UNIVERSITÉ DU QUÉBEC À MONTRÉAL

RÉAPPROPRIATION DE L'ESPACE NUMÉRIQUE ET POLITIQUE : L'UNION EUROPÉENNE ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR

VINCENT DUBOIS

OCTOBRE 2023

REMERCIEMENTS

Dans un premier temps, je souhaite remercier mon directeur de recherche Ting-Sheng Lin pour son aide et ses conseils dans l'orientation de ce travail.

À ma mère Sylvie et à Pierre, merci pour votre support dans la révision de ce long projet.

Merci à mon ami de longue date Loïc pour ses encouragements à la poursuite de mes études qui culmine avec le dépôt de ce mémoire.

À Napoléon, ton support moral infini fut d'une aide précieuse.

Finalement, je tiens à exprimer ma plus grande gratitude à ma copine Kaëla pour son support constant. Son aide avec mes nombreuses interrogations, son écoute de mes idées les plus farfelues et sa patience sans limites lors de la production de ce mémoire ont rendu ce projet possible.

Je suis grandement reconnaissant de votre aide à tous. <3

DÉDICACE

À Marie-Thérèse, une femme, une mère et une grand-mère extraordinaire

TABLE DES MATIÈRES

REMERCIEMENTS ii

DÉDICACE iii

LISTE DES FIGURES vi

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES vii

RÉSUMÉ viii

ABSTRACT ix

INTRODUCTION 1

CHAPITRE 1 CADRE D'ANALYSE ET DE RECHERCHE 7

1.1 Comprendre l'environnement social et politique en Europe par l'étude de l'impact du GDPR sur les pratiques en matière de données à travers le Web et les sociétés 8

1.2 Problématique et question de recherche 10

1.3 Perspective d'analyse 11

1.4 Méthodologie 16

CHAPITRE 2 AU CENTRE DU CYBERESPACE, L'UNIVERS DES DONNÉES DE MASSE 20

2.1 La place du cyberespace dans nos vies 21

2.2 Le capitalisme des données 24

2.3 L'importance des données dans notre société pour les différents acteurs 27

2.4 Responsabilités et éthique liées au secteur des données privées 33

CHAPITRE 3 LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES POUR RÉDUIRE LES ABUS LIÉS À L'UTILISATION DES DONNÉES DE MASSE 36

3.1 Analyse de la situation pré-GDPR : politiques, abus et écosystème Web 37

3.2 Les objectifs de la nouvelle législation face aux défis que posent les données Web 40

3.3 Les articles clés du GDPR dans la lutte aux abus 42

3.4 Union européenne post-GDPR : analyse de la transformation de la situation des données 48

CHAPITRE 4 ENJEUX LIÉS À L'UTILISATION DES DONNÉES PERSONNELLES PAR LES GÉANTS DU WEB 61

4.1 La sécurité 61

4.1.1 Paradigme de sécurité lié aux données 64

4.1.2 Les défis liés à l'utilisation sécuritaire des données 65
4.2 Les droits individuels et collectifs au sein de l'Union européenne 68
4.2.1 Réglementations sur l'utilisation des données 70
4.2.2 Enjeux du mode de fonctionnement actuel de collecte et d'utilisation des données pour les droits des individus 72
4.2.3 Les pratiques commerciales des grandes entreprises du web et l'impact sur les acteurs 75
4.3 La souveraineté 76
4.3.1 Impact des données de masse sur la souveraineté du système politique en place 77
4.3.2 Analyse des positions et de l'évolution des discours des acteurs concernant l'enjeu de souveraineté 78

CONCLUSION 82

ANNEXE A Évolution historique de la réglementation de l'Union européenne sur la protection des données 87

ANNEXE B Part de marché mondiale des principaux moteurs de recherche de janvier 2010 à avril 2019 91

ANNEXE C Countries with the highest fines by total number of fines [under GDPR] 92

ANNEXE D Amendes par secteur, en fonction du nombre total d'amendes sous le GDPR 93

BIBLIOGRAPHIE 94

LISTE DES FIGURES

Figure 2.1 Les organisations auxquelles les individus font moins confiance seront confrontées à des actions plus signicatives.....25

Figure 2.2 Surestimation de la confiance des consommateurs par les organisations.....28

Figure 2.3 Classification de sensibilité des données par les individus.....29

Figure 2.4 Décomposition selon l'origine du trafic vers les clients des principaux FAI en France (FIN 2021).....32

Figure 3.1 Conformité au GDPR par pays 49

Figure 3.2 Somme globale des amendes sous le GDPR 51

Figure 3.3 Nombre total d'amendes sous le GDPR 51

Figure 3.4 Évolution de l'environnement réglementaire de 2010 à 2022 55

Figure 4.1 Amendes par type d'infraction et nombre total d'amendes sous le GDPR 69

Figure 4.2 Traitement des données conformément au GDPR.....72

Figure 4.3 Formulaire de témoin par pays (Octobre 2018).....73

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

ADM	Algorithmes de destruction massive
API	Application programming interface / Interface de programmation
CDFUE	Charte des droits fondamentaux de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
CoE	Council of Europe / Conseil de l'Europe
DPA	Data Protection Authorities
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
FTC	Federal Trade Commission
GAFAM	Google, Amazon, Facebook (Meta), Apple, Microsoft
GDPR/RGPD	General Data Protection Regulation / Règlement général sur la protection des données
UE	Union Européenne

RÉSUMÉ

Cette recherche s'intéresse à l'évolution du Web et ses composantes, en Europe, suite à l'entrée en vigueur du Règlement général sur la protection des données (RGPD/GDPR) en mai 2018. L'Union européenne s'est placée de l'avant comme étant un défenseur contre les abus dans l'utilisation des données de masse sur ses citoyens. Au cours des quatre dernières années, comment la situation concernant l'utilisation des informations acquises par les technologies du Web s'est-elle réellement transformée ?

Nous examinerons (A) l'évolution du cyberespace au cours des vingt dernières années et nous brosserons un portrait d'ensemble sur l'organisation de cet espace, les défis, les acteurs et la position de l'Union européenne face à l'utilisation des données tout en regardant les impacts de ces pratiques sur l'Union européenne et ses citoyens. Nous parlerons de l'importance des données dans un système mondial étroitement connecté au Web et des conséquences que peuvent avoir ces informations sur la vie des individus. Nous toucherons aux responsabilités des entreprises dans ce milieu. Nous regarderons (B) les objectifs de l'UE par l'introduction d'un document d'une telle portée afin de faire face aux défis en matière d'utilisation des informations des individus. Nous traiterons de ces changements politiques au sein de cet espace et poserons un regard sur les différents articles clés du document législatif. Nous comparerons la situation avant et après 2018 et traiterons des transformations au sein de cet écosystème à la suite de l'entrée en vigueur du GDPR. Nous inspecterons (C) le développement de trois thèmes importants dans la transformation de cet espace. (1) Comment la sécurité des individus au sein de cet espace s'est transformée depuis l'entrée en vigueur de la nouvelle règlementation ? (2) Est-ce que les droits des citoyens ont été placés de l'avant grâce aux changements sur le plan politique au sein de l'UE ? (3) L'adoption d'un cadre règlementaire plus strict pour les entreprises opérant avec les données de masse, a-t-il permis à l'Union européenne de retrouver un plus grand contrôle sur les actions des entreprises principalement étrangères à travers le Web ?

Nous traiterons de l'évolution de la situation grâce à la documentation disponible et l'analyse des comportements des différents acteurs et chercherons à savoir si l'adoption de règlementation plus stricte concernant les données Web constitue une réappropriation de cet espace par l'Union européenne. Nous retracerons les discours et les actions des différents partis ainsi que les conséquences de ces gestes pour le milieu.

La contribution de la recherche sur le plan théorique et empirique est multiple. D'abord, l'étude tente de voir comment l'adoption de règlementation sur les technologies du Web impacte réellement cet espace et ses acteurs, particulièrement les individus qui sont directement touchés par les actions des différents groupes. Dans un second temps, l'étude permet de recenser les changements au sein de cet espace, leur portée, ainsi que les conséquences de l'évolution de cet espace pour les acteurs et l'écosystème de manière plus générale.

Mots clés : GDPR, RGPD, Données de masse, Union européenne, Législation, Marché des données, Cyberespace, Régulations numériques, Gouvernance.

ABSTRACT

This research focuses on the evolution of the web and its components, in Europe, following the entry into force of the General Data Protection Regulation (GDPR) in May 2018. The European Union has placed itself forward as a defender against abuses in the use of mass data on its citizens. Over the past four years, how has the situation regarding the use of information acquired through web technologies actually transformed?

We will examine (A) the evolution of cyberspace over the last twenty years and give an overview of the organization of this space, the challenges, the actors and the position of the European Union regarding the use of data while looking at the impacts of these practices on the European Union and its citizens. We will talk about the importance of data in a global system closely connected to the Web and the consequences that this information can have on the lives of individuals. We will touch on the responsibilities of companies in this environment. We will look at (B) the objectives of the EU in introducing such a far-reaching document to address the challenges in the use of individuals' information. We will discuss these policy changes within this space and look at the different key articles of the legislative document. We will compare the situation before and after 2018 and address the transformations within this ecosystem as a result of the GDPR. We will inspect (C) the development of three important themes in the transformation of this space: (1) How has the security of individuals within this space been transformed since the new regulation came into force? (2) Has respect for citizens' rights been advanced and respected through changes on the political level within the EU? (3) Has the adoption of a stricter regulatory framework for companies operating with mass data allowed the European Union to regain greater control over the actions of mainly foreign companies across the Web?

We will discuss the evolution of the situation thanks to the available documentation and the analysis of the behaviors of the different actors and we will try to find out if the adoption of stricter regulations concerning Web data constitutes a reappropriation of this space by the European Union. We will trace the discourses and actions of the different parties as well as the consequences of these actions for the environment.

The contribution of the research on the theoretical and empirical level is multiple. First, the study attempts to see how the adoption of regulations on Web technologies really impacts this space and its actors, particularly the individuals who are directly affected by the actions of the different groups. In a second step, the study allows to identify the changes within this space, their scope, as well as the consequences of the evolution of this space for the different actors as well as this ecosystem more generally.

Keywords: GDPR, RGPD, Mass data, European Union, Legislation, Data market, Cyberspace, Digital regulations, Governance.

INTRODUCTION

L'évolution fulgurante de la place du Web dans nos vies a laissé peu de temps aux dirigeants et aux politiques d'emboîter le pas en matière de régulation, de prise de conscience des nombreux défis de cet espace et des dangers liés à un monde interconnecté par une toile numérique (Douzet, 2014; Gashi, 2016). L'omniprésence des produits du Web à travers nos sociétés a contribué à l'intensification des enjeux liés à ce dernier (Goldin, 2014; Harknett, 2011; Loiseau, 2017). La surveillance et le contrôle des activités œuvrant au sein de cet espace se sont centrés pour la majeure partie de leurs existences sur le contrôle des activités prohibées plus traditionnelles (Quéméner, 2011) tout en traitant plus légèrement ou en négligeant les autres sources de dangers pour les citoyens et les gouvernements. Il y a cependant plusieurs préoccupations majeures qui font régulièrement surface auprès des dirigeants politiques à travers le monde envers les activités liées au cyberespace, et ce depuis longtemps (Whitehouse, 2012; West, 2019). Nous constatons que la sécurité des infrastructures et de l'information y transigeant quotidiennement, l'impact des interactions avec divers contenus en ligne sur les droits des individus, la surveillance des activités des utilisateurs et la collecte massive de données représentent toutes des points de faille à la sécurité des États (Danzig, 2014). « [Les conséquences du capitalisme de surveillance combiné au laisser-aller de l'opinion publique en matière de réglementation face à ces modèles d'affaires peuvent être perçues comme une dérive de la démocratie] » (Zuboff, 2019). Il revient donc à l'État d'assurer la sécurité de ses citoyens contre les arnaques, mais aussi du respect des droits de ceux-ci (D'Elia, 2014). C'est le côté novateur des techniques utilisées afin de recueillir une quantité astronomique d'informations additionnée aux multiples possibilités rendue possible grâce à celles-ci qui les rendent aussi attrayantes que dangereuses (Thatcher, 2018). Ces bases de données combinées à des systèmes informatiques ainsi que des algorithmes ultra-complexes font de ces derniers des outils très pratiques au fonctionnement de l'économie mondiale ainsi que dans de nombreuses autres sphères dont celle de la recherche et le développement de nouvelles technologies. De plus, la puissance de ces multinationales du Web ne se limite pas seulement à leur activité économique de collecte et de vente d'informations sur les activités, les comportements et les personnes. La puissance de celles-ci s'étale aussi dans la sphère sociale et politique de nos sociétés, ce qui leur

confère une emprise immense et difficilement contrôlable sur nos institutions étatiques. Les défis et les risques sont aussi importants que les possibilités au sein de cet espace d'innovation. Cependant, la nécessité de réduire les nombreuses failles de sécurité sur le Web (Goldin, 2014) et de rendre un certain équilibre dans la balance des pouvoirs entre les différents acteurs, surtout en ce qui concerne les données personnelles, se ressent de plus en plus.

La prise en importance des nombreux défis liés aux données de masses et ses sous-enjeux se sont particulièrement fait remarquer ces dernières années avec les nombreuses histoires d'abus dans les pratiques des entreprises du Web envers les citoyens européens. Les questions liées à la sécurité de l'information en ligne, à l'accès à l'information par les différents acteurs et tout ce qui touche aux aspects juridiques de l'utilisation des données représentent tous des enjeux importants aux yeux de l'Union européenne et ses citoyens. Cette prise en importance du stockage et de l'utilisation des données de masse publiques et privées sur les entreprises et citoyens a poussé l'Union européenne à adopter des politiques de contrôle plus sévère afin de limiter la vulnérabilité des différents partis et aussi de réduire les abus liés aux pratiques excessives de collecte, d'entreposage et d'utilisation des données. Afin de permettre un développement plus durable du Web, un contrôle plus strict de ces pratiques en matière de données a été instauré au sein de l'Union européenne avec l'adoption du Règlement général sur la protection des données (RGPD/GDPR). Une supervision accrue des pratiques commerciales à travers le Web, au sein de l'Union européenne, symbolise cette volonté de vouloir mieux encadrer les pratiques au sein de cet espace afin d'en faire bénéficier les citoyens et aussi de renverser une certaine souveraineté effacée du groupe d'État face aux multinationales œuvrant à travers le Web. Touchant particulièrement l'aspect économique du Web, la volonté de modifier le fonctionnement d'une grande partie système économique sur l'internet, où le profit et la croissance économique sont souvent mis à l'avant-plan au détriment de certains autres aspects sociaux, représente un défi de taille pour l'UE. Reflétant sur la nécessité d'un front commun international afin de faire face aux défis du Web, Goldin (2014) parle de la nécessité de voir ce modèle de réponse, de stratégie commune, de bonnes pratiques afin de répondre aux défis croissants de cet espace. L'approche unie de l'Union européenne où plusieurs pays aux idéaux similaires tentent de faire face aux pratiques illicites et douteuses représente un avancement majeur pour cet espace dans le but de mieux contrôler les activités s'y déroulant. Cette même vision de la nécessité d'une approche collective est aussi abordée par d'autres auteurs, on parle, entre autres,

de l'adoption d'un cadre harmonisé de règlementation et de normes par les États membres (Quéméner, 2016; Mathias, 2018) ou encore des bénéfices d'une telle approche pour un environnement aussi complexe.

> « The Internet is developed by thousands of engineers, managed by tens of thousands of private entities, and used by more than four billion people around the world, regardless of frontiers. If governments want to find sustainable solutions for Internet-related issues, they will fail if they do not involve the developers, providers, and users of digital services in an appropriate way. When it comes to the governance of the Internet, there is no alternative to a multi-stakeholder approach. » (Kleinwächter, 2021)

Un espace aussi ouvert et multisectoriel que le Web ne peut pas être unilatéralement modifié par un État ou groupe d'individus. L'implication de différents groupes, communautés, visions, États, experts et entreprises du Web sont essentielles aux transformations souhaitées de l'environnement Web.

Dans le cadre de ce travail, l'analyse sera divisée en trois sections permettant de cerner le sujet des données de masse et des effets des changements politiques au sein de l'Union européenne. Au cours de la recherche, nous poserons un regard sur ces trois aspects importants à l'univers des données de masse en tenant compte d'une perspective critique des études en sécurité.

D'abord, nous dresserons un portrait d'ensemble du cyberespace et l'univers des données de masse ainsi que des aspects qui composent cet espace. Nous parlerons de l'organisation de ce dernier, de la place des données dans nos sociétés, des tendances qui influencent les comportements, des différents défis auxquels les acteurs font face. Aussi, il sera question de différentes visions des parties impliquées et leur approche face à la situation, dont celle des géants du Web par l'analyse de leurs politiques, leurs déclarations publiques et leurs actions concrètes. Ce regard sur l'état de cet espace nous permettra d'avoir une perspective sur l'ensemble des activités au sein de celui-ci et de l'impact qu'une nouvelle législation aurait sur les activités des acteurs.

Nous analyserons dans un second temps le règlement général sur la protection des données, qui est l'élément central aux changements politiques sur l'utilisation, la production, la conservation, le transfert et autres politiques liés aux données au sein de l'Union européenne. Nous analyserons les

buts de l'introduction d'un tel document législatif. Nous regarderons les différents articles clés inscrits dans le document et les impacts potentiels et réels de ceux-ci sur le milieu des données et les acteurs de cet espace. L'analyse des impacts et des transformations, suite à l'entrée en vigueur de la nouvelle législation européenne sur les données, en comparant les pratiques des différents groupes avant et après 2018, soit l'année de l'entrée en vigueur de cette législation et de cette position plus ferme de l'UE sur les données, permettra de voir les conséquences directes réelles des politiques de l'UE.

La dernière section se focalisera sur l'analyse de trois enjeux majeurs liés à l'utilisation abusive des données par les compagnies du Web au sein de l'Union européenne et qui ont poussé ce dernier à adopter une telle position politique et législative afin de mieux contrôler l'utilisation des données de masse. Pour ce faire, nous regarderons le thème de la sécurité à travers les comportements des entreprises et les répercussions pour les individus et l'UE. Nous toucherons ensuite au sujet du respect des droits individuels des utilisateurs du Web et l'architecture du système actuellement en place qui mise sur utilisation des données personnelles des individus. Troisièmement, nous regarderons la question de souveraineté du regroupement d'États à la suite de l'adoption de ces récentes politiques envers les pratiques des entreprises désirant opérer avec les données des personnes des individus au sein de l'espace Schengen. L'analyse des différentes actions prise l'UE dans leur réponse relativement à ce défi ainsi que la position des acteurs d'intérêt alimentera cette section sur la gouvernance et la souveraineté.

Cette recherche aura pour objectif de faire état de la situation concernant le monde des données de masse au sein de l'UE et également de répertorier les impacts dans le changement de législation sur ce milieu au cours des dernières années. De manière plus générale cette recherche nous aidera à cerner l'état de la situation actuelle au sein de l'Union européenne et du même coup à répondre à de nombreuses interrogations comme : quel est l'impact de la production, l'utilisation et le contrôle des données privées des individus par les différentes entreprises étrangères pour l'Union européenne et ses citoyens ? Est-il possible de trouver un équilibre entre vie privée et collecte de données au sein de l'Union européenne ? Est-il possible pour l'Union européenne de restreindre unilatéralement l'utilisation des données sur son territoire ou est-ce que la coopération avec les autres acteurs afin d'en assurer le succès ? Quelles sont les répercussions des politiques de données de l'UE sur le modèle économique en place ? Cette analyse nous en apprendra aussi davantage sur

les rapports entre les multiples acteurs dans le domaine des données. Puis, une telle recherche nous donnera l'opportunité de voir l'influence de l'UE sur le système politique et économique en Europe et sur les pratiques de gestion des données des entreprises du Web.

Plusieurs notions et concepts clés nécessitent d'être définis afin de bien cadrer la présente recherche qui compose un enjeu de sécurité dans les études en relations internationales. D'abord, la notion d'écosystème du Web cherche à faire référence à l'ensemble des éléments, physiques ou non. Ce système est composé d'acteurs qui interagissent au sein de cet espace virtuel et qui par leurs interactions contribuent à la reproduction de cet environnement.

Il est également nécessaire de définir la sécurité en soi dans le contexte l'enjeu étudié. Nous considérons la sécurité comme étant un objectif ou un état à atteindre par les acteurs, où règne l'absence de menaces (People, 2015). Cette sécurité s'opère par nos actions verbales et physiques qui impactent l'environnement en question. La sécurisation, quant à elle, représente le processus qui entraine un enjeu comme étant de nature relevant de la sécurité (Grondin, 2010).

À travers la question de recherche, la sécurité au sein du cyberespace constitue une notion essentielle afin de comprendre les comportements qui motivent les différents acteurs et leurs actions. La sécurité dans le cas présent n'est pas considérée comme étant essentiellement militaire. Cette sécurité est néanmoins étroitement liée à la souveraineté étatique, correspondant au pouvoir de gestion et de contrôle des actions s'opérant au sein de frontières déterminées. Au sein du Web, la gouvernance des données est liée à la manière dont les informations sont traitées. Elle peut être associée aux actions des entreprises, tout comme elle peut être liée aux actions politiques, prises à l'égard de ces données qui circulent, qui ont un impact sur la gestion de ces informations. En ce qui concerne le concept de la vie privée, nous adoptons la définition suivante : « Privacy can be thought of as "a claim, entitlement, or right of an individual to determine what information about himself or herself may be communicated to others" (Torra 2017, p. 5). » (Andrew, 2019).

En relation avec ce dernier concept, les données personnelles sont les informations, ou encore les traces des activités produites par les interactions des individus avec le Web et ses composantes. Ces informations sont volatiles et elles sont intangibles due au fait quelles sont produites en continu par le simple fait de nos actions quotidiennes. L'utilisation de ces informations nous amène au

concept du consentement. Nous définissons le consentement comme étant l'acceptation volontaire et en pleine conscience et sans coercition d'une action commise à son égard ou celui d'autrui.

L'intérêt de la recherche pour la science politique et les théories en Relations internationales consiste à vouloir mieux définir l'influence des transformations au sein du Web, un espace où tous coexistent et où les décisions de groupes d'acteurs sont en mesure d'influencer les transformations au sein d'un réseau complexe qui façonne les activités des sociétés à travers le monde.

CHAPITRE 1
CADRE D'ANALYSE ET DE RECHERCHE

Cette première partie de la recherche aura pour but d'introduire le sujet en présentant différents aspects importants liés aux défis des données au sein de l'Union européenne à la suite de l'introduction du GDPR. Nous présenterons les acteurs, les défis, les questionnements essentiels à la compréhension du sujet. Afin d'analyser le sujet, il est essentiel de comprendre l'environnement des données de masse et les différents éléments qui ont poussé l'UE à adopter une telle position politique envers cet espace. Nous aborderons en détail les effets de l'introduction de nouvelles politiques envers les pratiques sur le cyberespace et particulièrement dans le domaine de la sécurité, celui des droits des citoyens européens et celui de la souveraineté des États membres de l'UE. Dans le but d'arriver à analyser ces trois points, nous dresserons tout d'abord un portrait du cyberespace et des différents aspects qui composent cet espace, des tendances influençant les comportements, des approches des acteurs face aux nombreux défis. Ensuite, nous parlerons brièvement les effets du règlement général sur la protection des données. Nous terminerons cette section en définissant l'objectif de cette recherche ainsi que la pertinence d'une telle analyse pour la science politique. Par la suite, nous ferons une analyse en détail de la situation négative relative aux données de masse et nous définirons la question de recherche. Puis, nous aborderons le choix de l'approche de recherche utilisé afin de comprendre les transformations au sein de cet environnement. Nous parlerons entre autres de la manière dont les théories critiques en sécurité sont en mesure de fournir les outils nécessaires et les pistes de recherche pour être en mesure de cerner le sujet des données de masse et l'impact de l'adoption d'une pièce législative aussi important que le règlement général sur la protection des données par l'UE. Aussi, il sera question de la manière dont la vision de cette approche nous permet de produire une analyse complexe sur les différents éléments influençant la situation. Bien entendu, nous discuterons de cette approche d'analyse plus en profondeur et de la perspective d'une telle approche envers ce défi du cyberespace, après quoi nous l'utiliserons pour guider notre regard en vue de faire l'examen des transformations politiques au sein de ce milieu. Dernièrement, nous discuterons de la méthode de recherche utilisée afin d'acquérir nos données ainsi que l'analyse de ces données choisie et la validation de ces données.

1.1 Comprendre l'environnement social et politique en Europe par l'étude de l'impact du GDPR sur les pratiques en matière de données à travers le Web et les sociétés

La décision de l'Union européenne d'adopter une position plus sévère envers les entreprises à l'égard de l'utilisation et la collecte des données en sol européen, dans le but de minimiser les aspects négatifs de ces pratiques commerciales, représente une étape importante pour l'unité des membres. L'étude de l'impact du GDPR sur les pratiques en matière d'utilisation des données nous permet de mettre en lumière plusieurs aspects cruciaux de cet espace en perpétuel développement. Cette analyse permet aussi de mieux comprendre les interactions entre les différents acteurs dans le milieu et permet de mettre en lumière l'importance des données pour nos sociétés par l'analyse des impacts d'un document législatif aussi important que le GDPR. Dernièrement, cette étude nous permet de visiter trois champs d'analyse en lien avec la question de recherche soit celui du respect des droits des individus, celui de la sécurité des informations personnelles des différents acteurs au sein de l'UE et des pratiques dans cet espace et puis de suivre l'évolution de la gouvernance de l'UE vis-à-vis l'espace Web européen.

Le développement d'une vision de pensée collective sur l'importance de la question de l'utilisation des données à travers le temps dans nos sociétés émane des dangers perçus associés aux abus d'utilisation de ces informations. La difficulté pour les États de garantir un environnement sécuritaire et juste à leurs citoyens sur le Web, où une multitude de dangers les attendent possiblement à chaque lien Web ou courriel, est complexe (Goldin, 2014; Mathias, 2018; Ciuriak, 2018a). Faire de cet espace un endroit où les droits de ceux-ci sont respectés par l'ensemble des entreprises opérant avec leurs données représente un défi de taille auquel le GDPR tente de faire face.

L'utilisation non transparente des données de masse, les négligences dans l'utilisation de ces données et les abus variés d'utilisation de ces informations, par les entreprises opérant avec les données, ont contribué à la détérioration de la confiance des utilisateurs et des États envers ces compagnies qui utilisent ce modèle d'affaires. Ces négligences de ces entreprises du Web les

rendent tout autant responsables de l'état de la situation, concernant la sécurité du Web, que les individus perpétrant les actions illégales avec ces données obtenues de façon frauduleuse. Plusieurs situations négatives ayant fait surface au cours des dernières années sont liées aux négligences des entreprises dans leur usage des données, d'où la nécessité de consacrer davantage d'efforts afin d'analyser les effets de ces technologies sur les différents acteurs et nos sociétés. En termes d'évènements récents, nous pouvons penser notamment à l'utilisation des données personnelles de manière illicite dans la course électorale de 2016 aux États-Unis, dans l'affaire Cambride Analytica, permise par l'entremise de la compagnie Facebook. Il y a aussi eu les nombreuses fuites de données d'entreprises internationales comme Équifax, Uber, Yahoo et plus encore. Les informations personnelles et privées des utilisateurs compromis sont vendues illicitement et se retrouvent utilisées pour commettre d'autres fraudes impactant tout le monde, les individus, les entreprises et les États.

Étudier les effets de nouvelles réglementations en matière de données sur l'environnement politique et social en Europe nous permet de mieux comprendre l'état de la gouvernance du Web. Ensuite, nous pouvons examiner comment les différents acteurs s'adaptent à la situation et quels sont les impacts envers chacun des groupes respectivement. Ce regard sur la gouvernance nous permet aussi de voir si cette adoption de politique plus stricte, au sein de l'UE, envers le secteur des données a réellement un impact réel sur les comportements des entreprises du Web dans leurs façons d'opérer et de voir s'il y a un impact sur le modèle d'affaire de ces entreprises des données. Analyser les effets du GDPR nous aidera à voir les impacts locaux et internationaux économiques sur les pratiques des entreprises à travers le temps. À plus long terme, l'étude de ces effets permettra de voir si les objectifs des politiques européennes ont été atteints et dans le cas contraire, de voir le niveau de progression relativement aux objectifs établis.

Pour la science politique, il semble primordial de faire l'analyse des impacts à moyen et plus long terme du GDPR, considérant que ce dernier touche différents secteurs étroitement liés de l'écosystème mondial du partage d'informations numérisées. Cette occasion de mieux comprendre l'évolution de cet espace à travers la perspective des différents acteurs nous aidera à mieux saisir les impacts de cette régulation sur les pratiques d'utilisation des données en Europe.

