que plusieurs font est que nos données personnelles ne nous appartiennent plus. Le contrôle que nous avons sur ces données est assujéti à la volonté des grandes firmes technologiques.

Le sujet du travail dirigé porte sur les données personnelles, plus précisément sur la marchandisation de celles-ci. Les gains économiques que les internautes tirent grâce à leurs données personnelles sont inexistantes contrairement aux géants de l'Internet qui font fortune avec l'information. Ce travail explore la possibilité de voir les données

¹ La Presse Canadienne (2019, Juillet 30). Capital One victime d'une fuite massive des données. *Les Affaires*. Récupéré de <https://www.lesaffaires.com/bourse/nouvelles-economiques/capital-one-victime-d-une-fuite-massive-de-donnees/611743>

² La Presse Canadienne (2019, Novembre 1^{er}). Fuite chez Desjardins : 4.2 millions de membres touchés. *Les Affaires*. Récupéré de <https://www.lesaffaires.com/secteurs-d-activite/services-financiers/fuite-chez-desjardins-42-millions-de-membres-touchees/613897>

personnelles devenir une source de revenu pour les internautes à travers une restructuration de la gouvernance et de la régulation du cyberspace.

La protection des données personnelles remet en question la notion de contrôle que la population possède sur celles-ci. Ni l'État ni l'internaute n'exerce un contrôle sur la circulation des données personnelles dans le cyberspace. Ces données sont vulnérables. « *Les moteurs de recherche, l'adhésion à des réseaux sociaux permettent l'exploitation de données dans le cadre de finalités qui ne sont pas toujours affichées* »³. Plusieurs estiment que les données personnelles ne représentent qu'une identité numérique et qu'il n'y a pas vraiment de risque à l'atteinte de la vie privée. D'autres assurent que les données personnelles représentent le nouvel or de ce monde et moteur d'une économie numérique qui dominera le système international dans les années à venir; « *l'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue* »⁴.

La pertinence politique et juridique de ce travail repose sur le fait que les données personnelles donnent à la fois naissance à une nouvelle ère économique qui peut mettre en péril la vie privée des gens et bouleversent les théories politiques, sociales et économiques par le fait que ce n'est plus un contrat social entre État et individu, mais un contrat tripartite entre État, individus, et les géants du Net. La gouvernance et la régulation du cyberspace doivent être reformés afin de mieux protéger l'identité des internautes et d'assurer une répartition équitable des revenus du Big Data. Selon Dan Ciurak, ancien chef économiste du ministère des Affaires mondiales canadiennes, on assiste à l'essor d'une économie basée sur les données, qu'il nomme le *Data Driven Economy*. On passe d'un modèle axé sur l'exploitation du pétrole vers un modèle économique mondial axé sur l'exploitation du numérique. La dépendance au pétrole

³ Pouillet, Yves. « La loi des données à caractère personnel : Un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM*, vol. 42, no. 1, 2009, p. 47.

⁴ *Ibid.* p. 53.

tire à sa fin en raison des changements climatiques et des énergies alternatives⁵. Les flux numériques ont créé de nouvelles infrastructures, de nouveaux commerces, de nouvelles politiques et une canalisation des profits vers les géants du Net. Des milliards de personnes et même des objets sont connectés au cyberespace, l'univers digital croît de façon exponentielle à chaque année⁶. « Pomper » tout ce flux numérique est possible grâce aux mégas-centres de data dont Amazon et Microsoft sont les pionniers. Les firmes devront adapter leurs infrastructures et leurs modèles d'affaires pour s'adapter à l'économie numérique.

De plus, l'évolution des technologies oblige les législateurs à remettre en question le droit en termes de protection et de gestion de données personnelles. Il existe des divergences juridiques entre le pays. Par exemple, aux États-Unis, la vie privée n'est pas un droit garanti, mais un privilège légal. En Europe, la vie privée fait partie des Droits de l'Homme au même titre que la liberté⁷. Au Canada, qui reste en arrière-plan en raison de leur faible capacité économique, le gouvernement opte pour une approche européenne rénovée où il doit concentrer ses efforts à développer son expertise technique dans le champ de l'intelligence artificielle. Le Canada cherche à s'ériger comme acteur incontournable dans une économie basée sur les données. Dans le cas de la Chine, fier compétiteur des États-Unis, ils contrôlent étroitement leur cyberespace et optent pour des politiques de surveillance sur leur population. Au cours des prochaines années, les instances étatiques devront affronter un défi en matière d'économie numérique. Il faut assurer un respect de la vie privée sans ralentir le développement économique. L'aspect social indique que la protection de la vie privée est menacée par

⁵ Ciurak, Dan. « Economics of AI/ML and Big Data in the Data-driven Economy: Implication for Canada's Innovation Strategy », *CIPPO-CIGI Workshop on Intellectual Property and AI and Big Data*, Mars 2019, p. 2.

⁶ Anonyme (2017, Mai 6) Fuel of the future: Data is giving rise to a new economy. How is it shaping up? *The Economist*. Récupéré de <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>

⁷ Dumoulin, Régis, et Caroline Lancelot Miltgen. « Entreprise et respect de la vie privée du consommateur. De l'usage autorisé à l'utilisation souhaitable des données personnelles », *Revue française de gestion*, vol. 224, no. 5, 2012, p. 96

la dépendance des personnes avec la technologie. « *Plus nous sommes connectés, plus nos environnements sont complexes, mais plus nous sommes vulnérables* »⁸.

La question de recherche est : **pouvons-nous, en tant que consommateurs en ligne, tirer profit de nos données personnelles?**

Problématique

La problématique de ce travail repose sur l'atteinte à la vie privée causée par le manque de protection des données personnelles. Si les données ne sont pas protégées adéquatement il est impossible de penser à une marchandisation de celles-ci. Les internautes se contentent de cliquer un « oui » ou un « j'accepte » lors de leur navigation sur le cyberspace. « *De tous les biens informationnels, les données qui décrivent notre identité, nos opinions, nos affinités, sont les plus précieuses. À nos yeux, bien sûr, mais aux yeux des marchands qui nous traquent aussi* »⁹. Les internautes deviennent des objets étiquetés et exploités par des grandes compagnies comme Google, Amazon, Facebook, Apple et Microsoft (GAFAM). La société connectée sur le net est devenue une simple machine à produire de la plus-value pour les entreprises. « *Le travailleur intellectuel remplace le prolétaire de l'ère industrielle pour produire une plus-value issue de la transformation de l'information en connaissance* »¹⁰. Le manque de protection facilite l'exploitation des données personnelles par les géants du numérique qui font des profits monétaires aux dépens des internautes. Les données circulent librement et sont vendues sans consensus. Les compagnies utilisent des outils tels que le profilage et la publicité ciblée afin d'obtenir des grandes retombées économiques. Les internautes sont laissés à l'oubli et ne touchent aucun revenu monétaire.

⁸ Establier, Alain. « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *Sécurité globale*, vol. 8, no. 4, 2016, p. 36.

⁹ Arnaud, Michel. « Démonétiser l'identité numérique », *Médium*, vol. 16-17, no. 3, 2008, p. 191

¹⁰ *Ibid.* p.193.

Les GAFAM et Microsoft utilisent le concept de la technologie de l'ubiquité qui permet aux terminaux (objets) placés dans la maison d'enregistrer les faits les plus anodins de notre vie quotidienne tels que nos déplacements d'une pièce à l'autre, nos conversations, nos hésitations et notre consommation domestique. Cette technologie « adapte son fonctionnement aux données obtenues par nos actions quotidiennes. Exemple : arriver à la maison à 18h, allumer le four, ouvrir la télévision, régler la température, faire couler le bain, le café et bien d'autres.¹¹ Bien des questions restent sans réponse concernant cette technologie par exemple qui la lit? Quand? Quelles informations sont retenues? Pour qui sont-elles retenues et dans quel but? Quels profits font ces compagnies sur ces données collectées? Ces entreprises refont le monde sans doute en proposant des produits et des services qui sont incontournables dans notre quotidien. Elles sont complètement infiltrées dans nos vies, il est impossible de les éviter. Ces compagnies ont littéralement kidnappé, monopolisé puis monétisé une bonne partie de nos existences dans un vide législatif quasi total¹². En somme, les micros dans nos téléphones, les caméras des télévisions intelligentes et les GPS dans nos montres produisent des données fournies gratuitement à des marchands numériques qui ne veulent que vendre leurs produits ou services sans se soucier de la problématique de la protection de la vie privée. Ce travail souligne la dynamique invasive contre notre vie privée. Les données des internautes peuvent être mieux protégées, les revenus du Big Data ne sont pas distribués équitablement entre les GAFAM et les internautes.

¹¹Pouillet, Yves. *Op. cit.* p.62.

¹² Galloway, Scott « Le Règne des Quatre : La face cachée d'Amazon, Apple, Facebook et Google », Gallimard Ltee-Edito, p.12

Méthodologie

La revue de littérature se base sur deux écoles de pensées distinctes dans les questions de régulation et de protection des données personnelles, plus précisément l'école américaine et l'école européenne. Les États-Unis ont une vision libertaire sur la régulation tandis que l'Europe prône une régulation plus accentuée¹³. Ce choix méthodologique est fait afin de montrer le manque de standardisation de la régulation des données personnelles. Le Canada, qui opte pour une approche régulatrice comme l'Europe, exerce son expertise technologique dans l'intelligence artificielle. D'ailleurs, « *the concept of data trusts that is being explored in Canada and elsewhere could potentially create the institutional framework for data aggregation, integration and mobilization for commercial purposes within a framework subject to strong fiduciary requirements [...] Canada has good prospects in AI/ML and good credentials in this area and could use trust-based governance to become arbitrarily large in cyberspace* »¹⁴. Du côté de la Chine, sa régulation numérique permet de voir que l'État peut avoir le contrôle du cyberspace. La Chine possède « *strong incentives to use digital tools to counter their opponents and ensure their political survival* »¹⁵. La régulation chinoise envahit la vie privée de ces citoyens. Cette modélisation entre les quatre régions mentionnées ci-haut permet de voir le manque de cohérence et de protection de la vie privée dans la communauté internationale.

Dans la revue de littérature, les travaux de Dan Ciurak portent sur l'économie basée sur les données, le droit du data, l'intelligence artificielle, la souveraineté du cyberspace et la monétisation des données personnelles. Le choix de Dan Ciurak pour supporter l'argumentation du travail se justifie par son expertise en la matière. On fait

¹³ Dumoulin, Régis, et Caroline Lancelot Miltgen. *Op. cit.* p.96

¹⁴ Ciurak, Dan. *Op. cit.* p.4.

¹⁵ Feldstein, Steven (2020, Février 12) «When it comes to digital authoritarianism, China is a challenge – but not the only challenge», *War on the rocks*. Récupéré de <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>

recours aussi à des auteurs comme Lawrence Hunter, Esther Dyson et Peter Hustinx qui s'attaquent aux questions de la commercialisation et la sécurisation des données personnelles à travers les adresses IP. Le travail s'appuie aussi sur l'auteur Stephens-Davidowitz, qui a écrit le livre « *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*¹⁶ ». Il décrit comment l'Internet et toutes les données que nous mettons à sa disposition démontrent que le Big Data connaît et contrôle la société. Cet auteur a travaillé pour le centre de Google Data Analytics. Il nous assure que le Data est une source quantifiable et qualifiable lorsqu'elle est mise en relation, elle devient très puissante puisqu'elle peut faire rouler le commerce électronique et la publicité ciblée. Le Data peut lire nos émotions et influencer un événement politique comme ce fut le cas de l'élection de Donald Trump. Finalement, Scott Galloway, professeur à la Stern School of Business de l'Université de New York dévoile dans son livre « Le règne des quatre » comment les GAFA contribuent à la manipulation émotionnelle et l'exploitation en masse des données personnelles¹⁷.

Plusieurs auteurs français tels que Michel Arnaud, Arnaud Belleil, et Pierre Bienvenue, écrivent sur des enjeux de régulation numérique en Europe. Ils ont développé, dans leurs écrits, une logique fondée sur le respect de la vie privée. Nous reprenons cette logique dans la problématique de ce travail en raison du faible contrôle que la population possède sur leurs données personnelles. De plus, le recours à des revues comme *The Economist* et *les Affaires* nous permet de prendre en considération les développements les plus récents dans le monde du numérique. Des organes gouvernementaux tels que la Commission nationale de l'Informatique et des Libertés (CNIL) et le Commissariat à la protection de la vie privée au Canada permettent de

¹⁶ Stephens-Davidowitz, Seth, « *Everybody Lies: The New York Times Bestseller* », *Bloomsbury Publishing*, 2017, p. 12.

¹⁷ Galloway, Scott, « *Le Règne des Quatre : La face cachée d'Amazon, Apple, Facebook et Google* », *Gallimard Ltée-Edito*, p.45.

voir sur quels principes juridiques se base la protection des données actuelle dans les cas français et le cas canadien. Finalement, le Centre International de Gouvernance et Innovation (CIGI) est un *think tank* qui réunit une série d'experts sur la numérisation de l'économie et la gouvernance de l'Internet. Ces experts débattent sur les enjeux actuels qui touchent la protection des données dans le cyberspace.

Stratégie d'argumentation et structure du travail

Le travail cherche à répondre si les internautes sont capables de tirer un profit monétaire pour mettre à disposition des GAFAM leurs données personnelles. La réponse à cette question est : Oui, les internautes peuvent tirer profit à condition que l'État intervienne pour taxer davantage les GAFAM. L'intervention de l'État est nécessaire car le profit individuel pour chaque internaute n'est pas une somme significative comme on le constatera plus loin dans ce travail. Le gouvernement peut augmenter les impôts sur ces grandes firmes technologiques à condition que cette taxe soit distribuée à travers la société. Une condition doit être mise en place dès le début. Il est crucial d'implanter une régulation du cyberspace axée sur la protection de la vie privée des internautes pour éviter une mauvaise utilisation de nos données. Trois chapitres établiront les résultats de la recherche et montreront pourquoi il est préférable de reconduire les profits vers les États avant les internautes.

Le premier chapitre présente un portrait de l'économie numérique qui passe incontestablement par les grands acteurs de ce secteur qui sont les GAFAM. Le but de ce chapitre est d'exposer comment ces compagnies font du profit au dépend des internautes. **C'est la première étape qui démontre l'exploitation inégalée et sans consensus des données personnelles afin de créer des profits pour les géants du net.** La publicité ciblée est un élément crucial dans ce processus. Les GAFAM et Microsoft utilisent nos données à des fins de profit, de manipulation et de surveillance. Des éléments comme Alexa d'Amazon, Siri d'Apple et le marché des deux géants comme Google et Microsoft seront présentés dans ce chapitre.

Le deuxième chapitre présentera la configuration du cyberspace. Les internautes doivent avoir accès à un cyberspace totalement reconfiguré, car le système actuel ne favorise que les grands monopoles du web. Réguler de façon optimale ce cyberspace sera la clé pour diminuer la monopolisation de celui-ci par les grandes compagnies numériques. **C'est la deuxième étape à suivre afin de réussir une marchandisation juste et équitable des données personnelles.** Les éléments discutés dans ce chapitre aborderont la centralisation et canalisation des intérêts des géants du Net. Une radiographie des GAFAM montrera comment ils monopolisent le cyberspace. Finalement, le fonctionnement et la gouvernance du cyberspace seront présentés afin de voir la possibilité de voir un modèle décentralisé dans le cyberspace.

