UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

MASTER 2 DROIT COMPARÉ DES AFFAIRES

DIRIGÉ PAR MADAME LE PROFESSEUR MARIE GORÉ

2020-2021

Data et droit de la concurrence : États-Unis et Europe

Claire REYNAUD

Sous la direction de Monsieur le Professeur Laurent Benzoni

Séjour de recherche effectué à l'Université de Columbia

AVERTISSEMENT

La Faculté n'entend donner aucune approbation, ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

J’adresse mes plus sincères remerciements,

A Monsieur le Professeur Laurent Benzoni pour son suivi bienveillant, ses précieux conseils et son expertise académique,

Madame la Professeur Marie Goré ainsi que toute l’équipe administrative de l’Institut de Droit Comparé pour cette année enrichissante,

A mes parents pour m’avoir accompagné tout au long de mon parcours universitaire.

TABLE DES ABRÉVIATIONS

GAFA : Google Apple Facebook Amazon
CNIL : Commission nationale de l'informatique et des libertés
RGPD : Règlement général sur la protection des données
DSA : Digital Service Act
DMA : Digital Market Act
DoJ : Department of Justice
FTC : Federal Trade Commission
MIT : Massachusetts Institute of Technology
API : Application Programming Interface
SMS : Short Message Service
CP : Content Provider
FIP : Fair Information Practices

SOMMAIRE

INTRODUCTION

"In a lot of ways Facebook is more like a government than a traditional company"[1]
Mark Zuckerberg

Cette citation fait état du pouvoir inédit que dispose les plateformes numériques, plus communément les GAFAM – étant des plateformes très différentes entre elles - depuis quelques années. La situation actuelle est analogue à la période dorée qui a fait suite à la guerre de Sécession avec le monopole de la Standard Oil Company. Depuis son lancement en 2008, Facebook a pu cumuler plus de 2,85 milliards d'utilisateurs et a racheté Instagram puis Whatsapp. Il a également évincé son plus grand concurrent de l'époque à savoir Myspace. Aujourd'hui sa capitalisation boursière dépasse les 1000 milliards de dollars. Le résultat de cette hyperpuissance est problématique. Facebook est une application gratuite. C'est un bien numérique caractérisé comme non rival et non exclusif c'est-à-dire que le nombre d'utilisateurs n'est pas limité avec une utilisation simultanée. Le coût marginal de production est proche de zéro et les couts fixes parfois élevés. Cependant les coûts de transactions sont faibles voire nuls. Le caractère gratuit du service facilite l'accessibilité, sans discrimination à condition de renseigner certaines données personnelles et d'accepter qu'elles soient par la suite collectées, vendues et partagées. Sa gratuité en fait à la fois un produit original puisque la concurrence se base souvent sur des produits qui ont un prix mais à la fois dangereux car l'utilisation n'est pas toujours bien maitrisée. C'est donc l'exploitation des données personnelles qui est au cœur des pratiques anti-concurrentielles, elles sont les matières premières des nouvelles technologies. Cependant leur exploitation doit se faire de manière responsable. Seulement l'utilisateur est en interaction, au sein d'un cadre, avec ses amis mais également le monde virtuel : celui de la publicité. Lui-même se retrouve victime de sa propre utilisation puisqu'il va se retrouver « cibler » par des algorithmes.

Toutes les valeurs prônées par les entreprises de la Silicon Valley sont celles des années 60. Les entreprises de la Big Tech se présentent comme étant des plateformes pour la liberté

[1] *"Utilities for democracy: Why and how the algorithmic infrastructure of Facebook and Google"*, Josh Simons, Dipayan Ghosh, August 2020, Brookings.

personnelle. Tout le monde a le droit de dire ce qu'il pense sur les réseaux sociaux, tout le monde peut exprimer son individualité. Là où la télévision a fait des téléspectateurs, Facebook a créé des utilisateurs. C'est une plateforme participative, qui rend les gens propriétaire de leurs idées. Il y a des parties dans le monde où Facebook fédère, que ce soit aux États-Unis ou au Cambodge, il permet aux citoyens de s'organiser dans l'opposition du pouvoir. Facebook est en réalité un ensemble de règles, de procédures, d'algorithmes fait pour extraire la moindre information. Et ces informations ne vont profiter qu'à l'entreprise elle-même.

Les réformes apparaissent alors nécessaires tant au niveau des libertés fondamentales mais également économiques. Aux États-Unis, fort est de constater que certaines règles sont encore anciennes concernant le droit de la concurrence. La difficulté de réguler s'explique par les diverses stratégies menées par les plateformes. L'histoire de l'entrée sur le marché de Facebook et l'évolution de sa surveillance commerciale soulève un autre problème en droit de la concurrence. Conformément à la Section 2 du Sherman Act, il est illégal pour une entreprise d'acquérir le pouvoir du monopole en engageant une conduite à l'extérieur des barrières de mérites de la concurrence.

De quelle manière le principe de technologie inhérente au monde digital dont la liberté en est la norme peut être régulé ? De quelle manière les législations des États-Unis et de l'Europe œuvrent elles à leur régulation ?

PARTIE 1 : Les données, source de pouvoir de marché

Facebook. Dans le cadre de ce mémoire de recherche, il s'agira d'évoquer la relation entre les données personnelles et le droit de la concurrence en s'appuyant sur le cas de Facebook. Dans l'écosystème digital, les données sont considérées comme étant une matière première centrale des *business* modèles. Cette première partie examine les différentes exploitations des données personnelles, la façon dont elles peuvent représenter une entrave à la concurrence mais aussi à la sécurité des utilisateurs.

Titre I : Le contrôle des données

Dans les analyses concurrentielles, il est nécessaire de définir le marché pertinent pour délimiter l'objet d'étude. Il s'agira de s'intéresser aux données de manière générale ; qu'elles soient personnelles ou non. Leur collecte étant devenue systématique, elles sont devenues un objet difficilement saisissable. Est-ce un « bien », une « information », « une monnaie d'échange » ?

Chapitre I : Le rôle des données personnelles dans l'analyse concurrentielle

« Il n'y a rien de plus collectif qu'une donnée personnelle »[2]

D'après l'article 4 du Règlement général sur la protection des données, les données personnelles sont *« toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »*[3]

Les données personnelles concernent donc des informations privées, que l'on imagine mal partager avec des tiers inconnus. Elles peuvent *« fournir des informations sur des individus, des*

[2] Casilli & Tubaro, 2018
[3] RGPD

entités économiques ou des objets ; elles peuvent par exemple révéler des informations sur le comportement, les préférences ou la localisation géographiques des personnes, sur le volume d'affaires réalisé par une entreprise avec certaines transactions, ou enfin sur la localisation et la vitesse d'une voiture à un moment donné. »[4].

Section I : Le marché pertinent des données personnelles

Le traitement des données personnelles existe depuis plus de quarante ans en France. Il existe également depuis 2018 en Europe à travers le Règlement général des données personnelles. On génère des données à longueur de journée, que ce soit l'usage d'une application, la visite d'un site. L'Union Européenne, à travers le RGPD, a pu influencer des décisions de juridictions dans des États américains comme la Californie.

Il faut replacer la donnée dans une vision plus large c'est-à-dire qu'elle correspond à la personne et à sa vie privée. La jurisprudence a établi que le lien entre l'utilisateur à une plateforme était un contrat de consommation faisant fi du caractère gratuit du réseau social. Cependant toutes les données personnelles ne relèvent pas de la vie privée. La vie privée est entrée dans la loi française à l'article 9 du Code civil en 1970 à, la notion de vie privée n'existait pas. C'était totalement inconnu en droit français. C'est en 1999 que le Conseil Constitutionnel a consacré la vie privée en tant que condition indispensable à la liberté. Ainsi elle se rattache aux droits de l'homme qui sont placés au-dessus de la Constitution.

En 2006, la Charte des droits fondamentaux a classé la vie privée comme un droit fondamental ce qui risque de poser des problèmes du point de vue pratique. C'est sur la Charte que le Droit européen a construit l'ensemble des droits subjectifs des personnes s'opposant aux droits objectifs (ensemble des règles de droit). Chaque arrêt de la CJUE cite le texte de la Charte des droits fondamentaux.

Responsabilité du traitement. C'est la plateforme qui est responsable puisque c'est elle qui devient propriétaire des données. Il y a une véritable appropriation des informations. Si les plateformes décident d'utiliser les données personnelles, on ne sait pas directement ce qu'elles

[4] Autorité de la concurrence, « Droit de la concurrence et données »

vont en faire et comment elles vont le faire. Madame la Professeure Marie Anne Frison-Roche décrit ces données comme des « *métadonnées, en ce qu'elles permettent une transfiguration de la statistique à partir des informations sur le passé pour en tirer des conclusions sur le futur, pourraient conduire juridiquement des entreprises à prétendre être « propriétaires du futur » des personnes et à le vendre »*[5]. Elle insiste sur l'importance de ne pas laisser une autonomie trop importante aux données, c'est-à-dire de ne pas les couper de la personne à qui elles ont été extraite. Considérer la donnée comme extraite de la personne c'est la considérer dans la continuité du sujet de droit. Si on lui laisse une trop grande autonomie alors ceux qui vont en devenir propriétaires pourront en disposer à leur guise. Car la propriété emporte le droit de jouir, d'utiliser, de disposer et de léguer les biens que l'on a acquis selon l'article 17 de la Charte des droits fondamentaux de l'Union européenne.

Le règlement RGPD a permis de réguler le monde des données. Il l'a fait par le droit de la compliance qui est un droit se fixant une fin. Il a replacé la personne dans le contexte du numérique et en cela il devient un modèle.
L'arrêt de la Cour de Justice de l'Union Européenne *Schrems* du 6 octobre 2015 a attribué à la donnée deux caractéristiques principales qui lient la personne à la donnée : c'est l'information et l'objet de l'information qui est pertinente. C'est l'objet qui « colore l'information, laquelle colore la donnée »[6] et ce, même si la donnée est abstraite. Les données concernant les personnes ne sont pas cessibles en masse et sans consentement des personnes. Cette jurisprudence de la CJUE s'inscrit dans la même perspective que celle datant de 2014 *Google Spain*, laquelle pose que lorsqu'une personne est « concernée » dans un évènement de sa vie privée couvert par la prescription, alors la donnée n'est plus « trouvable ».

Sous traitement. Il y a plusieurs étapes et donc plusieurs acteurs. Le sous traitement c'est celui qui traite les données. Google par exemple est un sous-traitant : il stocke mais ne touche pas les données. Les obligations vont tomber sur les épaules du responsable, c'est lui qui aura des sanctions (prévues dans le RGPD 20 millions d'euros, ou bien 4% du chiffre d'affaires mondiale). La CNIL a imposé 60 millions d'euros d'amende à Google pour avoir manqué à la loi Informatique et Libertés.

---

[5] Marie Anne Frison-Roche, *L'apport du droit de la compliance à la gouvernance d'internet,* Rapport commandé par Monsieur le Ministre en charge du Numérique, Avril 2019
[6] *Ibid*

La sanction pénale française correspond à cinq ans de prison et 300 000€ d'amende. Aucun juge n'a encore infligé une telle peine. Le problème des données aujourd'hui c'est qu'elles sont connectées. Et une donnée nous concernant concerne aussi nos amis, les personnes avec qui nous avons interagi.

Les étapes d'exploitation des données. Il existe trois étapes à l'exploitation des data. Premièrement, les données personnelles vont être captées par des *« data brokers »,* des courtiers en données. Ce sont eux qui vont vendre des données à d'autres entreprises. Elles sont ensuite transformées afin d'être économiquement exploitable (smart data) et enfin être revendues et utiliser l'information dans le cadre d'algorithmes, de moteurs de recherches ou de publicité ciblée[7]. Juridiquement, ces transactions sont légales. Même si les utilisateurs ne sont pas toujours conscients des utilisations successives et l'enregistrement massif qu'il en est fait.

Section II : Interopérabilité, portabilité des données et coûts de transfert

Dans cette section, il s'agira d'aborder les opérations de données et leurs conséquences dans la concurrence.

La portabilité des données permet aux utilisateurs de télécharger instantanément leurs données qui ont été stockées numériquement. Les responsables de traitement doivent donc s'assurer que les données recueillies par leur système que ce soit sur les réseaux sociaux, sur les plateformes ou même sur des appareils connectés pourront par la suite assurer le portage et la transmission de données à l'intéressé. Deuxièmement, elle permet à un autre responsable de traitement de recevoir les données personnelles. Depuis 2010, Facebook a rendu possible aux utilisateurs de télécharger leurs propres données.[8]

La portabilité des données personnelles est l'un des principes majeurs du RGPD qui apparait ardus à mettre en œuvre, surtout pour les petites et moyennes entreprises. Cette portabilité apparait comme étant profitable du côté de l'utilisateur, elle l'est tout autant pour la plateforme.