1.2 Problématique et question de recherche

La prise en importance du Web dans nos vies sociales et privées ainsi que la transition des sociétés vers un environnement principalement numérique expose les citoyens, les États et les entreprises à travers le monde entier à des défis de taille dans leur manière de gérer les activités liées à l'usage d'internet. C'est particulièrement le cas pour tout ce qui concerne les données de masse. Le besoin d'assurer le développement et la mise en place d'une gouvernance mieux adaptée aux différents défis contemporains que pose cet espace s'est développé en Europe. L'accroissement de l'utilisation mondiale des outils, applications et sites Web en sont responsables. La prise en importance de puissantes sociétés du Web américaines, comme Google, Amazon, Meta (Facebook), Apple, Microsoft, Netflix et d'autres entreprises spécialisées dans la sphère des données comme les courtiers en donnés (Data brokers) et autres acteurs, pose des défis d'envergure pour les États afin d'assurer un contrôle sur les pratiques commerciales de ces entreprises et garantir un respect des politiques ainsi que des droits des citoyens européens. À travers cet espace, l'omniprésence des services dits « gratuits », qui sont presque indispensables à notre fonctionnement quotidien, que ce soit pour le travail ou nos vies sociales, en échange d'une collecte substantielle, voire intégrale, de nos données se trouve à être extrêmement lucratif et pratique à plusieurs niveaux pour ces entreprises (Loiseau, 2017). Cette utilisation massive d'informations sur les individus pose des défis considérables pour les États qui cherchent à reprendre un certain contrôle sur leur espace « virtuel » en déterminant quelles pratiques sont acceptables et définir celles qui sont prohibées. Au sein de cet environnement complexe évoluant ultra rapidement, le sujet des données de masse est d'actualité et nécessite une attention particulière de la part des dirigeants politiques dans la mesure où les répercussions des actions et politiques ont des effets sur différents secteurs au sein d'États. La nécessité pour l'Union européenne de garder un contrôle sur les pratiques commerciales de ces grandes entreprises sur leur territoire représente tout d'abord une nécessité pour les autorités d'assurer la sécurité de leurs citoyens et un respect des leurs droit, mais aussi un désir pour l'acteur de faire respecter son autorité et sa souveraineté.

La croissance fulgurante des services « gratuits » sur le Web a poussé le développement de discours et de politiques axés sur la sécurité et le contrôle des pratiques commerciales avec les données, la

souveraineté de l'Union européenne ainsi que sur le respect des droits des usagers. L'utilisation abusive des données individuelles, publiques et confidentielles, principalement par des multinationales américaines et générées par les interactions sur internet et avec les applications mobiles, est devenue un problème majeur aux yeux l'Union européenne. Est-ce que l'adoption de réglementation plus stricte concernant l'utilisation des données Web, notamment avec l'entrée en vigueur du GDPR en 2018, constitue une réappropriation de cet espace par l'Union européenne ?

1.3 Perspective d'analyse

À travers cette recherche, nous chercherons à comprendre pour quelles raisons et de quelles manières ces transformations au sein de l'UE et du cyberespace se produisent et nous analyserons les effets de ces transformations sur le système politique en place ainsi que sur les différents acteurs (Balzacq, 2016). L'analyse de l'impact du Règlement général sur la protection des données dans le cyberespace européen et sur la situation socio-économique et politique en Europe, plusieurs éléments clés nécessitent d'être examinés afin de délimiter notre objet d'étude. Il est essentiel de comprendre la structure de l'enjeu, de déterminer les points d'intérêts pour la recherche, de définir la situation actuelle selon différentes perspectives des différents acteurs, de démontrer les tendances et les dynamiques concernant le sujet et de recenser les propriétés quant à la nature et les tendances dans le domaine.

L'analyse critique du sujet nous permet de faire l'analyse des impacts des décisions politiques et juridiques de l'UE sur le secteur des données. Une analyse des conséquences de réglementer le milieu en question nous aidera à comprendre les dynamiques entre les différents acteurs (Waever, 2011). Dans un même ordre d'idées, cette approche nous permet d'obtenir une perspective d'ensemble sur le sujet et les différents éléments qui influencent ce dernier. Cette vision globale des divers éléments permet d'apporter une foule d'arguments et de points d'analyse afin de déterminer les champs d'influence sur le sujet de recherche. Dans le cas présent, il semble important de ne pas limiter la recherche aux champs d'analyse proposés par la théorie et de garder

une approche ouverte aux différents éléments pouvant avoir un impact sur la situation des données afin de garder une position critique et ouverte aux débats; nous élaborerons sur la question de ce choix plus loin.

Dans notre analyse critique en sécurité de l'impact du GDPR, nous retrouvons comme point central d'intérêt les citoyens européens. Les différents points choisis seront donc analysés en tenant compte des impacts à l'endroit de ces derniers. L'émancipation des individus de cet environnement, où les données des individus sont utilisées de manière abusive, est un point clé de cette recherche et sera un objet de référence à plusieurs égards. Le concept d'émancipation des individus pour les études critiques fait référence à la recherche de réduire les contraintes ou dangers. L'émancipation est considérée comme étant un processus et un objectif (Grondin, 2010). De plus, en tenant compte que ce sont les États qui représentent les citoyens à plus grande échelle et qu'ils sont donc une extension des individus, il sera question de l'UE de façon plus générale et des développements à plusieurs niveaux suite à l'entrée en vigueur du GDPR. Cette recherche prend aussi en compte les entreprises opérant au sein de cet espace. Celles-ci sont directement touchées par les politiques et leurs actions ont un impact sur les autres acteurs de cet espace. Il semble donc important de comprendre leurs agissements, leurs perceptions et leurs actions en matière de données. Nous parlerons brièvement des autres États internationaux qui influencent et qui sont influencés par les décisions de l'Union européenne de mettre en place un système de contrôle sur l'utilisation des données dans le but de nous fournir des points de référence concernant certains aspects de la recherche.

Les enjeux de sécurité présentent souvent des dilemmes complexes pour les États. Didier Bigo qui soutient que la sécurité de certains mène à l'insécurité des autres groupes (People, 2015) offre une perspective intéressante pour l'analyse des impacts de la réglementation du Web. La recherche d'une plus grande sécurité pour les citoyens, leurs données et leurs droits a un impact sur l'économie des données et les entreprises opérant dans ce milieu en laissant planer certaines incertitudes quant au futur de l'industrie. Un système économique basé sur l'accroissement constant de la production et du capital est confronté à de nouvelles barrières politiques. Cette dynamique dans l'impact des politiques européennes jumelée au concept de sécurité est centrale à l'étude du sujet. Cela nous aidera à voir comment les théories politiques en sécurité se traduisent à travers les positions politiques (Waever, 2011). Aussi, l'élément poststructuralisme concernant

l'évolution perpétuelle des États dans le but de s'adapter au système qui les entoure est un élément intéressant qui nécessite d'être pris en ligne de compte pour les études critiques en sécurité. À travers la perspective d'analyse, il est essentiel de prendre en considération que la sécurité est toujours pour un groupe et dans un but précis tout comme les pratiques en sécurité. Aussi, la séparation entre intérieur et extérieur n'est plus toujours clairement définie dans le domaine de la sécurité & l'insécurité comme le précise Bigo (People, 2015).

L'étude du sujet au travers des actes de langage représente un aspect important à la recherche, car « la parole elle-même n'est pas transparente ou dépourvue de pouvoir » (Hansen 2012). Ce côté présente directement la vision publique des acteurs d'un sujet précis. De l'autre côté, l'analyse des actes non verbaux présente une perspective additionnelle permettant d'apporter des éléments qui ne seraient pas clairement énoncés par les acteurs permettant ainsi de produire une analyse plus fidèle de la réalité. La gouvernementalité est aussi un point important pour cette recherche critique en sécurité. Dans la mesure où nous cherchons à voir l'évolution de la situation sur l'utilisation des données en Europe, de poser notre regard sur l'évolution du pouvoir au sein du regroupement d'États à travers les moyens utilisés à différents niveaux afin d'y arriver, nous aidera à mieux comprendre comment les différentes interactions des acteurs influencent le pouvoir des États et de leurs constituants par la même occasion. Dernièrement, l'équilibre des puissances est un point important à mentionner dans le cas présent. « Boundaries have become elusive phenomena, in ways that demand unfamiliar ways of understanding forms of subordination among various subsystems, [...] » (Beauman, 2014). L'ouverture des frontières virtuelles à travers le cyberespace pose des défis de taille aux États cherchant à maintenir certains principes de base et offrir à leurs constituants les mêmes droits que ceux dont ils disposent dans l'espace physique de leur pays. L'interconnexion mondiale des pays à travers le Web fait de la géopolitique un outil indispensable afin de bien comprendre les relations de pouvoirs s'y opérant (Douzet, 2014). Le monde des données étant principalement dirigé par les grandes entreprises américaines et la difficulté, voire l'impossibilité, de faire respecter les règlements nationaux aux entreprises étrangères se veut un défi pour l'UE (Grondin, 2010).

Le choix d'approche du sujet, c'est-à-dire les théories en sécurité, émane du fait que cette approche théorique permet l'analyse d'une situation précise dans un contexte précis, tout en permettant l'analyse d'éléments qui sont souvent ignorés par certaines théories plus classiques. De cette façon,

nous sommes en mesure d'explorer en profondeur certains éléments qui ont ou n'ont pas d'influence sur notre objet d'analyse. C'est notamment le cas lors que nous souhaitons comprendre les intentions des principaux acteurs en jeu. Les théories classiques qui font de l'État le seul intérêt ne tiennent pas compte des autres acteurs que l'on considère comme étant essentiel dans cette analyse. c'est-à-dire les individus et les entreprises. Autrement dit: « The world is social, and not purely material. » (Collins, 2019). L'approche choisie des théories critiques en sécurité et notre analyse des transformations du cyberespace permettent de mettre l'accent sur les divers acteurs et leurs interactions à travers le système et des pratiques en place, nous éloignant ainsi de ces approches classiques (Collins, 2019; Ragot, 2015).

Aussi, contrairement à certains mouvements de pensée, comme les néoréalismes, qui décrivent le système comme étant anarchique (Macleod, 2010), je suis d'avis qu'une certaine hiérarchie est au contraire présente, même si personne ne dirige à proprement parler. Cette hiérarchie économique, militaire et politique dirige sommairement les actions des individus, des groupes et des États. Ce même ordre, malgré la présence d'acteurs malveillants, est aussi perceptible à travers le Web. Lorsque l'on pense aux acteurs qui « dirigent » par leur influence à travers le système international et l'écosystème du Web, plusieurs « noms » (États-Unis, Unions européennes, Chine, GAFAM(s)) nous viennent à l'esprit. Nous ne disons pas que personne ne dirige ou ne domine, car chacun est à la poursuite unique de ses intérêts. Cette domination de certains acteurs instaure un certain ordre au sein du système international. Aussi, nous rejetons la thèse de l'anarchie du système sous l'affirmation que parfois les intérêts des certains coïncident avec ceux d'autres, créant ainsi des alliances afin d'atteindre des buts communs. À travers le Web, malgré le manque de structure qui est encore plus flagrant, cette même convergence d'intérêt et collaboration peut également être observée entre les acteurs. La recherche de la sécurité de la société civile par l'adoption de réglementations adaptées aux défis modernes de manière multilatérale nous rapproche quelque peu des néolibéraux comme approche en Relations internationales, mise à part la structure anarchique du système (Macleod, 2010). De plus, le besoin d'une approche post-positivisme dans l'analyse de la question se trouve essentiel pour comprendre l'influence de certains facteurs subjectifs entrant en ligne de compte, tels que la sécurité. « In contrast, for securitization theory, the 'security-ness' of an entity does not depend on objective features, but rather stems from the interactions between

a securitizing actor and its audience. » (Balzacq, 2016). Cette subjectivité des théories de sécurisation place l'analyse dans un contexte qui ne peut être réduit en une réponse binaire.

Partageant des prémisses ontologiques et méthodologiques similaires avec le constructivisme, notamment en ce qui concerne les éléments analysés et la manière d'analyser ces données, les études critiques en sécurité mettent aussi l'accent sur l'étude des actes de langages et l'étude des pratiques dans les éléments analysé (Balzacq, 2016). L'importance de l'identité, telle que les constructivistes la considèrent au sein de leurs recherches, dans l'objectif de comprendre les décisions des acteurs (Collins, 2019) se retrouve aussi au centre de cette analyse.

En ce qui concerne les possibles critiques de l'approche choisie, une critique formulée par Beauman (2014) concerne le choix des approches critiques en sécurité qui définissent la surveillance comme étant au service des puissants acteurs et de leurs intérêts. Ce dernier cherche à mettre en lumière l'ambiguïté des comportements des acteurs et cherche à savoir si les acteurs sont pleinement conscients de leurs intérêts, comme notre approche le sous-entend, étant donné les contradictions imprégnées à travers leurs actions et choix. Une autre critique à l'égard de l'étude de la question en termes d'enjeu de sécurité pourrait certainement être formulée. À la lumière de ces critiques, nous reconnaissons un certain degré d'incertitude qui à travers l'étude critique en Relation internationale, ne permettent de définition claire sur le concept de sécurité (Grondin, 2010), et que les approches post-positivistes n'offrent pas de certitudes quant aux connaissances, mais plutôt une perspective sur l'enjeu en question.

Les études critiques trouvent leurs racines à travers plusieurs champs, lui permettant ainsi d'avoir une portée d'analyse des éléments plus large en réduisant les facteurs limitatifs des approches aux idées fixes et selon moi au point de vue restreintes. Bien que l'approche choisie, à mon avis, permettte de bien comprendre les divers aspects clés de l'objet d'étude, certaines critiques peuvent lui être adressées. Cette analyse aurait peut-être pu être réalisée sous l'angle des enjeux de politique publique ou bien encore en droit international. D'autres angles d'approches critiques, telles que les approches féministes, postcoloniales ou culturelles, seraient probablement en mesure d'analyser la situation et fournir des informations complémentaires importantes sur le sujet (Singh, 2015).

Les limites de recherches dans l'étude de ce sujet sont multiples et elles peuvent avoir un impact sur celle-ci à plusieurs niveaux différents. Tout d'abord, l'accès à certaines informations surtout celles qui touchent les pratiques des entreprises avec les données des utilisateurs est parfois difficilement accessible, voire pas du tout. Les politiques des entreprises ne sont pas toujours clairement énoncés et les pratiques de celles-ci ne sont pas toujours vérifiables compte tenu des secrets commerciaux en jeu et rendent ces pratiques ''invisibles'' en quelque sorte au public. Aussi, la quantité innombrable d'entreprises, de pages Web et de transfert de données entre les entreprises à travers le monde entier chaque jour rend la traçabilité des activités très complexe rapidement. De faire l'analyse de chacune d'entre elles n'est pas une option envisageable et réaliste. Cette restriction d'accès à certaines informations peut avoir un impact sur les conclusions tirées à la suite de l'analyse de l'état de cet espace et l'analyse des développements depuis l'entrée en vigueur des nouvelles politiques. Comme autre limite, il est nécessaire de prendre en considération la rapide évolution de cet espace. Le développement rapide des pratiques employées par les entreprises du Web et des positions des acteurs pourrait venir contredire certains points et introduire des nuances au cours de la recherche. La dernière limite concerne le choix d'analyse, celle-ci représente une vision de la situation parmi une pluralité de perspectives possibles de l'enjeu à l'étude et donc se trouve être une « vérité » relative (Cornut, 2014).

1.4 Méthodologie

Dans le cadre de cette recherche, l'adoption d'une approche pragmatique basée sur les théories critiques de sécurité en Relations internationales nous permet de mieux cerner et répondre l'enjeu en question en s'intéressant aux événements (Cornut, 2014). Dans le but d'évaluer l'évolution concernant la situation sur l'utilisation abusive des données de masse, nous utiliserons une revue de la littérature du sujet afin de cerner le sujet, l'objet d'étude, les courants de pensée et les évaluations faites de ce champ d'études. Ensuite, dans le but de recueillir davantage

d'informations sur les interactions et position des acteurs, nous procéderons à une observation documentaire des discours et gestes des différents acteurs, ce qui nous permettra d'analyser des informations essentielles pour comprendre l'évolution de cet espace, les approches des acteurs, ainsi que des interactions entre eux (Loiseau, 2017). Pour ce faire, l'utilisation de discours rapportées par l'entremise d'articles de journaux nous aidera à établir la position de certains acteurs, tels que les GAFAM(s). Ces articles de journaux bien qu'ils ne soient pas scientifiques, offrent une perspective importante de la part de ces entités. De plus, ils seront utilisés quasi exclusivement de cette manière ou afin d'introduire une situation qui relate de l'actualité ou dans le but de rapporter des paroles d'une personne d'intérêt qui relate de la vision d'un groupe d'acteurs, comme un employé d'une multinationale des données. Bien que ces documents ainsi que les rapports et publications d'entreprises ne représentent pas en soi des documents scientifiques, ils émettent néanmoins une perspective importante de la part de ces entités en rapport à des événements ou des politiques internes qui sont intéressantes pour nos recherches (Ragot, 2015). Parfois, ces informations sont difficilement acquérable autrement. En croisant ces informations avec les faits observables nous serons en mesure de faire une analyse croisée de la réalité des pratiques au sein de ce milieu.

Dans un premier temps, la revue de littérature nous permettra d'établir un portrait de la situation concernant l'utilisation des données au sein de l'Union européenne. De voir ce que la littérature a déjà produit sur le sujet des données, des acteurs impliqués, des pratiques de l'industrie, des positions idéologiques et de la sécurité de l'écosystème, sera essentiel afin de produire une recherche sur l'impact du GDPR. Ces informations nous permettront également d'avoir un aperçu sur les positions publiques des acteurs importants de cet espace sur le sujet. Par l'analyse de ces informations, nous serons en mesure de voir l'évolution de leurs positions et les impacts de telles visions pour cette recherche. Ces sources de première main nous serviront à mieux comprendre et démontrer si des changements perceptibles quelconques ont eu lieu au sein de cet environnement suite à l'entrée en vigueur du règlement général de protection des données en 2018.

Dans un second temps, nous aurons recours à l'observation documentaire des comportements des acteurs. Cette méthode nous permettra une analyse en profondeur qui sera en mesure d'expliquer certains comportements et gestes non-dits des acteurs et donc d'avoir accès à des informations complémentaires importantes permettant ainsi de mieux comprendre le « monde vécu [du] monde

perçu » (Grondin, 2010). Ces observations nous aideront à compléter la documentation déjà établie sur le sujet afin de bien comprendre les différentes interactions et les comportements des acteurs face à l'adoption de nouvelles réglementations dans le domaine des données. Nous aurons ainsi une meilleure image des transformations de cet espace à travers les dernières années.

La pluralité de sources d'informations sera bénéfique afin de mieux recenser l'évolution de l'utilisation des données personnelles en Europe, comprendre les impacts des changements au sein de cet espace et répertorier les conséquences sur les géants du Web de l'adoption de nouvelles politiques et de mesures de contrôle (Fines, 2010). Une analyse basée en partie sur l'observation des comportements des différents acteurs nous aidera à comprendre comment ceux-ci interagissent entre eux et les impacts de ces interactions. L'observation des actions et non-actions des différents acteurs permettra de capter de l'information non écrite qui peut nous en dire tout autant sur la position des acteurs par rapport aux différents enjeux. Cela nous permettra également de voir comment les différentes pratiques commerciales et politiques sur les données s'articulent à travers cet espace. L'évaluation des sources pour l'opérationnalisation du cadre théorique portera sur les critères suivants :

- Quel est le contexte entourant cette source de données ?
- Quel est l'impact de cette information sur le sujet de recherche ?
- Est-ce que cette source touche un des concepts clés de la recherche ?

Il peut y avoir une importance significative à travers les messages et les paroles des représentants de ces grandes compagnies qui définissent les positions de celles-ci. Les théories en sécurité estiment qu'il est important d'analyser ces prises de paroles afin de mieux comprendre les intentions et les actions qui se produisent en parallèle de celles-ci. De pouvoir comprendre le but du message sera de nous permettre de comprendre les moyens décrits ou utilisés afin d'y parvenir. (Waever, 2011)

La seconde méthode de collecte de données s'effectuera par l'analyse de documents textuels. Cette littérature offrira une expertise sur différents aspects dans le domaine, dont celui des données de masse, celui des grandes sociétés du Web, des politiques en lien avec internet et les grandes industries, puis de la sécurité, et nous permettra de tracer des liens entre ces champs d'expertise.

Ces documents proviendront de bases de données, de livres provenant de bibliothèques, de livres électroniques, d'articles scientifiques, de lois et puis d'articles de journaux. Ces éléments proviendront de sources variées afin d'atténuer les possibles biais que pourraient avoir certains auteurs, revues ou autres sur le sujet. En ce qui concerne les articles de journaux, ceux-ci seront utilisés afin de représenter les positions de certaines entreprises du Web en tenant compte de la période et du contexte dans lequel ces articles ont été rédigés. Les sources issues de l'actualité seront en mesure de nous communiquer de l'information supplémentaire qui n'est pas toujours repérable ailleurs (Fines, 2010). À travers les différentes sources de données, les thèmes suivants seront analysés :

- L'influence des grandes compagnies qui possèdent et gèrent la majorité des données Web
- L'impact du système politique et économique de l'Union européenne sur l'enjeu des données
- Les effets des lois visant à réguler les activités liées à l'utilisation des données personnelles
- Les conséquences des politiques en matière de distribution et d'accessibilité aux données individuelles et privées sur les différents acteurs
- L'impact qu'ont les grandes entreprises, comme les GAFAM(s), sur l'UE par l'analyse du comportement de ces derniers et l'analyse de leur prise de position sur la place publique

Les thèmes et le cadre d'analyse choisis offriront l'opportunité de voir les effets des changements politiques sur les données dans une perspective locale. Nous serons aussi en mesure de voir dans quelle mesure l'UE est impactée par les changements notamment dans le secteur économique et voir si ces changements ont un impact sur la gouvernance du regroupement d'États. Dans le but de comprendre l'évolution de la situation, il est essentiel de tenir compte des idéaux qui ont historiquement structuré le développement de cet espace qu'est le Web (Letellier, 2017).

Ensuite, il semble essentiel de traité d'un certain désaccord, d'un manque théorique ou d'un manque d'éclaircissements dans le champ d'analyse, qui concerne à savoir dans quelles conditions politiques les théories de sécurisation s'opèrent et que doit-on considérer comme un élément de sécurisation (Balzacq, 2016). Certains justifient l'utilisation de cette méthode d'analyse lorsque la prise de décision ou la situation sort du cadre « normal des politiques » (Balzacq, 2016; Collins,

2019; Grondin, 2010), alors que d'autres ne considèrent pas ce facteur comme étant essentiel à de telles situations.

> « Bendrath, Eriksson and Giacomello seek to go beyond securitization theory by incorporating into their analysis three factors, namely, frame characteristics, framing actors and contextual conditions. They observe that, despite numerous securitizing moves during the 1990s, there were very few calls for extraordinary measures until the arrival of the Bush administration in 2001. » (Balzacq, 2016)

Dans le cadre de cette recherche, nous considérons que l'introduction du Règlement général sur la protection des données présente bel et bien ce caractère extraordinaire mis de l'avant par les théories de sécurisation. Ce caractère exceptionnel ne réside pas à travers des mesures prises qui sortiraient de l'ordinaire, mais plutôt dans le contexte, les acteurs et les caractéristiques qui animent l'adoption et la mise en place de ce document de loi politique. De la même manière, la primordialité du facteur militaire dans la sécurisation, avancée par plusieurs sous-catégories du champ théorique, est aussi un aspect requérant plus de nuances comme le mentionne Buzan : « but a way of structuring the relations of international security in much more sophisticated, large-scale and complex ways than suggested by a mere logic of individual unit survival. » (Buzan, 2009) Nous tiendrons compte de ces éléments lors de notre analyse.

CHAPITRE 2
AU CENTRE DU CYBERESPACE, L'UNIVERS DES DONNÉES DE MASSE

L'internet est dans tout ce qui nous entoure et tout ce qui nous entoure est dans internet. Directement ou indirectement, chacune de nos activités, gestes, comportements sont influencés par les données de masse. Que ce soit pour calculer les trajets empruntés par les camions qui ont livré les avocats que l'on vient d'acheter à notre supermarché, provenant de l'autre bout de la planète, ou encore pour calculer si nous sommes éligibles à recevoir un prêt par la banque afin de financer une nouvelle voiture, ou bien dans le but de nous suggérer du contenu et des produits, l'utilité de

ces informations semble infinie. Ces données de masse sont l'élément qui a permis au cyberespace ce développement exponentiel au cours des vingt dernières années en monétisant nos gestes du quotidien.

Dans ce chapitre, il sera question de la place du cyberespace dans nos vies quotidiennes et de l'évolution de celui-ci dans nos interactions avec le monde. Ce monde qui est dirigé par les données que nous produisons collectivement et qui sont utilisées à travers de multiples domaines d'expertises. Nous discuterons par la suite du monde dans lequel cette utilisation des données a évolué. Le capitalisme des données cherche avant tout à exploiter les informations disponibles afin d'en tirer profit en prédisant nos futures actions (Andrew, 2019). Dans un monde où les gains financiers sont des éléments clés aux activités de nos sociétés, le contrôle de ces données attribue une puissance quasi inégalée (West, 2019). Cette puissance de ces sociétés technologiques est directement accrue des quantités sans précédent d'informations accumulées (Zuboff, 2019). Directement liés au marché des données et aux intérêts financiers, nous parlerons de l'importance des données pour nos sociétés et principalement des individus. Il sera question de mettre en lumière les pratiques commerciales qui sont actuellement utilisées afin d'influencer nos quotidiens et comment les méthodes d'analyses choisies par les entreprises du Web nous touchent directement. Nous terminerons sur un sujet qui a longuement été ignoré à travers cet écosystème, celui de la responsabilité des entreprises utilisant ce modèle commercial basé sur l'utilisation des données de masse. La prise de conscience collective induite par l'adoption et l'entrée en vigueur du GDPR a contribué à une volonté à rendre les entreprises plus respectueuses envers les individus dans leurs utilisations des données personnelles.

2.1 La place du cyberespace dans nos vies

Nos sociétés ne font désormais qu'un avec le Web et les technologies associés à cet espace qui est central à nos activités quotidiennes. Ces technologies permettent aux sociétés une optimisation extraordinaire de nos activités en réduisant les barrières d'accès à l'information. Ces

informations, connectant ainsi les individus à travers le monde et permettent aux États d'accroître leurs modèles de gestion à travers l'ensemble des secteurs d'activités. Ces données représentent un élément clé pour l'économie mondiale, mais suscitent bon nombre d'inquiétudes à plusieurs niveaux. À travers la présente situation, les éléments qui définissent l'Union européenne comme les valeurs communes et l'identité du groupe d'États représentent des éléments importants qui dictent les comportements et choix de cet acteur. Les principes des droits et des libertés des citoyens et des individus sont cruciaux lorsqu'il est question des valeurs communes. En ce qui concerne l'identité des États membres, nous devons prendre en considération ce qui anime la société, notamment les aspects sociaux et économiques. Présentement, l'utilisation des informations recueillies au sein de cet espace entraine plusieurs inquiétudes pour les acteurs qui sont sujets aux pratiques discutables s'opérant quotidiennement à travers celui-ci. Les idéaux historiques qui structurent le Web, c'est-à-dire l'aspect social du Web, ont grandement contribué aux défis modernes de cet espace. L'échange de nos informations contre l'accès à ces services promeut une situation où les individus ont en théorie le choix de faire affaire ou non avec ces compagnies ce qui a introduit le concept et l'angle d'analyse intéressante qui est celui du paradoxe de vie privée. Ce concept cherchant à mettre en lumière certaines contradictions entre les actions des individus avec leurs données ainsi que leurs intentions et désirs en matière de partage des données. La question est à savoir si les gens se préoccupent réellement de leur droit à la vie privée si ces derniers sont prêts à échanger ces droits pour de simples récompenses (Kokolakis, 2017). Il est alors possible de soulever plusieurs interrogations en lien avec cette question, dont celle de la place du Web dans nos vies quotidiennes, l'importance des données dans nos sociétés et le degré de liberté auxquels les individus ont droit. Rapidement, et beaucoup plus qu'auparavant, cet espace d'interconnexions avec l'extérieur semble représenter un endroit essentiel à nos vies modernes. « These are the tools of modern life. They're necessary to a career and a social life. Opting out just isn't a viable choice for most of us, most of the time; it violates what have become very real norms of contemporary life. » (Leenes, 2015). Cette interconnexion entre les individus dans un espace commun vise à favoriser les échanges, le partage de connaissances et une multitude d'activités de nos vies courantes. Le Web est rendu le moyen de prédilection pour nos échanges, nos interactions et il structure même la vie sociale, économique et amoureuse d'une grande partie de la population mondiale. L'incapacité des individus à s'émanciper de ces modèles d'affaires les empêche d'atteindre une réelle sécurité (Baruh, 2017). De plus en plus, nos vies sont régies par ces modèles

de données qui à la fois nous sont invisibles, mais qui possèdent un impact gigantesque sur nos vies. Elles nous dictent ce que nous sommes, ce qu'on désire, nos aspirations, ce qu'on consomme, et tentent de nous façonner aux désirs de leurs créateurs. Cette place centrale du Web dans nos vies fait de nous des personnes vulnérables aux entreprises à la tête de cet espace et représente une faiblesse que nous avons tous, car individuellement, il nous est impossible de faire face à chacun des secteurs utilisant nos informations[1].

> « Control requires awareness of the use of personal data and real freedom of choice. These conditions, which are essential to the protection of fundamental rights, and in particular the fundamental right to the protection of personal data, can be met through different legal solutions. These solutions should be tailored according to the given social and technological context, taking into account the lack of knowledge on the part of individuals. The complexity and obscurity of Big Data applications should therefore prompt rule-makers to consider the notion of control as not circumscribed to mere individual control. They should adopt a broader idea of control over the use of data, according to which individual control evolves in a more complex process of multiple-impact assessment of the risks related to the use of data. » (CoE, 2016)

Au sein de l'Union européenne, ce risque lié à cet écosystème et la relation entre les données et l'économie du Web ont été rapidement saisis. L'importance des valeurs, des droits et de la sécurité des individus a été promue à différents niveaux à travers la société afin de mitiger les risques liés à la trajectoire empruntée au cours du développement de cet environnement.