Le troisième chapitre porte sur le rôle de l'État dans la protection des données personnelles dans le cyberspace. Les internautes doivent profiter d'un cadre juridique qui protège leurs données non seulement des vols et de la fraude, mais aussi de la collecte, du stockage et de l'exploitation sans consensus pour un usage à des fins de profit de la part des géants numériques. Les États doivent uniformiser la réglementation et s'appuyer sur l'intelligence artificielle pour mieux protéger les internautes. **C'est la troisième étape à suivre afin de réussir une marchandisation juste et équitable des données personnelles.** Les États-Unis, l'Europe, le Canada, et la Chine sont les quatre régions mises en perspectives pour comparer leur régulation et démontrer qu'il existe une nécessité d'uniformiser et simplifier la régulation du cyberspace à des fins de protection de la vie privée des internautes.

Chapitre I - Données Personnelles Moteur des GAFA et de Microsoft

En 2020, l'industrie de la technologie n'a jamais été aussi indispensable à l'économie. Les cinq plus grandes firmes technologiques du Silicon Valley font 20% de la valeur boursière du S&P 500. L'industrie technologique subit un renouveau. Ses modèles d'affaires sont basés sur les abonnements et le commerce électronique. D'ailleurs, Google a vu ses ventes augmenter de 13% au premier trimestre de 2020. Microsoft a enregistré des bénéfices de 10,8 milliards pour la même période. Les trois milliards d'utilisateurs de Facebook passent de plus en plus de temps sur cette application. Netflix a ajouté 16 millions de nouveaux abonnés au cours de ce trimestre Microsoft et Amazon fournissent l'infrastructure cruciale pour le travail à distance sans oublier la dépendance aux services de cloud computing et commerce en ligne offerts par ces géants informatiques¹⁸.

Les données personnelles sont le moteur du cyberespace. Les sociétés se numérisent et la crise sanitaire a accentué cette tendance. Par contre, les données personnelles ne sont pas mieux protégées, au contraire la régulation s'adaptant mal à l'évolution rapide de la technologie. En définitive, ce sont que les grandes firmes du cyberespace qui en tirent des profits.

Les préoccupations croissantes des consommateurs pour le respect de la vie privée ne sont pas prises en considération par les firmes technologiques qui désirent en connaître davantage sur leurs clients. Le plan d'affaire de ces grandes firmes s'oriente vers un contrôle plus étroit des données sur les individus (clients, consommateurs, salariés)¹⁹. Les internautes ne sont pas bien informés sur ce qu'est une information personnelle ni sur quelle instance un traitement de leurs données constitue une invasion à leur vie

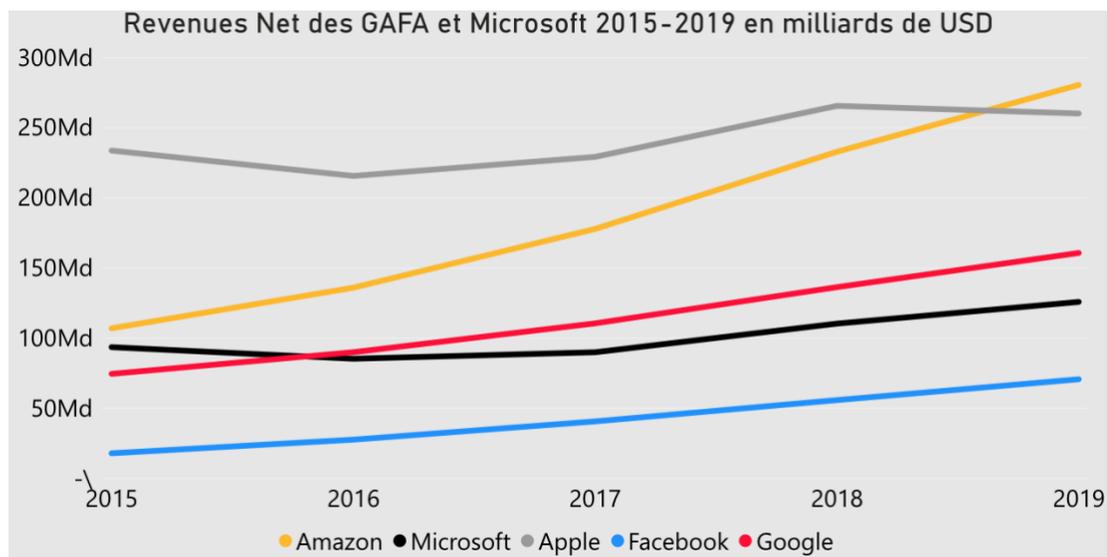
¹⁸ Anonyme (2020, April 30), «Big tech is thriving in the midst of the recession», *The Economist*, Récupéré de <https://www.economist.com/leaders/2020/05/02/big-tech-is-thriving-in-the-midst-of-the-recession>

¹⁹ Dumoulin, Régis, et Caroline Lancelot Miltgen. *Op. cit.* p. 96.

privée. Il est clair que les données personnelles doivent être protégées davantage par des règles plus strictes; mais il faut souligner aussi que les GAFAM peuvent être taxés davantage afin que la société voie une ristourne monétaire investie dans les biens publics, les systèmes de santé, l'éducation ou même dans la réduction du taux d'imposition des particuliers. Dans ce chapitre, nous allons faire une radiographie des GAFA et Microsoft afin d'exposer leur méthode de traitement des données personnelles ainsi que leurs revenus sur le Big Data.

1.1 Portrait économique des GAFA et de Microsoft (2015-2019)

Les graphiques suivants ont été faits grâce au logiciel Microsoft Power BI qui a permis de mettre en relation les états financiers des géants du net durant la période de 2015-2019. Tous les chiffres proviennent du centre des données de Statista²⁰.



Depuis 2015, les données montrent une tendance à la hausse des revenus des GAFAM. Le but de ce travail est de savoir si les internautes peuvent tirer profit de leurs données personnelles. Le graphique précédent montre les grandes retombées économiques de

²⁰ Statista [s.d.]. Récupéré le 21 mai 2020 de <https://www.statista.com>

ces compagnies par la vente de leurs produits, leurs services, et le Big Data. Nous connaissons la valeur de leurs produits, de leurs services, mais, connaissons-nous la valeur monétaire de nos renseignements? Une étude menée par le *think tank* américain Technology Policy Institute (TPI), soulève des questions sur la monétisation des données personnelles par les grandes plateformes technologiques ainsi que l'atteinte à la vie privée des internautes. L'étude démontre que les gens sont plus réticents à partager leurs données bancaires sur ces plateformes que de partager des données personnelles autres que financières. Les participants à l'étude proviennent des différents milieux culturels. Les Américains ne portent pas attention à la régulation et les Européens soulèvent l'importance d'instaurer des règles plus strictes en matière de régulation. Ceci démontre qu'il existe aussi une divergence culturelle en matière de régulation des données personnelles.

*«A technology platform, on average, across all people the study assessed. Would have to pay consumers a monthly \$8.44 to share their bank balance information, \$7.56 to share fingerprint information, \$6.05 to read an individual's texts, and \$5.80 to share information on cash withdrawals. By contrast, people wanted to be paid only **\$1.82** per month to share location data **and nothing** to be sent advertisements via text messages²¹ ».*

Voici une des raisons pour lesquelles les profits du Big Data doivent passer par l'États avant les internautes. Si on se fie à cette étude, le montant d'argent qu'un internaute pourrait avoir n'est pas significatif. Cependant, la mise en relation et la congrégation de toutes les données dans un ensemble, ce qu'on appelle le Big Data, représente une grande fortune pour les plateformes technologiques qui siphonnent ces données. Dan Ciurak mentionne que l'économie basée sur les données est asymétrique puisqu'elle ne répartit pas équitablement les profits aux participants de celle-ci :

²¹ Prince, Jeffrey and Scott Wallsten. «How Much is Privacy Worth Around the World and Across Platforms» *Technology Policy Institute*, January 2020, p.6.

« In the data-driven economy, data sometimes is the product itself [...] Sometimes it is monetized and hence its value is recorded in the conventional economic accounts, but in most current uses it is captured without payments and without generating an ensuing paper trail of invoices and receipt. Taking implicit value as a guide, one indicator of the value of data is the value of free services acquired by consumers from the Internet [...] Looking at the other side of the transaction, this data generates intangible assets for data-driven firms such as Google, Facebook, and Uber. This puts the likely market value of data in its emerging role as the essential capital of the data-driven economy in the trillions of dollars at the dawn of the data-drive-economy era, with potential for even greater expansion as the digital transformation races forward²² »

Suite aux propos de Ciurak qui démontrent l'inégalité des profits sur le data. Les internautes font face à un dilemme : Protéger leur vie privée ou assurer une division équitable des profits sur le Big Data entre les GAFAM et eux. Il est clair que le manque de protection de la vie privée dans le cyberspace représente un avantage économique pour les GAFAM, mais le profit qu'un internaute pourrait se voir concéder n'est pas significatif puisque le Big Data comme ensemble des données a plus de valeur qu'une seule donnée personnelle. C'est ici que l'État intervient puisqu'il peut taxer davantage ces firmes afin de redistribuer les profits sur la société.

1.2 « Alexa, Pouvons-nous tirer profit de nos données personnelles? »

Amazon s'invite au cœur même de nos foyers par des appareils domestiques intelligents (télévisions, frigidaires, haut-parleurs, entre autres). *«"Alexa, are you recording everything you hear? " It is a question more people are asking, though Amazon's voice assistant denies the charges. "I only record audio back to the amazon cloud when you say the word" [...] Apple's voice assistant, Siri gives a similar answer²³»*. Nous faisons face à une problématique d'invasion de la vie privée. On ne

²² Ciurak, Dan, «The economics of Data, Implications for the Data-Driven Economy», *Centre for International Governance Innovation*, Février 2018, p.6.

²³ Anonyme, (2019, Mai 11), «How creepy is your smart speaker», *The Economist*, Récupéré de <https://www.economist.com/leaders/2019/05/11/how-creepy-is-your-smart-speaker>

sait pas tous les dangers potentiels qui sont liés à la numérisation (appareils technologiques comme le cas d'Alexa) dans nos foyers. Le plus grand magasin virtuel au monde dépasse déjà la valeur de Walmart, Target, Macy's, Kroger, Nordstrom, Tiffany & Co., Coach, Williams-Sonoma, Tesco, Ikea, Carrefour et Gap réunis²⁴. La division d'Amazon Web Services est celle qui croît le plus rapidement. Cette division offre des services infonuagiques qui carburent en grande partie au traitement de nos données personnelles. « *The shift of our economy and society online is taking place without a referendum*²⁵ ». Dans la société capitaliste, un des concepts fondamentaux du commerce, est celui qui place le consommateur règne en maître. Le virage technologique vient bousculer le secteur du commerce de détail classique. Un secteur qui était autrefois caractérisé par le grand nombre de ses intervenants est en train d'être dévoré par un seul acteur : Amazon.

D'un côté, Amazon crée des nouvelles opportunités d'emplois notamment dans le domaine des services technologiques, dans les entrepôts, entre autres. D'un autre côté, il est la raison pour laquelle le secteur du commerce en détail est affecté. « *La nature virtuelle d'Amazon lui permet de conquérir des centaines de millions de consommateurs et de couvrir presque toutes les industries du commerce de détail, sans se coltiner la corvée habituelle de la construction de magasins en dur et du recrutement des milliers d'employés*²⁶ ». Cette nature virtuelle permet à Amazon Marketplace de devenir la référence des vendeurs qui cherchent une plateforme pour vendre leurs produits. Pendant ce temps, Amazon accumule les données personnelles des clients et établit des comportements d'achat qui lui permet d'entrer sur n'importe quel marché. Grâce aux économies d'échelle (baisse des coûts par augmentation du volume produit), le géant du commerce électronique est capable d'offrir des prix qu'aucun autre

²⁴Galloway, Scott. *Op.cit.* p.18.

²⁵ Ciurak, Dan et Bianca Wylie, «Data and Digital Rights: More Questions than Answers- But Enumerating the Questions is Essential», *Centre for International Governance Innovation*, December 2018, p. 4

²⁶Galloway, Scott. *Op.cit.* p.46.

détaillant n'est capable de rivaliser. D'ailleurs, Amazon mise sur la robotisation de ses entrepôts.

« Consider Amazon's fulfilment centres. [...] Inside one on the outskirts of Seattle, packages hurtle along conveyor belts at the speed of a moped. The noise is deafening – and the facility seemingly bereft of humans. Instead, inside a fenced-off area the size of a football field sit thousands of yellow, cuboid shelving units [...] Amazon call them pods. Hundreds of robots shuffle these in and out of neat rows, sliding beneath them and dragging them around »²⁷.

La robotisation et l'utilisation de l'intelligence artificielle est un fait dans les entrepôts de Amazon. Il ne faut pas oublier qu'Amazon souhaite que « *ses clients lui accordent une telle confiance qu'ils sont en train d'autoriser l'entreprise à écouter leurs conversations et moissonner leurs données de consommation*²⁸ ». Amazon devient profondément ancré dans la vie privée des gens. Nos habitudes d'achat, nos goûts, nos conversations en famille ne font plus partie de notre vie privée puisque notre consommation en ligne ou des dispositifs comme Alexa peuvent donner un portrait précis de notre personnalité.

En somme, alors que plusieurs considèrent Amazon comme un détaillant virtuel, il est discrètement devenu la référence des entreprises infonuagiques ou *cloud*; soit celle qui entrepose les données personnelles de la planète sous une seule entité : Amazon Web Services. Lorsqu'un client utilise Amazon, il bénéficie généralement du meilleur prix du bien ou du service qu'il recherche. Cependant, il néglige que les données qu'il fournit, en faisant son achat, représentent pour Amazon le plus grand bénéfice. « *La prédictibilité des comportements des consommateurs et des citoyens instituera une forme d'esclavage électronique : ils perdront le contrôle de leur identité et seront réduits d'unités réparables*²⁹ ».

²⁷ Anonyme, (2019, April 13) « Amazon's empire rests on its low-key approach to AI », *The Economist*, Récupéré de <https://www.economist.com/business/2019/04/11/amazons-empire-rests-on-its-low-key-approach-to-ai>

²⁸ Galloway, Scott. *Op.cit.* p.54.

²⁹ Arnaud, Michel. « Démonétiser l'identité numérique », *Médium*, vol. 16-17, no. 3., 2008, p.197.

1.3 « Hey Siri! Mes DP, sont-elles bien protégées avec Facebook? »

La compagnie du logo en pomme est une des plus innovatrices sur le marché actuel. Chaque année, sa gamme des produits est rénovée afin d'offrir la meilleure expérience pour ses clients. Quand on pense Apple, on pense qualité. Leurs produits figurent parmi les plus performants dans le marché technologique. C'est une compagnie cool, et innovatrice mais hypocrite lorsqu'on touche le sujet du respect de la vie privée. Steve Jobs était le messie de l'économie de l'innovation et sa création fétiche qui est l'iPhone est souvent dans l'œil de la tempête en matière de protection des données personnelles³⁰. Pourquoi?

« If Apple really cared about personal data, the company could take any number of actions to keep privacy violators off its platforms and away from its customers [...] Despite Tim Cook's claim in Brussels that "the stockpiles of personal data serve only to enrich the companies that collect them", Apple does lots of deals with those companies. Safari, the web browser that comes with every iPhone, is set up by default to route web searches through Google. All those searches help funnel out enormous volumes of data Apple's users »³¹.