---

[7] J. Hagel et M. Singer, « Net Worth: Shaping Markets when Customers Make the Rules », *Harvard Business School Press*, 8 Janvier 1999

[8] Matthew Rogers, *Facebook to Allow Users to Download Their Data* (Oct. 7, 2010)

En effet, si l'utilisateur peut avoir accès à ses données, la plateforme pourra également les manipuler et des personnes tierces pourront également en profiter notamment avec le ciblage publicitaire.

Le véritable enjeu de la portabilité des données est qu'il réduit les coûts de transfert et permet à de nouveaux produits entrants substituables aux produits déjà existants de présenter des coûts plus compétitifs et de ce fait accroit la concurrence. Si l'on prend l'exemple du *« one off export portability »* qui est d'ailleurs exigé au sein du RGPD, les consommateurs peuvent télécharger leurs données personnelles venant d'une plateforme numérique et les transférer vers un autre fournisseur de service. L'interopérabilité réduit encore plus les coûts de transferts puisqu'elle permet un transfert encore plus rapide et plus flexible.

L'interopérabilité est un type de données qui permet à deux ou plusieurs fournisseurs de services d'échanger les utilisateurs et les informations directement entre eux et autant que possible. Les données sont souvent échangées à travers des protocoles appelés APIs. L'interopérabilité peut être horizontale et de ce fait partagé entre des services en concurrence ou bien verticale en connectant des services complémentaires. Elle peut être influencée par des considérations technologique et légale. Elle permet des transactions et des informations moins coûteuses, booste l'innovation et la concurrence et offre un plus grand choix aux consommateurs. Chaque entreprise se positionne selon son propre degré d'offre d'interopérabilité et c'est au consommateur de faire le choix entre ce qui est plus ouvert et flexible ou plus fermé et potentiellement moins risqué au niveau de la sécurité et donc plus fiable. Cependant, dans un marché ou seulement quelques entreprises dominantes existent grâce à un monopole naturel, la concurrence peut ne pas générer d'interopérabilités très efficaces.

Les coûts de transfert. Une plateforme qui limite l'interopérabilité et la portabilité conduit à l'augmentation des coûts de transfert. Ces coûts peuvent limiter la faculté d'un consommateur de substituer entre des compétiteurs sur un marché. A terme, cela peut créer potentiellement une situation monopolistique ou les entreprises ont un pouvoir de marché et peuvent augmenter le prix au-dessus duquel il aurait dû se trouver sans la présence de coûts de transfert.

Par exemple, si un consommateur voulait changer de compte d'une banque à une autre, il devrait peut-être dépenser un temps considérable pour réaffecter ses comptes de débits et de crédits dans de nouveaux comptes.

Si les coûts de transferts sont suffisamment élevés, un consommateur peut être cadenassé dans une banque même si un concurrent propose des prix plus attractifs. La théorie économique a donc montré que les coûts de transferts rendaient les marchés beaucoup moins compétitifs.[9]

Si l'on prend le cas de Facebook, la FTC dans sa plainte opposée aux pratiques anticoncurrentielles de l'entreprise, a indiqué que les utilisateurs prenaient un temps relativement long pour construire leur réseau. Aussi, d'autres réseaux sociaux ne sont pas interopérables avec Facebook.[10]

Le rapport a conclu que cela conduisait à un « locking in » des utilisateurs de Facebook. Les prix de transferts isolent la plateforme de la concurrence. De plus, les utilisateurs ont la possibilité de télécharger leurs données personnelles seulement dans des formats limités. Dans leur condamnation, la FTC et le State attorney général ont cité l'interopérabilité comme étant directement liée aux pratiques anticoncurrentielles de la plateforme même si les plaintes mettent plus en avant les acquisitions des concurrents (WhatsApp et Instagram).

Plus spécifiquement, les poursuites mettent en lumière l'utilisation des APIs à travers lesquelles les applications tierces accèdent aux données personnelles des utilisateurs. En effet, Facebook aurait initialement encouragé les développeurs à créer des applications et des outils interopérant avec Facebook, ce qui conduirait à sa domination. Facebook aurait alors changé sa politique afin d'admettre uniquement l'accès des APIs à des applications tierces si elles ne concurrençaient pas les caractéristiques de Facebook ou si elle ne faisait pas de la publicité pour des concurrents de Facebook.

« September 2012 : no exporting data to competitor social networks. On September 12, 2012, Facebook introduced a new policy: "Competing social networks: You [developers] may not use Facebook Platform to export user data into a competing social network without our permission[...]"[11]

[9] M.Motto, *Competitive Policy : Theory and Practice* (Cambridge University Press, 2004)
[10] House Report, p 144
[11] FTC redacted complaint Case 1:20-cv-03590-JEB Document 51 Filed 01/13/21 Page 44 of 53)

C'est donc la preuve d'une restriction à l'accès des applications et de ce fait une restriction de l'interopérabilité puisque Facebook identifie exactement ceux qui lui font de l'ombre.
Ainsi les logiciels initiés par les développeurs empêchent les potentiels concurrents d'émerger. Dans les marchés dont les entreprises dépendent uniquement des données personnelles, de nombreux autres facteurs sont identifiés comme étant des barrières à l'entrée.

Le droit à la portabilité des données. La Commission européenne a standardisé une nouvelle façon d'information avec la formulation du droit général de « portabilité des données » pour les données personnelles en 2018 à l'article 20 du RGPD. Cependant un manque d'informations à son sujet demeure et la complexité technique complique sa mise en œuvre. Michael Wolftarth dans son étude sur la portabilité des données a montré à quel point cela pouvait être néfaste pour les utilisateurs. Les systèmes utilisant le « lock in »[12] font souvent entrave à l'émergence de nouveaux services et conduisent souvent les entreprises présentes sur le marché à percevoir un rendement excessif. D'ailleurs si l'on s'intéresse au chiffre d'affaires de Facebook sur l'ensemble de 2020, il a progressé de 22%, à 86 milliards de dollars, pour un bénéfice net de 29,1 milliards (+58%)[13].

Les effets économiques résultant du droit à la portabilité. Les content provider c'est-à-dire celui qui stocke et récupère des données pour les rendre accessibles à toutes les applications jouent un rôle important dans la portabilité des données. Si l'on considère deux « content provider » générant des revenus avec des données personnelles qui se révèlent à travers l'activité des utilisateurs sur la plateforme. A travers des stratégies économiques soit sur du ciblage publicitaire ou bien sur des ventes de données personnelles à des tiers, on se rend compte que ces données sont transformées en revenus. Ainsi les données personnelles ont un effet positif sur les revenus des CP. Cependant, est ce que les données personnelles représentent un coût pour les utilisateurs ?

En termes de temps, comme indiqué plus haut, l'utilisateur en prend pour communiquer ses données. Quotidiennement, Facebook est un lieu de partage. Chaque minute passée sur

---

[12] Michael Wohlfarth, *Data portability on the internet : An economic analysis*, August 2017

[13] Nicolas Rauline, *« Facebook ne connait pas la crise »,* Les Echos (28/01/2021)

l'application est en réalité monnayable. Les publications, les photos, les statuts, les likes sont autant d'informations recueillies par le CP qui vont collecter du temps et de l'argent. Ainsi, l'opportunité de changer d'application est mise à mal avec les coûts de transferts et les « lock ins ». Certes la portabilité des données personnelles permet de contourner ce problème mais il faut également prendre en compte les conséquences sur la consommation des données de la part des CP. La portabilité des données n'est pas nécessairement bénéfique pour les utilisateurs puisque joindre les CP demande également une révélation des données plus accrue. Le principal critère de la protection des utilisateurs n'est donc pas satisfait. Les CP dominants souffrent toujours de la portabilité des données, puisque les nouveaux entrants sur le marché vont défier les CP déjà présents. L'entrant profitera toujours plus de la portabilité des données puisqu'elle permet une plus grande variété de services car les nouveaux entrants pourront plus facilement faire leur entrée sur le marché avec des profits plus élevés. Si le marché est dominé par une seule entreprise, la portabilité des données peut donc être un dispositif adapté pour favoriser la compétition.

Instituer un droit à la portabilité des données est bien plus complexe que prévu. On peut se demander de quelle manière le droit à la portabilité affecte la variété de service et le consommateur. Aussi, on peut se questionner si la portabilité des données ou la non-portabilité des données est plus efficace au regard du bien collectif.

Du côté des perspectives politiques, l'introduction d'un droit général de portabilité des données s'explique à travers la protection des utilisateurs[14]. Les résultats de l'étude de Wolfarth montrent que la portabilité des données ne devrait pas être appliquée à tous les services en réseaux. D'un autre côté, si l'on considère l'économie dans son ensemble, rechercher des buts comme le Digital Single Market Strategy avec l'Union Européenne ou la directive de l'ancien président Obama sur la concurrence en Avril 2016 qui insistent sur l'importance du caractère ouvert, juste et non-discriminatoire du marché. Puisque le profit de l'entrant augmente avec la portabilité des données, un droit des portabilités des données peut donc répondre à cette problématique. Cependant, les politiques devraient être prudentes pour savoir s'ils veulent promouvoir l'entrée dans le marché pour stimuler l'innovation et la variété des services ou purement se concentrer les consommateurs.

[14] Commission Européenne, 2016 b, Article 1

Le principe du droit à la portabilité proposé par la Commission européenne se concentre sur les données personnelles révélées par les utilisateurs eux-mêmes. De ce fait, les données révélées par les parties tierces sont exclues de cette proposition. Le champ d'application devrait peut-être être élargi.

L'on doit considérer que transporter des données personnelles sensibles supporte d'important risque de sécurité, même si les utilisateurs entrent ces données et qu'il existe des instances ou les utilisateurs sont en réalité dans une situation plus mauvaise avec un droit à la portabilité. Sur Facebook, il y a les amis mais aussi les amis proches, les attentes de demande d'amis, les demandes d'amis déclinées et les amis « supprimés ». Les consommateurs seraient donc dans une pire situation si les qualités du services proposés sont asymétriques, l'entrant a une proposition de valeur supérieure permettant à l'utilisateur une plus haute base utile.

La portabilité des données a peut-être été une distraction dans le débat sur la concurrence, elle a fait l'objet d'une attention intense de la part des entreprises technologiques et des autorités politiques. Cependant, il se peut que le type de portabilité des données qui est au centre de ces discussions soit simplement un mauvais mécanisme pour augmenter la concurrence en ligne. Si tel est le cas, le temps passé à débattre d'aspects spécifiques d'un régime de portabilité des données donné peut être mieux dépensé en considérant différents types d'approches des problèmes de concurrence.

Chapitre 2 : La collecte des données personnelles et l'abus de position dominante

La collecte des données est donc une particularité des services en ligne qui permettent aux plateformes de pouvoir à la fois de connaitre les utilisateurs sur leurs préférences mais également les conduire à réitérer certaines actions. Les GAFA ont une stratégie très claire de rachat, en particulier des start-ups positionnées sur des secteurs intéressants, pour ne pas voir émerger de concurrents[15].

[15] Kamepalli 2020

Il faut rappeler que ce ne sont pas les positions dominantes qui sont problématiques mais les abus de position dominante. En outre, la fusion de deux entreprises qui occupent déjà` des positions importantes sur des marchés peut conduire à la forclusion de ces marchés au détriment de nouveaux concurrents. Les prestataires de services en ligne consommant des volumes importants de données personnelles peuvent par exemple acquérir des producteurs d'ordinateurs, de smartphones ou de logiciels afin de s'assurer un accès durable à des quantités importantes de données par le biais des utilisateurs de ces services.

Section 1 : Les phénomènes de concentration

Dans cette section, il s'agira de montrer comment les fusions dans le secteur des réseaux sociaux peuvent permettre de regrouper un nombre encore plus grand de données et de ce fait constituer un abus de position dominante.

En 2014, Facebook achète WhatsApp pour la somme de 19 milliards de dollars. La Commission européenne doit analyser la fusion afin de savoir si elle peut conduire à une position dominante. Les fusions sont encadrées par l'article 4 du texte législatif de régulation européenne sur les fusions.