En Europe, c'est 92 % de la population de l'UE qui ont accès au web (Insee, 2022). Chacune de ces personnes se voit bâtir un profil personnalisé à partir des données créées et fournies selon les pages qu'elles visitent, ces profils sont ensuite entreposés dans d'immenses bases de données à travers le monde. Ces bases de données sont généralement la propriété de grandes entreprises du Web, comme Google, Amazon, Facebook (Meta), Apple, Microsoft et autres. Le quasi-monopole (Loiseau, 2017) de ces plateformes qui interconnectent des millions de pages, documents, liens et services, réussit à bâtir des modèles de prédictions de nos comportements afin de nous proposer toujours plus d'objets, de services, d'activités, de contenu, nous faire consommer davantage et modifier nos comportements (Zuboff, 2019). La vente de ces données à des entreprises tierces a

[1] Voir Annexe D

créé ce que l'on appelle le marché des données. Ces activités économiques représentent un marché de quelques centaines de milliards de dollars par année en Europe (Commission européenne, 2020).

2.2 Le capitalisme des données

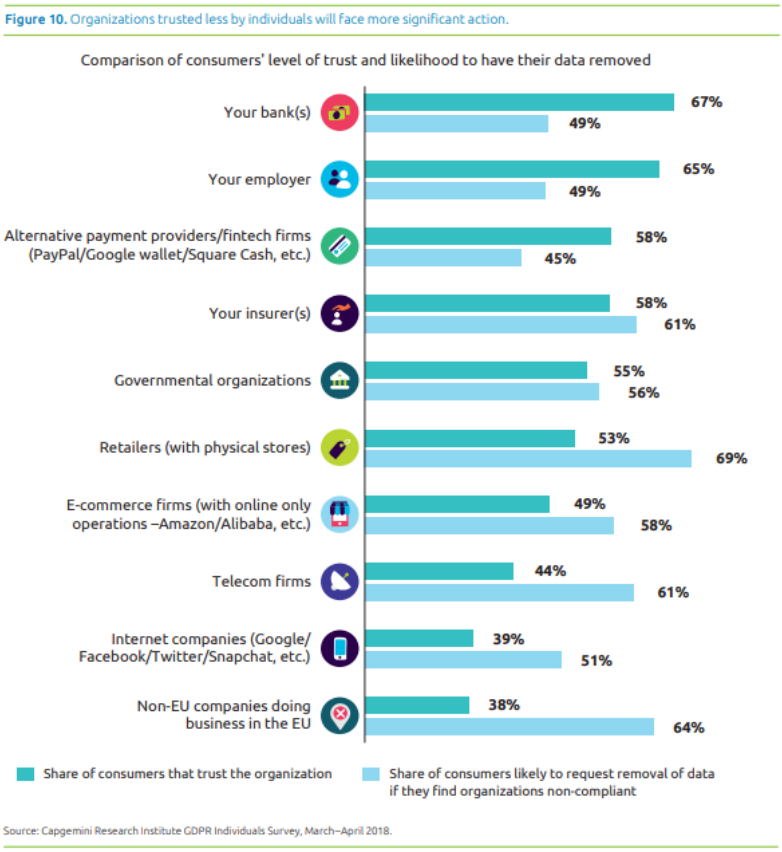
Le développement moderne du Web et des technologies liées à celui-ci repose sur une puissante vision économique dominante cherchant à extraire le plus de capital possible par l'utilisation d'informations capturées à travers la surveillance des interactions des utilisateurs produisant ainsi des données pouvant être utilisées (Letellier, 2017). Cette exploitation des informations se fait principalement par l'entremise de témoins,[2] aussi appelés « Cookies », qui sont employés dans le développement d'algorithmes de prédictions. Ces modèles servent à tisser des liens entre les comportements et les informations transmises à ces programmes, avec l'objectif d'anticiper ce qu'ils désireront et/ou influencer leurs comportements. Ensuite, ces modèles permettront, entre autres, le ciblage marketing, la vente d'informations à des entreprises tierces et la création de produits subséquents nécessitant une grande quantité d'informations afin de perfectionner ces derniers. Bien que le capitalisme des données soit souvent lié aux grandes multinationales du Web comme les GAFAM(s), qui centre principalement leurs activités commerciales à des fins de publicité et de recherche, nous retrouvons à peu près tous les secteurs d'activités de nos sociétés qui se fient et qui utilisent régulièrement les bases informations afin d'optimiser leurs opérations. C'est notamment le cas des gouvernements qui utilisent des sites tels que Facebook pour recueillir des informations sur les individus, ce qui entraîne des défis politiques

[2] « Les [témoins aussi appelés] cookies sont des paires clé-valeur strictement associées à un site web spécifique, stockées par le navigateur web d'un utilisateur final pendant une période donnée. Le navigateur web inclut les cookies dans chaque requête (ultérieure) au site web. Ainsi, en général, les cookies permettent au serveur web de conserver des informations sur l'appareil du client. » (Kretschmer, 2021)

et légaux, notamment en ce qui concerne les partenariats de transfert d'informations (European Court of Justice, 2015).

Ces données et leur utilité universelle représentent la source de la richesse des grandes entreprises de cet écosystème. La propension des plus petites entreprises et même des gouvernements à faire affaire avec ces géants vient du fait que très peu d'acteurs sont en mesure de déployer des modèles capables de recueillir, d'entreposer et de faire l'analyse d'une gigantesque quantité d'informations comme les GAFAM(s). Les modèles d'affaires de ces derniers ne sont cependant pas dénoués de tout risque. L'intrusion excessive et abusive dans la vie privée des individus génère des défis de sécurité liés pour l'ensemble des acteurs, individus, entreprises, groupes d'intérêts, personnalités publiques et gouvernements. Le fait que l'on retrouve les traqueurs[3] de Google dans près de 90 %

Figure 2.1 Les organisations auxquelles les individus font moins confiance seront confrontées à des actions plus signicatives



[3] Le terme traqueur réfère aux techniques utilisées afin d'identifier les individus sur le Web. Les cookies représentent une forme de traqueur couramment utilisée bien qu'il en existe plusieurs sortes et que ces derniers n'ont pas tous le même objectif (Kretschmer, 2021).

des applications et sites Web est un indicateur important quant au suivi en ligne (Naranjo, 2021). De plus, l'accès à ce méga laboratoire qu'est le Web, offre la possibilité aux grandes entreprises d'influencer les actions, les comportements et les pensées des individus en contrôlant le contenu diffusé sur leurs plateformes.

Le fonctionnement de ce marché des données passe par le développement d'algorithmes afin d'exploiter les informations à la disposition des entreprises. Ces algorithmes sont des programmes permettant l'analyse de l'information disponible et collectée par ces entreprises à travers le trafic internet, c'est-à-dire l'utilisation de leur site et le retour des sites ayant des liens avec ces derniers. La quantité de données produites se chiffre en zettaoctets[4] (Gaudiaut, 2021). La collecte de données se chiffre quant à elle en dizaine, voire en centaine de pétaoctets,[5] et ce chiffre augmente constamment. Ironiquement, il est difficile d'estimer la quantité réelle de toute l'information détenue par ces entreprises vu la nature confidentielle que représentent ces informations et la culture du secret entourant celles-ci. « Despite the apparent value they place on transparency, the processes and mechanisms through which companies like Google and Facebook enact their business objectives are closely guarded as their most prized trade secrets. » (West, 2019). Ces modèles de données très souvent opaques et qui appartiennent à des entreprises privées font de ces derniers des enjeux majeurs à différents niveaux pour les sociétés. Les conséquences que peuvent provoquer des modèles mal ajustés ou ajustés dans une optique précise sans tenir compte des répercussions pour les individus sont responsables de l'agrandissement des iniquités entre les individus et particulièrement les classes marginalisées. Au sein d'un système politique et économique tournant autour de cette technologie, les algorithmes de destruction massive, comme les appelle Cathy O'Neil (2016), imposent les conséquences des préjugés, des probabilités et des objectifs découlant de la programmation de ces outils d'analyse aux individus qui se retrouvent alors pris à devoir faire avec ces injustices. « Les ADM tendent en revanche à favoriser l'efficacité [à l'équité]. Elles se nourrissent, par nature de données qui peuvent être mesurées et comptabilisées. Mais l'équité est difficile à appréhender et à quantifier. C'est un concept. » (O'Neil, 2016). Cette forte propension à choisir l'option simple et qui est économiquement plus rentable contribue à la

[4] Un zettaoctet est égal à 10^{21} octets.

[5] Un pétaoctet est égal à 10^{15} (1 000 000 000 000 000) octets d'informations stockées et enregistré dans une base de données. Selon la base de données SOLEIL, qui a atteint ce chiffre en 2018, cela représentait approximativement l'équivalent à deux cents millions de fichiers d'informations.

vision négative que nous avons des pratiques faites par ces entreprises avec nos informations. Il y a cependant aussi de bons algorithmes et des compagnies qui utilisent aussi les données de masse, mais de façon responsable. Il serait injuste de penser que les monopoles de cet espace comme Google, Microsoft, Apple et autre ne produisent aucun bénéfice pour la collectivité. Ces derniers participent aussi positivement au développement de technologies permettant une foule d'avancée dans nos sociétés. Il y a beaucoup de zones grises et d'incertitude à travers cet espace, mais une chose est certaine, c'est que les dangers que peuvent poser les algorithmes pour la population ne font aucun doute (O'Neil, 2016). Intrinsèquement, ces modèles de prédiction ne sont donc pas nécessairement mauvais, car après tout ce sont simplement des programmes créer par des humains et donc ultimement ces modèles obéissent aux commandes. Le problème provient plutôt du modèle économique antidémocratique selon Zuboff (2019), où émerge l'origine de ces algorithmes de prédiction et dans la manière dont ces machines sont programmées. Intentionnellement ou non, la modélisation des algorithmes est grandement influencée par l'environnement d'apprentissage et les éléments auxquels ceux-ci sont exposés. Lorsque l'on additionne cela à la capacité d'apprentissage et de rétroaction de ces programmes, la possibilité pour algorithmes de devenir mauvais et d'avoir un impact immense sur la vie de millions de personnes sans même les connaître est réelle et inquiétante (O'Neil, 2016).

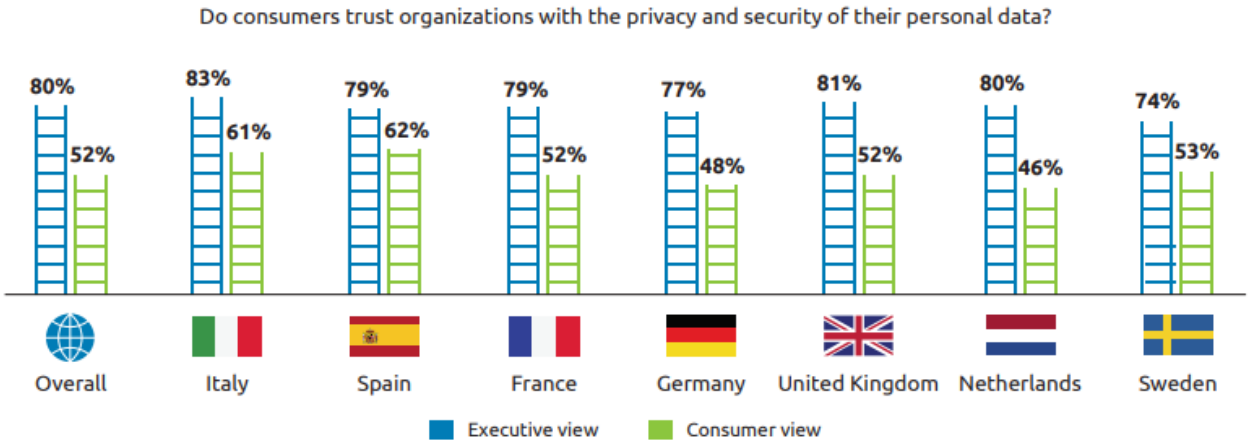
Un autre élément contribuant au problème précédemment mentionné est que l'économie des données est rendue un environnement tellement rapide que les politiques ne sont pas en mesure d'aller aussi rapidement et suivre le rythme de développement de ce dernier crée ainsi un décalage entre les deux mondes qui forment pourtant un tout (Ciuriak, 2018b). La nécessité pour le monde politique de s'adapter à la réalité du Web est essentielle pour faire face aux défis d'un monde interconnecté. De nos jours, chacune de nos activités est numérisée d'une certaine manière, lorsque l'on achète quelque chose, lorsque l'on souscrit à une assurance, lorsque l'on visite un endroit, etc. Ce monde interconnecté dans lequel nous vivons est gouverné par les données collectées.

2.3 L'importance des données dans notre société pour les différents acteurs

Au sein de nos sociétés, les données de masse n'ont pas une signification unique pour chacun des acteurs. Les individus, les États et les entreprises ont tous des intérêts propres à chacun et ceux-ci tentent d'utiliser le cyberespace à leur avantage tout en cherchant à éviter les inconvénients. Par conséquent, trouver des terrains d'entente sur les multiples enjeux afin de préserver une certaine harmonie serait la solution à ce défi. Au cours des deux dernières décennies, ce n'est pas ce qui a pu être constaté dans les positions des différents camps. L'entêtement des entreprises dominantes à imposer leur force avec leur armée d'experts juridiques et de lobbyistes (Grosbois, 2018) et à l'aide de différents moyens à leur disposition, le tout dans l'objectif de poursuivre leurs activités commerciales. Cette attitude s'est particulièrement fait ressentir à travers leurs comportements envers certains enjeux clés médiatisés (Anonyme, 2022a; Lapienyté, 2021c; Grim, 2021).

Pour les individus, les données représentent un enjeu important à plusieurs niveaux qui sont uniques à ces derniers et qui font des données un sujet d'intérêt et de conflit avec les entreprises concernant le respect des lois en place (Manancourt, 2021). La relation complexe entre les deux groupes où l'un et l'autre ont besoin de cette collaboration, dans un cas, pour avoir accès à des services qui sont rendus de base et de l'autre côté pour d'extirper cette « matière première » du Web dans le but de continuer à fournir des services largement gratuits à travers le monde crée un environnement d'interdépendance (Loiseau, 2017). Pendant longtemps et encore de nos jours dans une certaine mesure, les individus se retrouvent à devoir accepter les conditions d'utilisation en place sans avoir leur mot à dire ou presque (Zuboff, 2019) et le tout dans un environnement très

Figure 2.2 Surestimation de la confiance des consommateurs par les organisations



opaque quant aux opérations découlant des pratiques de ces organisations du Web. Cette situation a grandement contribué au développement d'un climat de confiance très faible envers la sécurité

de leurs informations et le respect de leur droit à la vie privée envers ceux qui contrôlent leur identité en ligne.

Source : De Paepe, W. et al. (2018). « Seizing the GDPR advantage: From mandate to high-value opportunity », Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf

Cette analyse nous offre une perspective intéressante sur l'état de la situation concernant les visions des acteurs au sein de cet espace. De plus, nous sommes aussi en mesure de constater l'existence d'un fort biais d'approbation de la part des entreprises quant à leurs activités commerciales menant à une surestimation élevée, avec une moyenne de 28 % d'écart, dans la confiance que leur attribuent les individus concernant la gestion de leurs informations et leur sécurité. Cette divergence entre les deux perspectives nous permet d'avoir un aperçu de la nécessité d'une position nationale plus claire et qui encadre mieux les comportements d'usage des données de masse. L'intérêt des individus envers les données réside dans l'utilisation faite de leurs informations. Le besoin d'avoir un sentiment de sécurité de leur personne sur le Web et par extension dans le monde matériel génère des inquiétudes pour ce groupe. La création de profils uniques avec parfois leurs informations

Figure 2.3 Classification de sensibilité des données par les individus

sensibles à travers des bases de données, rend les individus vulnérables aux acteurs malveillants qui désireraient profiter des nombreuses failles de sécurité au sein d'entreprises et compromettre l'intégrité de ces personnes. L'accroissement de telles situations à travers le monde et le manque flagrant de vigilance de la part d'entreprises ayant en leur possession les informations confidentielles de citoyens n'aident en rien la peur d'être victime d'acteur malveillant.

Source : De Paepe, W. et al. (2018). « Seizing the GDPR advantage: From mandate to high-value opportunity », Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf

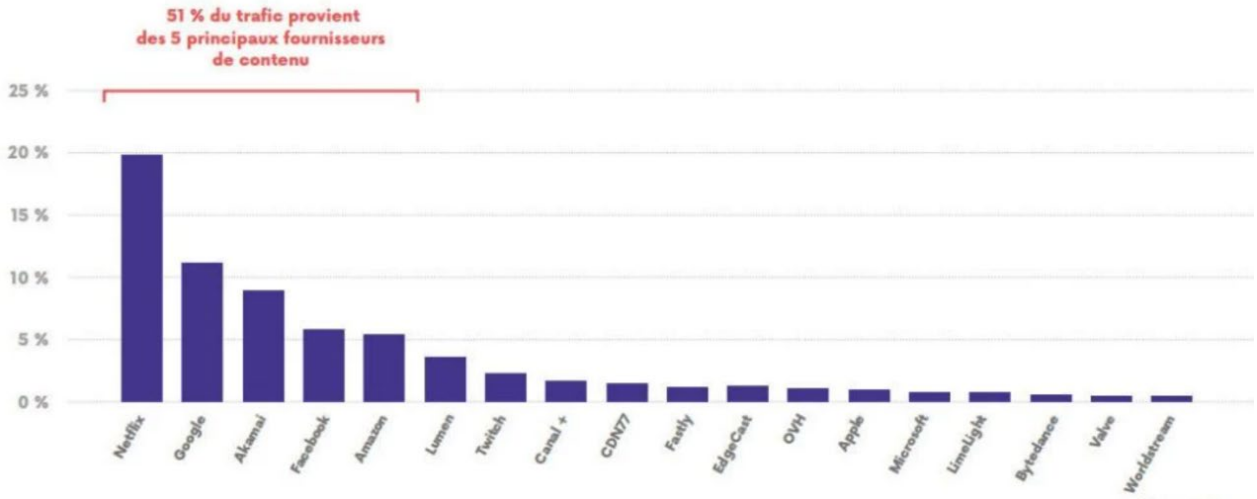
En regard au tableau ci-dessus, nous notons que les informations sensibles, comme les détails d'identification, les liens de contacts et les informations liées aux finances représentent des sources de préoccupation pour les individus et sont des champs où les individus seraient tentés de faire appliquer leurs droits, comme celui à l'oubli, en vertu des obligations des entreprises soumises au GDPR. De plus, l'utilisation d'informations sensibles dans la modélisation d'algorithmes peut entraîner des conséquences pour les individus où ultimement ceux-ci peuvent devenir victimes de prédictions des modèles créés par les compagnies et n'auront pas nécessairement les mêmes opportunités que d'autres personnes dues à certains facteurs parfois hors de leur contrôle (O'Neil, 2016). Il semble difficile d'ignorer l'ensemble des abus en matière de données perpétrées par les entreprises du Web (Barthelemy, 2020; Lapienyté, 2021a; CNIL, 2022; Reuters, 2022; Stokel-

Walker, 2022). Les comportements problématiques répétés n'aident en rien la création d'un lien de confiance et de l'instauration d'un potentiel sentiment de sécurité pour les individus.

Dans le cas des États membres de l'Union européenne, leurs intérêts pour le marché des données se centrent sur deux points centraux. Il y a d'abord, le respect des droits des citoyens et ensuite l'aspect de la gouvernance de cet espace. L'UE a comme mandat de faire appliquer les lois et garantir les droits acquis aux citoyens des États membres contre les abus de tout genre. L'utilisation abusive des données faite par les entreprises nécessite une réaction appropriée afin de rétablir la situation à un état normal. La gouvernance de cet écosystème est le deuxième point d'importance pour l'UE. Depuis trop longtemps, les compagnies du Web ont profité de la faible règlementation afin de dominer les acteurs plus faibles et imposer leurs visions aux autres. L'impact de tels comportements a fait en sorte de ternir l'image de la puissance absolue des États sur la gouvernance de leurs propriétés et leur territoire. Ainsi, l'adoption de nouvelles lois en matière de données permet à l'UE de contrôler ces entreprises utilisant les données de masse afin que celles-ci soient tenues responsables de leurs actions lorsqu'elles empiètent sur les droits des autres acteurs. Cette reprise de contrôle passe par l'application d'obligations afin de contrôler les activités commerciales en matière de données et par l'imposition de contraventions en cas de manquements au code de conduite. Un autre point d'intérêt pour l'UE en matière de contrôle des données est qu'actuellement les données extraites à travers le Web proviennent d'entreprises américaines (Samarasinghe, 2019). Cette concentration provenant d'un seul État étranger, bien qu'allié, est en mesure de causer des inquiétudes de niveau de sécurité. Ces inquiétudes d'une ingérence étrangère ne sont pas infondées, les révélations de surveillance du gouvernement américain par Edward Snowden en 2013 témoignent de cette réalité.

Dernièrement, les entreprises du Web sont grandement dépendantes de l'utilisation des données de masse pour leurs activités et leur modèle économique. L'utilisation massive des plateformes Web et des applications, dont les réseaux sociaux, les jeux vidéo, les applications de messagerie et la consommation de contenu médiatique provenant des principaux géants fournisseurs de contenu leur confèrent un pouvoir d'information immense et des revenus faramineux. De plus, l'impact de l'entrée dans le marché de nouveaux compétiteurs est quasi nul dû à l'impossibilité de compétitionner avec ces derniers. Afin de mettre en perspective la quantité massive de données que ces entreprises ont traitées et ce que cela représente pour eux, vers la fin de l'année 2014, c'était près de 40 % du trafic nord-américain par cellulaire qui était attribué à Facebook (Meta) et YouTube appartenant à Alphabet (Google) (Grosbois, 2018). Vers la fin de l'année 2021, en France, c'était plus de 50 % du trafic internet qui passait par cinq entreprises : Netflix, Google, Akamai, Facebook et Amazon (Manceau, 2022).

Figure 2.4 Décomposition selon l'origine du trafic vers les clients des principaux FAI en France



Source : Manceau, G. (2022). « Rapport d'activité : L'état d'internet en France », Tome 3, République française, Édition 2022. https://www.01net.com/actualites/netflix-occupe-une-part-hallucinante-du-trafic-internet-en-france.html.

Cette petite quantité d'entreprises qui fournissent la majorité du contenu aux utilisateurs du Web comme Netflix, Google, Facebook et Amazon domine le marché mondial du trafic à travers internet et donc possède un fort contrôle des données transigeant sur le Net. Cette montée en puissance

dominante d'entreprises comme Google [6] est due à leur modèle d'affaires précurseur, leur popularité et leur type d'activités commerciales. Ces conditions permettent aux entreprises des données de maintenir cette position de force (Waever, 2011). L'intérêt de ces derniers à avoir le moins d'obligations envers les autres acteurs leur permet de perpétuer leurs activités et leur réussite économique. De plus, l'offre de service incontournable par ces entreprises nécessite d'être financée d'une certaine façon. Les coûts associés au déploiement d'une force technologique pareille sont énormes.

2.4 Responsabilités et éthique liées au secteur des données privées

Il ne fait aucun doute que les entreprises du Web doivent prendre plus de responsabilités afin de protéger les individus des risques associés aux pratiques commerciales dont ces entreprises profitent. Il y a un besoin de trouver un point d'équilibre entre de saines pratiques d'utilisation des données par celles-ci permettant le respect des droits acquis des individus et un écosystème du Web étant en mesure de continuer de fleurir. La question se pose alors à savoir où se trouve ce point d'équilibre. Il importe aussi de se poser la question à savoir si ce modèle d'affaire d'utilisation des données est une pratique incompatible avec les désirs et besoins des deux autres acteurs. En explorant les possibilités, nous serons en meilleure posture pour y répondre.

L'accent sur les pratiques entourant les données offre un point de départ intéressant afin d'atteindre cet objectif. La nécessité de créer des produits qui prennent en compte la vie privée des individus dès la conception des produits (Custers, 2017) est un aspect important pour l'évolution de cet espace vers quelque chose de plus inclusif. Ce mode de fonctionnement permet le développement de techniques d'analyse respectueuse des besoins des individus tout en permettant la continuation des activités. Prenant cela en considération, il est important de noter qu'il n'y a probablement pas d'algorithmes qui soient parfaits, car ceux-ci reposent sur des choix. Cependant, il en existe des meilleurs que d'autres et cette différenciation entre les deux types passe par l'adoption de saines

[6] Voir Annexe B

pratiques de gestion des algorithmes (O'Neil, 2016). Un bon modèle d'algorithme nécessite une réévaluation constante afin d'évaluer la performance, l'atteinte des objectifs et de détecter les failles possiblement présentes.

Ensuite, si l'on analyse des positions défensives des entreprises et de leurs réactions concernant les changements dans le secteur économique, des données peuvent être perçues comme une réaction plus que normale pour ces géants du Web considérant que ce changement drastique dans une aussi grande industrie entraîne des variables inconnues. Cette position de statu quo requiert aussi moins d'efforts et cause moins de dérangement pour ces entreprises. Dans l'analyse des comportements de ces entreprises, il semble important de mettre en perspective une critique des analyses en sécurité : « As Huysmans (2002) pointed out long ago in a famous article on the 'normative dilemma of writing security', all security studies risks strengthening security, even when intentionally anti-security (see Wæver, 1999). » (Waever, 2011). La nécessité de prendre du recul et de regarder les impacts des politiques déjà en place sur l'environnement des données peut nous aider à éviter une interprétation erronée de la situation. Les conséquences du GDPR sur les entreprises du Web sont nombreuses. La nécessité pour celles-ci de revoir leurs opérations et de mettre à jour avec la nouvelle règlementation entraîne un fardeau financier et logistique pour celles-ci. Aussi, les plus grandes entreprises qui sont plus strictement surveillées dans leurs comportements et donc leurs responsabilités sont très élevées. Les plus petites entreprises quant à elles doivent dans leurs cas faire affaire avec les coûts des démarches de mise à jour qui représentent une difficulté de plus à survivre dans ce marché (Zarsky, 2016). Aussi, de tenir pour acquis que l'ensemble des entreprises ne désire pas contribuer aux changements des pratiques ne serait pas juste. Plusieurs initiatives de petites et grandes entreprises se sont développées afin de rendre cet espace plus éthique notamment par l'emploi de nouvelles techniques et une offre d'options plus grande en matière de contrôle de la vie privée (Li, 2019; Ketchum, 2022; Walker, 2022; Dillet, 2022; Romain, 2022; Anonyme, 2022b). De l'autre côté, sans l'imposition d'obligations et de limites par l'Union européenne envers les compagnies utilisant les données, il est difficile de croire que ces compagnies développeraient volontairement des produits qui pourraient nuire à leurs activités et/ou leur dominance à travers ce marché alors que leurs modèles d'affaire ultra lucratifs fonctionnaient déjà très bien. Il est évident que cette évolution technologique vers des techniques moins invasives et plus respectueuses des individus s'en

trouverait sans aucun doute ralentie dans leurs développements. Les bénéfices de continuer de promouvoir le développement de techniques respectueuses par une application stricte des politiques du GDPR dans le but de modifier les comportements des entreprises de cet espace sont selon moi démontrés. En terminant, il ne fait aucun doute à mes yeux qu'il y a possibilité de trouver une harmonie entre les principaux intéressés de cet enjeu. Près de 5 ans depuis l'entrée en vigueur du GDPR, il est forcé de constater que l'écosystème des données est toujours en place et prospère. Les activités des entreprises utilisant les données des utilisateurs à travers l'Union européenne ont développé des moyens afin de s'ajuster, pour ce faire, ils ont adapté dans une certaine mesure, leurs méthodes de fonctionnement relatives à l'obtention des informations des utilisateurs.

CHAPITRE 3
LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES POUR RÉDUIRE LES ABUS LIÉS À L'UTILISATION DES DONNÉES DE MASSE

Dans ce chapitre, nous parlerons de l'écosystème des données avant et après le règlement de 2016, qui est entré en vigueur en 2018, sur les données Web au sein de l'Union européenne. Nous aborderons aussi les changements introduits par cette récente loi et les impacts des nombreux articles sur les différents acteurs. L'adoption du règlement général de protection des données en Europe basé sur des idéaux de sécurité et de contrôle des activités commerciales des entreprises des données ainsi que les lois inspirant ce texte ont permis, depuis 2018, à l'UE de mettre en place des balises sur les comportements acceptables de ceux qui ne le sont pas avec les informations recueillies par les entreprises. Les 11 chapitres, 99 articles et 173 récitals de ce document, ainsi que les nombreux défis soulignés, établissent un portrait des objectifs, des principes, des droits, des méthodes de fonctionnement, des modèles de contrôle, des pénalités en cas de non-respect aux règlements et des spécificités relatives au milieu.

En faisant l'analyse de la stratégie de l'Union européenne en matière de sécurité des données, il est important de noter que celle-ci se base sur plusieurs aspects qui sont propres à leurs intérêts en tant qu'union d'États ayant une vision commune de cet espace. Il existe plusieurs facteurs qui entrent en ligne de compte dans la prise de décision lors de l'adoption du GDPR par ces derniers. Il y a d'abord les intérêts des États à limiter les abus d'utilisation des données des citoyens par les entreprises locales et principalement étrangères, la prise en considération des besoins des États et de leurs constituants afin de rendre ce milieu mieux adapté aux nouvelles réalités, la prise en considération des précédents en matière de réglementation et de comportements des acteurs impliqués, la nécessité de prendre en compte les obligations des institutions européennes envers les différents groupes, la perception de la situation de l'UE (Lewis, 2014). La prise en considération de ces facteurs, additionnés aux données relatives à l'analyse de la situation pré et post-GDPR, nous aiderons à faire l'état de la situation et comprendre l'évolution du milieu de données de masse au sein de l'Union européenne.