Aucune entreprise du secteur technologique n'a résisté au facteur de vieillissement, c'est-à-dire celui de perdre de son intérêt. Apple est la première firme technologique à avoir connu le succès multigénérationnel³². Pourquoi? Apple est une marque de luxe, une marque de standard social. Ses produits sont améliorés chaque année afin d'offrir les dernières technologies aux consommateurs. Cette dichotomie socio-économique comporte un prix élevé à la vie privée. « *Regarde toutes ces applications améliorant la productivité, elles sont si cool. Cet ordinateur portable fonctionne mieux. Cette montre m'encourage à faire 3000 pas de plus chaque jour³³* ». Comment notre vie privée est

³⁰ Galloway, Scott. *Op.cit.* p.99.

³¹ Bogonost, Ian, (2019, Janvier 31) « Apple's Empty Grandstanding About Privacy », *The Atlantic*, Récupéré de <https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/>

³² Galloway, Scott. *Op.cit.* p.107.

³³ *Ibid.* p.121.

affectée dans cet exemple? Après un entraînement suivi par votre Apple Watch qui connaît votre poids, votre âge, votre condition de santé, qui est lié directement à votre iPhone et à votre Mac. Vous allez certainement voir apparaître des publicités avec des offres pour des souliers de course, des vêtements de sport, des suppléments nutritifs, etc. Cet effet s'explique à travers la publicité ciblée. « *La publicité est désormais au cœur de nos sociétés libérales parce qu'elle fait vendre et pour le faire de manière efficace il lui faut avoir accès aux données personnelles*³⁴ ».

Facebook entretient une « relation profonde » avec deux milliards de personnes. Ce réseau social gratuit vivant de la publicité en ligne détient beaucoup trop d'informations sur la population. Il a un modèle d'affaires très simple : plus d'utilisateurs = plus de contenu = plus de publicité = plus d'argent³⁵. Ce concept de publicité en ligne sera développé dans la dernière partie du chapitre qui traite sur Google, champion de la publicité ciblée. De retour à Facebook, « *lorsqu'on s'intéresse aux influences poussant un consommateur à dépenser de l'argent, on constate que Facebook a inondé l'étape de la découverte, qui occupe le sommet de l'entonnoir du marketing*³⁶ ». Le moindre de nos actes en rapport avec Facebook est récolté et stocké. Nous sommes constamment redirigés vers ce que nous convoitons le plus en termes d'achats.

En somme, les utilisateurs d'iPhone ne réfléchissent pas au degré de protection de leurs données personnelles lorsqu'ils achètent un appareil d'Apple. Lorsqu'on visite le volet de Confidentialité sur la page d'Apple Canada, ils soulignent que le respect de la vie privée est un droit fondamental et un principe de base. « Ce que vous partagez, et les gens avec qui vous le partagez, ne devrait donc dépendre que de vous. Nous concevons les produits Apple pour protéger votre vie privée et vous donner le plein contrôle de vos données ». Ce n'est pas tout à fait vrai car Apple, « *avec sa montre connectée et*

³⁴ Arnaud, Michel. *Op. cit.* p. 192.

³⁵ Lyubareva, Inna, et Fabrice Rochelandet. « Modèles économiques, usages et pluralisme de l'information en ligne. Les nouveaux enjeux du pluralisme de l'information à l'ère des plateformes numériques », *Réseaux*, vol. 205, no. 5, 2017, p. 13.

³⁶ Galloway, Scott. *Op.cit.* p.139.

son enceinte vocale notamment, tend à collecter de plus en plus des données critiques sur la santé ou la vie du foyer de ses clients »³⁷. Cette vulnérabilité permet à d'autres compagnies de tirer des grands profits aux dépens des utilisateurs. Du côté de Facebook, il est en mesure de nous écouter, même dans un bruit ambiant, à partir du micro de notre iPhone. « Cela signifie que Facebook peut analyser ce bruit à l'aide d'un logiciel d'écoute dopé à l'intelligence artificielle, et déterminer qui vous détient compagnie, ainsi ce que vous faites »³⁸. Les cas d'Apple et de Facebook soulignent la vulnérabilité de nos données et accentuent le besoin de redistribuer les profits des GAFA et Microsoft vers la société.

1.4 Google vs Microsoft - Deux Géants, Un Marché

Les appareils mobiles seront le principal moteur de la croissance des dépenses publicitaires. Les compagnies veulent de plus en plus leur publicité affichée sur le net. Google et Facebook contrôlent 51% des dépenses publicitaires sur nos téléphones mobiles au niveau mondial, et leur part de marché augmente chaque jour³⁹. Google est la référence à toute question qu'un internaute peut se poser. C'est sans doute le moteur de recherche le plus puissant qu'il existe grâce à ses algorithmes.

« In 1998, Google showed up. And its search results were undeniably better those that of every one of its competitors. If you typed "Bill Clinton", you were given his website, the White House email address, and the biographies of the man that existed on the internet. Google seemed to be magic. [...] Today, people sick with the flu are likely to make flu-related searches. In essence, they would report their symptoms to Google. Indeed, searches such as "flu symptoms" and "muscle aches" have proven important indicators of how fast the flu is spreading⁴⁰ ».

³⁷ Mediavilla, Lucas (2019, Mars 22) « Données personnelles : Apple est-il vraiment le bon élève? » *Les Echos*, Récupéré de <https://www.lesechos.fr/tech-medias/hightech/donnees-privées-apple-est-il-vraiment-le-bon-eleve-1002692>

³⁸Galloway, Scott. *Op.cit.* p.146.

³⁹ *Ibid.* p. 159.

⁴⁰Stephens-Davidowitz, Seth. *Op. cit.* p. 57.

Toutes nos questions trouvent une réponse mais encore une fois à un prix très cher, celui de divulguer nos données personnelles gratuitement. Le moteur de recherche offre à chacun son savoir, si on doute sur l'achat d'un service ou d'un produit, on demande à Google. Comment survit-il? À travers la publicité en ligne qui représente une composante importante de son financement. Afin d'être rentable, la publicité doit être ciblée. Il faut afficher la bonne publicité, sur le bon terminal, du bon internaute et au bon moment⁴¹. Comment se fait le ciblage? En fonction du contenu (information que les internautes recherchent), de la localisation du consommateur et lors du moment de sa navigation. La publicité devient personnalisée. Comment on collecte? Par la récupération des données personnelles fournies volontairement par les internautes, c'est ce qu'on nomme une collecte active. Lorsque Google collecte ses données de façon passive, il le fait à travers les *cookies* (témoins de connexion) et autres techniques de traçage sur Internet permettant de distinguer le terminal de l'internaute des autres équipements terminaux. Les données personnelles permettent à Google de constituer des profils précis sur nous grâce à ces *cookies* qui sont des traceurs d'information dans l'équipement terminal de la personne concernée et que les fournisseurs des réseaux publicitaires y ont accès lorsque les personnes concernées visitent un site web partenaire⁴². « *Avec nos recherches, nous confessons des choses à Google que nous ne partagerions pas notre prêtre, notre mère, notre meilleur ami ou notre médecin*⁴³ ».

Microsoft est le système d'exploitation de 90% des ordinateurs de bureau. Office est toujours la suite bureaucratique par défaut dans le monde entier. L'offre du service cloud « Azure » est son pilier de croissance économique. Les GAFAs se focalisent sur les consommateurs. Microsoft se focalise sur les professionnels notamment avec LinkedIn, qui est une application de réseautage professionnel et développement de carrière. Cette application a trois sources de revenus : publicité sur son site, revenus

⁴¹ Dubois, Lorette, et Florence Gaullier. « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », *LEGICOM*, vol. 59, no. 2, 2017, p. 70.

⁴² *Ibid.* p. 72.

⁴³ Galloway, Scott. *Op.cit.* p.182.

des recruteurs pour mieux accéder aux données des candidats, et un abonnement premium aux utilisateurs qui permet d'optimiser ses recherches d'emploi⁴⁴. Voilà un autre exemple de comment stocker les données professionnelles des gens. D'un point de vue professionnel, quelle autre application offre ce que LinkedIn offre? Nulle autre. LinkedIn nous permet d'avoir un réseau de collègues de travail, d'effectuer des recherches d'emploi et de tracer une ligne entre notre réseau intime d'amis qu'on peut attribuer à Facebook et notre réseau de travail attribué à LinkedIn. De plus, Microsoft se démarque par ses puissants services *cloud* qui permettent que le Big Data soit exploité de façon optimale et rentable. « *Artificial Intelligence and Machine Learning engines that extract previously unattainable information, is being monetized to increase production and process efficiency to generate new products and disrupt existing markets [...] Moreover, while data cannot be owned, it can be sold*⁴⁵ ».

En somme, Google et Microsoft sont deux géants de la technologie. Leur seul marché à exploiter est celui des données personnelles. Les retombées économiques que cela représente pour les deux sont importantes. Pour nous, les internautes, les consommateurs, et les professionnels, les retombées sont inexistantes. Dans le prochain chapitre, on verra comment cette monopolisation des retombées économiques de la part des GAFAs et de Microsoft pourrait être altérée par la possibilité de voir une restructuration de la gouvernance du cyberspace.

⁴⁴ *Ibid.* p. 294

⁴⁵ Ciurak, Dan, «Data as Contested Economic Resource: Framing the Issues», *Centre for International Governance Innovation*, Novembre 2019, p. 3.

Chapitre II - La Reconfiguration du cyberspace est-elle possible?

Le 1^{er} février 2020, la capitalisation boursière des grandes compagnies technologiques, plus précisément les GAFA, atteignait environ quatre mille milliards de dollars américains. Pour leur part, la capitalisation des grandes compagnies asiatiques comme Tencent, Alibaba, Samsung atteignent environ mille milliards de dollars⁴⁶. Les GAFA possèdent quatre fois plus de valeur boursière que tous les autres compétiteurs dans l'économie numérique. De son côté, Microsoft possède des revenus atteignant les mille milliards de dollars US. Ces statistiques démontrent que l'influence américaine est incontestable dans le cyberspace.

L'américanisation du cyberspace est reflétée par la monopolisation du réseau global d'internet de la main des GAFAM. « *The biggest clouds have risen over America, which so far has set the rules of the data economy* »⁴⁷. L'américanisation du cyberspace est reflétée par la monopolisation du réseau global d'internet de la main des firmes technologiques⁴⁸. Les utilisateurs contribuent énormément au fonctionnement du cyberspace. Cependant, leurs données personnelles ne sont pas sécurisées. En fait, elles sont manipulées et exploitées de façon que les grandes compagnies du net effectuent des profits gigantesques aux dépens des utilisateurs. L'inégalité de profit se manifeste par le manque de protection des données personnelles causée par l'inertie centralisatrice du cyberspace. « *Ces entreprises sont au cœur des nouvelles économies numériques. Or, dans ce nouveau modèle d'activité économique, le terrain de jeu n'est pas national, il est immédiatement mondial et le leader rafle la mise en anéantissant du même coup toute la concurrence [...] Ces entreprises se nourrissent de l'analyse et de la revente de vos données, c'est-à-dire de vos choix, vos goûts et de vos centres*

⁴⁶ Anonyme, (2020, Février 20) « Who will benefit most from the data economy? », *The Economist*, Récupéré de <https://www.economist.com/special-report/2020/02/20/who-will-benefit-most-from-the-data-economy>

⁴⁷ Anonyme, (2020, Février 20) « Governments are erecting borders for data », *The Economist*, Récupéré de <https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data>

⁴⁸ *Ibid.*

*d'intérêt*⁴⁹ ». La question est de savoir s'il est possible de reconfigurer le cyberspace. À travers le chapitre suivant, on verra le comment et le pourquoi.

Ce chapitre se divise en quatre parties : en premier lieu, on abordera en quoi consiste la structure du cyberspace afin d'exposer sa tendance centralisatrice. En deuxième lieu, on présentera qui sont les acteurs monopolisant ce cyberspace. En troisième lieu, on démontrera comment la structure du cyberspace facilite sa monopolisation par les GAFAM et Microsoft. En dernier lieu, on présentera une alternative au cyberspace centralisé qui peut servir de solution vers une marchandisation des données plus juste et équitable de la part des internautes face aux géants du web.

2.1 Structure du cyberspace - centralisation des intérêts des géants du Net.

Les États-Unis proposent une architecture du cyberspace et du data ouvert et aligné avec la position dominante de ses firmes. Il existe deux grands cyberspaces, celui des firmes américaines qui couvrent toute la planète (sauf la Chine) et celui de la Chine, qui a son propre univers cybernétique⁵⁰. Il y a une *datification* de toute activité sociale, politique et économique. La capacité à exploiter les données croît de jour en jour; surtout avec l'industrialisation de l'intelligence artificielle. Ceci cause un effet du *Winner takes all* par les firmes *superstars* au détriment des autres firmes⁵¹. La société affronte une asymétrie de l'économie numérique où les firmes sont de plus en plus riches et les utilisateurs ne sont pas rémunérés en conséquence.

Historiquement, l'innovation a contribué à la richesse des États depuis des siècles. Le développement technologique va de pair avec des secteurs comme le financier, le pétrolier,

⁴⁹ La Finance pour tous, (2020, Décembre 1) « GAFAM, GAFAM ou NATU : les nouveaux maîtres du monde » *Institut pour l'éducation financière du public*, Récupéré de <https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles-economies/gafa-gafam-ou-natu-les-nouveaux-maitres-du-monde/>

⁵⁰ Ciurak, Dan et Maria Ptashkina, «Started the Digital Trade Wars Have: Delineating the Regulatory Battlegrounds», *Centre for International Governance Innovation*, Janvier 2018, pp.7.

⁵¹ Ciurak, Dan, «The Economics of Data, Implications for the Data-Driven Economy», *Centre for International Governance Innovation*, Février 2019, p.1.

le manufacturier et l'agricole. Il est axé sur la connaissance, l'expertise, et la propriété intellectuelle. On retrouve aux États-Unis les plus grandes firmes technologiques que le monde a connu dans les dernières années. Aujourd'hui, ces grandes firmes nous ont amenés dans l'ère du Big Data et de l'intelligence artificielle. Selon Dan Ciurak, on nomme ce modèle d'affaires le *Data Driven Economy* (DDE). « *This new economy features economies of scale, economies of scope, network externalities and pervasive information asymmetry [...] Big Data is by its nature not accessible to the human mind but is accessible to machines given computing power* »⁵². Qui détient le pouvoir des machines capables d'exploiter ces données de masse (Big Data)? Les grandes firmes technologiques, faisant partie du DDE, détiennent et exercent à leur guise l'exploitation des données personnelles aux dépens des utilisateurs. « *The data-driven-economy is also an asset-based economy, in this case based on capturing information and exploiting it for commercial advantage* »⁵³. En résumé, dans un contexte structurel, le cyberspace est conditionné à se former sous les capacités et innovations technologiques que ces grandes firmes américaines mettent à sa disposition.

Techniquement, les géants technologiques utilisent un modèle de concentration autour des puissants centres de données qui habilite l'accès aux contenus. Cette concentration crée des défis de durabilité, de déséquilibre et surtout de sécurité de données. D'ailleurs, Paul Baran, un des pionniers de l'Internet, « *prédisait depuis 1967 l'avènement d'un service informatique centralisé qui offrirait de la capacité de calcul, de la même manière que les fournisseurs d'énergie nous font parvenir l'électricité : modèle dont on peut facilement retrouver l'équivalent dans les empires informationnels d'Amazon, Google, et Microsoft* »⁵⁴. L'architecture technique du réseau est complexe et n'est seulement comprise que par les ingénieurs informatiques qui ont bâti ce système. L'architecture du cyberspace est certes celle du code, celle de

⁵² Ciurak, Dan. *Op. cit.* p. 3.

⁵³ Ciurak, Dan. *Op. cit.* p. 2.