La difficulté n'est pas apparue directement aux yeux de la Commission. Elle déclare que Facebook Messenger et WhatsApp ne sont pas dans le même marché. Elle s'est bornée à considérer Facebook comme un fournisseur d'application, en tant que réseau social qui permet à l'utilisateur de profiter des fonctionnalités de partages de photos, de vidéos mais également un espace de publicités. Plus particulièrement, Facebook offre une application de communication « Facebook Messenger » et enfin de partage de photo et vidéo « Instagram ». Quant à WhatsApp, c'est uniquement une application de communication à travers une application mobile, il n'y a aucune vente de publicité. La Commission établit deux théories qui, à terme, pourrait renforcer la position de Facebook en acquérant WhatsApp :

-soit Facebook introduirait de la publicité ciblée au sein de WhatsApp en utilisant la data collectée des utilisateurs WhatsApp (ou/et des utilisateurs Facebook qui sont également des utilisateurs WhatsApp). De cette manière, la position de Facebook dans la publicité en ligne

serait renforcée. Cependant, WhatsApp ne vend aucune publicité en ligne car selon l'application, cela modifierait significativement l'expérience que recherche ses utilisateurs.

-La deuxième théorie évoquée par la Commission est de considérer que WhatsApp puisse être une source potentielle de données personnelles supplémentaire à des fins publicitaires. C'est fatalement ce qu'il s'est passé par la suite c'est-à-dire la possibilité que la fusion puisse permettre une collecte de données encore plus large et que la data des utilisateurs de WhatsApp soient utilisées pour des publicités encore plus ciblées sur Facebook. Lors des analyses entreprises par la Commission cette théorie a été réfutée car la Commission considérait alors que les utilisateurs de WhatsApp pouvaient uniquement ajouter une photo de profil, leur nom et un statut. Ils ne pouvaient pas ajouter d'autres données que ce soit leur date de naissance, leur adresse ou autre qui puisse identifier l'utilisateur. De plus, à plusieurs reprises, Facebook s'est défendu de modifier la collection des données de WhatsApp :
« Facebook has publicly made it clear that it has no current plans to modify WhatsApp's collection and use of user data ».

Peu après l'annonce de la transaction, le directeur de WhatsApp, Jan Koum a déclaré sur le blog de WhatsApp's : *"respect for [users'] privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about [users] as possible." He added that "[i]f partnering with Facebook meant that we had to change our values, we wouldn't have done it."*.

La conséquence de cette fusion conduisant à la collection de données des utilisateurs de WhatsApp (par exemple l'âge, le genre, le pays, le contenu des messages) pourrait conduire à certains utilisateurs à changer d'applications moins intrusives. En effet, la Commission a noté un nombre élevé d'applications qui partageait tout autant les données personnelles au même titre que Facebook à travers la publicité. Cela incluait Google, Apple, Amazon, eBay, Microsoft, AOL, Twitter, LinkedIn etc. Or ces marchés ne s'adressent pas à la même catégorie d'utilisateurs et n'offrent pas les mêmes services que la plateforme Facebook.

Aussi, la Commission relève que les seuls facteurs prouvant que WhatsApp et Facebook sont de proches compétiteurs étaient basés uniquement sur leurs fonctionnalités et la taille de leur réseau :

"*160. The current plans of Facebook, as evidenced by its submissions to the Commission, public statements and internal documents, do not provide support for a future integration of WhatsApp with Facebook of the sort that would strengthen Facebook's position in the potential market for social networking services.*"[16]

De mon point de vue, la Commission a commis plusieurs erreurs dans ses considérations. Premièrement, baser sur des allégations peut se révéler décevant, voire dangereux. En 2014, Facebook occupait déjà une place prédominante dans le marché des applications gratuites. Elle s'est bornée à croire que Facebook n'allait aucunement profiter d'un réseau social, comptant alors plus de 500 millions d'utilisateurs en 2014. Cela allait inéluctablement renforcer sa position notamment de messagerie instantanée (Facebook Messenger étant déjà présent).

A la suite de la fusion, Facebook procède à l'utilisation des numéros de téléphone entrés sur l'application WhatsApp. La Commission inflige alors une amende de 110 millions d'euros à Facebook pour avoir fourni *« des renseignements inexacts ou dénaturés au cours de l'enquête »*. Le texte invoqué est l'article 14 de la régulation européenne sur les fusions.

"The Commission may by decision impose on the persons referred to in Article 3(1)b, undertakings or associations of undertakings, fines not exceeding 1 % of the aggregate turnover of the undertaking or association of undertakings concerned within the meaning of Article 5 where, intentionally or negligently : (a) they supply incorrect or misleading information in a submission, certification, notification or supplement thereto, pursuant to Article 4, Article 10(5) or Article 22(3)" [17]

C'est une application très rare, c'est d'ailleurs la première fois que la Commission européenne utilise et met en œuvre ce type de sanction. Pourtant la régulation concernant les fusions au sein de l'Union Européenne est présente depuis 2004. La Commission considère que la direction de Facebook était dès lors tout à fait conscients que les utilisateurs des deux plateformes avaient une possibilité d'être reliés. La question se pose afin d'examiner la possibilité d'une réouverture

[16] Regulation (EC) No 139/2004 Merger Procedure. Case M.7217 – Facebook/ WhatsApp Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004
[17] Article 14 de la Régulation européenne sur les fusions

d'enquête concernant la fusion. La Commission a la possibilité de revenir sur une décision d'accord notamment si cette décision était elle-même basée sur des informations incorrectes. Cela remet également en question le processus d'étude et d'enquête lors des projets de fusion ; est ce que la procédure participative par laquelle l'entreprise souhaitant fusionner est-elle pertinente aux regards des engagements pris par cette dernière. Qu'en est-il de la responsabilité sociale de l'entreprise ? Car il ne s'agit pas uniquement de non-respect à la loi et aux textes législatifs mais également à la vie privée des millions d'utilisateurs.

A ce sujet, l'un des fondateurs de WhatsApp, Brian Acton a déclaré *« Je suis un vendu. J'en suis conscient.* (…) *J'ai vendu la vie privée de mes utilisateurs* [à une entreprise] *qui veut en faire un plus gros business. »*[18]

L'autorité de la concurrence américaine a été la première à accepter la fusion. C'était sous le mandat du Président Obama, moment où l'antitrust n'était pas vraiment une priorité. Avant la fusion, le bureau de la protection des consommateurs de la FTC, alors dirigé par Jessica L.Rich, avait adressé une lettre aux deux entités, en imposant à WhatsApp d'adhérer à l'actuelle charte de confidentialité après la fusion, incluant une promesse que les données personnelles des utilisateurs de WhatsApp ne soient pas utilisées à des fins publicitaires. En effet, ce non-respect pourrait conduire à la violation de la Section 5 du Federal Trade Commission Act et l'ordre lui-même de la FTC. Si elle procède à un changement de quelque nature au regard de sa collecte de données, elle doit en faire part à la FTC et obtenir un consentement affirmatif. Cela n'a aucunement été respecté.

Depuis sa création, Facebook a donc violé plusieurs règles qui apparaissaient importante. La liste est longue concernant le non-respect de Facebook vis-à-vis de ses promesses :

-En décembre 2009, Facebook a changé la configuration de sa plateforme afin que certaines informations jusque-là privées, tel que la liste d'amis, soient rendues publiques. Ils n'ont pas prévenu les utilisateurs que le changement allait s'effectuer, ou n'ont pas demandé l'approbation en deçà.

[18] Le Monde, *Le créateur de WhatsApp explique pourquoi Facebook l'a mis en « colère »,* (27/09/2018)

-Les applications considérées comme étant parties tierces, qui n'avaient accès uniquement aux informations dont elles avaient besoin pour être opérables. En réalité, elles avaient accès à quasiment toutes les données personnelles dont elles n'avaient pas besoin.

-Facebook a déclaré à ses utilisateurs qu'ils pouvaient établir une limite dans leur partage de données, notamment avec les options « amis uniquement ». En réalité, sélectionner « amis uniquement » ne les protégeait pas du tout vis-à-vis du partage avec les parties tierces.
-Facebook avait des programmes « d'applications vérifiées » et certifiait qu'elles étaient sécurisées et participatives. Elles ne l'étaient pas.

-Facebook a promis à ses utilisateurs qu'il ne partagerait aucunes informations personnelles avec les publicitaires. Il l'a fait.

-Facebook s'est dit participé avec l'US-EU Safe Harbor Framework qui gouverne les transferts de données personnelles entre les États Unis et l'Union Européenne. Il ne l'a pas fait.

Section 2 : Une innovation moindre

L'abus de position dominante se traduit en générale par une innovation moindre. Il est difficile de vraiment noter une grande innovation entre MSN et la messagerie de Facebook. L'atout de Facebook c'est d'avoir *« pensé une stratégie juridique relative aux contenus produits par ses usagers afin de pouvoir les utiliser au cœur de son modèle d'affaires – en les valorisant à la publicité »*[19].

Le manque d'innovation est la conséquence directe d'une position dominante. Les effets d'éviction également[20]. La seule vraie innovation se trouve simplement dans la collecte plus accrue et le système interne d'utilisation des données. L'application en tant que telle ne fait que reprendre et introduire des services déjà existants : si l'on prend Marketplace c'est le principe d'un dépôt vente tout comme Le bon coin, si l'on prend Facebook rencontre c'est exactement le principe de Tinder, Dumble ou même adopteunmec. La plateforme centralise un grand nombre de fonctionnalités existantes extérieurement pour devenir indispensable aux

[19] Rapport Moral sur l'Argent dans le Monde 2015-2016
[20] Kamepalli 2020

utilisateurs. Cette capacité à pouvoir absorber des technologies nouvelles et potentiellement concurrentes est en principe relié à ce qu'on appelle en droit de la concurrence le droit des concentrations. Or, dans un milieu digitalisé qui ne connait pas vraiment de brevet ou de protection en tant que tel il est difficile de pouvoir empêcher une multiplication des services L'on peut se questionner sur l'avenir de Facebook au-delà de son *business* modèle actuel et donc de la publicité. Aujourd'hui, la publicité représente plus de 98% des revenus de Facebook alors que si l'on compare avec son concurrent chinois WeChat il ne représente que 18% en 2019. Cela traduit une vraie différence en termes de stratégie et de modèles économiques.

TITRE 2 : Les conséquences d'une exploitation accrue des données

Si l'on encourage l'interopérabilité ou le portage de données, on encourage également un partage accru et donc une sécurité moindre vis-à-vis des données. Finalement ce que l'on encourage c'est une utilisation qui peut échapper à l'utilisateur lui-même. Le régulateur devrait donc être conscient de cette ambivalence qui peut conduire à des risques accrus.

Chapitre I : Quand les données s'échappent

« La grande science est de faire vouloir à autrui tout ce que vous voulez qu'il fasse, et de lui fournir, sans qu'il s'en aperçoive, tous les moyens de vous seconder. »

L'art de la guerre, Sun Tzu

Section 1 : Un faux semblant de protection

Lorsque Facebook est entré sur le marché, il s'est immédiatement présenté comme étant la solution face à Myspace qui était alors pensé comme étant dangereux par les parents. *"MySpace, the largest social networking site in the world, has a poor reputation in terms of trust"*[21]. La stratégie de Facebook était donc d'apparaitre comme étant une solution en termes

[21] Catherine Dwyer, Starr Hiltz & Katia Passerini, Americas Conference on Information Systems, *Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace* (2007)

de confidentialité face à MySpace. Il fallait qu'il se démarque en tant qu'alternative de meilleure qualité. MySpace étant gratuit, Facebook était dans l'obligation de l'être. Sur MySpace, tout le monde pouvait voir les profils, c'était un site ouvert. A la différence de Facebook qui était fermé, il fallait être un camarade d'université ou l'ami d'un ami pour pouvoir visiter un profil. Tous les réseaux sociaux ne sont pas des réseaux fermés ; on peut prendre l'exemple de Twitter ou de LinkedIn par exemple. Facebook, lui, utilise ses différents réseaux pour le partage de données comme les photos. Le fait qu'il soit fermé contraint le potentiel utilisateur à entrer des données le concernant afin d'utiliser la plateforme. Dans son document **The Antitrust case Against Facebook**, Dina Srinivasan explique la contradiction de Facebook :*"The fact that the product is free falsely diverts attention from what antitrust policymakers and economists are most comfortable paying attention to : price."*[22]
Le prix est un élément fondamental dans le droit de la concurrence. Ce que l'on veut protéger c'est le consommateur du produit. Ainsi, on s'intéresse aux conséquences sur son pouvoir d'achat, sur sa façon de consommer le produit. Or, la logique est totalement différente ici.

A plusieurs reprises, Facebook a eu la volonté de convaincre et de renouveler la promesse de ne pas « tracker » les utilisateurs. Que ce soit en 2007, ou en 2010. Plus récemment avec son slogan *« Future is private »*.