3.1 Analyse de la situation pré-GDPR : politiques, abus et écosystème Web

Bien longtemps avant l'introduction du GDPR, plusieurs décisions prises par les pays membres ont contribué à la mise en place de cette réglementation majeure dans cet espace. L'UE étant un véritable pionnier dans le développement de réglementation afin de baliser les actions autorisées à travers ce secteur émergeant. L'adoption de la directive 95/46/EC sur la protection des données en 1995 a mis de l'avant la nécessité de devoir faire attention à l'utilisation faite par les entreprises de ces informations. Cette directive mise en place afin de contrôler l'évolution rapide des pratiques commerciales à travers le Web a été bonifiée peu après avec l'adoption d'un second texte majeur pour les citoyens. La charte des droits fondamentaux de l'Union européenne proclamée en 2000, une des références importantes pour la protection des individus, qui souligne la nécessité du respect à la vie privée et de la protection des données (CDFUE, 2000). Ces deux documents officiels ont en quelque sorte pavé la voie du développement futur de cet espace et du positionnement du regroupement d'États envers les pratiques problématiques des entreprises abusant des données de leurs citoyens.

Malgré la limpidité de ces documents dans leur but et une vision sociale forte des droits individuels, le faible respect des directives dans le milieu des données, par les entreprises, a permis à celles-ci, utilisant ces informations de façon massive, d'abuser de leur position de force envers les utilisateurs afin de pousser leur modèle d'affaires à l'extrême et ainsi engendrer toujours plus de profit au détriment de ces derniers. L'évolution des pratiques de transferts internationales des données où les standards de sécurité, de contrôle et d'utilisation de ces informations ne sont pas équivalents partout accentue le problème de respect des valeurs et des droits des individus. Les pratiques commerciales sont demeurées très vagues et difficilement contrôlables tout en engendrant beaucoup de risques pour l'Union européenne ainsi que leurs citoyens. L'apparition de courtiers des données facilitant une transmission fulgurante et incontrôlable des données personnelles publiques et privées des Européens contribuait également au développement de cette situation négative aux yeux du groupe d'États. Les comportements négligent de grandes entreprises, générant une grande partie du trafic Web envers les individus contribuant à amplifier les effets négatifs subis par ces derniers qui souhaitaient utiliser des services Web quasi incontournables.

L'utilisation abondante à travers la littérature sur l'enjeu de l'image d'un affrontement inégal, de David contre Goliath, afin de dépeindre la situation dans laquelle les citoyens se retrouvent décrit bien la situation post-GDPR. Le pistage perpétuel des individus à travers leurs interactions soulevait bien des interrogations quant au respect réel des droits de ces derniers. Actuellement, les applications peuvent même collecter nos données lorsque nous ne les utilisons pas et elles sont simplement installées sur nos objets qui sont connectés au Web (Hantouche, 2016). Ces abus et pratiques discutables ont contribué à la publication de multiples textes d'opinions, de recommandations par des groupes de travail et la formation de conseils afin de mettre de l'avant l'enjeu des données et de trouver des solutions aux différents problèmes pour ensuite déboucher par le développement du GDPR[7].

Une réception mitigée face au règlement a fait couler amplement d'encre à savoir si ce dernier était le moyen idéal et si les mesures en place n'étaient pas trop contraignantes pour les entreprises œuvrant dans le milieu. Le camp opposé à la nouvelle réglementation sur les données qui cherchent à faire annuler le projet de loi tente de dépeindre l'Europe comme une entité qui traîne la patte dans une course au développement technologique propulsé par des modèles d'analyses basés sur les données. Pour eux, cet argument qu'il y a un besoin d'accroissement de la réglementation, de la sécurité et des droits représente une excuse afin de reprendre du terrain sur les entreprises étrangères (Zarsky, 2016). De hauts dirigeants et anciens hauts placés de grande société des données, comme Andreas Weigend chez Amazon, ont clairement exprimé par le passé ne voir aucun problème au modèle de fonctionnement de l'utilisation des modèles de données avant l'entrée en vigueur du GDPR. Ces déclarations d'individus haut placés au sein de géants de l'écosystème des données ont clairement exprimé la position de ces entreprises vis-à-vis le domaine de la vie privée et de l'utilisation des modèles de données et de leur vision anti-GDPR. À leurs yeux, un monde dans lequel les entreprises étaient en mesure d'utiliser et dicter le mode de fonctionnement de l'utilisation des données des internautes était plutôt une opportunité pour tous de pouvoir accomplir davantage grâce aux modèles de collecte déjà en place. Et ainsi développer la recherche au profit de la surveillance des individus (O'Neil, 2017). Cette vision dualiste entre l'utilisation des informations personnelles des gens au profit de la science et l'économie versus le besoin de mieux baliser les comportements des entreprises à travers le Web au profit de la sécurité

[7] Voir Annexe A

et le respect des droits définit bien le débat mis de l'avant par les deux camps principaux. Une analyse de Zarsky publiée peu après l'adoption du GDPR laisse sous-entendre que l'essence du texte de loi vise uniquement la protection des individus et des groupes face aux pratiques commerciales dans un monde digital et que le document oublie de prendre en compte les conséquences de tels changements pour les entreprises opérant avec les données (Zarsky, 2016). Cette vision partagée par certains chercheurs et beaucoup d'entreprises tente de représenter l'adoption du GDPR comme étant l'acte de mort du marché des données, et ce malgré les accommodements, comme le récital 15 sur la neutralité technologie sur le moyen adopté afin de devenir conforme à la nouvelle loi, et l'article 99 concernant le délai d'entrée en vigueur de deux ans après l'adoption du GDPR, inscrit dans le texte de loi.

Le côté en faveur de l'entrée en vigueur du règlement général sur la protection des données au sein de l'Union européenne est présenté comme étant une manière d'harmoniser les pratiques commerciales aux droits et aux besoins de sécurité et liberté des citoyens. On parle aussi d'une possibilité d'accroître la confiance et la transparence entre les utilisateurs et cette industrie pouvant mener à une situation bénéfique pour tous, ce qui fut loin de convaincre l'industrie. Le mode de fonctionnement de l'utilisation des données pré-GDPR sans contrainte et sans mesure contrôle rigoureusement appliquées contribuait grandement à accroître les inégalités entre les individus. Les classes défavorisées se retrouvent grandement plus touchées par les impacts négatifs de l'utilisation des données de masses et de la surveillance Web. Ces derniers ayant un moins grand contrôle sur leur environnement social, économique et légal se retrouvent donc victimes d'une discrimination sociale encore plus forte (Madden, 2017; Baruh, 2017). Cette situation est due, entre autres, au mode de fonctionnement du monde des données de masse. Lors de l'utilisation de ces informations sur les individus le volume, la variété et la rapidité (Soria-Comas, 2016) se trouvent être un trio clé à la production d'algorithmes, de modèles et de bases de données pouvant être le plus utile aux compagnies œuvrant dans ce secteur. D'autres pratiques dans le domaine comme lorsque les données sont réutilisées à d'autres fins que ceux pour lesquels ils ont été collectés ou encore lorsqu'elles sont prises hors contexte, la création de bases de données de faible qualité impacte grandement le potentiel de recherche valide (Wigan, 2013). Ces trois facteurs dans le mode d'obtention des données additionné à plusieurs autres pratiques douteuses contribuent à la création d'un environnement où le profit devient le seul objectif pour beaucoup trop d'entreprises opérantes

avec les données de masse. L'absence du facteur qualité à travers les pratiques de beaucoup de ces entreprises au sein de l'UE avant l'année 2018 participait à la dégradation de cet écosystème et à l'empiètement sur les droits des citoyens de l'Union européenne.

L'entrée en vigueur de la pièce législative a laissé les entreprises dans un flou concernant l'avenir des pratiques commerciales en matière d'utilisation des données. Le scepticisme de certains individus envers le texte de loi et certains articles inscrits dans le document a fait croire à une incompatibilité entre ce dernier et le modèle d'affaires basé sur l'utilisation des données de masse, laissant présager une incapacité pour ceux-ci de conduire l'analyse des informations auparavant disponibles (Zarsky, 2016).

3.2 Les objectifs de la nouvelle législation face aux défis que posent les données Web

L'économie de données représente un marché très important pour plusieurs sphères de la société européenne comme partout à travers le monde. À travers l'adoption de nouvelles régulations, la nécessité de mieux réguler ce marché complexe, distinct et discordant avec les valeurs des pays membres de l'UE tout en essayant de ne pas le détruire complètement représentait un défi de taille pour cette institution supranationale. L'adoption du GDPR vient changer considérablement le marché des données en Europe et force les compagnies à revoir et à modifier leurs pratiques. Destiné à élever les standards en matière d'utilisation des données et à restituer les droits des citoyens face aux puissances du Web, ce dernier se trouve à être un document central pour la sécurité et les droits en ligne des résidents de l'Union européenne, des États membres. L'influence du document déteint aussi sur les pays partageant une vision commune avec l'UE afin de faire du Web une place plus juste pour les « Davids » de ce monde, plus sûr pour tous les individus, plus responsable dans les actions employées par les entreprises et plus coopératives entre acteurs. De faire de cet espace un modèle où les processus sont plus transparents et mieux adaptés à la réalité est essentiel. La nécessité pour l'UE d'imposer des règles plus strictes aux entreprises dans le but de faire réduire les comportements nuisibles à travers les pratiques commerciales qui

entrent en contradiction avec les valeurs des États membres, et dans le but d'atteindre les objectifs politiques et sécuritaires auxquels se souscrit ce dernier, devient la solution à privilégier.

Outre ces deux objectifs criants, le besoin pour les États membres de l'UE de restaurer leur souveraineté effacée à travers le temps par les puissantes entreprises monopolistiques du Web en reprenant le contrôle des activités se déroulant sur le territoire se fait sentir. Un tel outil législatif a pour ultime effet de rendre la balance de pouvoir entre les grandes entreprises du Web qui opèrent dans le marché des données et les individus au sein de l'UE qui utilise le Web, puis par extension les États qui se doivent d'assurer le respect de droits et libertés de leurs citoyens.

L'adoption d'une nouvelle loi afin de corriger une situation problématique n'est pas hors du commun et représente un passage souvent nécessaire afin de s'adapter aux changements dans le fonctionnement de nos sociétés. Le développement sur plusieurs années du GDPR et l'adaptation de celui-ci à l'évolution du Web ainsi qu'aux autres documents précédemment adoptés visant le contrôle des activités en lien avec les données démontre le côté significatif de celui-ci pour l'UE. Il serait possible d'argumenter que le côté réfléchi d'une telle loi qualifierait ce dernier comme n'appartenant pas au groupe de politique de sécurisation (Maciel-Hibbard, 2018). Cependant, nous soutenons le contraire dû aux trois facteurs clés précédemment énoncés au premier chapitre. Il semble essentiel de noter le côté extraordinaire de la pièce législative marquée par le fait qu'elle soit la première de ce type cherchant à moderniser un environnement qui se trouvait très peu limité politiquement dû à une multitude de facteurs économiques, politiques et sociaux. Ensuite, l'acteur choisissant d'imposer des contraintes joue un rôle essentiel dans la situation présente. Le fait qu'une puissance occidentale composée de plusieurs pays politiquement similaires et ayant des valeurs communes cherchant à réduire les impacts négatifs et incertitudes des données sur les utilisateurs du Web rend la situation unique. L'aspect de grandeur et de portée décrit comme étant crucial par Buzan (2009) est aussi présent prenant en considération l'économie liée aux pratiques commerciales des données. Puis, dans le contexte de cette situation, il semble logique de soutenir que l'objectif primaire du GDPR a pour objectif de faire bénéficier les citoyens d'une sécurité accrue tout en leur assurant un respect de leurs droits constitutionnels, représentant un aspect important de l'identité de l'Union européenne.

3.3 Les articles clés du GDPR dans la lutte aux abus

Lors des discussions sur le modèle à adopter dans l'intention de mieux répondre aux besoins des individus, la nécessité d'établir de nouveaux paramètres d'opération aux entreprises du milieu pour favoriser un environnement plus stable et sécuritaire se veut claire. À travers ces différents points abordés dans le document sur les comportements désormais encadrés par le règlement on y retrouve les éléments suivants : la mise de l'avant des droits des citoyens et la protection de ceux-ci, la nécessité de discussions ouvertes entre les partis, les responsabilités de chacun et un désir d'adopter un modèle plus durable pour cet espace sont ce qui compose l'essence du document (Soria-Comas, 2016). À travers les 11 chapitres et les 99 articles du GDPR, l'introduction de plusieurs éléments critiques dans l'optique de faire de cet espace un environnement plus juste et sécuritaire pour tous est détaillée. Nous y trouvons la portée du document, les objectifs, les principes importants, les droits des utilisateurs, les règlements spécifiques, les différents cadres et rôles importants, les conséquences pour les entités qui ne se soumettent pas aux lois, les détails importants concernant les transferts d'informations, la mise en application et les procédures. Plusieurs auteurs reprennent et développent sur l'essence de ces différents articles et explorent l'impact et l'importance de ces derniers (*GDPR*, 2018 ; Bieresborn, 2019; Leenes, 2018; Kretschmer, 2021; Soria-Comas, 2016; Degeling, 2022; Palmatier, 2019; Safari, 2017).

Parmi ces articles importants pour les citoyens, nous y retrouvons dans le chapitre 2, les principes qui sont couverts aux articles 5 à 11 qui cherchent à mettre de l'avant les comportements auxquels les entreprises devraient se souscrire afin d'en faire bénéficier le milieu des données et les individus :

- Dans le but de réduire les risques liés aux fuites de données et l'utilisation abusive des informations des individus, le GDPR cherche à faire réduire la quantité de données recueillies par les entreprises et limiter l'entreposage de ces informations au minimum nécessaire par l'introduction du principe de minimisation. Un tel principe de réduction de la portée de l'entreposage des entreprises pré-GDPR a un effet sur l'ensemble de l'écosystème des données dans la mesure où la diminution de l'accumulation des

informations stockées par les entreprises du Web contribue à un environnement plus sûr pour les utilisateurs et force à un renouvellement et une mise à jour des informations recueillies par le passé.

- Les entreprises ont le devoir de traiter que les données dont elles ont besoin, c'est-à-dire la quantité requise pour effectuer les opérations déclarées et planifiées.

- Le principe de légalité sur l'utilisation des données articulée dans l'article 6 réfère à plusieurs aspects déterminants sur les comportements acceptables, la légalité des activités en rapport à l'utilisation des données personnelles, ainsi que, l'encadrement les conditions nécessaires afin de procéder les informations des individus.

- Il est important pour l'UE que les citoyens soient dans un environnement où ces derniers se sentent en sécurité d'où l'introduction d'un principe sur la responsabilisation. Ce principe cherche à mettre en place un environnement dans lequel les entreprises sont responsables de protéger les données des utilisateurs en assurant l'intégrité et la confidentialité des informations qu'elles possèdent contre les acteurs malveillants.

- Le principe d'équité et de transparence cherche à promouvoir un environnement où les activités des entreprises du Web avec les données des utilisateurs sont transparentes et non abusives. Cette mesure mise en place afin de réduire les abus possibles dans les opérations, les transferts et l'utilisation des informations contribue à un environnement où les entreprises ne sont plus en mesure de profiter du rapport de force qu'elles ont par rapport aux citoyens et offre la possibilité de mieux comprendre ce que ces multinationales font avec les informations qu'on leur transfère.

- Il est aussi question du principe de responsabilité qui réfère au fait que les entreprises sont responsables de démontrer qu'elles se soumettent aux lois en vigueur et qu'elles répondent aux exigences légales. Aussi, les contrôleurs de données se voient obligés de fournir plus d'explications et justifier leurs décisions prises dans leurs actions avec les données en leur possession (Leenes, 2018). Ceux-ci doivent aussi porter une attention particulière aux

impacts possibles de l'exploitation d'informations et principalement dans le cas d'emploi de nouvelles technologies. Les développeurs sont responsables des produits qu'ils conçoivent et ils doivent en assurer la « qualité » en rapports aux normes du GDPR concernant l'utilisation des informations privées des individus. Il est nécessaire de produire un DPIA (The Data Protection Impact Assessment) afin de faire l'évaluation des risques pour les individus quant à leurs droits fondamentaux et les entreprises sont dans l'obligation de démontrer que les nouveaux produits en développement utilisant les informations personnelles des gens ne représentent aucun risque pour ces derniers, tout au long du cycle de développement du produit.

- En lien avec la minimisation des données, les entreprises ne doivent pas conserver les données plus longtemps que ce dont elles ont besoin, c'est-à-dire, une fois le mandat complété.

- Nous retrouvons aussi le principe de consentement. Ce dernier fait référence aux nécessités des entreprises d'obtenir auprès des utilisateurs une autorisation donnée de façon volontaire et en plein connaissance des impacts à l'utilisation de leurs données. Cette autorisation ne doit pas avoir été obtenue sous pression ou conditions quelconques. Ce principe permet d'octroyer plus de pouvoir aux individus et d'avoir accès à un choix réel sur la transmission de leurs infos au lieu d'être soumis à un faux dilemme de liberté de choix. Cette situation trop souvent présente où les gens peuvent avoir accès au produit qu'en contrepartie de leurs informations, crée une situation de discrimination si ces derniers ne souhaitent pas transmettre ces données. Ils se trouvent alors à ne pas avoir accès à certains services en ligne parfois essentiels.

- L'encadrement de l'analyse et l'utilisation de données privées spécifiques sur les individus comme la religion, l'orientation sexuelle, la position politique, l'origine ethnique, les données biométriques et les données concernant la santé sont interdits sauf sous conditions encore plus strictes.

(GDPR, 2018; Bieresborn, 2019; Leenes, 2018; Kretschmer, 2021; Soria-Comas, 2016; Degeling, 2022; Palmatier, 2019; Safari, 2017)

Habiliter les citoyens à avoir un plus grand pouvoir de contrôle sur leurs données et réduire la possibilité d'abus par les entreprises en surveillant les pratiques de ces derniers et en établissant un cadre règlementaire plus strict permet l'établissement d'un climat favorable pour un développement durable de cet espace. Cela permet aussi un retour vers un certain équilibre des pouvoirs entre les différents acteurs. Ce guide de principes au chapitre 2 du règlement général de protection des données permet à l'Union européenne une sorte de réaffirmation de leur pouvoir de contrôle des activités sur le territoire du regroupement d'États.

Au chapitre 3 du règlement européen sur les données, l'accent est mis sur les droits des individus au sein de cet espace contrôlé par les multinationales du Web. L'attribution de droits concernant les données ainsi que la réaffirmation de certains autres droits déjà en place au sein de l'Union européenne permet aux individus d'avoir plus de pouvoir de contrôle sur les données qu'ils produisent. Les articles 12 à 23 ainsi que plusieurs récitals (63, 65, 66, 68, 69, 75, 141, 142) et éléments problématiques soulevés au sein du document, établissent les obligations des entreprises envers les citoyens et les droits des utilisateurs du Web envers l'utilisation de leurs informations personnelles par les entreprises. Le GDPR parle entre autres des droits suivants :

- Le droit d'accès permet aux utilisateurs d'accéder via les entreprises, sur demande, aux données qu'ils ont produites au cours de l'utilisation d'un dit service. Ces entreprises ont l'obligation de transférer ces informations aux demandeurs. Aussi, ce droit permet aux citoyens d'avoir accès à plusieurs informations et détails importants concernant l'utilisation faite de leurs données. Nous y trouvons entre autres la possibilité de savoir l'identité des contrôleurs, les données concernées, les motivations à la base de l'utilisation des données, la période d'utilisation des informations personnelles et les gens ou groupes qui auront accès à ces informations.

- Complémentaire au droit précédent, le droit de faire transférer ces données est aussi octroyé aux individus protégés par le GDPR qui permet le transfert d'informations appartenant aux utilisateurs Web, à leur demande, d'un contrôleur à un autre.

- Le droit d'être oublié est pour les individus qui désirent ne plus être présents à travers certains sites Web. Ce droit est important pour toute personne qui ne désire plus être identifiable par une entreprise. Les gens peuvent demander que leurs informations personnelles soient effacées du Web sous certains critères et conditions.

- Le droit de faire rectifier les données inexactes permet à tout individu membre de l'UE de faire corriger toute information incorrecte à leur sujet sur le Web après avoir formulé la demande auprès du contrôleur de données concerné.

- Le droit pour les utilisateurs de s'opposer à l'utilisation de leurs données.

- Le droit de formuler une plainte ou de mandater une organisation non lucrative afin de porter plainte en son nom contre une situation allant à l'encontre d'un règlement du GDPR.

- À travers les articles sur les droits, on encadre aussi le droit de contester l'utilisation des données dans certains cas. C'est le cas lorsque des décisions sont prises de manière totalement automatisée.

(Soria-Comas, 2016; GDPR, 2018; Bieresborn, 2019; Calzada, 2019; Kretschmer, 2021; Safari, 2017)

Ces droits représentent, pour les utilisateurs du Web au sein de l'UE, l'opportunité de devenir réellement propriétaire de leurs données sur internet et d'avoir un plein contrôle sur une multitude d'aspects importants auxquels ces derniers n'étaient pas en mesure d'avoir accès par le passé. Ce mouvement législatif de l'internet permet de redonner aux utilisateurs plus de pouvoir de contrôle de leur identité digitale et offre la possibilité au ressortissant de l'UE d'évoluer au sein d'un internet plus sûr, plus compréhensif et plus juste envers ces derniers, en plus de créer un plus grand équilibre de pouvoir entre les individus et les grandes entreprises utilisant les données Web.

À travers les huit autres chapitres ainsi que les récitals, plusieurs autres aspects importants sont abordés dans le but de mieux encadrer le milieu des données, les opérations des entreprises avec les données et afin de traiter des spécifications et des conséquences de l'instauration d'une nouvelle

législation sur les données Web. Voici quelques-uns de ces sujets, chapitres et articles qui impactent directement l'industrie des données et ses acteurs soit dans leur mode de fonctionnement, leur approche envers cet espace ou encore sur les droits des citoyens.

- Le chapitre 4 aborde les différents niveaux de contrôle, les acteurs impliqués et met en place les balises pour que les groupes concernés, comme le Data Protection Authorities (DPA) ainsi que le European Data Protection Board (EDPB), assument le rôle de responsables et de contrôleurs de la qualité en matière de code de conduite vis-à-vis l'utilisation des données et d'accepter ou refuser les approches soumises par ces entreprises lors de proposition en vue d'utilisation de modèle d'analyse (Leenes, 2018; *GDPR*, 2018).

- Toujours dans le même chapitre, le concept de vie privée dès la conception des produits (Privacy by design) et le concept de protection des données privées par défaut (Privacy by default) sont détaillés. Ces concepts se démarquent comme étant essentiel pour cet espace et l'évolution des pratiques dans le milieu. L'article 25 a pour but de créer un environnement où des mesures sont mises en place afin d'améliorer la conception des logiciels pour que la vie privée des gens soit prise en compte. Cet article représente un élément central afin de faire évoluer l'écosystème du Web. Les entreprises doivent désormais prendre en considération quatre notions afin d'être en règle avec ces principes. D'abord, une analyse des risques est nécessaire. Ensuite, il y a un besoin de prise en considération des besoins techniques afin de réduire les dangers liés aux opérations. Troisièmement, il est essentiel d'introduire ces principes dans les modèles de conception de ces logiciels. Finalement, il est nécessaire de faire une évaluation périodique des systèmes, modèles et logiciels en place (Leenes, 2018; *GDPR*, 2018; Bieresborn, 2019; Degeling, 2022; Soria-Comas, 2016).

- Le chapitre 5 encadre les transferts de données vers des pays tiers et vers l'international afin de rendre ces transferts plus sécuritaires, plus transparents et mieux réglementés (*GDPR*, 2018).

- L’article 83 du chapitre 8 met en place les conditions afin d’imposer des pénalités en cas de non-respect aux règlements du GDPR. Ces amendes potentiellement très élevées ont pour but d’avoir un effet dissuasif envers les entreprises des données. Il est aussi question d’avoir un système de justice proportionnel par rapport aux actions et aux acteurs dans le but d’avoir un maximum d’efficacité envers les contrevenants (Leenes, 2018).

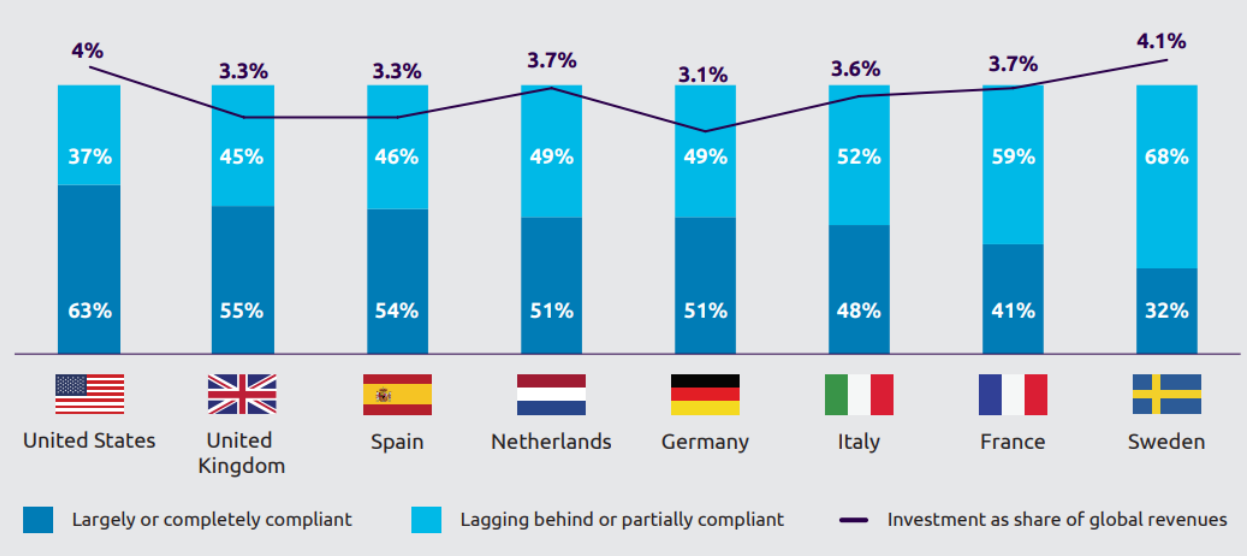
(Leenes, 2018; GDPR, 2018; Bieresborn, 2019; Degeling, 2022; Soria-Comas, 2016).

L’introduction de ces nouvelles façons de procéder auprès des entreprises par la règlementation sur les activités et l’ajout de balises cherche à faire de l’internet un environnement mieux contrôlé où les géants de cet espace n’ont pas un pouvoir d’abuser des utilisateurs. Les nombreux autres chapitres et articles non mentionnés permettent de définir certaines limites dans l’espace des données et ajouter des spécifications sur d’autres aspects du document.

3.4 Union européenne post-GDPR : analyse de la transformation de la situation des données

L’analyse de la situation des données en Europe suite à l’entrée en vigueur du récent règlement européen, dans le but de protéger les données des citoyens au sein de l’UE, offre un portrait de la situation très mitigé en matière d’atteinte des objectifs ciblés. Bien que le GDPR semble avoir contribué à instaurer un meilleur climat de confiance envers les entreprises du Web quant à leurs opérations commerciales et principalement quant à l’utilisation d’outils de pistage (Dabrowski, 2019), la réalité relative à leurs activités commerciales est qu’il y a encore beaucoup de problèmes à régler puisque les autorités en place ne sont pas en mesure d’analyser les multiples cas d’abus potentiels aux nouveaux règlements commis par plusieurs entreprises (Samarasinghe, 2019). Il y a encore une grande majorité d’entreprises qui ne se conforment pas aux obligations en matière de pistage et d’utilisation de témoins en contournent les restrictions (O’Neil, 2016; Samarasinghe, 2019; Liden 2020).