⁵⁴ Musiani, Francesca. « Les architectures P2P. Une solution européenne originale pour la protection des données personnelles ? », *Réseaux*, vol. 189, no. 1, 2015, p. 54.

la technique du logiciel et des équipements qui le définissent, mais elle contribue aussi à inscrire certains principes, à définir les termes d'utilisation de cet espace, et à influencer les pratiques qui y ont lieu⁵⁵.

Structurellement, on peut diviser le cyberspace en plusieurs couches. Au premier niveau il y a la couche d'interréseaux où se trouvent les appareils électroniques et les services d'internet branchés sur le réseau. Sur ce niveau, le contrôle est décentralisé. Ce sont par exemple tous les terminaux qui nous facilitent l'accès à Internet comme des ordinateurs ou des téléphones mobiles. Le deuxième niveau est celui du web, celui des applications internet et des services aux consommateurs. On y retrouve Facebook, Instagram entre autres. Le dernier niveau, qui est le plus centralisé, est celui du *cloud computing*. C'est le moyen par lequel les grandes firmes technologiques collectent, stockent et exploitent les données personnelles. C'est dans cette troisième couche que les Amazon, Google, et Microsoft exercent leur emprise sur les internautes. « *They can be seen as databases on a planetary scale which use the information, they store to sell targeted advertising and fuel artificial intelligence services* »⁵⁶. Avant le *Data Driven Economy*, les données personnelles restaient dans les ordinateurs personnels, tous les documents étaient enregistrés que ce soit dans la mémoire de l'ordinateur ou dans un disque dur externe. De nos jours, ce n'est plus le cas. La technologie du *cloud computing* a tout bouleversé. Nos données ne nous appartiennent plus.

En somme les géants du net mettent à disposition des internautes un service numérique basé sur une impression de confort et d'immédiateté au détriment de la vie privée. Pourquoi? « *Les services d'internet les plus répandus de nos jours proposent aux utilisateurs potentiels une prise en main presque immédiate, mais ils comportent de plus en plus souvent, en tant que **précondition à leur utilisation**, des politiques de confidentialité et de condition d'utilisations qui permettent aux entreprises de partager*

⁵⁵ *Ibid.* p. 51.

⁵⁶ Anonyme, (2020, Juin 28) «The story of the internet is all about layers» *The Economist*, Récupéré de <https://www.economist.com/special-report/2018/06/28/the-story-of-the-internet-is-all-about-layers>

ou rendre publiques leurs données personnelles »⁵⁷. La centralisation et la canalisation du cyberspace fait en sorte que tôt ou tard les données personnelles finiront par être dans les nuages des GAFAs et de Microsoft. Les niveaux de protection de ces données ne sont pas garantis.

2.2 Radiographie des responsables du monopole cybernétique

De nos jours, les modes de collecte de données se multiplient. Par exemple, les caméras de sécurité, les capteurs géolocalisables dans les autos et les téléphones jouent un rôle de surveillance et de localisation. Facebook et Google sont les journaux intimes des internautes en sachant leurs préoccupations et leurs intérêts. UberEats sait ce que les internautes mangent; AirBnB connaît leurs prochaines vacances; Apple Watch enregistre leur activité physique et état de santé. En d'autres mots, « *l'Internet nous connaît plus que nous nous connaissons nous-mêmes*⁵⁸ ». Alors, qui est responsable de traiter toutes ces données? Les grands fournisseurs des Cloud Services comme Amazon, Google, et Microsoft concentrent ces informations et peuvent la vendre à des tiers partis par exemple des banques, des assureurs, des employeurs, etc. Ces entités exploitent les données à des fins commerciales en utilisant le marketing digital, le profilage publicitaire comme méthode de ciblage de la clientèle. Malheureusement, ce processus ne tient pas compte des intérêts économiques des internautes puisque leurs données font faire des profits à ceux qui les exploitent et non à ceux qui la fournissent. « *Le public est de plus en plus conscient que le partage, le regroupement et le stockage des données personnelles répondent à un modèle où le trafic est redirigé vers un ensemble des machines, placées sous le contrôle direct et exclusif du fournisseur de service* »⁵⁹. En résumé, le *cloud* centralise les données et n'est pas une garantie de sécurité de

⁵⁷ Musiani, Francesca. *Op. cit.* p. 54.

⁵⁸ Stephens-Davidowitz, Seth. *Op. cit.* p.77.

⁵⁹ Musiani, Francesca. *Op. cit.* p. 68.

celles-ci. Des évènements tels que la fuite des données chez Desjardins, celle de Capital One et même l’Affaire Snowden démontrent que les données ne sont pas à l’abri.

Économiquement, les GAFAM et Microsoft ont connu leur succès grâce à la gratuité des services qu’ils mettent à disposition des internautes. Pour un individu, effectuer une recherche Google, avoir un compte d’Amazon, de Facebook et d’Apple ne coûte rien à la base. « *Le succès de l’Internet est né de la gratuité des informations que l’on y retrouve. La publicité représente une part importante de ces revenus* »⁶⁰. Le concept de l’innovation n’arrête jamais chez ces entités technologiques. Les applications numériques qui proviennent des GAFAM et Microsoft facilitent un mode de vie axé sur la consommation numérique. Les gens sont encouragés, à travers ces applications de modifier leurs habitudes de consommation. Tout peut se faire à travers d’un simple clic. Pourquoi appeler un taxi quand on peut utiliser Uber? Pourquoi payer pour un film ou si on a Netflix ou Apple TV? Pourquoi louer une auto chez un concessionnaire si on peut le faire à travers Turo, ou louer une chambre d’hôtel si on peut le faire avec AirBnB? Pourquoi magasiner dans les boutiques si on peut le faire avec Amazon en ligne? Plein d’autres exemples sont possibles aussi et démontrent que les GAFAM sont des incontournables du quotidien. Il existe une économie de réseau qui incite les internautes à adopter un comportement de consommation numérique. D’ailleurs, une étude menée par la firme Deloitte montre l’influence des réseaux sociaux sur la décision d’achat auprès des milléniaux. « *Assez logiquement, les réseaux sociaux jouent un rôle plus important auprès des consommateurs les plus jeunes. [...] Pour 34% YouTube a une influence modérée à forte dans leur décision d’achat. [...] Facebook 29% [...] Instagram 21%*⁶¹ ».

⁶⁰ Roux, Cécile. « Les nouveaux modèles économiques des sociétés de l’Internet. Les raisons de leur apparition », *Annales des Mines - Réalités industrielles*, vol. novembre 2010, no. 4, 2010, p.44.

⁶¹ Zobrist, Luc et Michael Grammp, (2017) « Le consommateur à l’ère du numérique », *Deloitte Research*, Récupéré de <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/consumer-business/ch-fr-cb-digital-consumer-swiss-retail.pdf>

L'économie numérique se distingue par l'expression *winner takes all*. Les GAFAs et Microsoft « *captent les consommateurs en leur offrant les utilités les moins chères et les plus rapidement croissantes [...] ils deviennent le portier (gatekeeper) de la toile du réseau* »⁶². Ces compagnies monopolisent le marché numérique et organisent les autres compétiteurs du marché à leur guise. Google sait tirer parti de cet effet de concentration, car ils captent la majeure partie de la publicité en ligne, au détriment des autres sites, qui ne peuvent traduire leur popularité en revenus. En Asie, la Chine dispose de plus de 770 millions d'utilisateurs dans le cyberspace. La Chine permet à ses trois grandes compagnies de centraliser les données personnelles chinoises. Alibaba collecte les données afin de pouvoir construire des « *smart cities* », Baidu le fait pour l'automatisation des véhicules et Tencent pour l'imagerie médicale. Cependant, en Chine c'est le gouvernement qui distribue les capacités en intelligence artificielle à ces compagnies afin d'éviter la formation d'oligopoles et la robotisation de la main d'œuvre chinoise qui créerait ainsi une pénurie d'emplois.⁶³

La centralisation du cyberspace fait en sorte que les internautes n'ont plus le choix de choisir la façon comment leurs données sont recueillies et traitées. La maison n'est plus un espace inviolable; « *cette préoccupation, physique ou territoriale n'a plus sa raison d'être [...] un individu est de plus en plus transparent dans un monde virtuel qui est de plus en plus opaque [...] nous pensons maîtriser parfaitement la circulation de notre image informationnelle mais un coup d'œil sur les privacy settings de ces opérateurs ébranle cependant cette assurance* »⁶⁴. En résumé, on assiste à une centralisation du flux numérique vers les grandes firmes technologiques. Dans les économies de réseau, la puissance économique revient à celui qui possède les plus de

⁶² Roux, Cécile. *Op. cit.* p.44.

⁶³ Anonyme, (2018, Juin 28). « China has the world's most centralised internet system» *The Economist*, Récupéré de <https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system>

⁶⁴ Pouillet, Yves. *Op. cit.* p. 53.

capacités techniques et économiques pour rendre son influence plus forte. Le cyberspace modifie les comportements de consommation en nous transformant en participants actifs de la nouvelle ère numérique. Il met à disposition des internautes des facilités de production et de stockage de contenu à bas prix voire gratuitement en échange des données personnelles. Les gouvernements doivent être proactifs dans la régulation pour la protection des données personnelles.

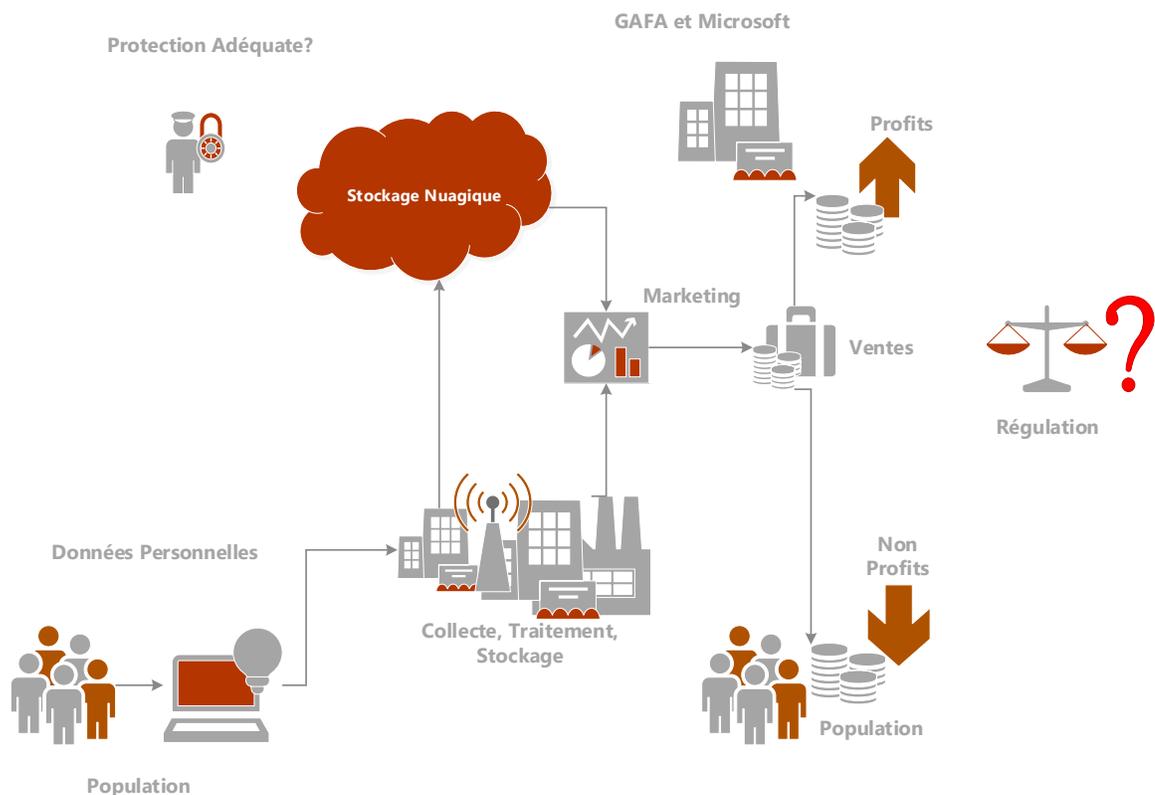
2.3 Fonctionnement du cyberspace :

D'un point de vue technique, il existe plusieurs entités technologiques qui sont indispensables au bon fonctionnement de l'écosystème numérique. Ces entités se retrouvent dans quatre niveaux. Le premier comprend des producteurs des réseaux et des terminaux. Ce sont les appareils qui permettent aux consommateurs de rentrer en contact direct avec l'écosystème numérique comme les équipements de transmission, les routeurs, les téléphones mobiles, etc. Le deuxième comprend les opérateurs de réseaux tels que Vodafone, AT&T, Bell, ou Rogers. Ces acteurs permettent la connexion du consommateur au réseau internet. Le troisième niveau comprend les fournisseurs de service comme Google, Amazon, Facebook, etc. Ce sont des plateformes d'intermédiation dans internet comme celle du commerce en ligne, moteurs de recherche, courriels, réseaux sociaux entre autres. Le quatrième comprend les producteurs et éditeurs de contenu tels que Netflix, Disney+, Amazon Prime, Google Play, YouTube, etc. Ces joueurs offrent un produit ou un service audiovisuel pour lequel les internautes vont payer afin de choisir le contenu qu'ils veulent consommer⁶⁵.

La présence des GAFAM s'immiscent dans les quatre niveaux mentionnés ci-haut. *« Ils se trouvent en position de free rider car ils bénéficient d'un bien ou d'un service sans avoir participé à son financement [...] ils utilisent ces infrastructures afin de vendre*

⁶⁵ Benhamou, Françoise. « L'État et l'internet. Un cousinage à géométrie variable », *Esprit*, vol. 7 Juillet 2011, p.98.

des biens et de diffuser des contenus d'un côté, et de vendre des espaces publicitaires de l'autre côté »⁶⁶. Le modèle d'affaires est simple : les firmes vendent un produit ou un service aux internautes. Ce profit est généralement créé par l'espace publicitaire qui est corrélé au nombre d'utilisateurs de la plateforme. Dans le schéma suivant, on peut voir un portrait du parcours que les données personnelles font dans le cyberespace à partir des informations retrouvées dans l'ensemble de la recherche de ce travail. Les profits ne sont pas bien distribués. Le marché est asymétrique entre internaute et entreprise. Les avancées technologiques permettent à ces entreprises de collecter et traiter l'information à un faible coût afin d'optimiser les profits⁶⁷.



⁶⁶ *Ibid.* p.99.

⁶⁷ Belleil, Arnaud. « La régulation économique des données personnelles ? », *LEGICOM*, vol. 42, no. 1, 2009, pp. 144.

Le schéma précédent montre le chemin que nos données font dans le cyberspace. Celui-ci se divise en quatre niveaux : transferts des données, collecte et stockage des données, marchandisation des données et répartition des profits. Tout d'abord, l'internaute utilise un outil qui lui permettra de se connecter sur le réseau. Par exemple un MacBook. L'accès en ligne d'un fournisseur de service tel que Videotron. C'est dans ce niveau qu'apparaissent les adresses IP. Elles sont indispensables au bon fonctionnement de l'Internet. *« Elles permettent d'identifier, par un numéro, des dispositifs connectés, au réseau tel qu'un ordinateur personnel. Chaque fois qu'un individu va sur Internet en utilisant un dispositif d'accès, le fournisseur lui attribue une adresse IP⁶⁸ »*. En d'autres mots, ce sont des outils de traçage où l'anonymat cède sa place à l'utilisateur identifié. Le propriétaire du site web peut savoir combien de fois l'adresse IP a visité son site pour éventuellement prévoir le comportement de l'internaute.