Sans comprendre la technologie de suivi, la *tracking technology*, il est difficile de comprendre comment Facebook a pu grandir en influence tout en dégradant la confidentialité de ses utilisateurs et construire un *business* modèle qui affecte les données personnelles et la publicité de millions d'entreprises. La méthode de suivi la plus commune pour surveiller les utilisateurs sont les « cookies », ce sont de courts textes que les sites peuvent installer sur les ordinateurs des utilisateurs. De cette façon, un cookie permet à un site d'identifier un navigateur utilisant un identifiant unique afin qu'il puisse se souvenir des actions antérieures de la part de l'utilisateur. Les cookies peuvent être utilisés pour se souvenir si l'utilisateur a placé des produits dans un panier, ou s'il s'est connecté ou rempli un formulaire. De ce fait les cookies peuvent permettre d'assister l'expérience de l'utilisateur sur le site. Mais ils peuvent également déterminer ce que l'utilisateur a recherché, lu ou acheté sur un site. Lorsqu'un un utilisateur

[22] Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, Berkeley Business Law Journal Vol.16, Issue 1

recherche un site URL dans le navigateur comme lemonde.fr, l'ordinateur va initier une requête http avec le serveur du site. Le serveur du site va alors renvoyer une réponse HTTP qui va permettre à l'utilisateur de voir la page web en question. Durant la réponse HTTP, les serveurs peuvent également renvoyer un cookie et l'implanter dans le dispositif de l'utilisateur. Les cookies vont donc laisser une empreinte dans le dispositif de l'utilisateur avec un identifiant unique, ou un « cookie ID » (des suites de chiffres par exemple). Ces cookies peuvent être par la suite lus par l'entreprise qui l'a émis lorsque l'utilisateur va effectuer des recherches successives. Lorsqu'ils sont lus, les cookies de l'utilisateur fournissent le cookie ID de l'utilisateur, et d'autres éléments de la requête HTTP peuvent apporter des informations spécifiques relatives à la session du navigateur : l'URL spécifique que l'utilisateur est en train de visiter, le moment ou l'utilisateur à visiter tel URL, l'adresse IP de l'utilisateur (qui divulgue la localisation géographique). De cette façon, une entreprise peut utiliser des cookies afin de savoir (et de se souvenir) que tel utilisateur lisait tel article, à tel moment et à tel endroit.

La généralisation de la surveillance commerciale du comportement du consommateur à travers internet a été limité par deux facteurs. Premièrement, une entreprise ne peut lire que ses propres cookies. Deuxièmement, elle peut lire les cookies seulement quand l'utilisateur a initié une requête HTTP au serveur de l'entreprise. Par exemple, si le Monde inscrivait un cookie dans le dispositif d'un utilisateur, il ne pourrait pas les lire si l'utilisateur était sur leFigaro.com. Ainsi, le Monde peut savoir ce que les utilisateurs font sur lemonde.fr mais pas sur d'autres propriétés. Cependant, une entreprise peut contourner ces protections de confidentialité en installant une pièce de leur propre code sur d'autres sites, qui génèrerait de façon invisible une requête http de la part de l'utilisateur du serveur de l'entreprise. Aucun publicitaire ne veut qu'un autre publicitaire traque le comportement de son propre consommateur. Afin de développer un profil complet et précis des utilisateurs, il devrait donc y avoir une coopération entre des milliers de sites qui pourraient être par ailleurs compétitifs.

La collusion des cookies demeure donc horizontale entre les concurrents. Lorsque Facebook est entré sur le marché, et ce pour les dix prochaines années qui ont suivi, il a promis de ne pas surveiller ses utilisateurs pour des fins commerciales. En tant que fournisseur de service de communication électronique, Facebook connaissait la vraie identité et pouvait de ce fait corréler les cookies ID anonymes avec de vraies identités. Ainsi, les personnes n'étaient plus simplement des suites de chiffres lisant tel article.

Un grand nombre d'études ont révélé que les consommateurs étaient soucieux de leur confidentialité et refusaient catégoriquement la publicité ciblée.

Section 2 : Le cas du Cambridge Analytica

"Data drives all we do" Slogan de Cambridge Analytica

Le scandale Cambridge Analytica est survenu durant la campagne présidentielle de 2016 aux États Unis. Cet évènement questionne la sécurité des données personnelles détenues par les plateformes, en l'espèce Facebook.

Tout commence en 2014 lorsque Facebook autorise l'utilisation de données personnelles à une étude dite scientifique conduite par Aleksandr Kogan, étudiant chercheur à Cambridge. Ses recherches reposaient sur la déduction de la personnalité et les tendances politiques à travers les profils Facebook. Kogan était également le fondateur et directeur du Global Science Research, qui est l'une des start up travaillant avec la SCL Elections Ltd, dirigée par Alexander Nix et majoritairement financé par Robert Mercer, milliardaire et proche de Donald Trump. Lors du Concordia Summit en 2016, Alexander Nix, alors patron de Cambridge Analytica disait pouvoir prédire la personnalité de chacun des adultes aux États Unis.

Les données de 87 millions d'utilisateurs ont donc été, insciemment, été exposées à des Cambridge Analytica est une société anglaise de « Conseil en gestion autres que la gestion financière ». Elle est spécialisée dans l'analyse de données à grande échelle et conseille dans la communication. Sa mission est claire : « *changer le comportement grâce aux données »*[23].

Ce qu'elle vend est principalement des outils d'influence c'est-à-dire qu'ils vont permettre de pouvoir analyser les publicités en ligne, sonder à grande échelle, disposer de catalogue de types d'électeurs (« data models »). Selon le Monde, au moins trois candidats républicains à la Maison blanche ont déjà fait appel à l'entreprise notamment Trump ou Ted Cruz. Par exemple, la campagne de Ted Cruz a dépensé environ 6 millions de dollars pour les services de

[23] William Audureau, *« Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook »,* Le Monde, 22 mars 2018

l'entreprise. Le 17 mars 2018, le Guardian, The Observer ainsi que le New York Times révèlent que les données premièrement recueillies par Global Science Research, un questionnaire imaginé par Aleksandr Kogan pour le compte de Cambridge Analytica l'ont été à l'insu des internautes. Le quiz, simplement présenté comme un exercice académique, absorba toutes les données des participants ainsi que de leur amis Facebook. Pourtant, Cambridge Analytica, ne se cache pas de collecter des données personnelles puisqu'elle en fait même son cheval de bataille. Sur sa page de politique de confidentialité elle dit collecter des informations grâce à «des applications tierces, soit d'entreprises extérieures qui leur revendent les données, soit par des formulaires diffusés pour son compte – ce que faisait GSR »[24]. Dans les plaintes qui sont opposée à Facebook, celle de la violation du « Consumer Protection Procedures Act » qui interdit les pratiques commerciales déloyales et trompeuses aux Etats-Unis.

Alexander Nix, qui était alors patron de Cambridge Analytica a été condamné à sept ans d'interdiction de diriger une entreprise pour cause de « comportement dépourvu d'éthique ».
Le constat, c'est qu'il n'y a eu aucune infraction légale comme on pourrait le croire. Ce qui est choquant cependant, c'est la capacité de ce type d'entreprise à pouvoir absorber et collecter des millions de données même celles placées sous la confidentialité de Facebook.

Chapitre II : L'encadrement législatif

Il s'agira de se questionner l'encadrement juridique des données personnelles. Comment réguler lorsque l'objet même de la régulation échappe au législateur qui doit rapidement encadrer de nouvelles pratiques ?

Section 1 : La protection des données en droit européen et étatsunien

Aux États Unis, le régime semble toujours plus laxiste qu'en Europe, peut être en raison des nombreux scandales qui ont touché les plateformes américaines ou même les révélations

[24] *Ibid*

d'Edward Snowden sur la NSA. D'ailleurs malgré le choc généralisé qu'avait suscité cette affaire peu de réaction du côté des politiques. Les États-Unis ayant continué de rechercher et de menacer le lanceur d'alerte.

Les approches étatsuniennes et européenne ne sont pas si antinomiques. Selon le professeur J.Maxwell[25] elles reposent sur un socle commun nommé les « FIPs » (Fair Information Practices) qui ont été développées par le Ministère de la Santé américain en 1973. Ce sont les FIPs qui ont formé le socle de la Convention 108 du Conseil de l'Europe, des recommandations de l'OCDE de 1980, et de la directive européenne 95/46/CE. Les approches étatsuniennes et européenne réussissent même à des solutions proches et des méthodes de « co-régulation ».

C'est l'Article 8 de la Charte des droits fondamentaux de l'Union européenne qui protège les données à caractère personnelle, et qui en fait un droit fondamental. Aux États Unis c'est le 4eme amendement de la Constitution qui définit un droit de protection de la vie privée, mais seulement à l'égard du gouvernement. De ce fait, il ne protège aucunement les atteintes à la vie privée commises par des acteurs privés. Les lois fédérales sont protectrices dans chaque État.

La loi sur la protection de la vie privée aux États-Unis s'est développée de manière fragmentée et est actuellement un mélange de diverses protections constitutionnelles, lois fédérales et étatiques, *torts*, règles réglementaires et traités. Contrairement aux lois sur la confidentialité de nombreux pays industrialisés, qui protègent toutes les données personnelles pour tous, la loi sur la confidentialité aux États-Unis est sectorielle, avec différentes lois réglementant différentes industries et secteurs économiques. Par exemple, si l'on prend l'exemple de l'HIPAA qui est *« The Health Insurance Portability and Accountability Act »* il protège la confidentialité des données de santé, elles bénéficient d'une protection élevée. Mais un régime différent va régir la confidentialité des données financières. De ce fait il existe plusieurs lois qui réglementent les données financières en fonction de l'industrie, et les données de santé ne sont même pas uniformément protégées : toutes les données de santé ne sont pas couvertes par l'act HIPAA, et diverses lois constitutionnelles et étatiques peuvent protéger les données de santé de manière plus stricte que l'HIPAA.

[25] Winston J. Maxwell, *La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne, Le cloud Computing*

Bien que les lois des États sur la notification des violations de la sécurité des données s'appliquent largement à différents secteurs, la plupart des lois sur la confidentialité des États sont également sectorielles. Dans l'ensemble, la loi américaine sur la protection de la vie privée ne réglemente que des types spécifiques de données lorsqu'elles sont collectées et utilisées par des types spécifiques d'entités.

L'approche sectorielle laisse également de vastes domaines non réglementés, en particulier au niveau fédéral. Par exemple, il n'existe aucune loi fédérale qui protège directement la confidentialité des données collectées et utilisées par des marchands ou des entreprises telles que Facebook. La plupart des lois des États sont inefficaces pour résoudre ces problèmes.

Bien que ces immenses domaines ne soient pour la plupart réglementés par aucune loi spécifique à l'industrie, ils sont néanmoins réglementés. Un nombre substantiel d'entreprises aujourd'hui, et presque toutes les grandes entreprises, ont des politiques de confidentialité, et les politiques de confidentialité sont appliquées par la FTC. La FTC peut intenter une action contre une entreprise pour manquement à une promesse de sa politique de confidentialité et, plus largement encore, pour tout acte ou pratique trompeuse ou déloyale. A terme donc, elle peut à la fois sanctionner un manque de protection des données personnelles et contrer des pratiques anti-concurrentielles. De plus, la FTC œuvre de plus en jurisprudence devenant l'une des forces régulatrices les plus influentes concernant la confidentialité aux États Unis.

La FTC a donc une compétence « tentaculaire » pour faire respecter la confidentialité, elle est l'agence qui s'occupe le plus de la vie privée. Cependant, on remarque qu'il y a très peu d'étude sur la règlementation de la FTC en matière de confidentialité. La principale raison s'explique par l'aboutissement constant à des règlements plutôt qu'à une jurisprudence.[26] Aussi l'on peut s'interroger sur la non-utilisation du droit des contrats qui reste tout le temps séparé des conditions notamment dans la gestion des litiges civils et des violations de confidentialité. Il est vrai que l'on peut se questionner sur la nature des politiques de confidentialité souvent écartées du reste en ce qu'elles ne représentent ni un contrat ni même des promesses exécutoires.

[26] *Daniel J. Solove & Woodrow Hartzog,* THE FTC AND THE NEW COMMON LAW OF PRIVACY , Columbia law review

On remarque que le droit de la responsabilité délictuelle ne convenait pas réellement à ce type de litige. Par exemple, dans l'affaire Dwyer v.American Express Co, un tribunal a conclu qu'American Express n'avait pas violé le délit d'appropriation en vendant les noms de ses titulaires de carte à des commerçants car *« les pratiques des défendeurs ne privent aucun des titulaires de carte de la valeur que leur nom individuel peut posséder. »*. Dans une autre affaire Shibley v. Time, Inc., un tribunal a rejeté une action « en appropriation » contre un magazine qui a vendu ses listes d'abonnements de courriels à des entreprises. *Privacy torts,* c'est-à-dire les délits liés à la confidentialité Le Privacy Act de 1974

Comme on peut le remarquer pour le cas de Facebook, c'est l'autorité de chaque État qui ont en charge l'application des lois de leur propre état en matière de protection des datas. Elles vont donc venir compléter les recommandations de la FTC. C'est l'attorney general Letitia James qui a donc déposé une plainte contre Facebook en décembre 2020, accompagnée de 48 autres états pour violation de la section 2 du Sherman Act ainsi que de multiples violations de la Section 7 du Clayton Act.