Figure 3.1 Conformité au GDPR par pays

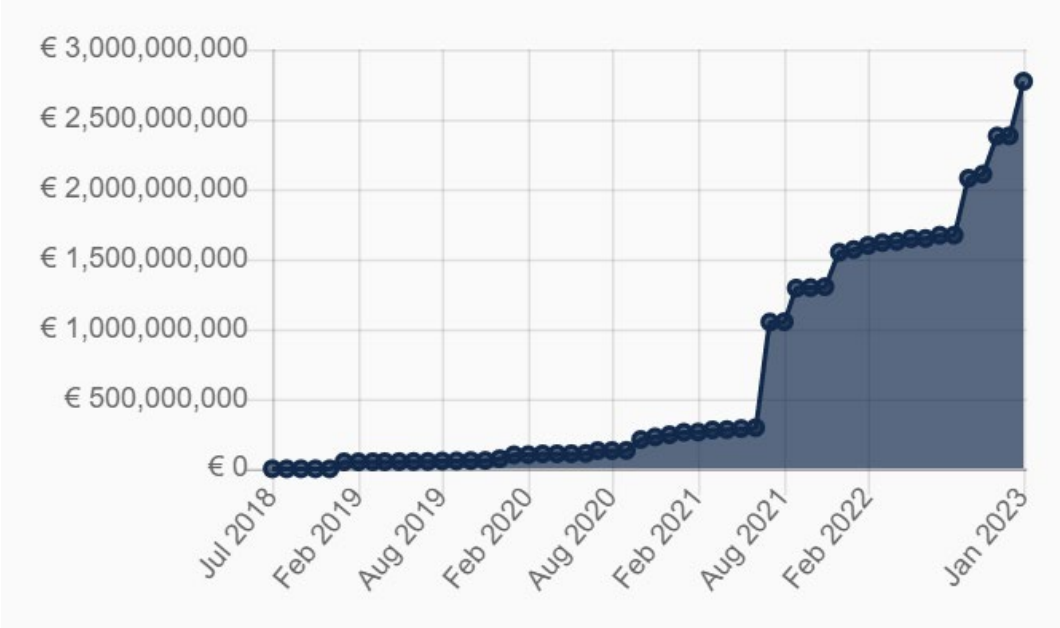


Source : De Paepe, W. et al. (2018). « Seizing the GDPR advantage: From mandate to high-value opportunity », Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf

À travers l'analyse des pratiques d'utilisation de témoins par les pages Web, Bollinger note qu'une majorité des sites étudiés n'était pas en mesure de respecter la règlementation européenne. « Only 8.13% of all 26 403 websites we analyzed did not produce any evidence for potential GDPR violations, suggesting that most hosts still have trouble fulfilling the requirements of the GDPR. » (Bollinger, 2021). Cet état de situation où encore beaucoup d'entreprises tardent à satisfaire aux exigences, malgré le délai de deux ans accordés dans le GDPR, est aussi constaté par plusieurs autres auteurs, dont Degeling (2022), qui dans son cas souligne qu'encore 34.4 % des entreprises en 2022 n'étaient pas conformes en matière de transparence de leurs pratiques (Linden, 2020; Degeling, 2022). La transparence des acteurs s'est améliorée, mais il demeure qu'une bonne partie d'entreprises ne sont pas en règle. Il est aussi nécessaire d'ajouter les autres problèmes, plus difficilement distinguables, comme les pratiques déceptives. Parmi celles-ci, on retrouve plusieurs types de suivi en ligne illégaux qui demeurent toujours très présents. Nous explorerons trois types de suivi couramment répandu à travers le Web au sein de l'UE. Premièrement, le modèle ou le consentement des individus est accepté par défaut et il revient donc à ces derniers d'entreprendre

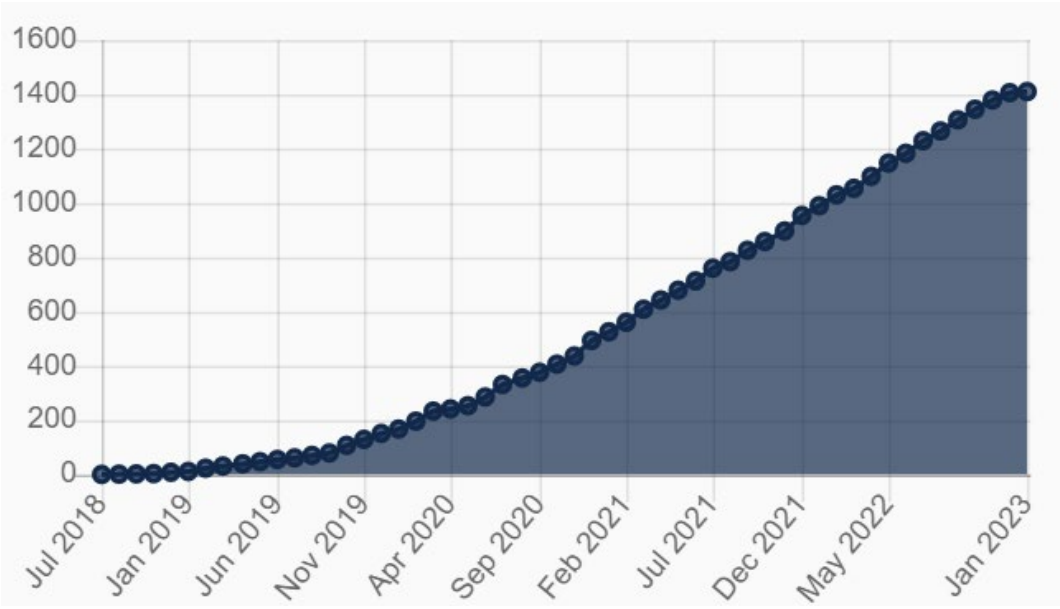
les démarches afin de faire cesser le pistage : « We further found that actual practices did not change much: The amount of tracking stayed the same and the majority of sites relies on opt-out consent mechanisms. » (Degeling, 2022). Illégal, ce mode de fonctionnement offre au moins l'opportunité aux individus de se soustraire aux pratiques malgré l'inconvénient de la situation. Deuxièmement, un autre modèle de suivi illégal est que même si les utilisateurs ont plus régulièrement accès à la possibilité d'accepter ou de refuser les témoins, il y a encore beaucoup d'entreprises qui ne respectent pas le choix des utilisateurs lorsque ceux-ci déclinent le consentement. Cette possibilité offerte aux citoyens leur permet une certaine forme de reprise de pouvoir sur la circulation de leurs données, mais encore est-il nécessaire que l'ensemble des entreprises respectent le choix de ces derniers (Kretschmer, 2021; Papadogiannakis, 2021). Certaines entreprises se contentent de donner l'impression de respecter le choix des utilisateurs : « While consent notices give the user the impression that they have control over their privacy and personal data rights, many websites use dark patterns to nudge and deceive users, and others outright ignore the user's privacy preferences. » (Bollinger, 2021). Cette image de transparence projetée par certaines entreprises, qui par la suite décident de profiter des individus et de la difficulté à retracer ce genre de comportements malhonnêtes marque la sournoiserie de certaines d'entre elles. Troisièmement, l'utilisation de techniques de pistage illégales alternatives afin d'identifier les individus. Nous reparlerons en détail de ces techniques plus loin dans le document. Ce non-respect de la volonté des personnes de ne pas être pisté et des obligations de ces entreprises envers l'UE contribue au bilan mitigé de la situation sur les données en Europe (Sanchez-Rola, 2019; Trevisan, 2019). Ce bilan peut être observé à travers la quantité d'amendes imposées au fil du temps ainsi que le total cumulatif émis par le DPA depuis l'entrée en vigueur du GDPR en 2018. Les résultats de l'application des mesures de contrôle envers les entreprises sont encore requis dans le but de réduire l'utilisation non conforme des données et la mise en place de pratiques illégales envers les citoyens et leurs droits.

Figure 3.2 Somme globale des amendes sous le GDPR



Source : GDPR Enforment Tracker. https://www.enforcementtracker.com/

Figure 3.3 Nombre total d'amendes sous le GDPR



Source : GDPR Enforment Tracker. https://www.enforcementtracker.com/

Ces amendes représentent une faible partie des violations au GPDR, car beaucoup de contrevenants au règlement en place ne sont pas repérés. Cependant, le suivi des activités des grandes entreprises et l'application de pénalités aux puissants acteurs de ce marché comme Google, Apple, Amazon détenant une part majoritaire du marché des données (AGMC, 2021) ainsi que plusieurs autres impacts sur les plus petites compagnies de l'industrie, qui font affaire avec ces géants, se retrouvent à devoir modifier leurs méthodes de fonctionnement afin de s'adapter à la nouvelle réalité.

Concernant les impacts directs sur les individus, des études sur l'opinion des utilisateurs vis-à-vis les politiques de confidentialité ainsi que les pratiques en place sur l'utilisation des témoins post-GDPR (Bollinger, 2021) ont cherché à expliquer les effets négatifs sur les utilisateurs des méthodes employées par les entreprises afin de leurrer les gens à accepter leurs pratiques commerciales. En référence à ces articles, Bollinger explique que le comportement des utilisateurs dans leur prise de décision et l'attribution de leur consentement aux pratiques d'utilisation des données par ces entreprises sont dictés par certains facteurs déterminants.

L'un d'entre eux étant le manque de mesure en place afin de faciliter la compréhension et réduire la lourdeur de ces documents légaux qui avaient un impact négatif sur les utilisateurs se retrouvant à devoir prendre des décisions concernant leurs données sans être éclairé sur les finalités de ces décisions. Ces derniers se retrouvaient plutôt poussés vers un choix qui semble au bout du compte inévitable. Ce comportement des utilisateurs peut être causé par deux facteurs : il y a d'abord le temps nécessaire afin de faire un choix éclairé et ensuite la répétition de ce type de pratiques à travers de nombreux sites Web visités quotidiennement qui inévitablement poussent les utilisateurs vers le choix facile afin d'avoir accès aux produits ou sites Web visités quotidiennement (Bollinger, 2021). Le système en place actuellement n'est pas en mesure de réellement aider les individus à prendre un réel contrôle sur leurs données. Ces deux facteurs seraient aussi liés à l'insensibilisation des utilisateurs envers les pratiques des compagnies du Web et l'incompréhension des pratiques de ces entreprises avec les données fournies par les utilisateurs. Finalement, Bollinger explique aussi qu'il a été démontré qu'une majorité d'utilisateurs qui ont été poussés vers l'acceptation des pratiques de suivi de ces entreprises ne se rappellent pas d'avoir accepté les politiques d'utilisation et qu'un sentiment de regret face à leurs décisions est souvent exprimé lorsque ces derniers sont informés des conséquences de la finalité de leurs choix (Bollinger, 2021). Bien que le GDPR adresse ce défi concernant le manque de clarté à travers les politiques de confidentialité dans le

chapitre 3 du document, les politiques en place ont de la difficulté à faire converger les pratiques vers des changements réels pour le moment :

> « This overhaul of the policies, manifesting in extensive textual changes, especially for the EU-based websites, does not necessarily come at a benefit to the users. Policies have become considerably longer. Our presentation analysis, however, identified a positive trend in user experience, specifically for the EU policies; such a trend was not found for Global policies. » (Linden, 2020)

La présence de tels résultats démontre qu'il y a encore un manquement à atteindre les objectifs de transparence souhaités par les autorités. Cependant, une amélioration de l'expérience des utilisateurs à travers les sites Web européens a été constatée et constitue un point positif dans la lutte aux transformations des méthodes de fonctionnement en place.

D'autres effets positifs sur certains aspects liés à l'écosystème des données en Europe et principalement lorsque l'on compare à ce qui peut être observé à l'international sont présents (Linden, 2020). Des modifications dans les comportements des entreprises afin d'ajuster leurs actions pour être en règle avec la législation ont mené à certaines observations positives à travers les sites européens même si les objectifs n'ont pas été totalement atteints. Ces changements touchent notamment l'usage fait des témoins, le partage d'informations entre les entreprises, l'influence internationale du document et la transparence sur les activités des compagnies du Web, le tout aux bénéfices des citoyens de l'Union européenne. D'abord, il a été observé qu'une augmentation de 16 % de la divulgation sur l'utilisation des témoins par les sites Web, une baisse de 22 % dans l'utilisation des témoins sans le consentement et une baisse de 40 % dans l'utilisation des « third-party cookies »[8] ainsi que du partage des informations des individus (Bollinger, 2021). Ces modifications des pratiques au sein de certaines entreprises à travers le Web, et particulièrement dans les entreprises basées en Europe, ainsi que dans le suivi des activités des utilisateurs européens sont attribuables à trois facteurs importants liés aux nouveaux règlements sur les données.

[8] Les « third-party cookies » sont des témoins provenant d'un autre domaine Web que celui qui a été visité et sont implantés sur des pages web afin de recueillir des données de navigation.

1. Tout d'abord, l'effet de sensibilisation et de médiatisation massive auprès des citoyens et des entreprises des conséquences des données sur de multiples aspects entourant la vie privée et la sécurité des entreprises.

2. L'effet d'une plus grande unification et standardisation des pratiques dans le domaine de la vie privée et d'une responsabilisation des pratiques à travers les pays membres de l'Union européenne.

3. L'effet de coercition par l'imposition d'amendes non négligeables introduites par le document afin de faire face aux pratiques néfastes allant à l'encontre des nouvelles politiques relatives aux données.

Les effets de ces facteurs sur l'écosystème des données représentent un avancement pour l'UE dans leur objectif de rééquilibrer la balance quant aux pratiques d'utilisations des données.

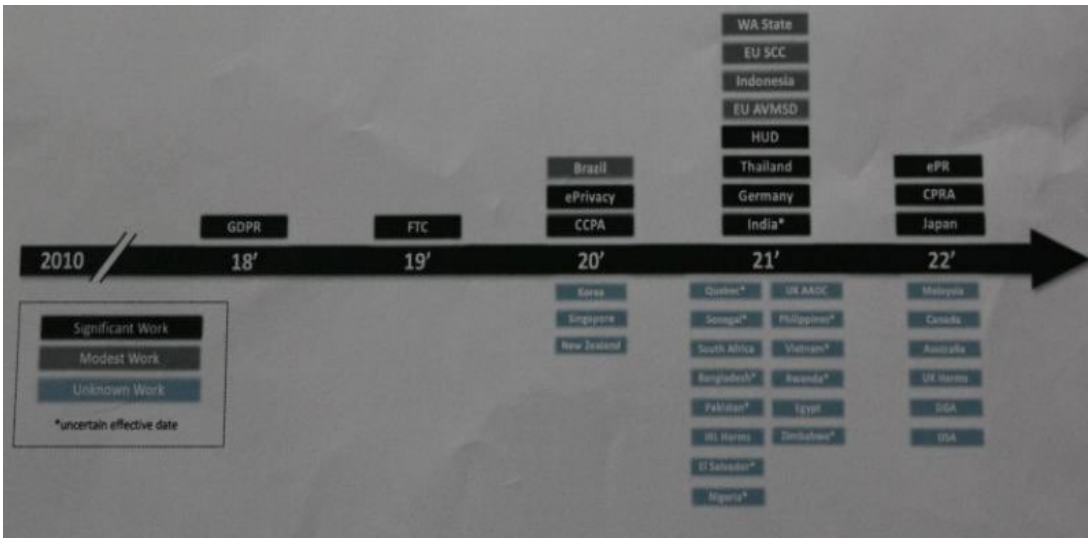
En ce qui concerne les affichages légaux sur les pages Web, c'est-à-dire la transparence, les changements apportés par le GDPR à engendrer des effets positifs par rapport aux comportements des entreprises vis-à-vis leurs pratiques sur le Web et leurs rapports avec l'acquisition des données auprès des utilisateurs. En date de 2022, une augmentation de près de 5 % dans la transparence des sites dans leurs pratiques en matière transmission d'information et de notifications des pratiques reliées aux témoins a été constaté (Degeling, 2022). Bien qu'il s'agisse d'une augmentation marginale comparée aux attentes, celle-ci représente tout de même une amélioration dans les pratiques à travers le Web afin d'atteindre les objectifs établis.

Un effet positif important qu'a eu le GDPR est celui d'avoir influencé le développement du volet législatif de cet écosystème au sein de l'Union européenne. Cette volonté de vouloir reprendre le contrôle des politiques sur ce secteur, afin de faire profiter les États et par conséquent les individus, se traduit par l'implantation progressive de nouvelles mesures complémentaires facilitées par GDPR (EDPS, 2021). L'adoption du Digital Services Act (DSA), du Digital Market Act (DMA) et du Data Governance Act (DGA) afin de compléter certains points, introduits dans le règlement sur les données, témoigne de deux aspects importants sur l'évolution de cet espace. D'abord, il souligne ce désir en Europe de vouloir assurer le succès du contrôle des activités économiques sur

le Web et dans l'utilisation des données afin de minimiser les impacts collatéraux du secteur sur les individus, tout en rétablissant une balance des pouvoirs entre les acteurs. Ensuite, cela démontre l'influence qu'a le Règlement général sur la protection des données dans l'évolution de la législation et la réglementation de cet espace afin d'assurer la réussite des mesures de contrôle jugées bénéfiques pour ces sociétés (Tielemans, 2020; Tielemans, 2021).

Il est intéressant d'analyser l'impact mondial qu'a eu le GDPR sur la réglementation de l'utilisation des données. L'importance et l'impact du regroupement d'États ont permis d'influencer mondialement les autres pays : « The EU's defensive interests also made it the first major jurisdiction to move against the market power of the platforms — a policy shift that has since been followed to some extent by both the United States and China, albeit for somewhat different reasons in the latter jurisdictions. » (Ciuriak, 2021). Un changement de paradigme ou une prise de conscience de l'impact de données sur une multitude de facteurs politiques, économiques et sociaux ont propulsé ce champ au centre de l'intérêt mondial.

Figure 3.4 Évolution de l'environnement réglementaire de 2010 à 2022



Source : Franceschi-Bicchierai, L. (2022). « Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document », Vice. https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

La prédisposition au rôle de leader mondial dans le changement en termes de régulations des données s'est concrétisée avec le temps (Ciuriak, 2018c). Des pays n'étant pas membre de l'UE comme la Norvège, l'Islande, la Suisse, la Corée du Sud, le Japon, le Brésil et le Canada, ont décidé d'adopter des dispositions similaires afin de faire face à ce défi d'envergure mondial (Degeling, 2022). Cette force d'influence qu'a eue le GDPR a permis le développement international de réglementations et d'une manière de percevoir cet écosystème.

Le GDPR a aussi forcé indirectement certaines entreprises de l'industrie à développer des technologies afin de se conformer aux changements dans la législation. Le développement de technologies respectueuses de la vie privée, avancées par des entreprises comme Google, afin de limiter l'emprise des témoins sur la vie privée des utilisateurs du Web tout en permettant à l'industrie de conserver un modèle d'affaire relativement similaire (Sullivan, 2021). Cette transformation progressive des acteurs importants permet de voir une évolution au sein des pratiques de cet espace.

Dans son analyse sur les impacts de l'introduction du GDPR, Andrew (2019) parle du fait que les efforts de l'UE visant à modifier les comportements des entreprises ont plutôt nui en matière de surveillance en favorisant une situation où il n'y a aucun contrôle sur les données désidentifiées, et que le texte de loi promeut la légitimation de ces nouvelles pratiques dangereuses qui ont été accélérées, bien que le GDPR représente le « gold standard » en matière de réglementation (Andrew, 2019). Il est important de prendre en considération les risques que le GDPR peut entraîner sur les comportements des entreprises en ce qui concerne les données « sans propriétaire », où celles-ci ont été désidentifiées, afin d'éviter une réidentification croisée de ces informations (Andrew, 2019). Cependant, il semble optimiste de sous-entendre que la situation de surveillance n'aurait pas empiré et que les entreprises n'auraient pas profité d'un environnement politique stable ou neutre pour amplifier leurs activités commerciales. Les transformations des pratiques à travers le cyberespace, notamment dans l'utilisation des données, sont vouées à s'adapter avec le temps. L'introduction de réglementations n'a fait qu'accélérer cet état d'évolution des pratiques en place des entreprises dans le but de s'ajuster aux politiques, notamment en délégitimant certaines autres pratiques nuisibles. Que les objectifs des politiques soient atteints ou non, une transformation importante au niveau politique par l'adaptation de nouvelles méthodes s'opère et permet ainsi l'évolution vers un élément plus représentatif de l'image de l'UE. L'adaptation progressive et continue des politiques est

essentielle afin de faire face aux nouveaux défis. De plus, en permettant un meilleur équilibre entre une plus grande vie privée pour les individus tout en permettant aux entreprises de poursuivre leurs activités commerciales à l'aide de ces mêmes données transformées représente un avantage important pour l'économie et l'évolution technologique. Il serait nécessaire de se demander si l'aspect surveillance des activités liées aux données est réellement important si la sécurité de ces informations ne peut être compromise.

De manière générale, l'état de la situation post-GDPR présente des résultats mitigés. Certains chercheurs dont Iwańska (2020), Bollinger (2021), Degeling (2019) et Naranjo (2021) sont d'avis que l'industrie des données semble tout autant brisée qu'auparavant malgré certains effets positifs des changements apportés par le GDPR. Selon ces derniers, plusieurs facteurs semblent être responsables de cette situation ambivalente. Certaines pratiques et tendances toxiques de l'industrie semblent persister à travers plusieurs entreprises qui abusent des vulnérabilités des autres acteurs malgré la sévérité et les conséquences possibles découlant de ces actions. Il reste que plusieurs défis demeurent afin de surmonter le problème de sécurité que posent les actions des entreprises à travers le Web qui ne se souscrit pas aux obligations en matière de données. Il y a d'abord la nécessité de reconstruire le mode de fonctionnement de l'industrie des données de masse et surtout celle de la publicité en ligne afin de permettre un changement de culture dans le milieu, ce qui prend du temps. Actuellement, les réglementations en matière de vie privée et de données en Europe favorisent involontairement un environnement où le développement de nouvelles technologies représente un couteau à double tranchant. Cette situation contribue à la persistance de pratiques malsaines de cette industrie. L'apparition de technologies plus difficilement détectables représente des alternatives attrayantes comparativement aux anciens modèles de fonctionnement et permet aux entreprises de recueillir les données des utilisateurs sur le Web comme par le passé de manière plus discrète. Le développement et l'utilisation de ces techniques comme les

evercookies[9], le canvas fringerprinting[10], les cookie synching[11] et autres, dans le but de traquer intensivement nos activités, tout en ignorant les préférences des utilisateurs en matière de suivi, ont contribué à faire de cet espace un endroit à l'image de nos modèles économiques où le capital financier est placé à l'avant-scène par les entreprises (Leenes, 2015; Szymielewicz, 2018; Papadogiannakis, 2021). Si l'UE désire protéger ses citoyens des pratiques abusives de certains géants de ces industries, le renversement des pratiques commerciales d'utilisation des technologies par cette industrie est nécessaire. Aussi, l'application d'une surveillance encore plus étroite sur les pratiques des entreprises du Web est impérative (Naranjo, 2021). À travers les études sur les actions des entreprises dans le domaine des données, le comportement de ces derniers envers le citoyen européen montre que l'UE ne peut se fier à la bonne volonté de ces derniers à se conformer aux règlements en place. La nécessité pour l'Union européenne d'agir sur les problèmes à la source de cet enjeu de l'utilisation abusive des données, comme le suivi entre sites Web représente un point de contrôle important afin de renouer avec une utilisation saine du Web pour tous et le développement d'un environnement plus juste pour les fournisseurs de données (Iwańska, 2020). De plus, la nécessité d'une mise en application beaucoup plus sévère du GDPR, par tous les États membres de l'UE, est essentielle afin de permettre le développement d'un environnement où la vie privée des gens représente une priorité pour tous, et ce de manière uniforme (Iwańska, 2020). Aussi, un autre défi majeur pour le GDPR est dans la nécessité pour les autorités de l'UE de créer un lien plus solide entre les champs techniques principalement impliqués au sein de cet enjeu, c'est-à-dire le besoin d'une plus grande clarté entre le côté légal et le côté technique dans le développement de logiciels. Les développeurs de logiciels et les juristes n'ont pas nécessairement les capacités pour comprendre et intégrer la vision proposée par l'autre corps de métier et de comprendre les défis

[9] Les « evercookie » sont des interfaces de programmations d'applications (API) qui ont pour but d'identifier et de reproduire les témoins supprimés intentionnellement par les utilisateurs favorisant ainsi un pistage constant de ceux-ci. En entreposant les informations de navigation à l'intérieur de plusieurs compartiments différents sur le navigateur local des clients, ces supercookies sont en mesure de se régénérer perpétuellement.

[10] La prise d'empreintes digitales aussi appelée canvas fingerprinting consiste à traiter toute combinaison de paramètres d'application, de système ou de dispositif dans le but d'identifier un internaute lors qu'il navigue sur une page Web, et ce même si ce dernier désactive les cookies/témoins. (Kretschmer, 2021)

[11] « Cette pratique consistant à associer plusieurs cookies distincts les uns aux autres est appelée "synchronisation des cookies". Si au moins un des cookies est utilisé pour identifier un individu, tous les cookies peuvent donc être associés à cet individu. » (Kretschmer, 2021)

auxquels chacun fait face. C'est notamment le cas lorsqu'il s'agit d'intégrer une nouvelle législation dans un produit déjà existant, cela représente un défi qui n'est pas toujours évident pour les entreprises. Aussi, le défi d'introduire la granularité de concepts légaux dans des logiciels peut aussi entraîner de multiples imprévus ou défis quant à l'ajustement des compréhensions des deux champs professionnels afin d'arriver à un produit qui répond aux besoins de tous sans créer de confusion (Leenes, 2018).

> « Software engineers often have an approach to privacy that is limited to the protection of individuals' personal pace. Furthermore, they often understand data protection' to be limited to security measures aimed at preserving the confidentiality of information. In contrast, legal experts instrumentalise broader notions of privacy and 'data protection' and situate them in the framework of fundamental rights. » (Leenes, 2018)

Ce défi entre les différents corps de métier est notamment présent à travers la notion d'intérêt légitime à l'article 14 et la notion de consentement éclairé à l'article 7, qui représentent des termes ambigus. Le fait que ces termes peuvent être interprétés différemment par chacun des partis cela favorise un environnement où chacun d'entre eux définissent ces deux notions selon leurs intérêts. Cette ambiguïté est aussi présente lorsqu'il est question de légalité de certaines pratiques comme le browser fingerprinting (Kretschmer, 2021). Il ne semble pas avoir de consensus quant à certaines des pratiques à savoir si celles-ci sont acceptables ou non aux yeux de la loi. Le flou juridique qui découle du langage technique utilisé abondamment à travers le GDPR. De la même manière, la vision de l'UE d'une transition optimale par l'adoption du principe de neutralité au récital 15 offre la possibilité à ces derniers de développer et de choisir les moyens voulus pour respecter le règlement de l'Union européenne afin d'accommoder ceux-ci au lieu de forcer ces derniers vers un modèle unique. Cependant, le développement de plusieurs modèles parfois complexe pour les individus, contribue à l'intensification de la confusion des acteurs, individus et entreprises, et contribue à ralentir l'atteinte des objectifs fixés. Dernièrement, le besoin d'une réforme du modèle économique global du Web et non seulement du secteur des données exposé par Naranjo (2021) représente une tâche colossale allant bien au-delà de la protection des données des citoyens. Dans cet espace interconnecté et international, la nécessité d'une collaboration globale paraît essentielle afin d'augmenter les chances d'une transformation réussite des pratiques commerciales actuelles.

Bref, le cyberespace après l'entrée en vigueur du GDPR a vu certaines transformations positives qui ont permis l'avancement de l'enjeu à un niveau mondial. Cependant, il serait juste de dire que les gens sont plus informés des pratiques de l'industrie, mais tout autant suivis qu'auparavant. Les différents facteurs responsables de cette faible augmentation dans la prise de responsabilités des entreprises et l'adaptation de leur modèle d'affaires sont tous des défis qui semblent perpétuels. Le manquement de beaucoup d'entreprises à se soumettre aux règlements, même après un délai de 6 ans, marque la difficulté qu'a l'UE à faire changer les méthodes d'opérations de celles-ci et de conscientiser certains acteurs aux enjeux relatifs aux données de masse. Ultimement, il n'y a pas de standards clairs afin de définir ce qui représente une transition réussite de cette industrie, mais la combinaison de ces multiples facteurs soulevés démontre actuellement un échec partiel des politiques du GDPR, du moins à court terme, à faire de cette industrie un endroit plus respectueux, sécuritaire et responsable dans leurs pratiques d'utilisation des données malgré l'observation d'améliorations et d'une vague de changements mondiaux.

CHAPITRE 4
ENJEUX LIÉS À L'UTILISATION DES DONNÉES PERSONNELLES PAR LES GÉANTS DU WEB

Dans ce chapitre, nous observerons trois champs d'intérêt touchés par l'adoption du règlement général sur la protection des données afin de mieux contrôler l'utilisation faite des données au sein de l'Union européenne par les entreprises à travers le monde. Il sera question des effets des pratiques commerciales sur la sécurité des différents groupes d'acteurs, du droit des individus face aux méthodes employées par les compagnies du Web et du pouvoir de gouvernance du groupe d'États sur les entreprises du Web afin de contrôler et légiférer sur les comportements acceptables de ceux qui ne le sont pas. Plus spécifiquement, nous traiterons des impacts de l'imposition de limites sur les pratiques commerciales des données envers les entreprises du Web et particulièrement celles des géants monopoles américains et des autres entreprises étrangères opérant sur le territoire de l'UE. Nous analyserons les répercussions du GDPR sur les comportements des acteurs concernant l'utilisation faite des données, et ce, dans l'objectif de comprendre les transformations du secteur visé et des pratiques abusives affectant la société de multiples manières. À travers ces défis, le désir d'émancipation de l'UE, des pratiques commerciales toxiques, marque un changement de paradigme dans la puissance de l'économie du Web face aux systèmes politiques.

4.1 La sécurité

Le thème de la sécurité est un élément clé lorsque l'on parle de l'application du GDPR aux pratiques commerciales du cyberespace et aux activités des utilisateurs du Web. Au sein des Relations internationales, la sécurité est un enjeu critique afin de bien comprendre ce qui définit et qui motive les actions des acteurs ainsi que leur manière d'y parvenir. Dans la réappropriation de

l'espace numérique et politique du cyberespace, l'étude de la sécurité à travers les pratiques, nous aide à analyser les impacts du GDPR sur les acteurs et les conséquences des réponses de ceux-ci. Le choix d'introduire un tel document législatif de la part de l'UE est aussi un élément important à considérer lors de notre analyse de l'état des lieux. Le thème de la sécurité peut être appliqué de multiples façons et angles dans le but de nous apporter une quantité d'informations importantes sur cet environnement et mieux comprendre son fonctionnement. Nous devons regarder le thème de la sécurité comme un besoin pour les acteurs afin de comprendre les enjeux pour ceux-ci. Nous devons regarder la sécurité en tant qu'idéal pour la société, c'est-à-dire de comment traiter l'enjeu afin de subvenir aux besoins de tous dans la mesure du possible sans nuire aux autres acteurs. Puis, il faut regarder la sécurité en tant qu'état de la situation pour le secteur des données dans son environnement. Ces trois visions définissent l'importance d'étudier cet aspect clé pour voir de multiples impacts du GDPR sur cet espace : « […] security is a process as much as a condition and throughout history this process has focused on determining the most appropriate relationship between individuals and political communities. » (Williams, 2004). De la même manière qu'il est primordial de définir les besoins et la relation entre les entreprises, les individus, les gouvernements et les groupes d'intérêts, car ceux-ci sont tous affectés d'une certaine façon par les changements dans la réglementation des pratiques commerciales du Web et le résultat de ces changements influence le comportement de ceux-ci en retour.