Ensuite, toujours en référence au schéma précédent, on utilise, les *cookies* afin de mieux tracer l'individu sur le réseau Internet. *« Des nombreux sites font recours aux cookies d'identification qui sont stockées sur l'ordinateur du visiteur afin de permettre une reconnaissance lors de la prochaine visite⁶⁹ »*. L'internaute se fait doublement tracer par les adresses IP et les *cookies* au moment de son entrée sur le net. Le deuxième niveau comprend la collecte, le stockage et le traitement des données qui se fait soit à travers des centres de données ou dans le *cloud*. Le troisième et le quatrième niveau du schéma précédent comprend les différentes méthodes d'exploitation des données personnelles comme la publicité ciblée. *« Les entreprises n'ont aucune incitation de nature concurrentielle à protéger la vie privée de leurs clients lorsqu'elles ont intérêt à revendre les DP et que les protéger représente, au contraire, un cout net »⁷⁰*. La vente

⁶⁸ Hustinx, Peter J. « Protection des données à caractère personnel en ligne : la question des adresses IP », *LEGICOM*, vol.42, no. 1, 2009, p.120.

⁶⁹ *Ibid.* p. 121.

⁷⁰ Cecere, Grazia, et Fabrice Rochelandet. « Modèle d'affaires numériques, données personnelles et sites web. Une évaluation empirique », *Revue française de gestion*, vol. 224, no. 5, 2012, p.113.

des données personnelles à des tiers permet de faire un profit monétaire qui n'est pas distribué équitablement dans la société.

En résumé, la régulation ne protège pas adéquatement les données personnelles. Aujourd'hui, on ne peut se passer du numérique. Les nouvelles générations assisteront à une numérisation de leur quotidien. « *L'essor du numérique permet en quelque sorte de mettre des données le monde, parfois sans même qu'on se s'en rende compte, souvent qu'on y participe, dans un mouvement d'exposition volontaire de soi de plus en plus marqué*⁷¹ ».

2.4 Reconfiguration du cyberspace – vers un modèle décentralisé?

La reconfiguration du cyberspace passe par le changement du modèle centralisé, c.-à-d. un modèle pro GAFAM, vers un modèle décentralisé. Est-ce possible? Techniquement oui, mais économiquement non. Pourquoi? L'architecture actuelle des services numériques orchestrés par les géants du web converge vers la centralisation. Le modèle Peer to Peer, qui peut être une alternative à la centralisation, est un mode de réseau informatique structuré de manière décentralisée afin que les communications et les échanges qui y ont lieu se fassent entre des nœuds dotés d'une responsabilité égale⁷². Dans ce modèle, que l'on nomme aussi P2P on retrouve le concept de Privacy by Architecture (PbA) qui consiste à inscrire la *Privacy* dans l'architecture technique d'un système en réseau, grâce à un certain nombre de techniques d'anonymat, d'obscurcissement, de stockage décentralisé et d'attribution d'identités multiples et d'effacement⁷³. En d'autres mots, l'internaute qui accède un réseau internet décentralisé voit son identité mieux protégée en raison de la façon de comment les données circulent sous l'anonymat.

⁷¹ Bensamoun, Alexandra, et Célia Zolynski. « *Cloud computing et big data. Quel encadrement pour ces nouveaux usages des données personnelles ?* », *Réseaux*, vol. 189, no. 1, 2015, p. 108

⁷² Musiani, Francesca. *Op. cit.* p.49.

⁷³ *Ibid.* p.49.

Faroo est un moteur de recherche qui utilise comme approche conceptuelle de protection de données le Privacy by Architecture. Faroo n'indexe que l'information qui est déjà rendue accessible au public; contrairement à Google qui trace tous les mouvements des internautes dans la recherche⁷⁴. Les systèmes informatiques d'aujourd'hui prônent une optimisation et une efficacité opérationnelle auquel des exemples comme celui de Faroo, qui prône un modèle P2P ne peut pas rivaliser ni atteindre le haut niveau opérationnel de Google.

Les internautes font part d'une ère technologique programmable, dans lequel les géants numériques appliquent la formule 5V qui comprend le Volume (quantité des données personnelles), la Variété (données personnelles hétérogènes pour être appréhendées par le Big Data), la Vitesse (vitesse du traitement des données), la Véracité (la fiabilité des données exploitées) et finalement la Valeur (exploitation des données). La formule 5V rend la navigation internet plus fluide, plus agréable et plus rapide mais à un prix très cher pour les internautes puisqu'ils ignorent en général le sort de leurs données personnelles⁷⁵. De nos jours, le cyberspace est un « *c'est un ensemble de services basés sur le web partageant des propriétés communes, mais il désigne également un social software : partage de l'information, mise en relation et de participation des utilisateurs à la production collective de biens communs numériques*⁷⁶ ». Les internautes fournissent leurs données gratuitement dans le cyberspace et les seuls gagnants dans cet échange sont les GAFA et Microsoft.

Lorsqu'on navigue sur le web, c'est rare voir des options telles que la possibilité de recourir à l'anonymat ou de voir la possibilité de désactiver les terminaux qui permettent de nous localiser. Les internautes sont poussés dans une dynamique imposée par les géants numériques par le confort, l'efficacité et la gratuité des services

⁷⁴ *Ibid.* p.63.

⁷⁵ Bensamoun, Alexandra, et Célia Zolynski. *Op. cit.* p.108.

⁷⁶ Rallet, Alain et Samy Guesmi, « Web 2.0 et outils de coordination décentralisée. Un entrelacement des sphères privées et professionnelles », *Revue française de gestion*, 2015, Vol. 2, No. 224, p.140.

dans le cyberspace. Il a été mentionné ci-dessus l'alternative du modèle P2P qui est techniquement possible mais opérationnellement impossible, car « *il est difficile de persuader les utilisateurs d'abandonner la commodité du cloud Google ou Facebook, en dépit des procédures de prise en main et d'appropriation des dispositifs qui sont plus compliqués*⁷⁷ ». Le réseau P2P reste à l'ombre des grands géants numériques. Économiquement c'est impossible de dénouer tout le système numérique qui nous entoure pour en mettre un comme le P2P car les capacités économiques des GAFAM n'ont, à ce jour, aucun rival. D'ailleurs, d'un point de vue technique, Google peut faire votre demande en quelques secondes en scannant plus de 500 000 sites dans le monde comparativement à Faroo ou d'autres moteurs de recherche qui ne sont pas dans la possibilité de le faire aussi rapidement⁷⁸.

Malgré tout, la technologie de la chaîne de blocs, soit la *Blockchain*, représente une solution en ce qui regarde la protection des données personnelles. Il sera difficile de défaire le monopole des GAFAM et Microsoft sur le cyberspace mais les États peuvent imposer l'adoption systématique du *Blockchain* dans le cyberspace. Cette technologie se base sur le modèle P2P, elle contient un registre de transactions (financières, informationnelle, contractuelles, etc.) qui est décentralisé, anonyme, incorruptible et complètement transparent Rallet, Alain et Samy Guesmi, « Web 2.0 et outils de coordination décentralisée. Un entrelacement des sphères privées et professionnelles », *Revue française de gestion*⁷⁹. La gouvernance du cyberspace doit être revue par les États pour créer un modèle décentralisé où les internautes ne subissent pas des bris de confidentialité ou d'atteinte à leurs données personnelles.

La prochaine image montre comment serait un cyberspace décentralisé grâce à la technologie Blockchain⁸⁰. On aperçoit toutes les parties prenantes du cyberspace

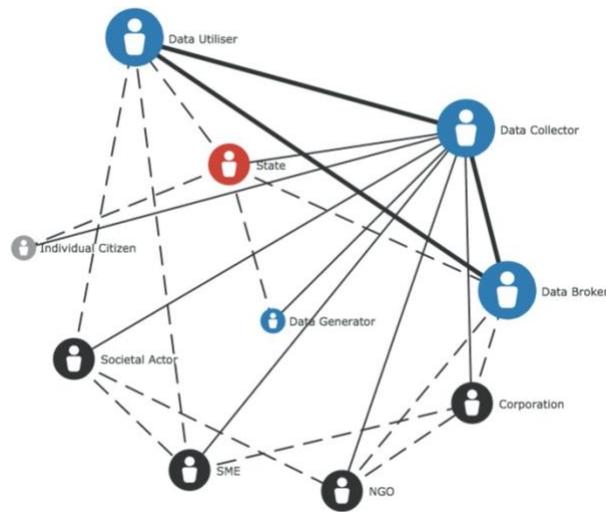
⁷⁷ Musiani, Francesca. *Op. cit.* p.67.

⁷⁸ Pouillet, Yves. *Op. cit.* p.59.

⁷⁹ Zwitter Andrej, et Jilles Hazenberg. « Decentralized Network Governance: Blockchain Technology and the Future of Regulation » *Frontiers in Blockchain*, Vol. 3, Art. 12, 25 mars 2020, p.8.

⁸⁰ *Ibid.* p.7

interconnectées sans aucun ordre hiérarchique. Ce n'est qu'en ayant un cyberspace décentralisé que les internautes peuvent avoir une meilleure protection des données personnelles et ainsi viser une possible marchandisation de celles-ci.



En conclusion, ce chapitre a présenté les grandes lignes de la structure du cyberspace de façon à démontrer sa centralisation. Le fonctionnement de ce système et ses responsables font en sorte que la reconfiguration s'avère très compliquée et nécessite d'une intervention de l'État. Il ne faut pas oublier que les géants du numérique ont rendu les frontières poreuses de ce qui sépare la vie privée et la vie publique non seulement par le contrôle du web mais aussi par le développement de l'Internet des objets (IoT) qui sera abordé dans le chapitre III. Les internautes doivent avoir accès à un cyberspace totalement sécuritaire et transparent avec le sort de leurs données personnelles. Il faut un écosystème numérique mieux géré et régulé de façon optimale et fiable. Il ne faut pas voir le droit comme la seule réponse aux problèmes de gestion de la sécurité des données personnelles, si la technologie constitue le problème, elle peut aussi être la solution. Le droit doit s'appuyer sur la technologie comme c'est le cas de la *Blockchain*. L'État doit jouer le rôle d'intermédiaire entre les internautes et les grandes firmes technologiques pour instaurer l'encadrement nécessaire afin que toutes les parties à cet écosystème en sortent gagnantes. L'allocation d'un profit

monétaire passe par une meilleure régulation de la part des États afin de contraindre les géants numériques à centraliser la structure du cyberspace qui permettent d'exploiter inadéquatement les données des internautes. On verra dans le chapitre III le volet de régulation et le rôle de l'État qui donneront suite à la thèse défendue dans ce travail.

Chapitre III - Régulation du Cyberspace, atteinte à la vie privée

« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes⁸¹ ». C'est la Déclaration universelle des Droits de l'Homme de 1948 qui avait pour bonne foi de protéger la vie privée des personnes mais qui n'a pas sa place dans le contexte numérique d'aujourd'hui. En 1980, l'Organisation de coopération et de développement économiques (OCDE) a adopté les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*. Encore une fois, on perçoit une volonté de protéger la vie privée de la part de la communauté internationale. Ces lignes ont été révisées en 2013 pour les mettre à jour au contexte numérique actuel. « Bien qu'elles soient volontaires et n'aient pas de force de loi, les Lignes directrices de l'OCDE servent de fondement aux dispositions législatives sur les pratiques équitables en matière de renseignement au Canada et dans bien d'autres pays⁸² ».

En somme, les renseignements personnels ne sont pas protégés adéquatement et on constate qu'au niveau étatique les grandes puissances technologiques telles que les États-Unis, l'Europe, et la Chine ont toutes des différentes approches juridiques concernant la protection des données personnelles. Le Canada est plus enclin à adopter une approche européenne. Ce chapitre servira à présenter les grandes lignes de ces approches juridiques afin de pouvoir les comparer et proposer un cadre juridique qui peut être une solution à la problématique de ce travail, celle du non-respect de la vie privée. Le chapitre sera divisé en quatre parties, soient une comparaison de la

⁸¹ *Déclaration Universelle des Droits de l'Homme*, (1948, 10 Décembre), « Article 12 ». Récupéré de <https://www.un.org/fr/universal-declaration-human-rights/>

⁸² Canada. Division de l'économie, des ressources et des affaires internationales. (2020, Novembre 17) *Les lois fédérales du Canada sur la protection de la vie privée*, Publication No. 2007-44-F. Récupéré de https://bdp.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/200744E

régulation canadienne avec l'approche chinoise, l'américaine, et l'européenne. La dernière partie du chapitre proposera un modèle de régulation standardisé en matière de protection des données personnelles. L'objectif du chapitre est de démontrer qu'une régulation harmonisée est nécessaire afin qu'un profit monétaire soit envisageable pour les internautes au détriment des GAFAs et Microsoft. Le système canadien et européen seront les guides vers cette solution.

3.1 Chine vs Canada - La régulation contraignante vs la régulation responsable

Trois concepts seront importants à travers ce chapitre : Le droit d'être laissé seul, le contrôle de l'accès à ses informations personnelles et la liberté face au contrôle des autres. Ils sont importants, car ils sont culturellement subjectifs, c'est-à-dire, que la Chine, le Canada, les États-Unis et l'Europe n'ont pas le même regard sur ces concepts.

Tout d'abord, la Chine est considérée par plusieurs comme un modèle autoritaire en ce qui concerne le contrôle et la régulation du cyberspace puisque le Big Data rencontre le Big Brother. Pourquoi? Au lieu de voir l'Internet comme un instrument de liberté, d'information, et de libre association, le Parti communiste chinois utilise le cyberspace comme architecture de contrôle social, et de propagande du parti dans lequel ce Parti peut manipuler, façonner ses citoyens, garder la stabilité sociale et contrôler la contestation de ses politiques⁸³. Il existe en Chine un système de Crédit Social qui permet de tracer tous ses citoyens. Ce système est considéré comme une initiative très dangereuse du Big Data⁸⁴.

«It is the desire of the state to monitor, control, and shape its information environment. It is shared among authoritarian and democratic governments alike [...] Such system includes input and output categories. The outputs are credit scores for the users, impacting many things ranging from hotels, traveling, and insurance

⁸³Ming, Jiang et King-Wa Fu. « Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit? » *Policy & Internet*, Vol. 10, No. 4, 2018, pp. 373.

⁸⁴ *Ibid.* p.374.

premiums, to school admissions, government jobs, and access to social services. Inputs can be grouped into three categories: Traditional (income-tax records, loan payments). Social (traffic violations, criminal records, academic integrity). Online (interaction with other users, reliability of information posted online, shopping habits, etc.⁸⁵ »

Liu Hu, journaliste accrédité comme un des « Cent Héros de l'Information » par Reporters Sans Frontières, a été arrêté injustement après avoir critiqué le Parti communiste qui est, selon elle, un parti corrompu. Grâce au Système de Crédit Social, le gouvernement chinois a pu imposer au journaliste des sanctions et restrictions dans le voyage, l'accès au crédit, et l'accès à un prêt hypothécaire⁸⁶. Cet exemple démontre clairement à quel point la vie d'un citoyen peut être contrôlée par un système de Big Data tel que celui de la Chine. Le problème n'est pas le système en tant que tel mais la politisation de celui-ci. C'est une régulation contraignante, car elle est politisée et elle ne respecte pas la vie privée des individus. Elle sert seulement à défendre les idéologies du Parti communiste.

Ensuite, selon Dan Ciurak, la Chine a créé un univers cybernétique parallèle au monde occidental. Alibaba, Baidu, WeChat sont des firmes technologiques chinoises qui opèrent sous un même territoire, donc sous la même juridiction contrairement aux grandes firmes américaines qui opèrent de façon globale (en excluant la Chine). Ceci permet à la Chine d'avoir un contrôle total des données personnelles sur leur territoire. « *There are mandatory security inspections of equipment prior to installation; China does not share commitment to open its digital borders and claims sovereignty inner its cyberspace*⁸⁷ ». Avec le pare-feu que la Chine s'est construit autour d'elle, elle empêche les GAFAs et Microsoft d'exploiter sans cesse les données personnelles des Chinois et érige un contrôle souverain sur les messages que la société chinoise accède.