En droit européen, toute exploitation de données constitue une violation potentielle d'un droit fondamental et doit être justifiée par un intérêt légitime, un consentement, l'exécution d'un contrat, etc. L'auto-régulation est méfiée en Europe, le choix se porte donc plus sur la co-régulation puisque l'État demeure actif et contrôle l'élaboration des règles et leur mise en place. Ainsi, les BCR révèlent une forte tendance pour les mesures de co-régulation. Il est interdit d'envoyer des données personnelles vers les États-Unis car la Commission européenne n'a pas encore reconnu le pays comme était suffisamment protecteur des données personnelles (sauf exception prévue par la directive). Aussi l'accord Safe Harbor, qui était un ensemble de principes régissant l'échange de données entre les États-Unis d'Amérique et l'Union européenne avait été déclaré invalide par la Cour de justice européenne le 6 octobre 2015. La décision a conduit à la création du bouclier de protection des données UE-États Unis.

Les binding corporate rules (BCRs) sont des approches de co-régulation puisqu'elles convoquent deux entités ; l'une privée et l'autre publique. Selon le Professeur J. Maxwell, les BCRs sont *« des procédures internes qui garantissent un niveau élevé de protection des données à caractère personnel partout dans le groupe, y compris dans des filiales établies dans*

des pays sans protection « adéquate » des données à caractère personnel. »[27] De ce fait, les autorités européennes protégeant les données personnelles ont une implication directe vis-à-vis de ces procédures. *« Les BCRs sont négociées point par point avec l'autorité´ chef de file, et lorsque l'autorité´ chef de file est satisfaite du contenu des BCRs, le dossier est ensuite envoyé à deux autres autorités de régulation qui examinent le contenu du dossier. »*[28]

Les acteurs privés agissent donc à l'intérieur d'un cadre établi par des acteurs publics que sont les autorités de régulation. Ces BCRs une fois adoptées peuvent être opposables et leur violation peut conduire à deux types de actions ; l'une privé intenté par les victimes directes mais également publique par l'autorité de régulation.

Les pouvoirs étendus de la FTC. La FTC peut conclure des accords transactionnels avec des entreprises américaines sur des pratiques déloyales. C'est d'ailleurs ce qu'elle a fait avait fait avec en 2012 au regard des données personnelles avec Facebook. Elle a constaté que l'entreprise a violé l'accord, notamment en partageant des données avec Cambridge Analytica. La violation de l'accord de 2012 a permis à la FTC de sanctionner l'entreprise et de négocier un nouvel accord de 20 ans avec une amende de 5 milliards de dollars, amende la plus élevée jamais infligée : elle représente 9% du chiffre d'affaires de Facebook. La question qui se pose est de comprendre dans quelle mesure les entreprises souhaiteraient réaliser des accords transactionnels avec la FTC, surtout si ces derniers les conduits à des sanctions. En réalité, les entreprises préfèrent affronter la FTC que d'obtenir des procès de la part du gouvernement, qui peuvent déboucher sur des actions de groupes qui sont encore moins contrôlables. De plus, les accords transactionnels avec la FTC ne créent pas de précédents car dans ce cas-là Facebook n'admet pas sa culpabilité dans l'accord.

La FTC peut également imposer des règles supplémentaires en matière de protection des données personnelles lors de violation d'accords transactionnels. L'accord qui a fait suite à Cambridge Analytica a vivement remis en cause l'efficacité des audits effectués au sein de Facebook pour la période 2015-2017. En effet, ils ne détectaient aucune anomalie quant au partage des données. Le nouvel accord qui est apparu met donc en place de nombreuses mesures de responsabilisation qui s'appliqueront jusqu'en 2039. Entre autres, il *« oblige Facebook à*

[27] *Ibid, p29*
[28] *Ibid*

obtenir le consentement explicite de l'utilisateur avant toute utilisation de ses données de reconnaissance faciale, ou de tout partage de son numéro mobile avec des tiers. L'accord de 2012 obligeait déjà Facebook à effectuer des études d'impact, et cette obligation a été renforcée dans l'accord de 2019. Le nouvel accord oblige Facebook à mettre en place un comité d'administrateurs indépendants pour contrôler l'application de l'accord au sein de l'entreprise, et les statuts de Facebook devront être modifiés pour garantir que Mark Zuckerberg n'a pas le pouvoir seul de licencier les personnes chargées de contrôler les obligations de Facebook à l'intérieur de l'entreprise. Le nouvel accord oblige Mark Zuckerberg à signer une attestation personnelle sur la conformité de l'entreprise avec les engagements pris dans l'accord. Une fausse déclaration exposerait Monsieur Zuckerberg à des sanctions pénales, y compris l'emprisonnement. Surtout, les accords obligent Facebook à documenter l'ensemble de ses mesures prises pour réduire les risques, et à effectuer un audit tous les deux ans par un auditeur indépendant. »[29]

Mark Zuckerberg, à la suite de cette décision en 2019 avait décidé de mettre en place un « conseil indépendant de surveillance » qui est habilité à renverser les décisions prises par le CEO lui-même sur les questions de conformité des contenus. Le 17 septembre 2019 était publié la charte pour son « conseil indépendant de surveillance ». La décision du comité sera contraignante, *« La décision du conseil sera contraignante, même si quelqu'un chez Facebook, y compris moi-même, n'est pas d'accord »*[30]. Il est important de noter qu'ils n'ont aucun droit d'avis sur l'intelligence artificielle ou la hiérarchisation des algorithmes mais uniquement sur la modération des contenus.

Le professeur W.Maxwell introduit dans son document deux autres catégories de régulation aux États-Unis notamment le *multi-stakeholder process*, une initiative gouvernementale qui encourage de nouvelles formes de régulation. En prenant l'exemple de la NTIA, la *National Telecommunications and Information Administration (*l'agence spécialisée dans les télécommunications), elle invite les acteurs privés à développer des codes de conduite relatifs à certains secteurs de l'Internet. L'agence organise des réunions entre acteurs et facilite

[29] Winston Maxwell, « *Amende contre Facebook : comment la FTC américaine s'est transformée en « Super CNIL » »,* I'MTech,
[30] Mark Zuckerberg

l'échange d'informations et peut alerter si l'une des mesures de régulation est trop contraignante ou inapplicable. Elle permet donc un lien entre les acteurs publics et privés.

Enfin *l'accountability* peut également être un concept qui pourrait instaurer une norme mondiale en matière de protection des données personnelles. Selon la Commission Nationale de l'Informatique et des Libertés en France, l'accountability se définie comme « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

Elle consiste en la mise en place de programme de *compliance* au sein des entreprises qui sont par la suite supervisés par l'Etat. Le problème qui va surgir est l'élaboration d'un système pouvant coupler à la fois le BCRs européenne et les Cross Border Privacy Rules (CBPR) développées au sein de l'APEC (Asia-Pacific Economic Cooperation). Le système de règles de confidentialité transfrontalières de l'APEC (CBPR) est une certification de confidentialité des données soutenue par le gouvernement que les entreprises peuvent adhérer pour démontrer leur conformité aux protections de confidentialité des données reconnues à l'échelle internationale. Le système CBPR met en œuvre le cadre de confidentialité de l'APEC approuvé par les dirigeants de l'APEC en 2005 et mis à jour en 2015.

On peut également voir ce phénomène en France avec Orange qui a créé un Conseil d'éthique de la Data et de l'IA. Ce qui est le plus intéressant à observer dans le droit étatsunien est le concept de pratique déloyale étendu au traitement de données personnelles développé par la FTC et qui fait écho au RGPD.

Section 2 : La territorialité

Le marché global des données personnelles remet en question la territorialité de la législation. On voit se dessiner deux forces de marché, l'une se trouvant d'un côté aux États Unis et l'autre en Chine. L'Europe au milieu tente de réguler tant bien que mal les exploitations de données qui la traverse. En effet, si les États Unis ont une approche dite de la « compliance » qui a pu effrayer plus d'une entreprise, l'Europe a adopté le RGPD qui n'est peine à s'harmoniser au sein du territoire, puisque selon le considérant n°8 du règlement, une marge de

manœuvre est laissée aux États membres dans la transposition et l'application du règlement. C'est l'article 3 du RGPD qui annonce le champ d'application territorial :

1. *« Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :*

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

3. *Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public. »*

Il y a donc trois principaux liens qui permettent d'établir le rattachement des personnes soumises au texte. Le premier point à considérer est celui du lieu c'est-à-dire là ou l'établissement de la société est établie. Cela peut être également un rattachement à un lieu pour la société du moment où la société mère ou bien une succursale ou même l'une de ses filiales, un sous-traitant est établi en Europe. Ensuite c'est le ciblage effectué par la société et enfin le territoire doit être régi par le droit européen.

La territorialité constitue la problématique la plus importante pour la régulation des données personnelles. Ce débat se base sur la question de savoir si un juge américain peut obliger la divulgation de données personnelles en Europe sans recourir aux mécanismes des traités internationaux. Cette problématique a en parti été considéré dans le cas United States v Microsoft. La question est de savoir si une loi américaine relative aux mandats de perquisition peut être interprétée comme s'étendant à une recherche de données situées en dehors des États-Unis ; en l'espèce, les données sont situées en Irlande. La Cour d'appel des États-Unis a estimé qu'en l'absence de formulation expresse dans la loi relative à l'application extraterritoriale, la loi devrait être interprétée comme étant limitée aux perquisitions effectuées sur le territoire des États-Unis. La Cour suprême examine actuellement l'affaire. En décembre 2017, la Commission européenne a déposé un mémoire exhortant la Cour suprême à tenir dûment

compte des principes internationaux et de territorialité lors de l'interprétation de la loi américaine.

Selon la Commission Européenne : "*any domestic law that creates cross-border obligations – whether enacted by the United States, the European Union, or another state – should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of 'mutual regard to the spheres of jurisdiction' of sovereign states and the need to interpret and apply EU legislation in a manner that is consistent with international law*."

PARTIE 2 : Les moyens mis en place

De quelle manière peut-on appréhender aux États Unis et en Europe la question de la régulation des plateformes en ligne. Quels sont les moyens mis en place par les autorités régulatrices au niveau de la concurrence ? Les États-Unis, pays dans lequel le libre échange règne, les règles ont du mal à émerger face à une Europe qui tente tant bien que mal à s'imposer en légiférant.

Titre 1 : L'innovation de la régulation

Chapitre I – Les États-Unis, une résistance à la régulation

« *Ce n'était rien de moins que l'organisation tout entière du commerce et de la politique de l'Amérique qui était en jeu, autrement dit la question de savoir qui allait diriger le pays* » disait l'historien Richard Hofstadter à propos du monopole de la Standard Oil Company.

Aujourd'hui, le problème est à peu près le même. On peut se questionner sur la raison de cet alarment général tardif, depuis 2020, alors que de nombreux travaux de recherches avaient déjà fait état sur la dangerosité des plateformes depuis quelques années. Évidemment c'est un sujet très politisé, puisque la dernière fois qu'il y avait des campagnes engageant le sujet des monopoles remonte probablement à 1912 avec l'élection de Wilson Roosevelt. La difficulté à réguler de tels secteur s'explique par son empreinte économique incroyable dans le pays. C'était d'ailleurs la raison pour laquelle Obama tentait de calmer les acteurs politiques européens face à une régulation des plateformes numériques.

La régulation de la concurrence aux États Unis se partage entre le Department of justice (DoJ) qui est la voie traditionnelle de mise en application et la FTC qui détient de nombreuses autorités régulatrices. Le Congrès a été placé sous silence ces dernières décennies comparer au rôle qu'il avait dans les années 50 et 60. Le Congrès avait une vue d'ensemble et essayait de prendre en compte tous les acteurs. Il prenait du recul afin de savoir précisément ce qui avait heurté le marché et les complications qui s'en suivaient. Il se posait souvent la question des lois peut être mal appliquées par lui-même ou le travail mal fait des agences. Depuis les années 80, il s'est retiré. Aujourd'hui c'est véritablement la branche judiciaire et les agences exécutives qui sont actives. Si l'on devait reporter un préjudice sur le marché aujourd'hui le plus intéressant serait de se reporter au Congrès qui est extrêmement intéressé puisque ce qu'il constate c'est l'inactivité des agences.