Dans les mots de Wendt, la sécurité est ce que l'on dit et ce que l'on en fait (Grondin, 2010) et à travers les prises de décision de règlementer cet espace et les comportements des entreprises, l'approche de l'UE s'inscrit dans une ligne directrice qui définit l'enjeu des données comme étant un élément central à la sécurité. Cette conception de la sécurité caractérise les dangers perçus par les individus et les États. Le modèle d'affaires des entreprises utilisant abondamment les données comme les réseaux sociaux est potentiellement lourd de conséquences pour la sécurité des individus et la sécurité nationale des États ce qui représente un défi important aux yeux de l'UE. Cette ambition qu'ont beaucoup d'entreprises à vouloir de recueillir le plus d'informations possible sur les individus et leurs comportements contribue à l'augmentation des risques de toute sorte pour ces derniers. L'objectif de l'Union européenne de mieux règlementer le comportement symbolise la volonté du groupe d'États à vouloir retrouver cette souveraineté effacée à travers le Web et ce désir de réduire leur vulnérabilité face aux entreprises des données et ultimement, de ne plus être à

la merci de celles-ci. Si l'on considère l'État comme étant un véhicule pour les idées et désirs des citoyens, cette volonté de reprise de possession des droits de gouvernance des États membres de l'Union européenne à travers le Web et sur les actions des entreprises dans cet espace émane directement des citoyens et bénéficie directement aux communautés de ces États.

À travers la poursuite de cet objectif de sécurité par l'UE, la notion d'émancipation prend une place importante dans l'analyse de l'enjeu, surtout lorsque l'on tient en compte des défis et de l'histoire remplie d'abus qui précède cet espace (EDRi, 2019). La résistance des pays membres, face aux méthodes employées par les entreprises, par l'adoption de politiques (Peoples, 2015) a pour but de réduire les risques inhérents et tente de transformer les comportements abusifs des acteurs au sein de cet espace. À travers cette poursuite du changement des comportements, un facteur élément important a besoin d'être pris en considération. Il est essentiel que cette émancipation vis-à-vis les multiples facteurs menaçants pour les individus et les États ne puisse se réaliser aux dépens des autres et qu'une certaine collaboration entre les différents acteurs soit présente afin d'assurer le succès de cette transition dans l'état de la situation. Pour plusieurs, le besoin de revoir le fonctionnement économique de cet espace et plus précisément, le modèle d'affaires basé sur les données se trouve essentiel afin de s'émanciper progressivement de la situation, ce qui n'est cependant pas un processus simple et ne peut non plus se réaliser rapidement. Cette vision où la dépendance aux données s'estompe graduellement est plutôt une aspiration qui est en constante évolution et transformation (Grondin, 2010). L'atteinte d'une gouvernance du Web idéale satisfaisante à tous les critères de sécurité de l'Union européenne et des citoyens nécessite d'être travaillé et révisé continuellement afin de prendre en compte les changements dans nos sociétés. Ce point est intéressant dans le cas présent, car la relation de dépendance qu'entretiennent les différents groupes entre eux, et principalement celle entre les individus et les entreprises du Web, témoigne de cette nécessité de collaborer afin de trouver des compromis quant à l'utilisation des données, et ce dans le but que chacun des groupes impliqués y trouve leur compte et puis que progressivement la situation se résorbe. Les entreprises ont besoin d'être impliquées dans le processus de transformation de l'espace, car dans le cas contraire un système disproportionnel dans les comportements observés et dans son fonctionnement marque les changements encourus, ce qui est présentement le cas au sein de l'UE à la suite de l'adoption du GDPR. Il est clair que la recherche de solutions entrainant une plus grande sécurité pour l'ensemble des acteurs, dans ce

conflit multidimensionnel, présente un très grand défi en soi d'où la difficulté pour le GDPR à transformer les comportements des acteurs au sein de cet espace.

4.1.1 Paradigme de sécurité lié aux données

L'un des objectifs du règlement général sur la protection des données est de modifier le mode de fonctionnement de l'économie des données liées au Web qui est essentiellement basé sur la surveillance ouverte des individus et de leurs activités. Cette situation pose un dilemme de sécurité entre les entreprises et les États où leurs intérêts et leurs actions afin de résoudre la situation sont principalement en opposition avec ceux de l'autre groupe. En 2018, les effets temporaires, dans certains cas, de la panique induite par le document législation de l'UE a permis de, temporairement, maîtriser et réduire certains faits observables dans cet espace. « Additionally, pinpointing the reason for observable changes in third-party tracking is challenging, as trends show that the amount of trackers is close to pre-GDPR levels after a temporary decline. » (Kretschmer, 2021). L'effet temporaire des changements dans les comportements des entreprises et le rapide retour vers des comportements problématiques à l'encontre des États et des droits des individus montrent une partie des effets du GDPR sur l'écosystème des données. La prise d'actions par l'Union européenne a causé une réaction des entreprises et une adaptation des méthodes, ou plutôt, l'image d'une adaptation dans le but d'outrepasser les lois perçues par les entreprises comme étant problématiques et restrictives pour le déroulement de leurs opérations commerciales. En fin de compte, le résultat est que ce besoin de sécurité de chacun des groupes d'acteurs n'est jamais atteint et n'est que temporaire. Certes, une certaine évolution peut être observée à travers ce processus où chacun se renvoie la balle, mais concrètement, de nouvelles politiques seront adoptées par les États et de nouvelles tactiques afin d'éviter autant que possible les limitations imposées seront employées par les entreprises afin de perpétuer leurs modèles d'affaires basés sur les données. C'est pour cette raison que certains chercheurs considèrent comme incompatibles les deux visions.

4.1.2 Les défis liés à l'utilisation sécuritaire des données

Le Web est un endroit que l'on pourrait qualifier comme étant hostile pour l'ensemble de la société (Douzet, 2014). L'accroissement de comportements égoïstes et illégaux entre les différents acteurs pose des risques divers à travers le monde entier. La sécurité dans nos interactions avec cet espace est l'un des enjeux modernes qui occupent l'attention mondiale. La raison pour laquelle ce défi est un enjeu de taille est que la numérisation de l'ensemble de nos activités sociétales nous expose au maillon le plus faible de la chaîne de nos interactions. Notre vulnérabilité est liée au maillon le plus faible de la chaîne. Il suffit alors qu'un seul cède pour exposer les individus et les sociétés de manière générale aux impacts négatifs qui se traduit principalement en perte financière, en perte de temps majeur, en perte de sécurité qu'elle soit matérielle ou en bien-être de tout genre (Quéméner, 2011). Les défis complexes que doivent relever les États dans le but de faire du Web un environnement plus sécuritaire nécessitent une quantité importante d'investissement en temps et en argent. Voici quelques-uns des défis majeurs qui empoisonnent l'utilisation plus sûre du Web :

- L'utilisation de techniques et de technologies afin de contourner les législations visant la protection des individus, comme la création d'identités fantômes, constitue un enjeu complexe pour l'UE qui cherche à faire réduire les abus des entreprises envers leurs citoyens.

- La valeur des données en grande quantité (Deighton, 2015) combinée à la résurgence d'acteurs malveillants, qui cherchent à exploiter chaque vulnérabilité des entreprises trop souvent insouciantes, fait en sorte que les informations accumulées dans les bases de données de ces entreprises représentent des cibles de choix. La faible protection de ces informations pose des risques pour tous et c'est surtout le cas lorsque les systèmes d'entreposage des données ne répondent pas à des normes de protection des informations collectées.

- Le fonctionnement de la catégorisation des individus selon leurs intérêts est en mesure d'entraîner une restriction d'accès à certaines informations qui seront jugées moins pertinentes selon les intérêts de la personne concernée entraînant ainsi une bulle de rétroaction où ces personnes interagiront avec ce même contenu. Dans la majorité des cas, ce type d'effet sur les utilisateurs ne représente pas de risques, cependant, lorsqu'il est le cas de promotion d'idées jugées dangereuses, cela peut mener à une radicalisation des individus envers un ou plusieurs autres groupes ou manières de penser.

- Pour les sociétés, la création de dépendance par les individus envers le Web (Grosbois, 2018) et la mise en œuvre de techniques par les entreprises du Web afin de favoriser le développement de tels comportements nocifs est un enjeu de sécurité sur la santé mentale de la population. L'exploitation des vulnérabilités des utilisateurs par l'utilisation des informations de ces derniers et en les poussant à consommer toujours plus doit être signalée. Le développement de telles pratiques à travers le Web entraîne des risques pour les utilisateurs de manière générale, mais principalement chez la population plus jeune qui est plus à risque de souffrir des conséquences négatives liées à l'exposition à une consommation excessive.

- L'accès des entreprises à des données de nature confidentielle ou sensible comme l'orientation sexuelle, la préférence politique, la religion ou encore des données médicales représente un danger pour les utilisateurs et leur droit à la vie privée. L'exploitation possible de ces informations à des fins illégitimes pose un risque de confidentialité pour la société de manière générale. Ces informations pourraient, entre autres, possiblement devenir publiquement accessibles et utilisées malgré la volonté des utilisateurs.

- Parallèlement au point précédent, le non-respect à la vie privée des personnes qui ne souhaitent pas être traquées représente un défi quasi impossible en soi pour les États. La numérisation de nos activités quotidiennes pousse les individus à devoir recourir à certains services du Web quasiment essentiel et donc, nous exposent à cette surveillance sans possibilités de se souscrire à ces pratiques.

- Le danger de l'accroissement des inégalités dans nos sociétés envers certaines classes, ethnies et groupes de la population qui se retrouvent victime de profilage, crée des sociétés où les citoyens ne sont plus tous égaux et n'ont pas tous accès aux mêmes opportunités (O'Neil, 2016). Lorsque ces tendances de profilage par algorithmes sont mal surveillées, les dangers qui émanent de ces technologies sont eux-mêmes accentués par les préjugés et mesures en place, ce qui entraîne des boucles de rétroaction, qui peuvent à leur tour créer de faux positifs qui seront confirmés par les biais des données (O'Neil, 2016). De telles situations sont accélérées par les algorithmes qui permettent l'automatisation de ces analyses et où les révisions faites par des humains sont moins présentes. La présence de ce type de dangers a contribué, par le fait même, à propulser l'émergence d'un marché complet lié à la cybersécurité pour les entreprises, leurs infrastructures et pour les individus, ce qui représente un défi taille pour cet espace.

Le besoin de rendre l'environnement du Web plus sûr par la mise en place de régulations plus sévère envers l'utilisation des informations s'est particulièrement fait sentir à travers les abus dans les transferts des données et spécialement ceux hors du territoire européen où le contrôle en devient impossible. Les comportements insouciants des grandes entreprises du Web et ceux des gouvernements étrangers avec les banques d'informations disponibles ont incité l'UE à pousser de l'avant ces régulations pour faire changer les pratiques du milieu au sein de l'Union européenne. En ce qui concerne la gestion de la distribution de ce qui parvient à un auditoire ou non, pour le moment, ce sont ces géants du Web qui déterminent cet aspect (Grosbois, 2018). Les problèmes actuels et potentiels liés à une utilisation abusive des données des individus sont dus à un manque flagrant de contrôle des pratiques de cet espace entourant les algorithmes. Lorsque l'on parle d'algorithmes, il est essentiel de garder en tête que ces derniers restent des outils de profilage et de classification qui ne sont pas neutres et qui ont des objectifs propres à chacun d'eux, qui sont liés aux intérêts des entreprises ou États derrière ceux-ci.

Bien entendu, ces situations ne sont pas toujours présentes à travers l'ensemble des entreprises et bien que ces faiblesses liées aux données soient extrêmement difficiles à contrôler, le GDPR tente d'adresser ces divers cas, et tente de répondre aux obligations des États de protéger leurs citoyens,

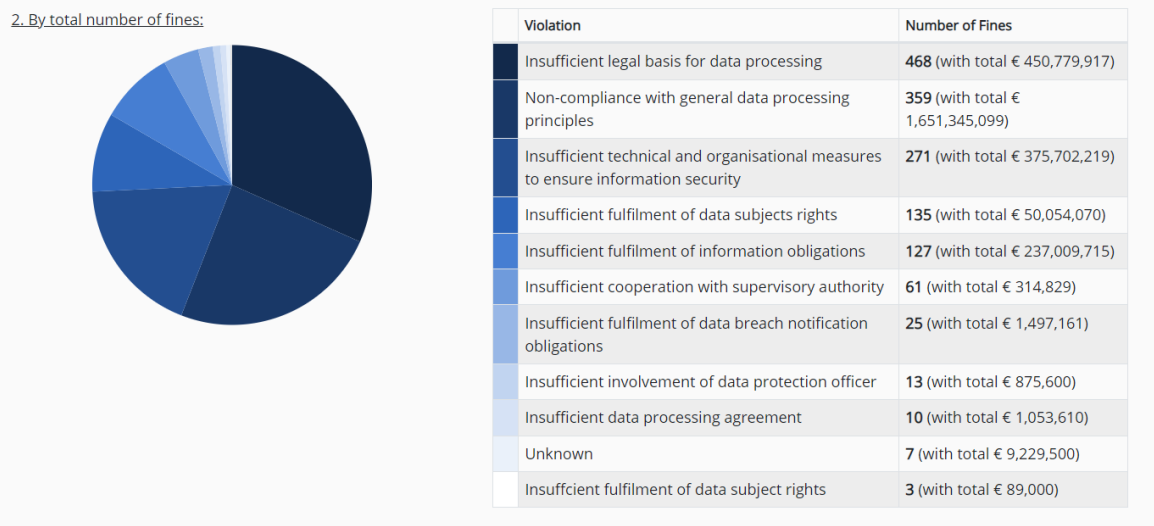
par l'imposition d'obligations envers les entreprises. Il reste cependant encore beaucoup de chemin à parcourir afin d'atteindre les objectifs établis par le GPDR en matière de sécurité.

4.2 Les droits individuels et collectifs au sein de l'Union européenne

L'importance des droits individuels et collectifs de citoyens au sein de l'UE fait de la collecte des données un sujet important pour les pays membres. L'effacement partiel de ces droits au cours de l'évolution du Web, permis par les comportements des entreprises, au profit de développements technologiques et d'une interconnexion globale a engendré un environnement en désynchronisation, par rapport aux autres espaces traditionnels. En Relations internationales, le droit constitue un point d'ancrage pour les sociétés afin de délimiter les actions acceptables, de celles qui ne le sont pas. En ce sens, le désir de voir une meilleure protection des droits numériques des citoyens caractérise l'origine de l'adoption du GDPR et la réappropriation du cyberespace. Pour ce faire, l'Union européenne cherche à limiter les actions ayant des impacts négatifs directs sur ces droits symboliques acquis par les individus. À travers les mesures mises en place afin de mitiger les impacts négatifs des pratiques à travers le Web, nous pouvons penser au fait que désormais les individus doivent donner leurs approbations aux entreprises dans presque tous les cas où leurs données seront collectées et analysées par les entreprises permettant ainsi un meilleur contrôle de la diffusion de leurs informations. Aussi, offrir la possibilité pour les utilisateurs de faire presque ce que bon leur semble avec leurs informations même après avoir donné leur approbation, comme la possibilité de demander la suppression des données sur leur personne si ces derniers désirent de ne plus faire partie des « statistiques » qui sont vendues à qui le veulent bien. Cette reconnaissance des droits acquis par les individus sous le GDPR représente un avancement considérable pour les citoyens de l'UE et les utilisateurs du Web. La nécessité de présenter une équivalence et une reconnaissance des droits et ça, peu importe l'espace d'action, introduit un sentiment de protection pour les individus envers ceux qui tenteraient d'abuser de leurs capacités et de leur pouvoir afin de contourner leurs obligations.

La mise en place d'un tel modèle idéalistique est significative pour le droit des citoyens avec l'introduction de réglementations, bien qu'en réalité ces règles sont loin d'être totalement respectées par les entreprises de l'industrie. Les changements radicaux dans la reconnaissance des pouvoirs des individus au sein du Web dans les dernières années font de l'industrie de la surveillance qu'elle cherche toujours à utiliser plus de données et de ce mouvement des éléments diamétralement opposés en termes d'intérêt (Naranjo, 2021). Ces changements ont forcé les entreprises à devoir adapter leurs modèles d'affaires sur le territoire de l'UE sous peine de conséquences introduites par le GDPR.

Figure 4.1 Amendes par type d'infraction et nombre total d'amendes sous le GDPR



Violation	Number of Fines
Insufficient legal basis for data processing	**468** (with total € 450,779,917)
Non-compliance with general data processing principles	**359** (with total € 1,651,345,099)
Insufficient technical and organisational measures to ensure information security	**271** (with total € 375,702,219)
Insufficient fulfilment of data subjects rights	**135** (with total € 50,054,070)
Insufficient fulfilment of information obligations	**127** (with total € 237,009,715)
Insufficient cooperation with supervisory authority	**61** (with total € 314,829)
Insufficient fulfilment of data breach notification obligations	**25** (with total € 1,497,161)
Insufficient involvement of data protection officer	**13** (with total € 875,600)
Insufficient data processing agreement	**10** (with total € 1,053,610)
Unknown	**7** (with total € 9,229,500)
Insuffcient fulfilment of data subject rights	**3** (with total € 89,000)

Source : GDPR Enforment Tracker. https://www.enforcementtracker.com/

À travers l'ensemble des contraventions émises pour non-respect du GDPR dans la figure 4.1, trois des quatre premières catégories totalisent près de mille infractions distinctes touchant directement au respect des droits des individus et de leur sécurité. Ces quatre catégories sont : des raisons insuffisantes pour l'utilisation des données, le non-respect des principes du GDPR sur l'utilisation des données, l'insuffisance dans les mesures techniques mises en place afin d'assurer la sécurité des informations et un respect insuffisant des droits des usagers. La quantité impressionnante d'infractions aux mesures en place certifie le besoin accru de mesures de contrôle des pratiques de

l'industrie dans le but de pallier les abus d'utilisation des données et de la confiance des utilisateurs au sein de cette industrie.

4.2.1 Réglementations sur l'utilisation des données

Les défis légaux que pose la réglementation des données sont complexes. Le besoin de rendre l'espace et les pratiques commerciales en plus grande harmonie dans le but de permettre une émancipation des citoyens se fait sentir pour les États. Plusieurs objectifs sont visés par le texte de loi qui cherche à mieux encadrer cet écosystème et les pratiques essentielles à l'économie principale liée à celui-ci. La lecture du GPDR nous offre un aperçu clair des motivations et des objectifs de l'UE afin de mieux contrôler cet espace. Dans les divers articles et les mesures de réglementations sur les pratiques commerciales touchant la surveillance des utilisateurs, la priorisation des besoins de leurs citoyens aux dépens de l'économie des données qui est actuellement utilisé, illustre la volonté de l'UE face aux comportements jugés déplacés de ceux-ci. L'introduction de défis significatifs envers cette industrie ne démontre cependant pas une volonté l'anéantir, mais bien un désir de réformer ces méthodes en promouvant un environnement qui sera en mesure de mieux répondre aux besoins des citoyens européens (European Commission). Au contraire, les avancées technologiques sont essentielles et la flexibilité du GDPR sur certains points importants, comme la neutralité technologique, en témoigne (Pagallo, 2017). Le rééquilibrage des pouvoirs entre les acteurs et cette réappropriation par les États du pouvoir de contrôle dans la façon de procéder à travers le Web en imposant leurs conditions aux entreprises apparaît comme étant essentiel au développement pour le futur du Web.

> « Data must be processed according to European values if we aim to shape a safer digital future. As we move to create new opportunities for data use, we must ensure that the existing data protection framework remains fully intact. Access to data by public authorities should always be properly defined and limited to what is strictly necessary and proportionate, […]. — Wojciech Wiewiórowski, contrôleur européen de la protection des données » (EDPS, 2022)

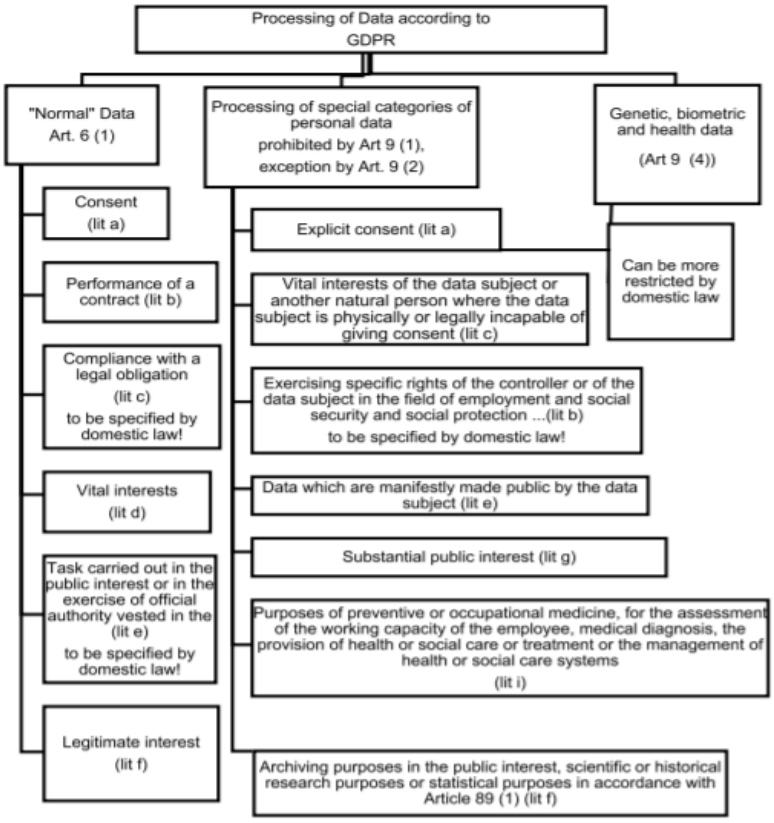
L'incitation à adopter de tels comportements plus respectueux par la promotion de mesures clés dans le but de faire progresser les techniques employées par les entreprises, qui en plus permettent une plus grande vie privée aux utilisateurs, est aussi présente. Ces techniques comme l'anonymisation[12], la pseudonymisation[13] ainsi que d'autres (Torra, 2014) dont certaine nous avons précédemment abordé comme le concept de vie privée dès la conception des produits et le concept de protection des données privées par défaut sont toutes des méthodes incitées par l'UE à travers le GDPR afin d'accroître la sécurité et le respect des droits des citoyens au sein du Web.

Aussi, comme mentionné précédemment dans le chapitre trois, le règlement sur l'utilisation des données n'est pas parfait et présente certaines failles qui doivent être adressées. Il est question notamment de la présence de termes vagues qui entraînent des difficultés pour les utilisateurs ainsi que les entreprises à déterminer et à classifier la conformité de services, ce qui représente un enjeu important dans la règlementation en place : « Thus, both web service providers, as well as their users, face difficulties assessing whether a particular service is compliant with the GDPR or not. » (Kretschmer, 2021). La nécessité pour l'UE d'adapter les politiques en place et le langage utilisé dans le GDPR dans le but de faciliter la compréhension et permettre à tous d'évaluer et décider si l'utilisation faite de leurs données correspond aux attentes serait une amélioration très bénéfique pour chacun des acteurs et le Web. Dans la figure ci-dessous, le traitement des informations selon la catégorie à laquelle ces informations appartiennent tente d'expliquer à quelle classe chacune des informations se rattache, il peut cependant avoir place à confusion si des informations peuvent être liées à plusieurs catégories. Il faut être un expert du GDPR pour pouvoir comprendre certaines nuances dans le traitement des informations et les utilisateurs ne sont pas équipés pour cela (Baruh, 2017).

[12] « L'anonymisation signifie que les données ne peuvent pas être réattribuées à un individu. » (Lapienyté, 2021)

[13] « La pseudonymisation est une technique qui remplace ou supprime les informations permettant d'identifier un individu. Par exemple, il peut s'agir de remplacer les noms ou autres identifiants par un numéro de référence. » (Lapienyté, 2021)

Figure 4.2 Traitement des données conformément au GDPR



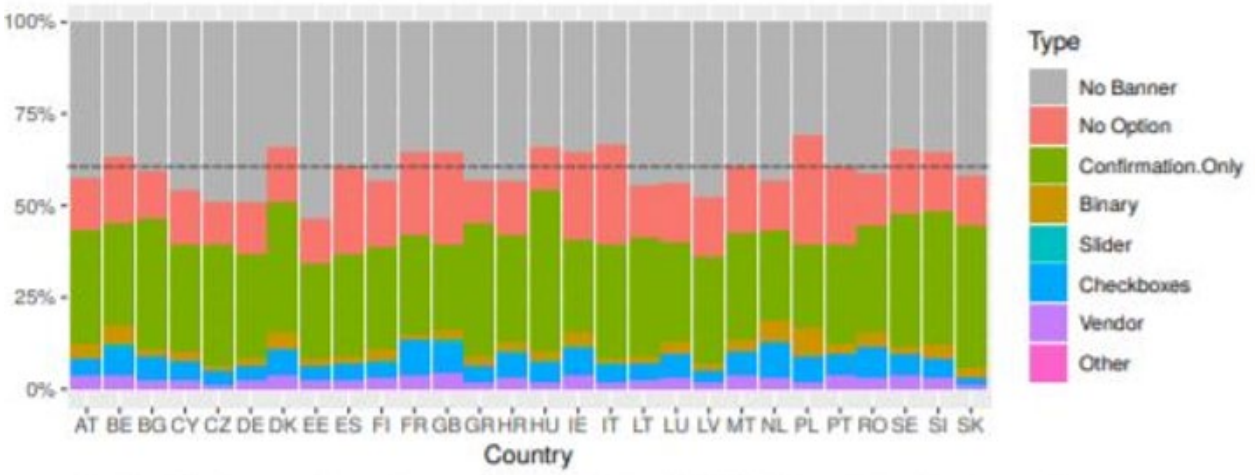
Source : Bieresborn, D. (2019). « The Impact of the General Data Protection Regulation on Social Security », *Era Forum : Journal of the Academy of European Law*, vol. 20, no. 2, pp. 285–306. https://link.springer.com/article/10.1007/s12027-019-00565-x.

4.2.2 Enjeux du mode de fonctionnement actuel de collecte et d'utilisation des données pour les droits des individus

La difficulté pour l'Union européenne à faire respecter l'ensemble des conditions mises en place concernant le traitement des données demeure forte même après plus de 5 ans depuis l'entrée en vigueur du GDPR. La figure 4.3 illustre le respect et la transparence des entreprises vis-à-vis leur obligation de laisser les gens choisir d'accepter ou non d'être suivi. Les résultats de cette étude démontrent que, même plusieurs mois après l'entrée en vigueur du règlement général sur les

données, il y a toujours un besoin pour l'UE de prendre des mesures supplémentaires plus concrètes et nécessaires afin d'améliorer la situation.

Figure 4.3 Formulaire de témoin par pays (Octobre 2018)



Source : Degeling, M. et al. (2019). « We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy », Université du Michigan. https://arxiv.org/abs/1808.05096

Ces résultats concernant la divulgation de l'utilisation des témoins par les entreprises ont démontré aussi la présence de pratiques encore très problématiques à travers l'industrie. Si nous regardons les résultats plus en profondeur dans le tableau précédent, les couleurs en gris, en rouge et en vert qui dominent le graphique sont toutes des options et méthodes utilisées qui sont non conformes et qui vont à l'encontre des règles mises en place par le GDPR. Toujours selon les résultats observés, il y aurait donc approximativement environ dix pour cent des entreprises, à travers l'Union européenne, qui étaient en bonne et due forme avec les attentes conformément au GPDR en matière témoins à l'année 2019. Les droits des individus ne sont donc pas respectés, pour la grande majorité du temps, par les entreprises.

S'ajoutant aux difficultés du contrôle des pratiques utilisées par les compagnies, les États et leurs citoyens doivent aussi faire face aux entreprises qui ont en quelque sorte perdu le contrôle de leurs données parce qu'elles sont mal gérées. Il y a donc un besoin à devoir démêler leurs procédés employés, leurs informations en leur possession, en plus de devoir trouver une solution aux

contraintes ajoutées par le GDPR. Dans la dénonciation suivante, se déroulant au sein de l'entreprise Facebook, l'informateur illustre que les données des utilisateurs sont en quelque sorte prises au sein d'un système quasi incontrôlable dû à l'approche d'analyse des informations choisies par l'entreprise.

> « We've built systems with open borders. The result of these open systems and open culture is well described with an analogy: Imagine you hold a bottle of ink in your hand. This bottle of ink is a mixture of all kinds of user data (3PD, 1PD, SCD, Europe, etc.) You pour that ink into a lake of water (our open data systems; our open culture) … and it flows … everywhere," the document read. "How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake? » (Franceschi-Bicchierai, 2022)

Les résultats inquiétants concernant ce manque de contrôle à long terme dans les pratiques de certaines des entreprises utilisant les données de masse, additionnées au chaos qui semble régner lorsque vient le temps du traitement de ces informations, participe à faire de cet espace un endroit hostile pour les droits et la vie privée des citoyens européens de façon plus générale.