⁸⁵ *Ibid.* p.378

⁸⁶ *Ibid.* p.381

⁸⁷ Ciurak, Dan et Maria Ptashkina. *Op. cit.* p.7

D'un point de vue commercial, « *China has the advantage of economies of scale in exploiting the positive externalities for commercial gain but lacks the internal checks and balances to restrain the state from exploiting externalities*⁸⁸ ».

En somme, au Canada il existe la *Loi sur la protection des renseignements personnels* (qui régit la manière dont le gouvernement fédéral traite les données personnelles). Plusieurs principes sont énumérés dans cette loi et sont mis de l'avant par le Conseil canadien des normes et le Commissaire canadien à la vie privée. Parmi ces principes on retrouve la responsabilité, la transparence, le consentement, les mesures de sécurité, l'exactitude, etc.⁸⁹. Cependant, lorsqu'on compare ces fondements avec la régulation chinoise, les Canadiens peuvent porter plainte au Commissariat à la protection de la vie privée du Canada si leurs données sont compromises. Le but de cette entité fédérale est d'amener les Canadiennes et Canadiens à exercer un meilleur contrôle sur leurs renseignements personnels. Le commissaire travaille avec le secteur public, le privé, le milieu universitaire, et la société civile pour assurer le respect de la vie privée. Le modèle canadien est axé sur la data-responsabilité⁹⁰. Dans le cas chinois, le journaliste Liu Hu s'est vu affecté non seulement par la discrimination qu'il a subie de la part du gouvernement chinois mais aussi ses renseignements personnels ont été divulgués au public et utilisés contre lui pour servir comme précédent afin de montrer les conséquences que peuvent subir les personnes qui ne partagent pas la même idéologie du Parti communiste. « *Liu was arrested for fabricating and spreading rumors*⁹¹ ». Le Canada se dote d'une data-responsabilité tandis que la Chine se dote d'une data-iniquité.

⁸⁸ Ciurak, Dan, *Op. cit.* p. 5.

⁸⁹ Conseil canadien des normes, (2020), Récupéré de <https://www.scc.ca/fr/RGPD>

⁹⁰ Commissariat à la protection de la vie privée, (2018, Décembre) Récupéré de <https://www.priv.gc.ca/fr/a-propos-du-commissariat/qui-nous-sommes/commissaire-a-la-protection-de-la-vie-privee-du-canada/>

⁹¹ Ming, Jiang et King-Wa Fu. *Op. cit.* p.381

3.2 États-Unis vs Canada - la régulation laxiste vs la régulation cartésienne

Le 19 mai 2020, le gendarme canadien de la concurrence a annoncé l'imposition d'une amende de 9,5 millions de dollars canadiens à Facebook pour avoir fourni des indications *fausses ou trompeuses* au sujet de la protection des renseignements personnels des utilisateurs canadiens. Entre 2012 et 2018, Facebook a permis à des tiers partis l'accès aux données personnelles des Canadiens. Situation qui a été déplorée par le Commissariat à la protection de la vie privée⁹². Ces situations font surface régulièrement et sont juste un exemple parmi tant d'autres que nos données ne sont pas protégées. Des scandales comme celui de Cambridge Analytica, Desjardins, Capital One ont plusieurs choses en commun : le manque de protection des données personnelles. Facebook a décidé de payer l'amende. Le gouvernement canadien fait preuve de rationalité en imposant ce type d'amende puisqu'il condamne les compagnies qui ne protègent pas les données personnelles des citoyens. Le Canada montre le chemin à d'autres pays pour punir ce type d'abus et pour mieux encadrer la protection des données personnelles. Cette approche proactive et préventive permet de limiter les abus sur la vie privée des internautes⁹³. Il faut démanteler ces profits et ces abus pour conscientiser les gens qu'il faut prendre nos données personnelles plus au sérieux.

De plus, aux États-Unis, « *the Right to Privacy means that individuals shall have full protection in person and in property. It has been found necessary from time to time to define a new exact nature and extent of such protection. Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demand of society*⁹⁴ ». Selon Dan Ciurak, la régulation des États-

⁹² AFP, (2020, Mai 19) « Facebook à l'amende pour tromperie sur la confidentialité » *Les Affaires*, Récupéré de <https://www.lesaffaires.com/techno/internet/facebook-a-l-amende-pour-tromperie-sur-la-confidentialite/617803>

⁹³ Gola, Romain. « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, vol. 59, no. 2, 2017, p.32.

⁹⁴ Chassigneux, Cynthia, « Vie privée et commerce électronique », *Virginie Mesguich*, 2004, p.8.

Unis promeut une architecture légale ouverte qui s’aligne parfaitement avec ses grandes firmes GAFAM. D’ailleurs, « *Facebook will do anything to make sure they are not the next Yahoo killed by disruption and failure to innovate [...] this translates into paying obscene sums for technology that might challenge their dominance one day* ⁹⁵ ». En d’autres mots, ces firmes américaines restent au sommet, car il n’y a pratiquement pas de concurrence. Ils détiennent l’expertise technologique le pouvoir économique pour être la référence dans le cyberspace. Washington fait face à un dilemme : doit-on protéger les renseignements personnels de la population américaine ou doit-on accorder aux firmes technologiques la latitude nécessaire à leur croissance économique? Le défi est de voir comment ils vont apprivoiser les GAFAM qui ne céderont pas leur pouvoir si facilement au gouvernement. Pour le moment les États-Unis optent pour un cadre juridique permissif afin d’avantager ces firmes et atténuer la menace cyber chinoise⁹⁶. En résumé, les États-Unis offrent une approche juridique décentralisatrice et fragmentée du cyberspace basé sur l’autorégulation dans le but de ne pas nuire au développement économique de ses firmes.

En somme, le Canada doit faire preuve de fermeté face à ses voisins puisque le cyberspace américain envahit le quotidien de notre société que ce soit dans les produits qu’on achète, le contenu audiovisuel, la musique, etc. L’innovation contribue à la richesse des États mais surtout des firmes comme les GAFAM et Microsoft. L’avantage canadien est que Montréal est devenu l’une des capitales mondiales de l’intelligence artificielle. Celle-ci est un outil indispensable au bien-être opérationnel et économique des grandes firmes technologiques américaines. Alors pourquoi le Canada ne pourrait faire pareil?

« Canada has good prospects in the AI sector, and should capitalize on. Its assets by substantially expanding public sector investment, including by strategically

⁹⁵ Ciurak, Dan. *Op. cit.* p.3.

⁹⁶ Ciurak, Dan, *Op. cit.* p.4.

using public sector procurement to develop new technological capabilities. Canada should work with other small open economies to develop a rules-based framework that enables their full participation in the data driven economy⁹⁷ »

La numérisation de l'économie nous ramène dans un cyberspace incertain qui ne peut pas faire la distinction de ce qui est privé ou de ce qui est public. Après les déclarations de Edward Snowden sur la surveillance et l'atteinte à la vie privée de la part de l'Agence de sécurité nationale américaine, il suggère que « *la communauté qui construit Internet représente les pompiers qui puisse la sauver⁹⁸* ». Il existe un vide juridique qui laisse les géants technologiques à agir selon leurs intérêts économiques et non à ceux de la communauté. Les entreprises en position dominante réagissent plus lentement aux pressions sociales⁹⁹. Alors que la confiance des citoyens américains en ce qui concerne la protection des données personnelles s'émousse, après des scandales comme celui de Snowden, la confiance des canadiens envers ses institutions se multiplie lorsqu'on impose des amendes comme celle imposée à Facebook dernièrement¹⁰⁰.

3.3 Europe vs Canada - Régulation Proactive vs Régulation Innovante

La notion d'anonymat disparaît à mesure que les fichiers et les technologies de traçage ne cessent de se multiplier. La traçabilité des comportements des utilisateurs créée par les grandes firmes américaines provoque une méfiance en Europe et au Canada qui s'inquiètent des données personnelles de leurs populations¹⁰¹. La vision européenne de la technologie numérique n'est pas libertaire comme aux États-Unis. D'ailleurs, la loi

⁹⁷ *Ibid.* p.4.

⁹⁸ Delesse, Claude. « La NSA, « mauvais génie » du cybermonde ? », *Sécurité globale*, vol. 8, no. 4, 2016, p.95.

⁹⁹ Pras, Bernard. « Entreprise et vie privée : le privacy paradox et comment le dépasser », *Revue française de gestion*, Vol.5, no. 224, 2012, p.91.

¹⁰⁰ Delesse, Claude. *Op. cit.* p.89.

¹⁰¹ Lancelot Miltgen, Caroline. « Dévoilement de données personnelles et contreparties attendues en e-commerce : une approche typologique et interculturelle », *Systèmes d'information & management*, vol. 15, no. 4, 2010, p.47.

française de 1978 dictait que la technologie doit être au service de chaque citoyen et non l'inverse. « *La technologie ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni à la liberté individuelle ou publique*¹⁰² ». Aujourd'hui, les citoyens utilisent un cyberspace largement influencé par les GAFA et Microsoft. Ces compagnies siphonnent les données personnelles des internautes pour accroître leurs revenus. L'Europe a fait preuve de proactivité en édifant une régulation sur la protection des données personnelles qui encadre de façon plus efficace la vie privée des citoyens. Les Européens ne veulent pas se voir réduits à un numéro, à voir des messages et des courriels de boîtes aux lettres comme des ventes sous pression, ils ne veulent pas être suivis et surtout voir leurs données personnelles être une marchandise aux profits des firmes américaines. « *La démarche régulatrice européenne intervient pour empêcher qu'on passe de la gestion des données personnelles à la gestion de la personne, ce qui serait contraire au principe de liberté dans une société démocratique*¹⁰³ ».

Le règlement général n° 2016/679 sur la protection des données (RGPD) est le bouclier qui protège les renseignements personnels des européens. Ce règlement remplace la directive sur la protection des données personnelles (95/46/CE) adoptée en 1995. Six pratiques sont considérées comme atteinte à la vie privée¹⁰⁴:

- La collecte : données sensibles soient récoltées (Numéro d'Assurance Sociale)
- Stockage non autorisé : lié à la confidentialité et l'intégrité des données fournies.
- Les erreurs : altération accidentelle ou délibérée des données fournies
- Accès impropre : personnes non autorisées aient accès aux données.
- Utilisation interne : réception d'offres commerciales non désirées.

¹⁰² Pouillet, Yves. *Op. cit.* p.65.

¹⁰³ Frayssinet, Jean. « La régulation de la protection des données personnelles », *LEGICOM*, vol. 42, no. 1, 2009, p. 65.

¹⁰⁴ Dumoulin, Régis et Caroline Lancelot Miltgen. *Op. cit.* p.100.

- Utilisation externe : transfert des données à des tiers partis sans autorisation.

L'approche européenne est évolutive et priorise de mobiliser plusieurs modes de régulation et l'association de la réglementation, de la co-régulation et de l'autorégulation. « *La Commission européenne ou le CNIL œuvrent de cette manière. Seule une bonne compréhension de la protection des données personnelles des utilisateurs par ces nouveaux services de cloud computing et de Big Data permettra d'assurer la pérennité des usages*¹⁰⁵ ». Les citoyens européens peuvent consentir ou non à certaines utilisations de leurs renseignements, notamment à des fins de publicité ciblée. La sensibilisation à mieux protéger les renseignements personnels est plus ancrée dans la société européenne. D'ailleurs, le droit à la portabilité des données rentre en fonction afin de permettre aux citoyens de télécharger toutes les données récoltées sur eux par une plateforme, un commerçant ou un fournisseur Internet. Les entreprises sont tenues de spécifier quelles données sont retenues au risque d'avoir des grosses amendes si elles ne le font pas. De plus, il est possible qu'un site Internet américain ne soit pas disponible en Europe puisque celui-ci ne se soumet pas au RGPD. Il existe aussi l'exemple qui protège les mineurs de 13 à 16 ans qui doivent avoir la permission de leurs parents afin d'utiliser Facebook¹⁰⁶. Ces exemples cherchent à instaurer une confiance dans la population européenne après les révélations de Snowden. Il est important que les gens soient toujours informés de ce qu'il se fait avec leurs données.

En revanche, le RGPD comporte plusieurs désavantages. Par exemple il faut déterminer quelle est la loi applicable et la juridiction compétente en cas de litige? « *Cela impose de recourir à des critères ratione loci, fondés sur la géographie physique, qui s'avèrent difficiles à penser lorsque la pratique appréhendée à un*

¹⁰⁵ Bensamoun, Alexandra, et Célia Zolynski. *Op. cit.* p.107.

¹⁰⁶ Tremblay, Janic (2019, Février 8) « Le RGPD ou comment l'Europe protège les données personnelles », *Radio-Canada*, Récupéré de <https://ici.radio-canada.ca/nouvelle/1151913/donnees-personnelles-rgpd-europe>

*caractère fortement ubiquitaire*¹⁰⁷ ». Une autre critique envers la régulation européenne est son caractère contraignant puisqu'elle compromet l'innovation et le développement de l'intelligence artificielle et c'est probablement pour cette raison que des grandes firmes technologiques européennes n'ont pas vu le jour ou ne peuvent concurrencer avec les GAFAs et Microsoft. Aujourd'hui, les principaux défis de la régulation des données sont l'exploitation et la localisation. « *En définitive la problématique juridique majeure posée par les Big Data tient au fait que les données collectées vont être traitées pour des finalités qui n'auront pas été déterminées au moment de la collecte [...] le cloud crée un problème de localisation des données. Celles-ci sont mises dans les nuages en traversant souvent des nombreuses frontières donc elles sont difficilement localisables*¹⁰⁸ ». La contrainte la plus importante est celle de bloquer les entreprises européennes à innover et surtout dans un secteur tel que celui de l'intelligence artificielle. Laurent Alexandre, entrepreneur du Web et auteur du livre sur la montée de l'intelligence artificielle, dénonce que dans le monde d'aujourd'hui « *c'est la guerre entre les technologies d'intelligence artificielle chinoises et américaines! Et l'Europe est sortie de cette guerre parce qu'elle est remplie de bécassines et de bizounours bienveillants*¹⁰⁹ ».

Dans le contexte canadien, l'institut Québécois d'Intelligence Artificielle (MILA) est un exemple montréalais d'une organisation à but non-lucratif. C'est une communauté des trois-cents chercheurs en intelligence artificielle. Ceux-ci se spécialisent en apprentissage machine (*Machine Learning*) et innovation. C'est une organisation d'IA qui a comme objectif le bénéfice de tous¹¹⁰. Le contexte de crise sanitaire actuel avec la COVID-19 a permis à MILA de mettre au service de la société l'intelligence artificielle. Comment? Avec l'application de traçage nommé COVI. C'est une application que l'on peut installer dans les téléphones mobiles afin de permettre si on

¹⁰⁷ Bensamoun, Alexandra, et Célia Zolynski. *Op. cit.* p. 106.

¹⁰⁸ *Ibid.* p.113.