Section 1 : La pensée américaine qui se pare d'une résistance à l'oppression

Dans cette section, il s'agira d'étudier l'efficacité des mécanismes propre au droit de la concurrence aux États-Unis et d'en rappeler l'héritage notamment celui de l'école de Chicago. On peut se questionner sur la capacité des États-Unis à se réguler sur cette question : Est-ce que le Sherman act et le Clayton Act sont-ils suffisamment protecteurs ? Comment expliquer la difficulté à se réformer ?

Il est difficile aujourd'hui de prôner la dérégulation des plateformes, ou de critiquer le RGDP. Comment affirmer la liberté de circulation des données, discours pourtant tenu par Zuckerberg lors d'un entretien le 8 janvier 2010 avec le fondateur du blog TechCrunch, Michael Arrington sur *« la fin de la vie privée »*[31]. Les temps ont changé et Lina Kahn a été nommée commissaire à la FTC. Cela révèle la volonté de l'administration Biden de contrer la puissance des GAFA.

Les discussions sur la politique de la concurrence des États-Unis du début des années 1970 à nos jours mettent souvent l'accent sur la montée des perspectives de l'école de Chicago dans l'orientation de la doctrine et des politiques. Des années 40 au milieu des années 70, les États-Unis ont développé un corps de doctrine juridique et politique interventionniste envers les entreprises dominantes que peu de système de droit de la concurrence n'a égalé. Les décisions judiciaires étaient dotées d'une vision exceptionnellement large de l'abus. Pendant un certain temps, dans les années 40, dans des décisions telles que United States v. Griffith, les tribunaux semblaient prêts à se passer de l'exigence de comportement abusif et entériner une théorie de monopolisation sans faute. Bien que les affaires de la Section 2 de cette période aient continué à insister sur certains éléments de mauvais actes, les tribunaux ont défini le concept de comportement fautif de manière si large qu'un large éventail de comportements suffisait pour les entreprises dominantes.

La politique publique d'exécution à l'égard des entreprises dominantes durant cette période n'était pas moins ambitieuse. Habitués que nous sommes aujourd'hui à considérer les infractions à la Section 2 comme des infractions civiles, il est facile d'oublier que, jusqu'au milieu des années 1960, le ministère de la Justice a parfois poursuivi la monopolisation ou la tentative de monopolisation comme des crimes. À trois reprises au début des années 1960, le DoJ a inculpé des entreprises pour des violations de la Section 2. Le ministère a même inculpé des individus.

[31] Casilli, 2013

De 1969 au début des années 1980, le DoJ et la FTC ont entrepris un programme singulièrement ambitieux d'affaires civiles. Bon nombre d'entre eux cherchaient à restructurer les industries touchées par des cessions ou des licences obligatoires de propriété intellectuelle. Les industries les plus touchées étaient celles des pneus automobiles, du pain, des céréales pour petit-déjeuner, des ordinateurs.

La tendance de la doctrine antitrust américaine au cours des trente dernières années a été de donner aux entreprises dominantes une plus grande liberté dans le choix des stratégies de tarification, de développement de produits et de distribution. La progression vers une plus grande permissivité n'a pas été ininterrompue. Par exemple, dans Eastman Kodak Co. v. Image Technical Services en 1992, il est apparu que la Cour suprême pourrait approuver des applications plus larges de la loi sur la monopolisation. Cette évolution ne s'est pas produite, même si certaines décisions récentes des cours d'appel et la FTC ont montré que le pouvoir discrétionnaire des entreprises disposant d'un pouvoir de marché substantiel n'est pas illimité.[32]

Les commentateurs acceptent largement le rôle central de l'école de Chicago dans l'élaboration de la politique antitrust américaine moderne et traitent la tension entre les idées de l'école de Chicago et de l'école post-Chicago comme le concours intellectuel qui déterminera l'orientation future de la politique américaine.[33] Certains récits retracent l'ascension des préférences de l'école de Chicago dans les années 1980 et attribuent largement les idées de l'école de Chicago par les tribunaux à la présidence de Ronald Reagan. D'autres voient les origines d'une *« révolution de Chicago »* dans les décisions judiciaires des années 1970 et dans un mélange d'ajustements politiques et institutionnels au sein de la Division antitrust du Département de Justice et à la FTC au cours de la même décennie. Les points de vue de l'école de Chicago sont considérés comme la principale base de l'analyse judiciaire de la fin des années 1970 à nos jours, bien que les interprétations varient quant à la mesure dans laquelle la politique d'application publique dans les années 1990 s'est éloignée de l'école de Chicago.

Section 2 : La récente poursuite de la FTC ainsi que des 46 états

[32] William e. Kovacic, *The intellectual DNA of modern U.S. competition law for dominant firm conduct: the chicago/harvard double helix,* Columbia Business law review
[33] *Ibid*

La FTC a poursuivi Facebook, alléguant que l'entreprise maintient illégalement son monopole sur les réseaux sociaux grâce à une conduite anticoncurrentielle s'étalant sur plusieurs années. À la suite d'une longue enquête en coopération avec une coalition de procureurs généraux de 46 États, le district de Columbia et Guam, la plainte allègue que Facebook s'est engagé dans une stratégie systématique, y compris son acquisition en 2012 de son rival en plein essor Instagram, son Acquisition en 2014 de l'application de messagerie mobile WhatsApp et imposition de conditions anticoncurrentielles aux développeurs de logiciels, afin d'éliminer les menaces pesant sur son monopole. Cette ligne de conduite nuit à la concurrence, laisse peu de choix aux consommateurs pour les réseaux sociaux et prive les annonceurs des avantages de la concurrence.

En 2021, la FTC conjointement aux 48 États est revenue sur son accord de la fusion de Facebook et WhatsApp. « Les réseaux sociaux personnels sont au cœur de la vie de millions d'Américains », a déclaré Ian Conner, ancien directeur du Bureau de la concurrence de la FTC. *« Les actions de Facebook pour consolider et maintenir son monopole privent les consommateurs des avantages de la concurrence. Notre objectif est de faire reculer le comportement anticoncurrentiel de Facebook et de rétablir la concurrence afin que l'innovation et la libre concurrence puissent prospérer »*[34].

La FTC demande une injonction permanente devant un tribunal fédéral qui pourrait, entre autres : exiger la cession d'actifs, y compris Instagram et WhatsApp ; interdire à Facebook d'imposer des conditions anticoncurrentielles aux développeurs de logiciels ; et exiger que Facebook demande un préavis et une approbation pour les futures fusions et acquisitions. Les chefs d'accusation reposent sur deux arguments. L'un relève des acquisitions anti concurrentielles et l'autre insiste sur des conduites anti-concurrentielles au sein même de l'application.

Le 28 juin 2021, le magistrat James Boasberg a déclaré que *« la FTC n'est pas parvenue à présenter suffisamment de faits pour établir de manière plausible » que le groupe disposait vraiment d'un pouvoir monopolistique sur les réseaux sociaux. La plainte de l'agence « ne dit presque rien de concret sur la question clé du pouvoir réel de Facebook (…), c'est presque*

[34] FTC Sues Facebook for Illegal Monopolization, ftc.gov

comme si l'agence s'attendait à ce que le tribunal approuve sans broncher l'idée répandue selon laquelle Facebook est un monopole »[35].

Chapitre II – Une application hétérogène en Europe

Il est question d'étudier les différentes décisions au sein de l'Europe qui ont tenté de condamner Facebook. Car comme le dit la Commissaire européenne à la concurrence, Margrethe Vestager, *«With size comes responsibilities »,* perpétuant une guerre acharnée contre les GAFA. Ce chapitre se concentrera sur les décisions nationales et non européennes. Même si la décision du Bundeskartllamt n'est pas tout à fait aboutie pour le moment, elle est intéressante en ce qu'elle tente d'inclure les données personnelles dans l'analyse concurrentielle. Cette décision met en lumière la problématique de la masse de données que recueillent les GAFA sur ses utilisateurs et en quoi cela peut être délétère en termes de protection de la vie privée mais également en droit de la concurrence.

Section 1 : La décision du Bundeskartllamt à l'encontre de Facebook

En 2019, la Bundeskartellamt condamne Facebook pour abus de position dominante. L'argument opposé à Facebook est qu'il ne respectait pas ses obligations en matière de droit des données personnelles. Le chef d'accusation combinait à la fois ces deux arguments réunis c'est à dire que c'est précisément le fait qu'il soit en position dominante tout en enfreignant ses obligations de protection de la vie privée qui constitue une infraction au droit de la concurrence selon la Bundeskartellamt. Les accusations se fondaient principalement sur la collecte des données des utilisateurs notamment les « likes » et la mise en commun des données sur ses diverses applications notamment Instagram, Facebook et WhatsApp qui permettent un profilage *« très précis des utilisateurs »* sans pour autant recueillir leur consentement explicite. L'ordonnance du Bundeskartellamt imposait dès lors à la firme de modifier ses pratiques et de lui présenter sous quatre mois un « concept » susceptible de mieux calibrer ses conditions d'utilisation.[36]

---

[35] Source AFP, *Concurrence : Facebook gagne une manche contre les autorités américaines*, Le Point 29/06/2021

[36] Basile Dekonink, *Données personnelles : Facebook remporte une bataille en Allemagne,* Les Echos 27/08/2019

Le RGPD est invoqué ainsi qu'un abus de position dominante. De ce fait l'office fédéral de lutte contre les cartels ordonne à Facebook de cesser le traitement de données provenant de sources tierces telles que Instagram ou de sites web tiers. Cependant la Cour d'appel fédérale de Düsseldorf le 26 août 2019 suspend la décision. Le juge du tribunal régional supérieur de Düsseldorf, Jürgen Kühnen, ayant déclaré que l'utilisation des données par Facebook ne constituait pas un abus de sa position dominante. C'est un échec pour le droit de la concurrence ainsi que le devoir de protection des données. Andreas Mundt, le patron de l'office anti-cartels allemand espérait contraindre les géants de la tech à modifier leur modèle économique basé sur l'exploitation des données personnelles

Selon le chef économiste de la Commission l'effet d'exclusion est loin d'être évident à établir. Pourtant l'abus d'exploitation des données personnelles révèle la position dominante de l'entreprise. L'abus de Facebook consiste en des pratiques commerciales excessives. Il y a une protection insuffisante des données personnelles qui menace les utilisateurs et en même temps renforce la position dominante de Facebook. Un appel devant la Cour suprême fédérale de Karlsrühe, déposé par l'autorité allemande de la concurrence, a suivi et a été gagné par l'équipe de Mundt.

Le 24 mars 2021, les juges de Düsseldorf sont revenus au dossier pour rendre leur verdict final sur l'appel de Facebook contre la décision initiale. Le tribunal est parvenu à la conclusion suivante : « *La question de savoir si Facebook abuse de sa position dominante en tant que fournisseur sur le marché allemand des réseaux sociaux, parce qu'il collecte et utilise les données de ses utilisateurs en violation du GDPR, ne peut être tranchée sans en référer à la CJUE* ».

Le juge Kunhen décide donc de remettre le dossier à la Cour de Justice de l'Union Européenne puisque c'est le droit communautaire qui est impliqué.

A la suite de l'affaire, plusieurs rapports ont fait la corrélation entre le droit de la concurrence et la protection des données. Le rapport commun publié par l'autorité et la Bundeskartellamt publient une étude commune. L'étude conclut que dans les situations envisagées jusqu'à présent, le cadre juridique contemporain, en particulier l'art. 101 TFUE et la jurisprudence qui l'accompagne, permet aux autorités de la concurrence de traiter d'éventuels problèmes de

concurrence. En effet, les autorités de la concurrence ont déjà traité un certain nombre d'affaires impliquant des algorithmes, qui n'ont pas soulevé de difficultés juridiques spécifiques.

En ce qui concerne le débat scientifique sur la question de savoir si l'art. 101 TFUE doit être compris de manière plus large, et dans la mesure où certains auteurs appellent à une interprétation plus large de l'art. 101 TFUE, le document rappelle qu'il n'est pas encore clair à quels types de cas les autorités de concurrence seront confrontées à l'avenir ; par conséquent, il n'est pas encore possible de prédire s'il y a un besoin de reconsidérer le régime juridique actuel et la boîte à outils méthodologiques et, si oui, de quelle manière.