> « We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation. » (Franceschi-Bicchierai, 2022)

La collecte des données et leur utilisation sont des enjeux problématiques persistants. C'est le manque de contrôle généralisé qui a perduré jusqu'à ce jour qui a eu un impact à long terme sur l'environnement actuel. La prise de conscience de ces impacts sur les modèles d'utilisation des données est une étape clé pour parvenir à répondre adéquatement aux besoins des citoyens en matière de respect de leurs droits.

4.2.3 Les pratiques commerciales des grandes entreprises du web et l'impact sur les acteurs

Les pratiques des entreprises et les divers modes opératoires choisis afin de collecter les données de navigation des utilisateurs sont un enjeu à prendre en compte si l'on cherche à revoir le fonctionnement de cet espace. La cueillette des données ne passe pas seulement par l'hébergeur du site visité et aux applications utilisées, mais aussi par l'emploi de différents types de traqueurs, de cookies[14] et de scripts afin de suivre les activités des internautes dans leur utilisation du Web ou lorsqu'ils utilisent leur téléphone (Grosbois, 2018). Aussi, pour les individus, de manière générale, il semble impossible de vivre dans notre société sans avoir recours aux services du Web directement ou indirectement. De s'émanciper du modèle d'affaires principal que l'on retrouve sur internet et de s'éloigner de ce réseau d'objets interconnectés, qui nous suivent à la trace, par le droit à la déconnexion et le droit à l'oubli demeure un défi majeur afin de réduire la vulnérabilité de tout un chacun (Grosbois, 2018).

La difficulté pour les individus à contrôler leur environnement technologique et les données qui circulent à leur propos puis qui les impactent directement dans leur quotidien ont un effet négatif pour nos sociétés. Il est important de prendre en compte que les algorithmes ne font pas qu'apprendre, ils évoluent aussi dans l'environnement dans lequel ils sont déployés et cherchent à illustrer un portrait qui peut être réel ou biaisé de cet environnement. Au fil de l'évolution de ces machines, celles-ci créent leurs propres biais par rapport aux éléments introduits lors du processus de création de cet instrument. Il devient ensuite difficile, voire impossible, pour un individu, surtout les personnes marginalisées, de se sortir de ce cadre d'analyse et de développer son identité propre à travers le temps (Leenes, 2018). Le besoin de sensibilisation sur les impacts des algorithmes et la nécessité d'imposition de mesures plus strictes de supervision impartiale sur les activités des algorithmes permettraient d'atténuer ces risques de dérive des technologies qui contrôlent notre quotidien.

[14] Il existe plusieurs types de cookies remplissant divers objectifs.

4.3 La souveraineté

Les impacts de l'adoption du GDPR sur l'enjeu de la souveraineté au sein de l'Union européenne ont été multiples pour les différents acteurs. Le thème de la souveraineté dans la question de la réappropriation de l'espace souverain numérique est particulièrement intéressant, compte tenu de l'aspect international qu'apporte l'interconnexion de cet espace. Du point de vue des Relations internationales, la souveraineté est ce qui définit l'essence même des États dans leur forme la plus primaire. Le contrôle des actions des acteurs par des politiques, voire par la force lorsque cela s'avère nécessaire pour faire respecter les règles en place, est essentiel. L'expansion des comportements allant à l'encontre de certaines valeurs européennes, facilitée par le capitalisme des données et l'évolution du rôle du Web dans nos vies, a atténué la souveraineté de l'UE et de ses États membres. La mise en place de mesures de contrôle plus strictes sur les comportements a permis aux pays membres de l'UE de prendre en main leur pouvoir de souveraineté sur les activités se déroulant sur leur territoire et ayant un impact direct sur leurs citoyens. Les effets de ces transformations dans la règlementation sur l'attitude des entreprises et la vision de ces derniers de manière générale sur l'évolution de cet espace ont permis une prise de conscience marquée sur l'importance de bien gérer les informations des utilisateurs en leur possession. « The less data you have, the less you have to lose. But data has been a commodity for many years, and only recently have companies started to learn that it is also a huge liability. » (Lapienyté, 2021b). Au sein du Web, les quantités astronomiques d'informations (Loiseau, 2017) et le faible contrôle exercé sur les entreprises du Web par les États quant à l'utilisation de ces données ont contribué au développement de cet environnement dans lequel nous nous situons. En réponse à cette croissance exponentielle d'acteurs malveillants dans cet espace, l'application de conséquences envers les entreprises qui exposent l'ensemble du système dû à une mauvaise gestion et des failles de sécurité liées aux données, transforme l'image qu'ont les compagnies des données de masse en quelque chose de plus que simplement des informations permettant la transmission de publicités vers des informations sensibles devant être protégées. Désormais, les entreprises sont plus conscientes de leurs devoirs et de leurs responsabilités envers les consommateurs et les États, même si celles-ci décident d'assumer ou non leurs devoirs envers ces derniers. L'établissement d'une vision collective des données en Europe et le désir de responsabilisation des actions des entreprises

établies par le règlement général sur la protection des données ont permis de rétablir un certain climat de confiance envers la classe politique afin de mieux gérer cet espace.

4.3.1 Impact des données de masse sur la souveraineté du système politique en place

Le fonctionnement de l'économie des données est principalement géré par quelques puissances qui chacune de leur côté favorisent leurs propres intérêts (Berthier, 2016; Deighton, 2015; Ciuriak, 2018c). Ciuriak décrit cette situation comme une sorte de force gravitationnelle où inévitablement, les plus petits acteurs sont contraints d'agir selon la volonté de ceux-ci. « Smaller economies are being pulled into the orbit of or another of the [the United States, the European Union and China]. » (Ciuriak, 2018c; Ciuriak, 2021). Souvent supérieurs à la puissance de certains États, les oligopoles des données ont ce même effet à travers le système. Ces compagnies souvent plus puissantes que bien des pays ont un fort potentiel à influencer le cours des choses. La montée en puissance d'entreprises des données, ayant à leur portée une source inépuisable d'informations sur nos actions et interactions, un capital financier dépassant celui de plusieurs pays, une grande capacité de faire du lobbying et fournir des contributions politiques, ainsi qu'une armée d'experts juristes (Grosbois, 2018 ; O'Neil 2016), leur permettent de créer une sorte de barrage permettant ainsi à tout le moins de ralentir considérablement les décisions allant à l'encontre de leurs positions, d'où la difficulté à appliquer ou pousser de l'avant des changements dans le mode de fonctionnement de cet espace. Ces transformations ne sont cependant pas impossibles. À travers cette évolution, l'application du concept de la gouvernementalité de Foucault à l'évolution du Web traduit bien cette évolution du cyberespace et l'extension du pouvoir des gouvernements vers les différents secteurs rattachés à cet espace. L'observation de l'emploi de moyens de contrôle dans le but d'établir ce droit de souveraineté étatique sur les pratiques des entreprises du Web trouve écho auprès des États qui ont la puissance pour faire face aux GAFAM(s). Pour l'Union européenne, l'unité du groupe d'États avec des valeurs et des idéologies communes donne une position de force face aux entreprises des données. « […] state as just one player among others and reveal the inability of states or transnational security organizations to act as the monopoly of force enforcing

preferred cyberspatial outcomes. » (Mueller, 2013). Ces changements, peu importe leur portée initiale, aussi faibles soient-ils, marque tout de même un tournant dans la gouvernance du Web. Il est cependant important de noter à travers l'analyse des tendances au sein de l'UE, dans la régulation des opérations en lien avec les données, qu'il y a une nécessité d'appliquer les mesures de contrôle du GDPR de manière concomitante entre les nombreux régulateurs de ce marché.

> « It is crucial to solidly embed the GDPR in the overall regulatory architecture that is being developed for the digital market. Not just for this proposal, but also concerning other legislative proposals, such as the Data Governance Act or the Digital Markets Act. A clear distribution of competences amongst the relevant regulators will need to be ensured, as well as efficient cooperation to avoid the risk of fragmented supervision, the establishment of a parallel set of rules and to ensure legal certainty for organisations and data subjects. — Présidente du Comité européen de protection des données » (EDPS, 2022)

Cette volonté introduite dans le GDPR de laisser aux États membres la possibilité de proposer et d'instaurer des mesures additionnelles dans le but de faire face aux défis et à l'évolution de ces dernières repose sur une étroite collaboration entre les divers partis pour en assurer le succès. Cette ouverture laisse la possibilité d'une collaboration avec les divers partis concernés afin d'accroître les chances de succès des politiques en place, car la gouvernance des données du Web nécessite la collaboration de chacun des groupes dans le but d'arriver à des solutions concrètes pour cet espace.

4.3.2 Analyse des positions et de l'évolution des discours des acteurs concernant l'enjeu de souveraineté

L'utilisation des données est un sujet polarisant pour les différents acteurs du milieu. Ceux qui sont sujets à la surveillance comme les utilisateurs favorisent généralement un environnement où il y a plus de contrôle sur l'utilisation des données et tendent à avoir une faible confiance envers les entreprises quant à la gestion de leurs informations. Pour leur part, les États tendent à percevoir ces entreprises comme des menaces à leur souveraineté due au fait qu'elles sont difficilement contrôlables due à leur taille et à leur puissance économique. Lorsque l'on fait l'analyse de

l'évolution de la position de pays membre de l'UE concernant l'enjeu de la souveraineté à travers le Web ou le contrôle des pratiques commerciales à travers le Web, le désir de réappropriation des pouvoirs décisionnels sur les comportements des différentes entités en harmonisant les lois sur les données à travers l'Europe transparaît à travers l'adoption du GDPR et représente un aspect important de l'évolution de cet espace pour les individus, le respect de leurs droits et mode opératoire des entreprises.

Cette réappropriation du pouvoir étatique est importante pour les États de l'UE et leurs citoyens, car après tout, les pays représentent les besoins et les désirs des citoyens et ne sont pas que de simples entités observatrices n'ayant aucun intérêt au sein de ces communautés. En référence à Rothschild, William définit cette relation et l'importance de prendre en compte cette relation pour les études critiques en sécurité : « But human beings are not the isolated, society-less, homo economicus of neoliberal theory. Rather, proponents of CSS recognize that although 'security is an objective of individuals', it 'can only be achieved in a collective political process' (Rothschild 1995: 70). » (Williams, 2004). La recherche d'une plus grande sécurité collective en tant que société par l'adoption de mesures permettant cette transition et dans le cas présent la réappropriation du pouvoir de gouvernance à travers le Web dans le but d'atteindre les objectifs de contrôle des pratiques commerciales des données, constitue un processus en soi qui permet l'émancipation des membres de ces communautés, c'est-à-dire les pays membres de l'UE. L'atteinte d'un plus grand contrôle sur les pratiques commerciales de cet environnement par l'adoption de politiques spécifiques définit la position des pays membres de l'UE et le changement de leur position initiale plus passive, et/ou la coercition n'était pas à l'avant-plan, marquant ainsi un virage important pour la souveraineté du groupe de pays. Cette prise de position ferme par le durcissement du ton avec l'adoption du GDPR visant directement les pratiques de cet écosystème des données et les comportements jugés abusifs des entreprises caractérise le désir du groupe d'États à instaurer sa dominance et son désir de reprendre pleine possession de son droit de gouvernance sur le Web sur le territoire de l'UE.

Le désir d'émancipation des citoyens européens des pratiques des entreprises du Web s'est opéré par l'adoption d'une position critique vis-à-vis les pratiques des entreprises du Web. La prise en puissance avec le temps d'un mouvement cherchant à faire respecter les droits des citoyens par l'utilisation du politique s'est fait entendre. Dans le but de résoudre la situation problématique, et

apporter un état de plus grande sécurité pour eux-mêmes et mettre de l'avant l'importance des droits des individus définit la position d'intérêt des citoyens et l'évolution de leur vision sur le sujet.

En ce qui concerne ceux qui dépendent des données pour assurer le succès de modèle d'affaires comme les médias sociaux, les moteurs de recherche, les outils d'analyse et de prédiction et les vendeurs de publicité supportent un environnement avec le moins de restrictions possible afin de favoriser le développement et l'innovation au sein de cet espace. La position réfractaire aux changements introduits par le GDPR représente assez fidèlement de manière générale la vision qu'ont les entreprises des données des changements de leur mode opératoire. Les contraintes introduites par le texte de loi obligent les entreprises à revoir leurs modes opératoires et contraignent leur pouvoir d'action à travers le Web. Dans le but de préserver une image positive avec les différents groupes, l'adoption d'une position plus ouverte est souvent mise de l'avant par ces différentes entreprises.

> « Considering this document does not describe our extensive processes and controls to comply with privacy regulations, it's simply inaccurate to conclude that it demonstrates the current measures we have in place to manage data and meet our obligations," — Porte-paroles de Facebook » (Franceschi-Bicchierai, 2022)

> « We continuously update our personal data protection practises to ensure we meet the needs and expectations of clients and regulators which are in constant evolution. — Porte-paroles d'Amazon » (Barthelemy, 2020)

> « People trust us to respect their right to privacy and keep them safe. We understand our responsibility to protect that trust and are committing to further changes and active work with the CNIL in light of this decision — Porte-paroles de Google » (Reuter, 2022b)

Ces positions publiques sont cependant souvent en opposition avec leurs actions dans cet espace. Nous pouvons penser aux nombreux cas où ces entreprises laissent planer des coupures de services dus à « l'impossibilité de se soumettre aux conditions en place » (Anonyme, 2022a) ou ils défient les règles en place et attendent de se faire prendre avant d'agir et modifier leurs méthodes (Dillet, 2022), contestant ainsi à leur manière le pouvoir décisionnel de l'UE. D'un autre côté, ces grandes

compagnies sont aussi capables de coopérer sur certains points et elles sont aussi en mesure d'apporter des éléments positifs pour cet espace. « Boniface et al. also found six of the largest tech companies (Google, Facebook, Microsoft, Instagram, Twitter, and LinkedIn) to handle personal data requests most securely and conveniently […]. » (Kretschmer, 2021). De plus, de nouvelles initiatives en faveur des droits des individus (Anonyme, 2022b; Ketchum, 2022; White, 2022) font leur apparition marquant ainsi un apaisement de leur position vis-à-vis les changements au sein de cet espace. Cette transformation offre une lueur d'espoir afin d'atteindre un plus grand respect pour la vie privée des citoyens.

CONCLUSION

Au cours de cette recherche, l'analyse d'enjeux clés pour l'Union européenne liés au cyberespace et aux données de masse m'a permis de mieux comprendre les différents facteurs d'influence qui ont incité l'UE à adopter une position plus stricte concernant l'utilisation de ces informations par les entreprises. Au moyen de la question de recherche, portant sur l'utilisation du GDPR par l'UE comme manière de réappropriation du pouvoir de gouvernance et les effets de ces changements dans l'écosystème du Web, nous avons analysé les impacts du règlement dans trois champs d'application distincts dans le but valider ou d'infirmer notre thèse. Les conséquences soulevées à la suite de l'introduction du GDPR offrent une perspective sur l'évolution de cet espace tout en exposant les impacts et la portée de ces changements sur les pratiques commerciales du Web. L'étude de la question dans une approche pragmatique à travers le prisme des études critiques en sécurité en Relations internationales nous a permis de mettre de l'avant les effets de ces transformations sur l'Union européenne dans une perspective axée sur les individus, la communauté et l'identité.

Dans le premier chapitre, il a été question de l'enjeu des données et l'environnement dans lequel celui-ci persistait. Pour ce faire, nous avons cerné la problématique entourant les comportements abusifs des entreprises avec les données des citoyens européens. Nous avons aussi regardé l'angle d'analyse du sujet et des thèmes principaux à l'étude. Nous avons par la suite défini en détail la problématique et la question de recherche en parlant des impacts du fonctionnement des activités commerciales des données pour l'UE. Après quoi, nous avons déterminé l'intérêt d'une telle recherche pour la science politique.

Au cours du second chapitre, nous avons regardé les impacts de l'utilisation de pratiques abusives envers les droits des citoyens. Pour cela, nous avons défini l'organisation de cet espace et les différentes composantes importantes qui influençaient directement le sujet. Notamment, nous avons regardé la place du capitalisme des données dans nos sociétés, son impact sur les différents acteurs, la place et l'importance des données dans nos vies. Les comportements des entreprises, ayant une puissance monopolistique grâce aux ressources politiques et financières à leurs

dispositions, ont démontré la nécessité pour l'UE d'agir en accord avec ses valeurs et ses besoins. Ensuite, il a été question du lien de dépendance entre les individus et les services quasi essentiels offerts par les grandes entreprises du Web. Nous avons parlé du besoin d'avoir un environnement interconnecté où les citoyens européens ne sont pas laissés à eux même afin de faire face aux conséquences négatives du système en place. De plus, l'éthique et le besoin de responsabilisation liés aux comportements des entreprises ont été discutés. En terminant, la nécessité d'adopter une position ouverte face aux enjeux vécus par chacun des acteurs nous a permis d'avoir une position plus compréhensive sur l'évolution de cet espace.

L'objectif du troisième chapitre était de mieux comprendre l'évolution du monde des données et les impacts des modèles d'affaires avant et après le GDPR sur les individus. Il a été question de la période où la montée fulgurante des technologies de traçage du Web a permis l'essor de l'économie basé sur la collecte des informations des individus. Nous avons par la suite mis en lumière les objectifs de l'adoption et de la mise en application du GDPR. Ensuite, nous avons mis en lumière les politiques clés du GDPR dans le but de faire face aux défis modernes du Web. Parmi ces politiques, il y a l'introduction de réglementations mieux définies, l'imposition de limites, l'imposition d'obligations et l'application de conséquences aux entreprises dans l'objectif d'accroître la responsabilisation de l'industrie. Nous avons conclu ce chapitre sur l'état de la situation post-GDPR par l'analyse de constatations sur les comportements des entreprises du Web, leur utilisation des données et les transformations observées à travers le Web en Europe.

Dans le chapitre quatre, il a été question des trois thèmes clés de cette recherche, c'est-à-dire la sécurité, les droits des individus et la gouvernance de l'UE. Dans chacun des secteurs, les constats d'analyse ont été multiples et ils ont permis de mieux comprendre l'impact direct du règlement général sur la protection des données en Europe.

Dans la première sous-catégorie, concernant la sécurité des pratiques, des individus et de cet espace de manière générale, à la question : « (1) de quelle manière la sécurité des individus au sein de cet espace s'est transformée depuis l'entrée en vigueur de la nouvelle réglementation ? ». Nous avons pu voir que la sécurité des individus au sein de cet espace s'est légèrement améliorée avec la récente législation. Des réductions de certains comportements nuisibles, l'adoption de meilleures pratiques de sécurité, une augmentation dans la transparence des activités marquent cette avancée pour

l'écosystème. Cependant, la difficulté d'atteindre les objectifs principalement, par les entreprises provenant de l'étranger et la lenteur dans les changements des comportements nuit au bilan de l'efficacité réelle du GDPR. Ces difficultés anticipées par certains (Safari, 2017) pour les petites entreprises ont également été perçues au niveau des grandes entreprises, mais à une échelle différente. Les petites entreprises sont principalement confrontées à des défis économiques, tandis que les grandes entreprises sont confrontées à la complexité de faire pivoter le navire du capitalisme des données, une tâche qui demande beaucoup de temps.

Dans le thème s'intéressant au respect des droits des citoyens, à la question : « (2) est-ce que les droits des citoyens ont été placés de l'avant grâce aux changements sur le plan politique au sein de l'UE ? ». En produisant une loi centrée sur les besoins de ses citoyens, l'UE montre sa volonté de faire la promotion du respect des droits constitutionnels de ces derniers contre les abus de pouvoir des entreprises du Web. En consacrant un chapitre complet du GDPR, la prise en considération et l'importance du respect des besoins de ces derniers se veulent primordiales dans les pratiques commerciales.

À l'égard de la gouvernance au sein de cet espace interconnecté, en ce qui concerne la question : « (3) l'adoption d'un cadre règlementaire plus strict pour les entreprises opérant avec les données de masses, a-t-il permis à l'Union européenne de retrouver un plus grand contrôle sur les actions des entreprises principalement étrangères à travers le Web ? ». Je serais d'avis que la gouvernance est l'aspect qui a subi la plus grande transformation entre les trois catégories analysées. Les pratiques commerciales du cyberespace en matière de données sont perçues par plusieurs comme étant dépassées et nécessitant d'être reconstruit sur de nouvelles bases (Liden, 2020), cependant, la prise de pouvoir des États membres de l'UE (bien que de manières non uniformes entre les différents membres) a permis à ceux-ci de retrouver un plus grand contrôle des pratiques à travers cet espace. Principalement attribuable au fait que le Web est en majorité dirigé par un petit groupe d'entreprises, la surveillance plus étroite de celles-ci permet une influence plus généralisée sur les pratiques à grande échelle. Aussi, l'influence précurseur du GDPR a permis l'adoption mondiale d'approches similaires dans le but de reprendre le contrôle de cet espace des mains des entreprises opérant dans le domaine des données de masse.

Il est possible de conclure que le GDPR a permis à l'Union européenne de se réapproprier une partie de ses pouvoirs de gouvernance au sein de cet espace. Les changements dans les pratiques commerciales d'un aussi grand marché prennent forme sur le long terme. Les objectifs ambitieux des nouvelles mesures en place ont créé un sentiment de déception pour certains biens que plusieurs améliorations ont pu être constatées. À court terme, les nouveaux standards en matière d'utilisation de données ont permis à l'UE de se démarquer vis-à-vis la communauté internationale particulièrement en ce qui concerne la volonté politique à modifier les méthodes de fonctionnement de cet espace. En termes d'efficacité réelle des mesures en place, les résultats n'étaient pas très convaincants en matière de pistage. La poursuite du suivi des activités des individus et le non-respect de leurs volontés en matière de pisteurs en témoigne (Sanchez-Rola, 2019; Trevisan, 2019). La volonté politique du groupe d'États a permis une prise de conscience majeure des défis et des besoins d'avoir une meilleure gestion des pratiques dans cet espace. Le GDPR a aussi influencé d'autres pays à travers le monde à entreprendre des démarches similaires dans le but de protéger leurs intérêts (Linden, 2020). À long terme, les mesures en place dans le GDPR offriront la possibilité d'adapter les politiques afin de corriger les problèmes persistants et transformer les pratiques du milieu en promouvant le développement de technologies et techniques qui soient plus respectueuses pour le cyberespace.

Les limites de cette recherche ont certainement influencé la quantité des informations disponibles et sur l'exactitude de la situation concernant les pratiques d'utilisation des données par les entreprises. Dans ces limites, il y avait l'accessibilité à certaines informations précises comme les pourcentages réels d'entreprises souscrivant aux règlements. En second lieu, il y a les débats concernant la conformité de certaines pratiques discutables et sur la validité des intentions des entreprises notamment dans le cas d'intérêt légitime pour les utilisateurs des pratiques de traitement de données. Il est normal et même nécessaire de remettre en question les intentions des entreprises dans l'utilisation des données, surtout quand ces mêmes entreprises demandent aux utilisateurs de renoncer à leur vie privée en quelque sorte (Andrejevic, 2014). Ensuite, la limite concerne l'évolution rapide des politiques et positions des différents acteurs au sein de cet espace. Malgré les circonstances de ces facteurs influençant la recherche, les informations sur l'état de la situation ont permis de brosser un portrait somme toute très fidèle à la réalité du terrain. Enfin, en ce qui concerne la dernière limite sur le choix d'approche à la question, un cadre théorique critique et

pragmatique cherchant à se concentrer sur un phénomène précis nous permet de mieux comprendre et expliquer les conséquences des décisions de l'UE en matière de réglementation des pratiques du Web (Cornut, 2014).

Les apports de cette recherche touchent principalement l'aspect gouvernance de cet espace et les conséquences de l'adoption de réglementation majeures sur la souveraineté de l'Union européenne. Cette question des impacts du GDPR sur la souveraineté se trouve aussi très peu étudiée à travers la science politique. Comme piste de recherche supplémentaire, il serait intéressant de comparer les résultats des changements sur le territoire de deux groupes ou États distincts dans l'objectif de voir si deux modèles ou sociétés distinctes arriveraient au même résultat quant aux comportements des acteurs vis-à-vis les changements politiques en matière de données.

ANNEXE A

Évolution historique de la réglementation de l'Union européenne sur la protection des données

10 janvier 2017

Deux nouveaux règlements (vie privée et communications électroniques) ainsi que sur la protection des données au sein des institutions européennes

La Commission européenne propose deux nouveaux règlements sur la vie privée et les communications électroniques (règlement «vie privée et communications électroniques») et sur les règles en matière de protection des données applicables aux institutions européennes [actuel règlement (CE) n° 45/2001] qui harmonisent les règles existantes avec le règlement général.

Lire plus

24 mai 2016

Le règlement entre en vigueur, vingt jours après sa publication au Journal officiel de l'Union européenne

Le saviez-vous?

Vos droits à la protection des données

- Le règlement général renforce un large éventail de droits existants et en confère de nouveaux aux personnes physiques.
  Ces derniers comprennent le droit à l'effacement (droit à l'oubli): vous pouvez demander à ce qu'une organisation efface les données à caractère personnel qu'elle détient vous concernant, par exemple lorsque vos données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou lorsque vous avez retiré votre consentement.

27 avril 2016

Règlement Général sur la Protection des Données

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

Lire plus

2 février 2016

Le groupe de travail «article 29» publie un plan d'action pour la mise en œuvre du règlement général.

Le saviez-vous?

Vos droits à la protection des données (suite)

- Le règlement général renforce un large éventail de droits existants et en confère de nouveaux aux personnes physiques, notamment :
- le droit à la portabilité des données: vous avez le droit de recevoir les données à caractère personnel vous concernant de la part d'une organisation dans un format couramment utilisé afin que vous puissiez les partager aisément avec d'autres personnes ;

Lire plus

15 décembre 2015

Le Parlement européen, le Conseil et la Commission sont parvenus à un accord sur le règlement général.

Le saviez-vous?

Transferts Internationaux de Données

- Le règlement général veille à ce que les droits et les protections conférés aux personnes physiques au sein de l'Union européenne soient conservés lorsque les données de ces derniers sont transférées vers un pays hors de l'Union.

Lire plus

27 juillet 2015

Recommandations de l'EDPS sur le texte final du GDPR

Le Contrôleur européen de la protection des données publie ses recommandations aux colégislateurs européens responsables de la négociation du texte final du règlement général sous la forme de suggestions d'ordre rédactionnel. Il lance également une application mobile permettant de comparer la proposition de la Commission avec les derniers textes du Parlement et du Conseil.

Lire plus

15 juin 2015

Le Conseil parvient à une orientation générale concernant le GDPR

Did you know

Le Comité Européen de la Protection des Données

12 mars 2014

Le Parlement européen adopte le GDPR

Avec 621 votes pour, 10 votes contre et 22 abstentions, le Parlement européen manifeste son ferme soutien au règlement général en séance plénière.

Lire plus

5 octobre 2012

Le groupe de travail «article 29» participe au débat sur la réforme de la protection des données.

Le groupe de travail «article 29» apporte une contribution supplémentaire au débat sur la réforme de la protection des données.

Lire plus

23 mars 2012

Le groupe de travail «article 29» adopte un avis sur la proposition de réforme de la protection des données.

Le groupe de travail «article 29» adopte un avis sur la proposition de réforme de la protection des données.

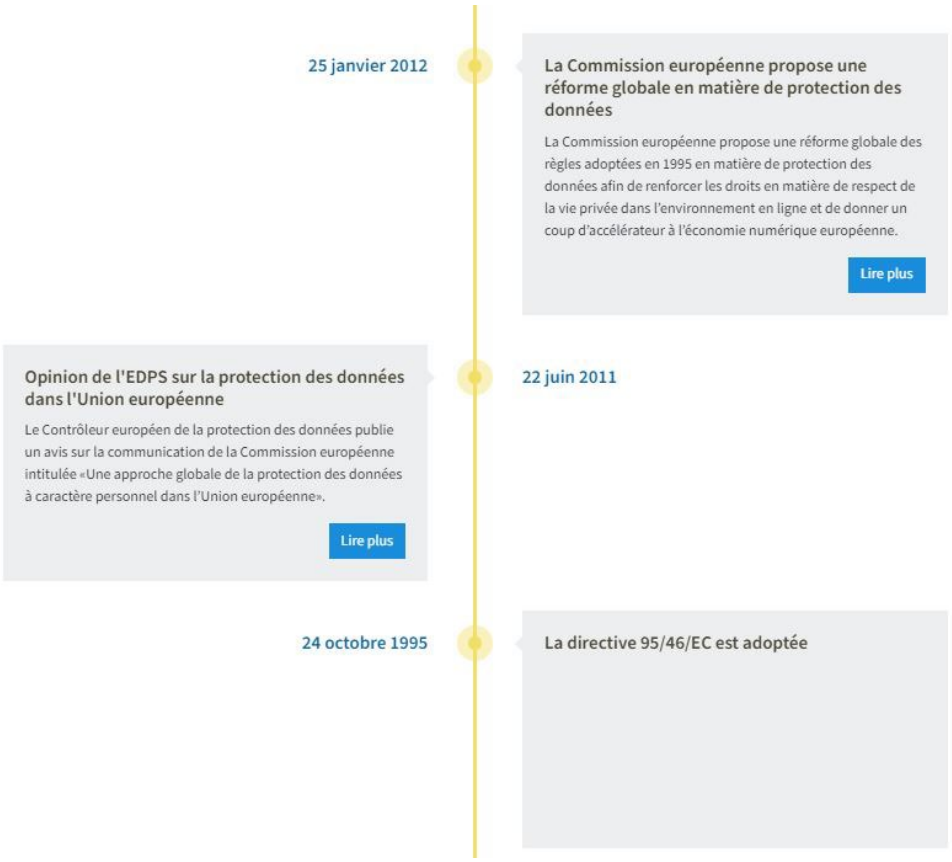
Lire plus

7 mars 2012

Le Contrôleur européen de la protection des données adopte un avis sur les réformes proposées par la Commission.