¹⁰⁹ Tremblay, Janic. *Op. cit.*

¹¹⁰ MILA, Récupéré de <https://mila.quebec>

a été en contact ou si nous sommes proches de quelqu'un qui a été en contact avec le virus. Tout ceci est possible grâce à la géolocalisation du téléphone et l'IA. Le 21 mai 2020, Jean-François Rénaud, co-fondateur d'Adviso (firme d'experts en stratégie et marketing numérique) a interviewé (sur Facebook Live) Valérie Pisano, présidente et chef de la direction de Mila sur le sujet de l'application COVI. Dans cette interview, Mme Pisano explique l'importance de mettre en place des applications telles que COVI pour que Montréal s'érige comme pôle mondial de l'IA. Selon elle, l'IA est un vecteur de croissance économique qui doit être au bénéfice de tous : État, Citoyens et Entreprises. D'ailleurs, le gouvernement fédéral est un important partenaire de cet Institut puisqu'il le finance en partie et met à disposition, du comité d'experts en AI, le Commissariat à la protection de la vie privée du Canada pour s'assurer que l'application est en conformité avec les règles et principes canadiens liés à la protection des renseignements personnels¹¹¹. Cependant, l'application est rejetée au mois d'août 2020 car le Canada a lancé une application fédérale de notification de contact Alerte Covid. Le système de traçage d'Alerte Covid est déjà mis en place tandis que celui de l'application COVI ne l'était pas¹¹².

En conclusion, en Europe le RGPD présente une solution à la protection des données personnelles. Cette réglementation a pour objectif de respecter les libertés et les droits fondamentaux des Européens. Cependant, le développement économique et technologique européen est désavantagé par ce type de régulation. Le cyberspace est laissé à la guise des grands joueurs technologiques tels que les GAFAs et Microsoft qui subissent une régulation permissive du gouvernement américain. En revanche, le Canada fait preuve d'innovation en mettant à disposition du gouvernement des comités d'experts comme celui de MILA afin d'établir un pont entre régulation, développement

¹¹¹ Renaud, Jean-François (2020, Mai 21). *Entrevue avec Valérie Pisano*. Récupéré de https://www.facebook.com/watch/live/?v=253126652679764&ref=watch_permalink

¹¹² Girard, Joëlle (2020, Septembre 20) « Le Québec adopte finalement l'application fédérale Alerte COVID », *Radio-Canada*, Récupéré de <https://ici.radio-canada.ca/nouvelle/1737406/coronavirus-pandemie-application-notification-tracage>

économique et bénéfice à la population dans le contexte d'urgence sanitaire actuel. Le chemin à suivre devrait compter une voie de régulation européenne et une expertise canadienne en intelligence artificielle. Cette partie sera discutée dans la prochaine section de ce chapitre.

3.4 Régulation Hybride Canadienne - IA à la Rescousse de la Vie Privée

Dans le chapitre II, il a été mentionné qu'il fallait une décentralisation de la gouvernance du cyberspace afin de dé-monopoliser celle-ci de l'emprise des GAFA et Microsoft. Ce n'est qu'en décentralisant à l'aide des technologies *Blockchain* qu'il sera possible d'exercer une meilleure protection des données personnelles afin de pouvoir répartir les profits à travers la société. Maintenant, selon un point de vue juridique, on a pu comparer différentes approches entre les grands joueurs du cyberspace actuel comme la Chine, les États-Unis, et l'Europe. Selon Dan Ciurak, le Canada peut jouer un grand rôle dans cette *Data Driven Economy* puisqu'il possède un outil indispensable à l'avenir numérique : soit l'expertise dans l'intelligence artificielle. Cette expertise montréalaise doit être mise en relation avec le « *norm entrepreneurship* » de l'Europe. En mai 2019, Matthias Kettemann, expert juridique dans la gouvernance d'Internet, souligne que :

« Europe remains a key normative power. Its legitimacy as a force for ensuring the reign of rule law in international relations is substantial. It also packs an economic punch [...] Europe will become a norm entrepreneur and lead the normative reform of internet governance in light of its liberal, human rights-based values, prior legal commitments and normative pedigree [...] Europe should engage in a forward-looking process of establishing the contours of a New Deal for Internet Governance¹¹³ ».

¹¹³ Anonyme, (2019, Avril 3) *The Global Internet Governance Academic Network*, Récupéré de <https://www.giga-net.org/gig-arts-2019-16-17-may-2019-salerno/>

Par ailleurs, le Parlement français a voté, mercredi le 27 mai 2020, en faveur de l'adoption de l'application de traçage numérique comme StopCovid. Cette application suit les mêmes directives que l'application montréalaise COVI qui a été décrite auparavant dans ce travail. 186 sénateurs l'ont approuvé tandis que 127 s'y sont opposés et finalement 29 se sont abstenus¹¹⁴. Il est important de rappeler qu'aucune conséquence négative n'est associée à télécharger cette application. Les Français le font sur une base de volontariat, et les données sont pseudonymisées et supprimées au bout de 14 jours. L'application cessera de fonctionner après la crise sanitaire actuelle. La CNIL (commission nationale informatique et libertés) considère que les garanties de protection des données sont suffisamment sécuritaires¹¹⁵. Cependant, certains sénateurs croient que StopCovid est la pire des privations de libertés que les citoyens aient connues puisque c'est un outil de traçage et localisation de la personne¹¹⁶. Cet exemple français démontre que l'État peut et doit débattre afin de mieux encadrer les technologies qui touchent le sujet de la protection des données personnelles. Il est certain que ces décisions ne feront pas l'unanimité mais StopCovid et COVI sont des applications au service de la société qui ne sont pas imposées sur les personnes. Ce n'est que sur une base volontariste, anonyme et temporaire.

Dans une interview à la présidente et chef de la direction de Mila, Valérie Pisano, celle-ci mentionne l'importance qu'il existe un organe, un tiers parti, ou un « ombudsman » qui soit capable de garantir l'efficacité opérationnelle des nouvelles technologies de traçage, de collecte des données et de la protection de la vie privée des gens¹¹⁷. Le Commissariat à la protection de la vie privée travaille en concert avec les firmes technologiques comme c'est le cas de MILA afin de mettre au service de la population une application qui assure l'intégrité des données personnelles. En France, l'article 32

¹¹⁴ Jacquot, Guillaume, (2020, Mai 28) « Stop Covid : le Sénat approuve à son tour l'application de traçage numérique », *Public Sénat*, Récupéré de <https://www.publicsenat.fr/article/parlementaire/stop-covid-le-senat-approuve-a-son-tour-l-application-de-tracage-numerique>

¹¹⁵ Jacquot, Guillaume. *Op. cit.*

¹¹⁶ Jacquot, Guillaume. *Op. cit.*

¹¹⁷ Renaud, Jean-François. *Op. cit.*

de la loi Informatique et Libertés cite : « *Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète [...] de la finalité. De toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques*¹¹⁸ ». La CNIL souligne trois règles de base pour la protection des données : Comprendre vos droits, maîtriser vos données et agir en cas de faute¹¹⁹.

Le concept d'accountabilty fait surface dès 1980 dans les lignes directrices de l'OCDE sur la protection de la vie privée et des flux transfrontaliers de données personnelles. L'ancienne présidente de la CNIL, Isabelle Falque-Pierrotin, définit ce concept comme « *le processus permanent et dynamique de mise en conformité d'une entreprise aux principes informatiques et de liberté grâce à un ensemble de règles contraignantes et de bonnes pratiques correspondantes, l'entreprise étant accompagnée dans cette démarche par l'autorité de régulation*¹²⁰ ». Ce principe implique l'obligation pour le responsable du traitement des données (firmes technologiques) de se conformer et de montrer aux autorités et aux internautes comment ils manipulent les renseignements personnels. Cependant, la vision américaine sur ce principe est plus flexible que celle de l'Europe puisque l'US Consumer Bill of Rights ne parle pas des règles contraignantes contre les responsables de traitement des données, il parle plutôt d'une « *forme de co-régulation entre les responsables de traitement et les autorités, consistant en la mise en place de programmes de conformité à l'intérieur des entreprises et de la supervision de ces mesures par les autorités de l'État*¹²¹ ». La vision américaine démontre que l'internaute n'est pas pris en considération. On ne parle que d'une co-régulation entre entreprise et gouvernement.

¹¹⁸ Dubois, Lorette, et Florence Gaullier. *Op. cit.* p. 40.

¹¹⁹ Anonyme (2020, Mai 28), *Commission Nationale de l'Informatique et des libertés*. Récupéré de <https://www.cnil.fr/fr>

¹²⁰ Gola, Romain. *Op. cit.* p.30.

¹²¹ *Ibid.* p. 31.

La vision canadienne se base sur sept principes tirés de la Privacy by Design¹²². Le premier principe vise une mise en place d'un système juridique qui instaure des mesures de protection des données personnelles préventives plutôt que coercitives¹²³. Le deuxième principe est celui concept Privacy as the Default Setting, qui tout en reconnaissant le droit à la vie privée comme un droit fondamental, laisse le choix aux individus de diminuer eux-mêmes cette protection. Le troisième principe nommé Privacy Embedded into Design propose d'assurer dès la conception de la technologie la protection de la vie privée¹²⁴. Le quatrième principe est celui du « positive-sum, not zero-sum » où les concepteurs de la technologie et les juristes offrent à l'internaute un service ou produit certifié aux règles de la vie privée. Le cinquième principe est celui du « end-to-end security » qui correspond à une obligation de sécurité pendant toute la conservation des données durant son cycle de vie¹²⁵. Le sixième principe « keep it open » correspond à la transparence et à la visibilité afin que les internautes aient contrôle absolu sur leurs données. Le dernier principe « keep it user-centric » propose que l'internaute soit le centre du cyberspace. Tout raisonnement de la part de l'État ou les firmes technologiques doit tenir compte de l'utilisateur¹²⁶.

Le 13 juin 2020, Sonia LeBel, ministre de la Justice du Québec, a déposé le projet de loi 64 devant l'Assemblée nationale. C'est un projet de loi qui vise à renforcer les mesures de protection des données personnelles. Un an après le scandale de la fuite des données chez Desjardins, le gouvernement décide de prendre des mesures qui sont, d'après moi, tardives mais qui démontre une volonté de la part du gouvernement de « serrer la vis » envers les compagnies qui ne protègent pas adéquatement les données de leurs clients.

¹²² *Ibid.* p. 32.

¹²³ *Ibid.* p. 32.

¹²⁴ *Ibid.* p. 32.

¹²⁵ *Ibid.* p. 32.

¹²⁶ *Ibid.* p. 32.

« Le document enjoint aux entreprises de détruire ou à tout le moins d’anonymiser un renseignement personnel lorsque les fins auxquelles il a été recueilli ou utilisé sont accomplies [...] Le projet de loi 64 précise le droit d’un individu d’exiger le droit au déferencement : Google, pour ne pas le nommer, fasse en sorte que si je fais une recherche sur Sonia LeBel, sur un tel sujet, bien, que ça soit difficile de trouver l’information. Dans les objectifs, c’est de rendre l’information plus difficilement accessible [...] Par ailleurs, le document encadre à la fois collecte et l’utilisation de renseignements personnels obtenus au moyen d’une technologie comprenant des fonctions d’identification, de localisation ou de profilage. Parce que vous êtes allé magasiner un barbecue sur internet, tout à coup, sur votre Facebook, on vous offre des barbecues à répétition. Maintenant, avec le projet de loi, bien, je vais avoir le droit de désactiver cette fonction-là [...] Les amendes imposées aux entreprises en défaut fluctueront entre 15 000 dollars et 25 millions de dollars¹²⁷ ».

Cet exemple démontre que le Canada veut mettre de l’avant des mesures de protection plus adéquates concernant les données personnelles ainsi que des sanctions à la hauteur des conséquences qu’entraîne une fuite de données.

En résumé, la perspective canadienne et européenne offre une panoplie de principes qui doivent être mis de l’avant sur la scène internationale afin d’émettre les fondements d’une régulation internationale qui soit standardisée, agile, proportionnelle et établie dans le cadre d’une coopération entre les trois principaux acteurs : Internaute, État, et Entreprise. L’exigence en matière de sécurité doit être garantie ainsi que la stabilité financière de ce secteur. Yoshua Bengio, directeur scientifique de MILA, est une des figures le plus respectée et talentueuse dans le milieu de l’intelligence artificielle à l’échelle mondiale. La régulation au niveau des données personnelles passe par la collaboration entre les gouvernements, des experts en IA et la société civile afin d’assurer que les renseignements personnels ne soient pas vendus à des tiers partis à des fins lucratives, que les données soient détruites lors de la fin de leur utilisation, que les données soient conservées localement sur l’appareil de chaque utilisateur, que

¹²⁷ Bélaïr-Cirino, Marco (2020, Juin 13) « Sonia LeBel veut encadrer l’utilisation des données personnelles », *Le Devoir*, Récupéré de <https://www.ledevoir.com/politique/quebec/580726/un-projet-de-loi-pour-encadrer-l-utilisation-des-donnees-personnelles>

l'envoi des données soit crypté et anonymisé. En droit international, le droit positif se base sur le droit déjà existant, et dégagé de toute perspective historique, comparative ou réformatrice¹²⁸. Peut-être il est venu le temps de reformer le droit et utiliser la technologie, l'IA, pour établir une régulation efficace qui encadrerait les données personnelles?

¹²⁸ Cyr, Hugo et François Chevette. « De quel positivisme parlez-vous », *Mélanges Andrée Lajoie*, 2008, p. 36.

Conclusion

Google, Apple, Facebook, Amazon et Microsoft ont tous un point commun : exploiter nos données personnelles afin de faire augmenter leurs recettes. Nous, en tant que consommateurs, ne touchons aucun profit. On a vu dans ce texte comment ces géants font leur argent à nos dépens, comment ils monopolisent le cyberspace mais on a vu aussi que la régulation nécessite d'être adaptée au contexte numérique. Si l'intelligence artificielle représente un moyen pour que ces firmes exploitent de manière efficace nos données, pourquoi l'État ne ferait pas pareil et utiliserait l'intelligence artificielle pour mieux réguler et distribuer les profits de ces compagnies. De toute façon la technologie devrait être au service de la société et non seulement des entreprises.

Pourrait-on voir un organe international légitime qui pourrait veiller à la protection des données personnelles? Pourquoi ne pas s'inspirer d'une organisation comme l'ICANN qui est une autorité de régulation de l'Internet. « *ICANN is a body perceived as legitimate by a reasonable number of players, being vested with the power to control core resources of the network in a shared manner, turning the governance of the internet into a global endeavor*¹²⁹ ». L'ICANN est la société pour l'attribution des noms de domaine et de numéro sur Internet. Elle coordonne le système mondial des adresses internet pour que lorsqu'on saisit une adresse web on soit dirigé à la bonne page. L'ICANN signe des contrats avec des bureaux d'enregistrement dans le monde entier. L'exécution de ces contrats est assurée par le service de conformité contractuelle de l'ICANN. Cette organisation non gouvernementale contribue à rassembler les parties prenantes du monde entier afin de créer des politiques qui permettent à l'Internet de continuer à fonctionner. *It is serving a global purpose, serving the entire world [...] Every government is to sit next to the U.S government in an equal way to manage our*

¹²⁹ Datsygold, Mark. « Understanding the role of States in Global Internet Governance: ICANN and the Question of Legitimacy » *GIGANET: Global Internet Governance Academic Network, Annual Symposium 2017*, p. 7.