Alors que les marchés numériques continuent d'évoluer, les autorités devraient continuer à étendre leur expertise sur les algorithmes, dans un échange entre elles ainsi qu'en interagissant avec les entreprises, les universitaires et d'autres organismes de réglementation. Un tel effort s'inscrit dans la tendance plus générale des autorités à consacrer davantage de ressources aux défis posés par la numérisation en cours.[37]

Aussi au niveau européen, le contrôleur européen de la protection des données, dans son rapport de 2014, a demandé à ce que le droit de la concurrence prenne en compte la protection des données personnelles en particulier en matière de concentrations. De nombreux cas antérieurs sont en cohérence avec celui-ci, l'un d'eux en mai 2017, l'autorité de la concurrence italienne avait opposé à WhatsApp la communication et le partage de données avec Facebook. Cette fois-ci les arguments se basaient sur le code italien de la consommation. La CNIL avait mis en demeure WhatsApp pour des faits similaires se fondant sur la Loi informatique et libertés. L'intervention grandissante de la CJUE en tant que juge de dernier ressort est noter. Notamment la décision rendue le 29 juillet 2019, nommée *Fashion ID,* qui questionnant la personne qui doit faire la police des consentements dans l'espace numérique.

Section 2 : Démantèlement ?

Le démantèlement. Le mot a été utilisé à plusieurs reprises notamment pour caractériser une possibilité d'action face au monopole de Facebook. En effet, si on laisse

[37] Algorithms and Competition, Autorité de la Concurrence, Bundeskartellamt

perpétuer ce rachat incessant de start-ups et donc de concurrents, la position dominante ne sera que renforcée. Et jamais aucun nouveau concurrent n'aura le temps d'émerger. Cependant, ces acquisitions ne représentent pas toujours des achats d'une ampleur comparable à celle de WhatsApp et peuvent donc passer entre les mailles du filet aux yeux des autorités de régulation. Il faut donc limiter ces acquisitions un maximum. La dynamique des marchés pourrait également faire évoluer les choses *« car les plus grands concurrents des GAFA sont les GAFA eux-mêmes » selon* Jean Pierre Benghozi[38]. Même si leurs activités respectives n'ont pas grand-chose à voir entre elles, ils se mettent tout de même à être en concurrence entre eux. Il faut également prendre en compte l'arrivée des entreprises chinoises montantes comme Tencent ou Alibaba qui ont déjà fait leur place au sein du marché occidental.
Réaliser un démantèlement est un acte grave et c'est rarement qu'un projet de telle ampleur a abouti. Le mot démantèlement (notamment celui de Facebook et de WhatsApp et d'Instagram) a été utilisé par 50 procureurs américains depuis 2020, par Tim Wu (2018) et Elisabeth Warren[39].

La raison du refus de démanteler aux États-Unis semble clair. Pour le gouvernement américain, le danger de poursuivre une telle réforme pourrait ne pas justifier le démantèlement de ces entreprises. Encore faudrait-il les pousser à partager leur data, leurs plateformes et logiciels avec leur compétiteurs. Cela conduirait à un échec pour lancer une nouvelle vague de jurisprudence en la matière qui pourrait être appliqué à d'autres entreprises de différentes industries et redynamiser l'application des *lois antitrust*. *L'enjeu selon Gene Kimmelman, ancien conseiller au Département de la* concurrence, le gouvernement ne doit pas aller si loin. Il ne doit pas aller si loin pour convaincre les tribunaux que leurs anciennes décisions étaient mauvaises. Cependant, ils doivent convaincre les juges que ces dernières jurisprudences doivent être adaptées aux réalités concurrentielles actuelles, celles du *« winner take-all markets »*. Des marchés ou les consommateurs veulent tous utiliser les mêmes services ou fournisseurs, que les prix peuvent être gratuit et que les menaces de concurrences peuvent venir de petites start-ups offrant des produits différents ou des technologies similaires.

[38] Pierre-Jean Benghozi, Faut-il démanteler les GAFA ?, La découverte « Regards croisés sur l'économie ».
[39] Dominique Boullier, *Puissance des plateformes numériques, territoires et souverainetés*, SciencesPo, Mai 2021

Titre 2 : Des remèdes possibles

Chapitre I : Le droit qui se créer

En réponse à ces multiples problématiques, la Commission Européenne a décidé d'initier une série de législation pour encadrer le pouvoir des GAFA au sein de l'Union Européenne. Il s'agira de présenter de quelle façon le Digital Market Act peut être une solution.

Section 1 : Le Digital Market Act

La régulation des plateformes numériques est difficilement saisissable en droit de la concurrence, cela est dû à l'évolution constante des technologies mais également des critères déterminant le pouvoir de marché qui sont difficilement quantifiables, comme la détention de données[40]. La Commission européenne a donc proposé un règlement pour un marché plus juste dans le domaine du numérique, actuellement soumis à la procédure législative de l'Union européenne. Le texte devrait entrer en vigueur début 2022. Il nécessite l'examen du Parlement européen et l'approbation du Conseil de l'Europe.

Le Digital Market Act a pour principal but de moderniser le cadre existant en Europe. Selon l'article 1 du DMA, son champ d'application concerne les marchés des réseaux de communications électroniques. L'article 2 identifie les services et acteurs concernés par la Directive. L'alinéa 2 explicite le secteur des produits et services de la société de l'information, c'est-à-dire le secteur du numérique. Les *Core Platform services* sont les services qui posent des problèmes de concurrence notamment les réseaux sociaux. A priori Facebook en fait partie, est correspond à un *Gatekeeper,* puisqu'il remplit les critères indiqués à l'article 3 du DMA : c'est-à-dire que sa taille a une incidence sur le marché intérieur, condition supposée remplie si son chiffre d'affaires est d'au moins 6,5 milliards d'euros au cours des 3 derniers exercices dans l'UE, et/ou sa valorisation boursière s'est élevée à au moins 65 milliards d'euros au cours du dernier exercice avec un service actif dans au moins 3 pays membres. Deuxièmement, son service cumule plus de 45 millions d'utilisateurs finaux mensuel actifs au sein de l'UE et/ou plus de 10 000 entreprises utilisatrices. La dernière condition concerne sa position qui doit être

[40] Autorité de la Concurrence et Bundeskartellamt, *Droit de la concurrence et données*, 10 mai 2016

durable et stable, l'on considère ce critère acquis si les deux précédents le sont. Mais une évaluation peut être engagée en fonction de la dynamique du marché en cause pour évaluer la situation effective de tout acteur opérant. La Commission pourra donc réaliser une évaluation qualitative.

Selon l'article 3, alinéa 8, le fournisseur de services déclaré *Gatekeeper* dispose de 6 mois pour se conformer aux obligations lui incombant.

La Commission entend imposer ses décisions aux États membres de l'UE car selon l'Article 1 ils ne peuvent prendre des décisions opposées à celles de la Commission. Ils ont la possibilité de saisir la Commission pour demander une enquête de marché, la Commission a 4 mois pour examiner la requête.

L'article 6 est celui qui intéresse notre propos puisqu'il concerne les données générées par les utilisateurs. Le DMA qualifie les données comme des données privées dont le *Gatekeeper* ne peut faire usage à des fins concurrentielles. Le texte fait une distinction entre les données privées c'est-à-dire les données non publiques générées par les entreprises et utilisateurs de son service et les données générées via la plateforme. L'alinéa 2 Article 6 dispose : « *data that is not publicly available shall include any aggregated and non aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers on the core platform service of the gatekeeper* »

Ainsi les Gatekeeper ont un libre accès aux données générées via la plateforme.

L'article 5 concerne les services publicitaires, le DMA impose une transparence accrue car le *Gatekeeper* prestant des services de publicité doit fournir les informations sur le prix des espaces publicitaire payé par les annonceurs et les sommes reversées aux éditeurs pour les espaces achetés par les annonceurs.

La Commission dispose de moyens de contrôle assez puissants, selon l'article 19, car elle peut exiger des Gatekeepers l'accès à leurs informations et bases de données et réaliser des inspections directement dans les locaux européens des *Gatekeepers* (Article 21). Aussi en cas d'urgence, elle peut prendre des mesures provisoires contre un *Gatekeeper* selon l'article 22.

En cas de violation, on voit que ce sont les amendes qui sont encore imposées. L'article 26 alinéa dispose que les amendes ne peuvent dépasser 10% du chiffre d'affaires annuel en cas de non-respect des articles 5, 6, 7, 16, 22 et 23. Ou même le non-respect des délais de transmission d'information, de transmission d'informations erronées ou de non-respect des obligations des articles 12, 13, 19, 20 ou 21, la Commission peut fixer des amendes allant jusqu'à 1% du chiffre d'affaires annuel.

La grande révolution concerne aussi le pouvoir de Bruxelles de démanteler les grandes entreprises technologiques qui refuseraient l'autorité et les règles européennes. Le risque c'est qu'il y ait un lobbying massif, qui grandit déjà à Bruxelles. Le texte est très prometteur encore faut-il qu'il se fasse respecter équitablement. J'espère qu'il pourra réellement avoir un impact sur l'abus de position dominante de certaines firmes. Je ne pense personnellement pas qu'il y ait de conséquences directes sur l'exploitation données, l'article 6 apparaît vague. Je ne pense pas non plus que Facebook soit vraiment directement contrarier.

Chapitre II : La doctrine

Section 1 : Penser la théorie de la *« fairness »* au carrefour du droit de la concurrence, des données personnelles et du droit de la consommation

Étant donné que la notion d'équité sous-tend les régimes de concurrence, de protection des données et de droit de la consommation, elle peut servir de facteur permettant d'aligner les protections et les mécanismes d'application dans les trois domaines. L'équité est un traitement ou un comportement impartial et juste sans favoritisme ni discrimination.

Jusqu'à présent l'attention s'est portée sur la manière dont une application rigoureuse du droit de la concurrence peut rendre les règles de protection des données plus efficace.

Si l'on prend l'exemple dans l'autre sens c'est-à-dire si les principes de la protection des données ou de droit de la consommation peuvent être intégrés dans l'analyse de la concurrence afin de renforcer la capacité des autorités de concurrence à faire face aux nouvelles formes de

comportement commercial dangereux, cela peut être pertinent. Les concepts de concurrence de définition du marché et de pouvoir de marché peuvent aider à interpréter l'ampleur des obligations que les responsables du traitement et les sous-traitants doivent respecter en vertu de la législation sur la protection des données conformément à l'approche fondée sur les risques du RGPD. Des tensions surviennent lorsque l'application de la concurrence favorise le partage ou la fusion d'ensembles de données pour des raisons d'efficacité économique contraire à l'esprit des règles de protection des données, mais il existe également une marge de synergie en impliquant les autorités chargées de la protection des données ou des consommateurs dans les enquêtes sur les fusions et en envisageant la protection des données ou les intérêts des consommateurs de manière plus proactive dans la conception des recours en matière de fusion.[41]

On remarque également que les trois domaines du droit se complètent et protègent différentes dimensions du bien-être des consommateurs. Alors que la loi sur la protection des données vise à protéger les personnes concernées, mais inclut également plus largement la sauvegarde d'un environnement de traitement des données personnelles sécurisé et équitable, la loi sur la protection des consommateurs permet aux individus de faire des choix autonomes en toute connaissance de cause. Par conséquent, bien que la protection des consommateurs et la protection des données se chevauchent clairement, comme la protection des données s'applique chaque fois que des données personnelles sont traitées, elle est distincte car elle n'est pas uniquement liée à la protection de la capacité de décision et des choix d'un individu. Le droit de la concurrence, pour sa part, vise à maintenir la compétitivité des marchés afin de garantir que les consommateurs aient de tels choix. En tant que tel, l'application de la concurrence est vitale pour protéger les consommateurs contre les problèmes de concurrence, mais une condition préalable à l'existence d'un marché qui fonctionne bien est celle que les individus puissent être en mesure d'exercer un choix authentique et informé. De ce fait, la mise en œuvre et l'application effectives des exigences d'information dans le droit de la protection des consommateurs et des conditions d'un consentement valable dans le droit de la protection des données en particulier, sont essentielles. Le droit de la concurrence vise ainsi à garantir la disponibilité du choix, tandis que le droit de la protection des données et des consommateurs vise à permettre effectivement aux individus d'exercer ce choix.

[41] Inge Graef, Damiam Clifford and Peggy Valcke, *Fairness and enforcement : bridging competition, data protection, and consumer law,* International Data Privacy Law, 2018, Vol. 8, No.3

La concurrence, la protection des données et le droit de la consommation doivent aller de pair afin de protéger adéquatement les intérêts des consommateurs. C'est la cohérence envisagée par des protections substantielles et les mesures d'exécution se complétant et se renforçant mutuellement, protégeant ainsi les différentes dimensions du bien-être des consommateurs de manière unifiée.