Le Contrôleur européen de la protection des données adopte un avis sur le train de réformes sur la protection des données proposé par la Commission.

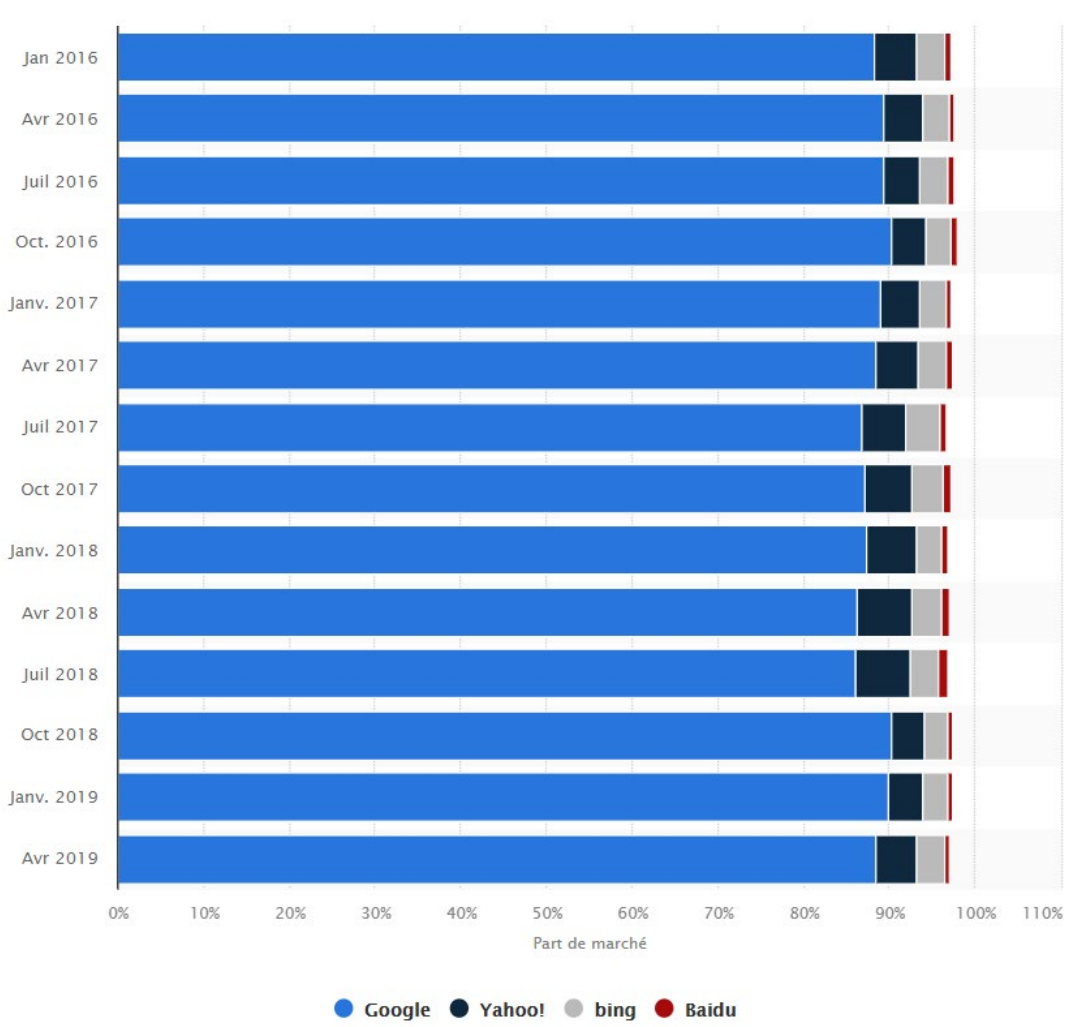
Lire plus



Source : European data protection supervisor (EDPS). « Évolution historique du règlement général sur la protection des données ». https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_fr.

ANNEXE B

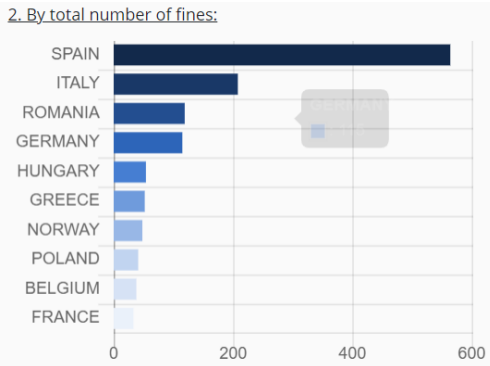
Part de marché mondiale des principaux moteurs de recherche de janvier 2010 à avril 2019



Source : Statista. (2019). « Part de marché mondiale des moteurs de recherche 2010-2019 ». https://fr.statista.com/statistiques/559394/part-de-marche-mondiale-des-moteurs-de-recherche-2010/

ANNEXE C

Countries with the highest fines by total number of fines [under GDPR]



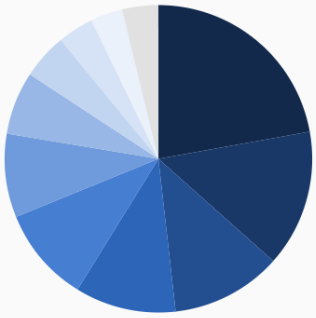
Country	Number of Fines
SPAIN	**564** (with total € 57,570,710)
ITALY	**208** (with total € 142,182,096)
ROMANIA	**119** (with total € 831,550)
GERMANY	**115** (with total € 54,741,853)
HUNGARY	**54** (with total € 1,750,761)
GREECE	**52** (with total € 30,464,000)
NORWAY	**48** (with total € 9,297,950)
POLAND	**41** (with total € 3,396,348)
BELGIUM	**38** (with total € 1,819,500)
FRANCE	**33** (with total € 293,419,300)

Source : GDPR Enforment Tracker. https://www.enforcementtracker.com/

ANNEXE D

Amendes par secteur, en fonction du nombre total d'amendes sous le GDPR

2. By total number of fines:



Sector	Number of Fines
Industry and Commerce	**328** (with total € 854,315,597)
Media, Telecoms and Broadcasting	**213** (with total € 1,688,555,541)
Public Sector and Education	**172** (with total € 23,798,763)
Individuals and Private Associations	**157** (with total € 1,599,196)
Finance, Insurance and Consulting	**148** (with total € 34,346,108)
Health Care	**130** (with total € 15,015,009)
Employment	**98** (with total € 48,112,677)
Transportation and Energy	**71** (with total € 86,485,214)
Not assigned	**56** (with total € 750,308)
Accomodation and Hospitalty	**50** (with total € 22,340,057)
Real Estate	**48** (with total € 2,579,210)
Unknown	**7** (with total € 51,040)
Property Owners Association	**1** (with total € 2,000)

Source : GDPR Enforment Tracker. https://www.enforcementtracker.com/

BIBLIOGRAPHIE

Livres, articles scientifiques, rapports, documents officiels et lois

Andrejevic, M., et Gates, K. (2014). « Big Data Surveillance: Introduction. », *Surveillance & Society*, vol. 12, no. 2, pp. 185–196. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/bds_ed

Andrew, J. et Baker, M. (2019). « The General Data Protection Regulation in the Age of surveillance Capitalism », Journal of Business Ethics, pp. 1-14.

Autorité de la concurrence et des marchés (AGMC). (2021). « Sanctions de 20 millions à Google et Apple pour utilisation des données des utilisateurs à des fins commerciales », Italy. https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150?fbclid=IwAR1dTr1FhT9D9U9kbqoSopvBr9rx7YjXlwm95o2r4tA4szHGXViADhnGjeg.

Balzacq, T. et al. (2016). « 'Securitization' Revisited: Theory and Cases ». *International Relations*, vol. 30, no. 4, pp. 494-531.

Baruh, L. et Popescu, M. (2017). « Big data analytics and the limits of privacy self-management », *New Media & Society*, vol. 19, no. 4, pp. 579–596.

Beauman, Z. et al. (2014). « After Snowden: Rethinking the Impact of Surveillance », *International Political Sociology*, vol. 8, no. 2, pp. 121-144.

Berthier, T. et Kempf, O. (2016). « Vers une géopolitique de la donnée », *Annales des Mines - Réalités industrielles*, vol. août 2016, no. 3, pp. 13-18. https://doi.org/10.3917/rindu1.163.0013

Bieresborn, D. (2019). « The Impact of the General Data Protection Regulation on Social Security », *Era Forum : Journal of the Academy of European Law*, vol. 20, no. 2, pp. 285–306. https://link.springer.com/article/10.1007/s12027-019-00565-x.

Bollinger, D. (2021). « Analyzing cookies compliance with the GDPR », Mémoire. ETH Zurich. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/477333/1/Bollinger_Dino.pdf.

Buzan, B. et Wæver, O. (2009). « Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory », *Review of International Studies*, vol. 35, no. 2, pp. 253–276.

Calzada, I. (2019). « Technological Sovereignty: Protecting Citizens' Digital Rights in the AI-driven and post-GDPR Algorithmic and City-Regional European Realm », no. 4, 17 pp. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415889

Charte des droits fondamentaux de l'Union Européenne (CDFUE), 2000/C 364/01, 2000. https://www.europarl.europa.eu/charter/pdf/text_fr.pdf.

Ciuriak, D. (2018a). « Digital Trade : Is Data Treaty-Ready? », CIGI Pappers, no. 162.

Ciuriak, D. (2018b). « The Economics of Data: Implications for the Data-Driven Economy », Chapitre 2 in *Data Governance in the Digital Age*, Centre for International Governance Innovation, 9 p. http://dx.doi.org/10.2139/ssrn.3118022

Ciuriak, D. et Ptashkina, M. (2018c). « The digital transformation and the transformation of international trade », RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank. 39 p. https://ssrn.com/abstract=3107811

Ciuriak D. (2021) « The Geopolitics of the Data-Driven Economy », 33 p. http://dx.doi.org/10.2139/ssrn.3770470

Collins, A. (2019). « Contemporary Security Studies », 5e ed., Oxford University Press, 560 p.

Commission européenne. (2020). « Incidence des données ouvertes ». https://data.europa.eu/fr/publications/open-data-impact#:~:text=Il%20s'agit%20de%20la,milliards%20d'euros%20en%202025

Commission Nationale de l'Information et des Libertés (CNIL). (2022). « Cookies : la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 millions d'euros pour non-respect de la loi ». https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions

Cornut, J., et Battistella, D. (2014). « Le Pragmatisme Problem-Driven ». *Les Excuses in. La Diplomatie Américaine: Pour Une Approche Pluraliste Des Relations Internationales*, Presses de l'Université de Montréal, pp. 31–44. *JSTOR*, http://www.jstor.org/stable/j.ctv69t972.5

Council of Europe (CoE). (2016). « Bureau of the consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data ». https://rm.coe.int/09000016806aafa7

Custers, B. et al. (2017). «Enabling big data applications for security: responsible by design», The Hague Centre for Strategic Studies. https://hcss.nl/report/enabling-big-data-applications-for-security-responsible-by-design/

D'Elia, D. (2014). « La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine », *Sécurité et stratégie*, vol. 19, no. 4, pp. 72-80.

Dabrowski, A. et al. (2019). « Measuring Cookies and Web Privacy in a Post-GDPR World », *Passive and Active Measurement*, vol. 11419, p.258 à 270. ISBN: 978-3-030-15985-6.

Danzig, R. J. (2014). « Surviving on a Diet of Poisoned Fruit, Reducing the National Security Risks of America's Cyber Dependencies », *Center for a New American Security*, 57 p.

De Grosbois, P. (2018). « Les batailles d'internet : Assauts et résistances à l'ère du capitalisme numérique », Écosociété, 264 p.

De Paepe, W. et al. (2018). « Seizing the GDPR advantage: From mandate to high-value opportunity », Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf

Degeling, M. et al. (2019). « We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy », Université du Michigan. https://arxiv.org/abs/1808.05096

Deighton, J. et Peter, J. A. (2015). « The value of data: Consequences for insight, innovation & efficiency in the U.S. economy », New York, NY: International Post Corporation, 26 p.

Desforges, A. et Déterville, E. (2014). « Lexique sur le cyberespace », *Hérodote*, vol. 1, no. 152-153, pp. 22-25.

Directive 95/46/CE, Parlement européen et du Conseil, 24 octobre 1995. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

Douzet, F. (2014). « La géopolitique pour comprendre le cyberespace », *Hérodote*, vol. 1, no. 152-153, pp. 3-21.

European Commission. « A European Strategy for data ». https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Court of Justice. (2015). « The Court of justice declares that the commission's US safe harbour decision is invalid ». PRESS RELEASE, No 117/15, Luxembourg, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

European data protection supervisor (EDPS). « Évolution historique du règlement général sur la protection des données ». https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_fr.

European Data Protection Supervisor (EDPS). (2021). « On the Proposal for a Digital Services Act ». https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

European Data Protection Supervisor (EDPS). (2022). « The EU's Data Act : data protection must prevail to empower data subjects ». https://edps.europa.eu/press-publications/press-news/press-releases/2022/eus-data-act-data-protection-must-prevail-empower_en

Fines, L. (2010). « Recherche qualitative et cyber-espace-temps : Crimes en col blanc et autres problématiques contemporaines », Presses de l'Université du Québec, 148 p.

Gashi, B. et Zendeli, F. (2016). « The impact of security and intelligence policy in the era of cyber crimes », *ILIRIA International Review*, vol. 6, no. 1, pp. 157-164.

Gaudiaut, T. (2021). « Le Big Bang du Big Data », Statista, https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde/

GDPR Enforment Tracker. https://www.enforcementtracker.com/

General Data Protection Regulation, (EU) 2016/679, 2018. https://gdpr-info.eu/

Goldin, I. et Mariathasan, M. (2014). « Infrastructure Risks », In. *The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It*, Princeton University Press, pp. 100-122.

Grondin, D., D'Aoust, A.-M. et Macleod A. (2010). « Les études en sécurité », Chapitre 22 in Théories des Relations internationales. Contestations et résistances, 2e édition, 662 p.

Hansen, L. (2012). « Reconstructing Desecuritisation: the normative-political in the Copenhagen School and directions for how to apply it ». *Review of International Studies*, vol. 38, no. 3, pp. 525-546.

Hantouche, C. (2016). « Peut-on sécuriser l'Internet des Objects ? », *Sécurité et stratégie*, vol. 22, no. 2, pp. 31-38.

Harknett, R. J. et Stever, J. A. (2011). « The New Policy World of Cybersecurity », *Public Administration Review*, vol. 71, no. 3, pp. 455-460.

Institut national de la statistique et des études économiques (Insee). (2022). « Accès et utilisation de l'internet dans l'Union européenne : Données annuelles de 2003 à 2021 ». https://www.insee.fr/fr/statistiques/2385835#graphique-figure1

Kleinwächter, W. (2021). « Cybersecurity, Internet Governance, and the multistakeholder Approach: The Role of the Non-State Actors in the Internet Policy Making. », Cyberstability Paper Series. https://cyberstability.org/paper-series/cybersecurity-internet-governance-and-the-multistakeholder-approach-the-role-of-non-state-actors-in-internet-policy-making/

Kokolakis, S. (2017). « Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon », *Computers & Security*, vol. 64, pp. 122–134.

Kretschmer, M., Pennekamp, J. et Wehrle, K. (2021). « Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. », *ACM Transactions on the Web (TWEB)*, vol. 15, no. 4, p. 1-42. https://doi.org/10.1145/3466722.

Leenes, R. (2015). « Data and Goliath: The hidden battles to collect your data and control your world », New York : W. W. Norton & Co., 383 p.

Leenes, R., et al. (2018) « Data Protection and Privacy : The Internet of Bodies », Edited by Ronald E Leenes et al., Hart Publishing, 344 p.

Letellier, A.-S. (2017). « Réseaux, libertés et contrôle : une généalogie politique d'internet », *Canadian Journal of Communication*, Toronto, vol. 42, no. 3, pp. 1-4.

Lewis, J. A. (2014). « Étude préliminaire sur les analyses en cybersécurité : l'affaire Snowden comme étude de cas », *Hérodote*, vol. 152-153, no. 1, pp. 26-34.

Li, H., Yu, L. et He, W. (2019). « The Impact of GDPR on Global Technology Development », Journal of *Global Information Technology Management*, vol. 22, no. 1, pp. 1-6. https://doi.org/10.1080/1097198X.2019.1569186

Linden, T. et al. (2020). « The Privacy Policy Landscape After the GDPR », Proceedings on Privacy Enhancing Technologies, pp. 47-64. En ligne. https://doi.org/10.48550/arXiv.1809.08396.

Loiseau, H. et Waldispuehl, E. (2017). « Cyberespace et science politique : De la méthode au terrain, du virtuel au réel », PUQ, 344 p.

Maciel-Hibbard, M. (2018). « Protection des données personnelles et cyber(in)sécurité », *Politique Étrangère*, vol. Été, no. 2, pp. 55-66.

Macleod, A. et O'Meara, D. (2010). « Théories des relations internationales: contestations et résistances », Montréal, CEPES, Athéna éditions.

Madden, M. et al. (2017). « Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans », *Washington University Law Review*, vol. 95, no. 1, pp. 53–125.

Mathias, G. (2018). « NIS : vers un cadre harmonisé pour la cybersécurité ? », *Sécurité globale*, vol. 15, no. 3, pp. 25-28.

Mueller, M., Schmidt A. et Kuerbis, B. (2013). « Internet Security and Networked Governance in International Relations », *Internationales Studies Review*, vol. 15, no. 1, pp. 86-104.

O'Neil, C. (2016). *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy*. Crown.

O'Neil, C. (2017). « Life in the Age of the Algorithm », *Science (New York, N.y.)*, vol. 355, no. 6321, 137 pp. https://doi.org/10.1126/science.aal2885

Pagallo, U. (2017). « The legal challenges of big data: Putting secondary rules first in the field of EU data protection », *European Data Protection Law Review*, vol. 3, no. 1, pp. 36–46.

Palmatier, R. W., et Martin, K. D. (2019). « The Intelligent Marketer's Guide to Data Privacy : The Impact of Big Data on Customer Trust », Palgrave Macmillan.

Peoples, C. et Vaughan-Williams, N. (2015). « Critical security studies: an introduction », 2e ed., Milton Park, Abingdon, Oxon ; New York, NY : Routledge, 226 p.

Quéméner, M. (2011). « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », *Sécurité et stratégie*, vol. 5, no. 1, pp. 56-67.

Quéméner, M. (2016). « La directive NIS, un texte majeur en matière de cybersécurité », *Sécurité et stratégie*, vol. 23, no. 3, pp. 50-56.

Ragot, S. Y. (2015). « Cyberespace, relations internationales et pays émergents : évolution ou révolution ? » Mémoire. Montréal (Québec, Canada), Université du Québec à Montréal. Maîtrise en science politique.

Safari, B. A. (2017). « Intangible Privacy Rights: How Europe's Gdpr Will Set a New Global Standard for Personal Data Protection », *Seton Hall Law Review*, vol. 47, no. 3, pp. 809–848.

Samarasinghe, N. et Mannan M. (2019). « Towards a global perspective on web tracking », Computers & Security, Vol. 87, No. 101569. https://doi.org/10.1016/j.cose.2019.101569

Sanchez-Rola, I. et al. (2019) « Can I opt out yet? GDPR and the global illusion of cookie control », In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, New York, p. 340-351. https://doi.org/10.1145/3321705.3329806

Singh, S. et al. (2015). « Doing Surveillance Studies (Part II): Critical Approaches to Methodology and Pedagogy », *Surveillance & Society*, vol. 13, no. 1, pp. 1–3. https://doi.org/10.24908/ss.v13i1.5581

Soria-Comas, J. et Domingo-Ferrer, J. (2016). « Big data privacy: Challenges to privacy principles and models », *Data Science and Engineering*, vol. 1, no. 1, pp. 21–28.

Statista. (2019). « Part de marché mondiale des moteurs de recherche 2010-2019 ». https://fr.statista.com/statistiques/559394/part-de-marche-mondiale-des-moteurs-de-recherche-2010/

Thatcher, J., et al., editors. (2018). « Thinking Big Data in Geography : New Regimes, New Research », University of Nebraska Press.

Torra, V. et Navarro-Arribas, G. (2014). « Data Privacy », *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 4, no. 4, pp. 269–280. https://doi.org/10.1002/widm.1129

Trevisan, M. et al. (2019). « Uncovering the Flop of the EU Cookie Law », Proceedings on Privacy Enhancing Technologies Symposium, Vol. 2019, No. 2, p. 126-145. https://doi.org/10.2478%2Fpopets-2019-0023

Waever, O. (2011). « Politics, security, theory », *Security Dialogue*, vol. 42, no. 4-5, pp. 465-480.

West, S. M. (2019). « Data Capitalism: Redefining the Logics of Surveillance and Privacy », *Business and Society*, vol. 58, no. 1, pp. 20–41. https://doi.org/10.1177/0007650317718185

White House. (2012). « Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy », Journal of Privacy and Confidentiality, vol. 4, no. 2. https://journalprivacyconfidentiality.org/index.php/jpc/article/view/623/606

Wigan, M. R. et Clarke, R. (2013). « Big Data's Big Unintended Consequences », Computer, vol. 46, no. 6, pp. 46-53. https://doi.org/10.1109/MC.2013.195

Williams, P. (2004). «Critical Security Studies », In. *International Society and its Critics*, Oxford, p. 135-150. https://doi.org/10.1093/0199265208.003.0008

Zarsky, T. (2016). « Incompatible: The GDPR in the age of big data », *Seton Hall Law Review*, vol. 47, no. 4, pp. 995–1020.

Zuboff, S. (2019). « The age of surveillance capitalism : the fight for a human future at the new frontier of power », New York : PublicAffairs, 691 p.

Articles techniques et publications spécialisées

EDRi. (2019). « EDPB confirms : Privacy Shield is still a shame ». https://edri.org/our-work/edpb-confirms-privacy-shield-is-still-a-shame/

Iwańska, K. (2020). « New report : To track or not to track? Towards privacy-frinedly and sustainable online advertising », Panoptykon Foundation. https://en.panoptykon.org/privacy-friendly-advertising

Naranjo, D. et Penfrat, J. (2021). « Surveillance-based advertising : An industry broken by design and by default ». https://edri.org/our-work/surveillance-based-advertising-an-industry-broken-by-design-and-by-default/

Szymielewicz, K. et Budington, B. (2018). « The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers », Electronic Frontier Foundation. https://www.eff.org/fr/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers

Tielemans, J. (2021). « EU officials reach Data Governance Act agreement », iapp. https://iapp.org/news/a/eu-officials-reach-data-governance-act-agreement/?fbclid=IwAR0S6fLPqkrh-S5QDyz9UaFWWlSDafI6o4Am3a49_Z-5EG6n8zTSSD19l6o

Tielemans, J. et Jungyun, S. C. (2020). « Proposal for an EU data governance Act – a first analysis », iapp. https://iapp.org/news/a/proposal-for-an-eu-data-governance-act-a-first-analysis/?fbclid=IwAR3k3yv7gihX-p0ldwLYoO2aIkPN0TstuFd2xxM19jkYiyKnievgP2t_LpM

Article de journaux non scientifique, magazines et Blogs

Anonyme. (2022a). « En difficulté sur les données personnelles, Facebook fait planer une menace fictive de fermeture en Europe ». Le Monde. https://www.lemonde.fr/pixels/article/2022/02/07/en-difficulte-sur-les-donnees-personnelles-facebook-fait-planer-une-menace-fictive-de-fermeture-en-europe_6112678_4408996.html?fbclid=IwAR0GyaE-HTeUBxa56jg6t4K_uloctH_8XXoj_DQv-6RWggq9Lz32vbCQpvI

Anonyme. (2022b). « Microsoft Privacy Report », Microsoft. https://privacy.microsoft.com/en-US/privacy-report

Barthelemy, L. (2020). « France Fines Google, Amazon 135 Mn Euros ». Barron's. https://www.barrons.com/news/france-fines-google-amazon-135-mn-euros-01607598604?fbclid=IwAR24mOcf4nYoVLvDjnkzsHgnKnnCQwanDP97V5mp8Uwvfo8kPKiT5vTmp74

Dillet, R. (2022). « Google to update cookie consent banner in Europe following fine », Techcrunch. https://techcrunch.com/2022/04/21/google-to-update-cookie-consent-banner-in-europe-following-fine/.

Franceschi-Bicchierai, L. (2022). « Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document », Vice. https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

Grim, R. (2021). « What Amazon and Facebook get wrong about FTC Chair Lina Khan », TheIntercept. https://theintercept.com/2021/07/18/what-amazon-and-facebook-get-wrong-about-ftc-chair-lina-khan/?fbclid=IwAR3quggeTKo0_78z9TcJJ5JUIwDyHhN21whk4a5lOLiFWHLgNP-uDZU3oM4

Ketchum, R. (2022). « Some facts about Google Analytics data privacy », Google. https://blog.google/around-the-globe/google-europe/google-analytics-facts/

Lapienyté, J. (2021a). « EU states reach an agreement on ePrivacy reform. Here's what worries privacy advocates », CyberNews. https://cybernews.com/news/eu-states-reach-an-agreement-on-eprivacy-reform-heres-what-worries-privacy-advocates/?fbclid=IwAR3aivxHHX_CYSULl0ZEzOxNy296pm8vR7S2aXjOrFB2-nZjQ9vUF7tuRAs.

Lapienyté, J. (2021b). « Privacy expert : most enterprises don't know where their sensitive data is », CyberNews. https://cybernews.com/privacy/privacy-expert-most-enterprises-dont-know-where-their-sensitive-data-is/?fbclid=IwAR3D4ytUGI1HmPQmACOnfUfS1UgIHKLLgvfdbPLPDZvLw0-UIBWeBIppmlo

Lapienyté, J. (2021c). « UK regulator : users are losing out because of Apple and Google's duopoly », CyberNews. https://cybernews.com/news/uk-regulator-users-are-losing-out-because-of-apple-and-googles-duopoly/?fbclid=IwAR0OPE74OitG1UUdwnrA6iPXKmr-aWE8XmbzRVgDzo_vOSvgfkWuQ0xkmM8

Manancourt, V. (2021). « Despite EU court rulings, Facebook says US is safe to receive Europeans' data », Politico. https://www.politico.eu/article/despite-eu-court-ruling-facebook-says-us-is-safe-to-receive-europeans-data/

Manceau, G. (2022). « Rapport d'activité : L'état d'internet en France », Tome 3, République française, Édition 2022. https://www.01net.com/actualites/netflix-occupe-une-part-hallucinante-du-trafic-internet-en-france.html.

Reuters. (2021). « Apple warns of cybercrime risks if EU forces it to allow others' software ». CyberNews. https://cybernews.com/news/apple-warns-of-cybercrime-risks-if-eu-forces-it-to-allow-others-software/?fbclid=IwAR1kglQxKNrkyltxxR3HKglJ2g2riNOXkAPCZ1gH94gIGuWyFdxa8XPI5SM

Reuters. (2022a). « French watchdog says Google Analytics poses data privacy risks ». CyberNews. https://cybernews.com/news/french-watchdog-says-google-analytics-poses-data-privacy-risks/?fbclid=IwAR0ZTz0PAZ612P_1aQpDPziyzpFcCY1JtVbPHAV2_c46UyM3ln4ScbCqWwc

Reuters. (2022b). « Google hit with 150 million euro French fine for cookie breaches ». CyberNews. https://cybernews.com/news/google-hit-with-150-million-euro-french-fine-for-cookie-breaches/?fbclid=IwAR0fZMwOT_-B1MEwkCfkStIgH9Xh4sut3m0DNZRWKXTw6THcRe-G4m2Klh4

Romain, D. (2022). « A new Search tool to help control your online presence », Google. https://blog.google/products/search/a-new-search-tool-to-help-control-your-online-presence/

Stokel-Walker, C. (2022). « GDPR fines topped 1 billion last year ». CyberNews. https://cybernews.com/privacy/gdpr-fines-topped-1-billion-eur-last-year/?fbclid=IwAR2hFGQf3DsOYDutROZmmvqiHVm8rvXFynG1xdhLbvVNZi1q_uaj4pO1NRo

Sullivan, L. (2021). « Google Patent Describes How its technology Authorizes transfer of Data Without Cookies », MarketingDaily. https://www.mediapost.com/publications/article/369847/google-patent-describes-how-its-technology-authori.html?fbclid=IwAR1dTr1FhT9D9U9kbqoSopvBr9rx7YjXlwm95o2r4tA4szHGXViADhnGjeg

Walker, K. (2022). « It's time for a new EU-US data transfert framework », Google. https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/

White, A. (2022). « Advertisers Demand Antitrust Probe of Google's Ad-Tracking », Bloomberg. https://www.bloomberg.com/news/articles/2022-02-01/advertisers-demand-antitrust-probe-of-google-s-ad-tracking