*affairs and govern ICANN. None of them would be in a control position but rather in a co-equal position where they are advising along with the private sector, and the civic sector*¹³⁰ »

Pourquoi l'ICANN? Parce que cette organisation est l'échelon suprême de régulation, de normalisation technique et surtout de standardisation des règles sur la gouvernance Internet. Le défi pour la communauté internationale est de standardiser les règles de protection des données personnelles. L'ICANN a été capable de le faire dans leur champ d'expertise alors pourquoi ne pas envisager une entité internationale qui ne veuille qu'à la standardisation des procédés juridiques concernant la protection des données personnelles. En ayant une protection uniforme, il est plus facile d'aller chercher une ristourne économique aux mains des Gafa et de Microsoft. Si chaque État défend les données de ses citoyens à sa façon, il est plus facile pour ces entreprises numériques d'exploiter les vides juridiques ou même d'exploiter d'autres marchés pour faire augmenter leurs recettes. Le Canada peut contribuer en matière de protection des données personnelles. Il doit former une organisation apte à standardiser les mesures de protection des données personnelles afin de mieux respecter la vie privée et mieux distribuer les profits des géants numériques.

À travers une telle organisation, les États peuvent restreindre l'exploitation inadéquate des données personnelles qui voient les Gafa faire des profits aux dépens des utilisateurs du web. Il ne s'agit pas de voir une ristourne d'argent directement vers l'internaute de la part de ces compagnies mais plutôt d'une meilleure allocation des profits par l'entremise de l'État. Pourquoi ne pas envisager, par exemple, une taxe envers ces compagnies qui permettrait de diminuer leurs grands profits pour le redistribuer d'une certaine manière par exemple : par une diminution du taux d'imposition aux contribuables ou des investissements dans des secteurs économiques en difficulté. Tout ceci dans le but de contribuer à une marchandisation des données

¹³⁰ ICANN, Récupéré de <https://www.icann.org/history>

personnelles qui soit juste et équitable autant pour la population que pour les compagnies.

Trois leçons sont tirées de ce texte :

- La technologie va plus vite que l'on croit : Les États ne peuvent pas suivre la vitesse dans laquelle la technologie évolue. Les cadres juridiques restent ancrés dans le passé avec des règles qui ne sont pas adaptées au contexte numérique actuel.
- Nous sommes et serons de plus en plus dépendants de la technologie : Notre réalité quotidienne comporte une réalité virtuelle parallèle. Le danger? La société néglige le sort de leurs données personnelles. Où vont-elles? À quelle fin?
- Le Canada a toujours été reconnu comme meneur par excellence des opérations de maintien de la paix durant les conflits armés. Pourquoi ne pas s'ériger comme meneur par excellence dans la protection des données personnelles? Lors de l'entrevue avec Valérie Pisano mentionnée plutôt, elle affirme que le Canada peut contribuer pour la lutte de la protection de la vie privée basé sur son expertise en IA¹³¹.

Trois éléments qui restent à comprendre après ce travail :

- La sensibilisation de la société civile : Éduquer la population aux risques qui encourent l'exposition de nos données personnelles est un élément crucial dans la protection des DP. Pourquoi ne pas envisager un programme éducatif pour les jeunes afin d'inculquer une éthique civile dans le cyberspace.
- La Chine : Qui dominera le cyberspace? Cèdera-t-elle sa souveraineté sur son territoire virtuel? Est-ce qu'elle va collaborer dans la création d'une organisation -hypothétique- chargé de protéger les renseignements personnels? Est-ce qu'on assiste à une transition de guerre commerciale vers une guerre cybernétique sino-américaine?
- Les géants numériques : Est-ce que c'est utopique de voir un jour la fin de ce monopole américain (GAFA et Microsoft)? Qu'arrivera-t-il quand les géants numériques chinois monopoliseront les marchés africains, ou ceux d'Amérique du Sud?

¹³¹ Renaud, Jean-François. *Op. cit.*

BIBLIOGRAPHIE

Monographies:

Chassigneux, Cynthia, « Vie privée et commerce électronique », *Virginie Mesguich*, 2004, 348 pages.

Stephens-Davidowitz, Seth, « Everybody Lies: The New York Times Bestseller », *Bloomsbury Publishing*, 2017, 352 pages.

Scott Galloway, « Le Règne des Quatre : La face cachée d'Amazon, Apple, Facebook et Google », *Gallimard Ltée-Edito*, 372 pages.

Articles périodiques :

Arnaud, Michel. « Démonétiser l'identité numérique », *Médium*, vol. 16-17, no. 3, 2008, pp. 191-199.

Benhamou, Françoise. « L'État et l'internet. Un cousinage à géométrie variable », *Esprit*, vol.7, Juillet 2011, pp. 96-110.

Belleil, Arnaud. « La régulation économique des données personnelles ? », *LEGICOM*, vol. 42, no. 1, 2009, pp. 143-151.

Bensamoun, Alexandra, et Célia Zolynski. « *Cloud computing* et *big data*. Quel encadrement pour ces nouveaux usages des données personnelles ? », *Réseaux*, vol. 189, no. 1, 2015, pp. 103-121.

Bienvenu, Pierre. « Les enjeux de régulation et de supervision liés aux *fintechs* et à la révolution numérique », *Annales des Mines - Réalités industrielles*, vol. février 2019, no. 1, 2019, pp. 73-76.

Cecere, Grazia, et Fabrice Rochelandet. « Modèle d'affaires numériques, données personnelles et sites web. Une évaluation empirique », *Revue française de gestion*, vol. 224, no. 5, 2012, pp. 111-124.

Ciurak, Dan. « Economics of AI/ML and Big Data in the Data-driven Economy: Implication for Canada's Innovation Strategy », *CIPPO-CIGI Workshop on Intellectual Property and AI and Big Data*, Mars 2019, pp. 1-6.

Ciurak, Dan, «Data as Contested Economic Resource: Framing the Issues», *Centre for International Governance Innovation*, Novembre 2019, pp.1-7.

Ciurak, Dan, «Phoenix Rising? A WTO 2.0 for the Digital Age», *Centre for International Governance Innovation*, April 2019, pp.-1-11.

Ciurak, Dan, «The Economics of Data, Implications for the Data-Driven Economy», *Centre for International Governance Innovation*, Février 2018, pp. 1-9.

- Ciurak, Dan et Maria Ptashkina, «Started the Digital Trade Wars Have: Delineating the Regulatory Battlegrounds», *Centre for International Governance Innovation*, Janvier 2018, pp.1-10.
- Ciurak, Dan, et Bianca Wylie, «Data and Digital Rights: More Questions than Answers- But Enumerating the Questions is Essential», *Centre for International Governance Innovation*, December 2018, pp. 1-5.
- Cyr, Hugo et François Chevette. « De quel positivisme parlez-vous », *Mélanges Andrée Lajoie*, 2008, pp. 33-60.
- Delesse, Claude. « La NSA, « mauvais génie » du cybermonde ? », *Sécurité globale*, vol. 8, no. 4, 2016, pp. 67-104.
- Dubois, Lorette, et Florence Gaullier. « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », *LEGICOM*, vol. 59, no. 2, 2017, pp. 69-102.
- Datysgeld, Mark. « Understanding the role of States in Global Internet Governance: ICANN and the Question of Legitimacy » *GIGANET: Global Internet Governance Academic Network, Annual Symposium 2017*, pp. 1-34.
- Dumoulin, Régis, et Caroline Lancelot Miltgen. « Entreprise et respect de la vie privée du consommateur. De l'usage autorisé à l'utilisation souhaitable des données personnelles », *Revue française de gestion*, vol. 224, no. 5, 2012, pp. 95-109.
- Establier, Alain. « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *Sécurité globale*, vol. 8, no. 4, 2016, pp. 11-56.
- Frayssinet, Jean. « La régulation de la protection des données personnelles », *LEGICOM*, vol. 42, no. 1, 2009, pp. 5-9.
- Gola, Romain. « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, vol. 59, no. 2, 2017, pp. 29-38.
- Hustinx, Peter J. « Protection des données à caractère personnel en ligne: la question des adresses IP », *LEGICOM*, vol. 42, no. 1, 2009, pp. 119-125.
- Lancelot Miltgen, Caroline. « Dévoilement de données personnelles et contreparties attendues en e- commerce : une approche typologique et interculturelle », *Systèmes d'information & management*, vol. 15, no. 4, 2010, pp. 45-91.
- Lyubareva, Inna, et Fabrice Rochelandet. « Modèles économiques, usages et pluralisme de l'information en ligne. Les nouveaux enjeux du pluralisme de l'information à l'ère des plateformes numériques », *Réseaux*, vol. 205, no. 5, 2017, pp. 9-19.
- Ming, Jiang et King-Wa Fu. « Chinese Social Media and Bid Data: Big Data, Big Brother, Big Profit? » *Policy & Internet*, Vol. 10, No. 4, 2018, pp. 372-392.

- Musiani, Francesca. « Les architectures P2P. Une solution européenne originale pour la protection des données personnelles ? », *Réseaux*, vol. 189, no. 1, 2015, pp. 47-75.
- Poulet, Yves. « La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et nos démocraties ? », *LEGICOM*, vol. 42, no. 1, 2009, pp. 47-69.
- Pras, Bernard. « Entreprise et vie privée : le privacy paradox et comment le dépasser », *Revue française de gestion*, Vol.5, no. 224, 2012, pp. 87-94.
- Prince, Jeffrey and Scott Wallsten. «How Much is Privacy Worth Around the World and Across Platforms» *Technology Policy Institute*, January 2020, pp.1-70.
- Rallet, Alain et Samy Guesmi, « Web 2.0 et outils de coordination décentralisée. Un entrelacement des sphères privées et professionnelles », *Revue française de gestion*, 2015, Vol. 2, Numéro 224, pp.139-151.
- Roux, Cécile. « Les nouveaux modèles économiques des sociétés de l'Internet. Les raisons de leur apparition », *Annales des Mines - Réalités industrielles*, vol. novembre 2010, no. 4, 2010, pp. 42-47.
- Zwitter Andrej, et Jilles Hazenberg. « Decentralized Network Governance: Blockchain Technology and the Future of Regulation » *Frontiers in Blockchain*, Vol. 3, Art. 12, 25 mars 2020, pp. 1-12

Reuves électroniques :

Les Affaires

- AFP, (2020, Mai 19) « Facebook à l'amende pour tromperie sur la confidentialité » *Les Affaires*, Récupéré de <https://www.lesaffaires.com/techno/internet/facebook-a-l-amende-pour-tromperie-sur-la-confidentialite/617803>
- La Presse Canadienne (2019, Juillet 30). Capital One victime d'une fuite massive des données. *Les Affaires*. Récupéré de <https://www.lesaffaires.com/bourse/nouvelles-economiques/capital-one-victime-d-une-fuite-massive-de-donnees/611743>
- La Presse Canadienne (2019, Novembre 1^{er}). Fuite chez Desjardins : 4.2 millions de membres touchés. *Les Affaires*. Récupéré de <https://www.lesaffaires.com/secteurs-d-activite/services-financiers/fuite-chez-desjardins-42-millions-de-membres-touches/613897>

The Economist

- Anonyme (2017, Mai 6) Fuel of the future: Data is giving rise to a new economy. How is it shaping up? *The Economist*. Récupéré de <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>

- Anonyme, (2018, Juin 28). « China has the world's most centralised internet system» *The Economist*, Récupéré de <https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system>
- Anonyme, (2019, April 13) « Amazon's empire rests on its low-key approach to AI», *The Economist*, Récupéré de <https://www.economist.com/business/2019/04/11/amazons-empire-rests-on-its-low-key-approach-to-ai>
- Anonyme, (2020, Février 20) « Governments are erecting borders for data», *The Economist*, Récupéré de <https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data>
- Anonyme, (2020, Février 20) « Who will benefit most from the data economy? », *The Economist*, Récupéré de <https://www.economist.com/special-report/2020/02/20/who-will-benefit-most-from-the-data-economy>
- Anonyme (2020, April 30), «Big tech is thriving in the midst of the recession», *The Economist*, Récupéré de <https://www.economist.com/leaders/2020/05/02/big-tech-is-thriving-in-the-midst-of-the-recession>
- Anonyme, (2019, Mai 11), «How creepy is your smart speaker», *The Economist*, Récupéré de <https://www.economist.com/leaders/2019/05/11/how-creepy-is-your-smart-speaker>
- Anonyme, (2020, Juin 28) «The story of the internet is all about layers» *The Economist*, Récupéré de <https://www.economist.com/special-report/2018/06/28/the-story-of-the-internet-is-all-about-layers>

Sites Internet:

- Anonyme, (2019, Avril 3) *The Global Internet Governance Academic Network*, Récupéré de <https://www.giga-net.org/gig-arts-2019-16-17-may-2019-salerno/>
- Bélaïr-Cirino, Marco (2020, Juin 13) « Sonia LeBel veut encadrer l'utilisation des données personnelles », *Le Devoir*, Récupéré de <https://www.ledevoir.com/politique/quebec/580726/un-projet-de-loi-pour-encadrer-l-utilisation-des-donnees-personnelles>
- Bogonost, Ian, (2019, Janvier 31) « Apple's Empty Grandstanding About Privacy », *The Atlantic*, Récupéré de <https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/>
- Commissariat à la protection de la vie privée, (2018, Décembre) Récupéré de <https://www.priv.gc.ca/fr/a-propos-du-commissariat/qui-nous-sommes/commissaire-a-la-protection-de-la-vie-privee-du-canada/>

- Canada. Division de l'économie, des ressources et des affaires internationales. (2020, Novembre 17) *Les lois fédérales du Canada sur la protection de la vie privée*, Publication No. 2007-44-F. Récupéré de https://bdp.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/200744E
- Conseil canadien des normes, (2020), Récupéré de <https://www.scc.ca/fr/RGPD>
- Déclaration Universelle des Droits de l'Homme*, (1948, 10 Décembre), « Article 12 ». Récupéré de <https://www.un.org/fr/universal-declaration-human-rights/>
- Feldstein, Steven (2020, Février 12) «When it comes to digital authoritarianism, China is a challenge – but not the only challenge», *War on the rocks*. Récupéré de <https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/>
- Girard, Joëlle (2020, Septembre 20) « Le Québec adopte finalement l'application fédérale Alerte COVID », *Radio-Canada*, Récupéré de <https://ici.radio-canada.ca/nouvelle/1737406/coronavirus-pandemie-application-notification-tracage>
- ICANN, Récupéré de <https://www.icann.org/history>
- Jacquot, Guillaume, (2020, Mai 28) « Stop Covid : le Sénat approuve à son tour l'application de traçage numérique », *Public Sénat*, Récupéré de <https://www.publicsenat.fr/article/parlementaire/stop-covid-le-senat-approuve-a-son-tour-l-application-de-tracage-numerique>
- La Finance pour tous, (2020, Décembre 1) « GAFA, GAFAM ou NATU : les nouveaux maîtres du monde » *Institut pour l'éducation financière du public*, Récupéré de <https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles-economies/gafa-gafam-ou-natu-les-nouveaux-maitres-du-monde/>
- Mediavilla, Lucas (2019, Mars 22) « Données personnelles : Apple est-il vraiment le bon élève? » *Les Echos*, Récupéré de <https://www.lesechos.fr/tech-medias/hightech/donnees-privées-apple-est-il-vraiment-le-bon-eleve-1002692>
- Renaud, Jean-François (2020, Mai 21). *Entrevue avec Valérie Pisano*. Récupéré de https://www.facebook.com/watch/live/?v=253126652679764&ref=watch_permalink
- Statista [s.d.]. Récupéré le 21 mai 2020 de <https://www.statista.com>
- Tremblay, Janic (2019, Février 8) « Le RGPD ou comment l'Europe protège les données personnelles », *Radio-Canada*, Récupéré de <https://ici.radio-canada.ca/nouvelle/1151913/donnees-personnelles-rgpd-europe>
- Zobrist, Luc et Michael Grammp, (2017) « Le consommateur à l'ère du numérique », *Deloitte Research*, Récupéré de <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/consumer-business/ch-fr-cb-digital-consumer-swiss-retail.pdf>