En outre, les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne (TFUE), les deux principales dispositions du droit de la concurrence de l'UE, contiennent également des références à l'équité. L'une des exigences de l'article 101, paragraphe 3, TFUE pour justifier des pratiques restrictives est qu'une «part équitable » du bénéfice, à savoir une amélioration de la production ou de la distribution de biens ou la promotion du progrès technique ou économique, résultant de la pratique va aux consommateurs. L'article 102 du TFUE, quant à lui, fait référence à l'imposition de « prix d'achat ou de vente déloyaux » ou d'« autres conditions commerciales déloyales » comme une forme d'abus de position dominante interdite en vertu de cette disposition.
Comme on a pu le voir avec la poursuite de la Bundeskartellamt, les principes du droit de la protection des données peuvent être utilisés comme points de référence pour évaluer si certains comportements d'exploitation d'une entreprise dominante doivent être considérés comme anticoncurrentiels au titre de l'article 102 du TFUE.

Section 2 : Un possible apport de la compliance ?

« La question numérique n'est pas un problème de régulation mais un problème de valeurs »[42]

[42] Marc Bourreau, Anne Perrot, *Plateformes numériques : réguler avant qu'il ne soit trop tard, Notes du Conseil d'Analyse économique*, 2020/6 (n°60)

Même si Mark Zuckerberg a récemment déclaré vouloir collaborer en vue d'une régulation. L'on peine à véritablement croire en sa bonne foi. Si l'on fait un constat des solutions actuelles, elles sont réactives et adoptées au fur et à mesure de l'apparition de comportement intolérables. L'efficacité des amendes seules est douteuse. Même si l'Europe s'est montrée plus agressive vis-à-vis des abus de position dominantes, elle est beaucoup moins concentrée sur des remèdes structurels comme il peut y avoir aux États-Unis. La compliance pourrait être une solution pour permettre une gestion des données personnelles.

Le Droit de la Compliance est une nouvelle branche du droit qui est née aux États-Unis. Cette nouveauté fait qu'elle est très flexible. Il est pertinent de conserver le terme anglais de *Compliance* car pour l'instant le seul terme disponible en français est *Conformité*. Mais la « conformité » selon Madame la Professeur Marie-Anne Frison Roche, renvoie simplement au fait de devoir être dans une situation qui ne contredit pas l'état du Droit, ou renvoie à la hiérarchie des normes juridiques ; ainsi une loi sera-t-elle « conforme » à la Constitution.[43] Le Droit de la Compliance est dans le prolongement du Droit de la Régulation, il fait simplement reposer l'obligation sur la tête des entreprises qui, elles-mêmes doivent s'organiser pour finaliser un but politique et structurel : « ici la prévention d'une crise systémique »[44]

Quel que soit le souci particulier pris en charge par le Droit de la Compliance, les obligations Ex Ante, propres au Droit de la Compliance, par lesquelles l'entreprise limite le risque de commission du comportement combattu. *« Cet Ex Ante prend la forme d'obligations structurelles, par exemple une cartographie des risques de corruption, des contrôles internes accrus ou spécifiques, des fonctions nouvelles : les chief compliance officers. »*[45]

S'appuyer sur les fragments d'un droit européen de la compliance pourrait permettre de consolider et unifier une gouvernance générale de l'internet en internalisant dans les opérateurs numériques cruciaux la protection de la personne. Le Droit de la Compliance n'est pas très apprécié en Europe, peut être car il s'est fait connaitre à travers des sanctions importantes dont des banques notamment françaises ont été condamnées. C'est pourquoi beaucoup de forces et

---

[43] Marie Anne Frison-Roche, *L'apport du droit de la compliance à la gouvernance d'internet,* Rapport commandé par Monsieur le Ministre en charge du Numérique, Avril 2019

[44] *Ibid*
[45] *Ibid*

de travaux sont consacrés à lutter contre le Droit de la Compliance, sa violence et son application extraterritoriale. En tant qu'il serait comme un tributaire d'une puissance étrangère. Cela est souvent sa perception dans les entreprises, les administrations et les responsables politiques. Selon Madame la Professeur Marie-Anne Frison-Roche, *« l'espace numérique, parce qu'il est naturellement sans frontière pourrait être une base de départ très efficace pour un Droit européen de la Compliance général, comme la zone euro fut une base de départ très efficace pour la construction de l'Union bancaire, dans laquelle la Compliance est au centre »*[46].

Mais de quelle manière modifier en profondeur la régulation pour répondre davantage aux défis du numérique ?

Selon Jean-Pierre Benghozi, il y aurait trois solutions possibles pour remédier aux problèmes contemporains de concurrence.

La première solution pourrait être celle de laisser chaque régulateur dans sa spécialité et ode mettre en place quelques coopérations. Jusqu'à aujourd'hui, c'est ce qu'il s'est passé avec l'Autorité de la concurrence et l'Arcep qui échangent d'ores et déjà des avis lorsqu'il y a des sujets croisés.

Une autre solution évoquée peut être celle d'une coopération accrue entre les autorités entre elles, ce qui se fait déjà. Par exemple, le CSA (Conseil Supérieur de l'Audiovisuel) et l'Arcep sont des services mis en commun. En effet, les enjeux qui concernent les réseaux et les contenus des plateformes sont très liés et les résultats de ces études pourront être appropriés, soit par l'un, soit par l'autre régulateur. Cela correspond assez bien au *multi-stakeholder process* présent aux États-Unis.

La dernière solution évoquée par Monsieur Benghozi serait de créer un régulateur global du numérique et pas simplement des réseaux *« La proposition serait de repartir de zéro en réaffectant les moyens existants, plutôt que de chercher à bricoler en composant avec les*

[46] *Ibid*

logiques institutionnelles existantes. En somme, définir un nouveau design complet des autorités de régulation serait sans doute plus simple et plus efficace. »[47]

Une telle perspective ne veut pas dire qu'il ne faut pas conserver des compétences propres à chaque agence qui sont naturellement indispensables.

CONCLUSION

L'introduction des principes de protection des données personnelles pourrait représenter à mon sens une augmentation de la concurrence. Actuellement, les autorités de la concurrence contestent rarement les comportements qui nuisent directement aux individus et se concentrent plutôt sur la conduite des entreprises dominantes conduisant à l'éviction de concurrents. La

[47] *Ibid 35, p43*

difficulté réside dans l'établissement de preuves qui peuvent matérialiser les infractions d'exploitations des données personnelles massives et non-respectueuses de la vie privée des utilisateurs. Comme on a pu le voir avec le rejet de la FTC des deux plaintes antitrust majeures qui auraient pu forcer Facebook à vendre Instagram et WhatsApp. Cela révèle la difficulté d'appréhender des outils que les juristes eux-mêmes ne saisissent pas encore par leur complexité et leur technicité.

Les principes de protection des données pourraient également être utilisés ici pour tester le caractère excessif de la collecte de données d'une entreprise dominante. En extrayant des données personnelles au-delà de ce qui est autorisé par la loi sur la protection des données, l'entreprise peut essayer de mieux comprendre les préférences des consommateurs au détriment des personnes exploitées. Par exemple, si une entreprise extrait des données personnelles au-delà de ce qui est nécessaire pour atteindre un objectif particulier ou les conserve pendant une période plus longue que nécessaire pour atteindre cet objectif, elle viole les principes de minimisation des données et de limitation des objectifs. Une telle violation de la législation sur la protection des données peut à son tour indiquer si l'extraction de données est excessive et pourrait être qualifiée d'abus d'exploitation en vertu du droit de la concurrence.

Aussi, le concept d'équité en tant que principe primordial peut constituer le fondement normatif d'une telle complémentarité entre les deux domaines.

De nombreuses solutions peuvent voir le jour notamment le droit de la compliance, où l'on imposera directement à l'entreprise des obligations qu'elles devraient gérer en interne. Enfin, reste à voir l'efficacité de l'Europe dans la régulation des plateformes avec le Digital Market Act et le Digital Service Act.

BIBLIOGRAPHIE

-William e. Kovacic, *The intellectual DNA of modern u.s. competition law for dominant firm conduct: the chicago/harvard double helix,* Columbia business law review

-ME Alexandre Lazarègue, *Là ou le RGPD a échoué, le droit de la concurrence peut encore gagner, Lazaregue avocats*

- Case Study : The WhatsApp Acquisition & Facebook Privacy Promises, *Golden Data Law*

- Natasha Dailey, *Lawmakers want to break up Facebook, but experts say restoring competition through regulation should be the goal,* Business Insider, 30/01/2021

-J.-S. Bergé, S. Grumbach et V. Zeno-Zencovich, « The Datasphere, Data Flows Beyond Control and the Challenges for Law and Governance », *European Journal of Comparative Law and Gorvernance*, vol. 5, n° 2, 2018

-Winston Maxwell, *European Commission urges respect for international law in data cases*, Hogan Lovells Chronicle of Data Protection

-Frédéric Marty, *Le contrôle des concentrations en Europe et aux États-Unis*, Critères économiques et sécurité juridique

-Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, Berkeley Business La Journal

-Antonina Yaholnyk, Anastasia Zeleniuk, *Antitrust Implications of using pricing algorithms*, Chambers and Partners, 13/03/2020

-Alexandre Piquard, Portabilité des données : Facebook avance mais à petits pas, Le Monde

-James Langenfeld, Senior Managing Director, Chris Ring, Senior Director, Samuel Clark, Associate, Ankura, Washington, DC, *Regulating digital platforms : Interoperability and data portability*

-Comment la portabilité des données peut être néfaste pour les utilisateurs?
M. Wohlfarth, Data Portability on the Internet : An Economic Analysis, Working Paper for the 28th European Regional Conference of the International Telecommunications Society, August 2, 2017

-Duhigg, C. (2012). How companies learn your secrets. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html[Accessed: 02/02/2020]

-Dan Prud'homme, How digital businesses can leverage the high cost for consumers to switch platforms, LSE, 24/09/2019

- Andrej Fatur, EU Competition Law and the Information and Communication Technology Network Industries

-Winston J. Maxwell, *La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne, Le cloud Computing*

-Marie Anne Frison-Roche, *L'apport du droit de la compliance à la gouvernance d'internet,* Rapport commandé par Monsieur le Ministre en charge du Numérique, Avril 2019

-Laurent Benzoni, *Le « Digital Market Act »,* Une synthèse de la proposition de règlement européen sur la régulation des plateformes numériques essentielles

- Florence G'sell, *Une nouvelle réglementation ex ante imposées aux gatekeepers : le digital markets act*, Science Po, 23/12/2020

- Peter Swire & Yianni Lagos, *Why the right to data portability likely reduces consumer welfare : Antitrust and privacy critique, The Ohio state university Moritz College of law, May 31 2013*

- Franklin Foer, *Facebook's war on free will*, The guardian, 19/09/2017

-David Forest, *Données personnelles : RGPD, loi informatique et libertés*, 2019

- Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la gouvernance européenne des données (acte sur la gouvernance des données)

- Vagelis Papakonstantinou, Paul de Hert, Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI

-Catherine Huguet, Hervé Bouilly, *Data – Les Gafam, maîtres du monde,* Le Point, 14/11/2019

-Bill Baer, *How Senator Klobuchar's proposals will move the antitrust debate forward*, Brookings, 08/02/21

-Liza Bellulo, *Dans la perspective du digital services act européen*, The digital new deal, Mars 2021

-Michael Wohlfarth, *Data portability on the internet : An economic analysis,* August 2017

-Pierre-Jean Benghozi, *Faut-il démanteler les GAFA ?,* La Découverte « Regards croisés sur l'économie » 2019/2 n° 25 | pages 235 à 243

- F. Pasquale, *« Paradoxes of Digital Antitrust: Why the FTC Failed to Explain its Inaction on Search Bias »*

-Nils Monnerie, *Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement,* Boeck supérieur | « Revue internationale de droit économique », 2018/4 t. XXXII | pages 431 à 452

- Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in Yearbook of European Law (Forthcoming 2018)

-Antonio Casili, Paola Tubaro, Notre vie privée, un concept négociable, Le Monde, 24/01/2018

- D. SOLOVE and W. HARTZOG, « The FTC's New Common Law of Privacy », Columbia Law Journal, august 2013

- J. Hagel et M. Singer, « Net Worth: Shaping Markets when Customers Make the Rules », *Harvard Business School Press*, 8 janvier 1999

- Matthew Rogers, *Facebook to Allow Users to Download Their Data*, SWITCHED DOWNLOADSQUAD (Oct. 7, 2010)

-Nicolas Rauline, « Facebook ne connait pas la crise » Les Echos, 28/01/2021

-Gabriel Nicholas, Michael Weinberg*, "Data Portability and Platform Competition", NYU School of Law*

-M.Motto, *Competitive Policy : Theory and Practice* (Cambridge University Press, 2004)

- Marc Bourreau, Anne Perrot, *Plateformes numériques : réguler avant qu'il ne soit trop tard, Notes du Conseil d'Analyse économique*, 2020/6 (n°60)