

Protection des données personnelles et droit de la concurrence : étude des relations entre le DMA et le RGPD

Auteur : Jacob, Elise

Promoteur(s) : Auer, Dirk

Faculté : Faculté de Droit, de Science Politique et de Criminologie

Diplôme : Master en droit, à finalité spécialisée en droit économique et social

Année académique : 2024-2025

URI/URL : <http://hdl.handle.net/2268.2/23628>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Protection des données personnelles et droit de la concurrence : étude des relations entre le DMA et le RGPD

Elise JACOB

Travail de fin d'études

Master en droit à finalité spécialisée en droit économique et droit social

Année académique 2024-2025

Recherche menée sous la direction de :

AUER Dirk

Professeur

RESUME

Le droit de la concurrence et la protection des données personnelles ne semblent à première vue pas avoir de points communs. En effet, le droit de la concurrence est plutôt analysé d'un point de vue économique, tandis que la protection des données se concentre sur la protection des droits fondamentaux des personnes physiques.

Cependant, en raison de la place de plus en plus importante des nouvelles technologies dans notre économie, ces deux disciplines tendent à se croiser au niveau juridique. En effet, les GAFAM (Google, Amazon, Facebook, Apple et Microsoft) sont devenues si puissantes qu'elles peuvent se permettre de maintenir une position monopolistique sur le marché et d'utiliser les données personnelles de leurs utilisateurs à leur guise.

Le législateur européen a adopté deux législations pour tenter de résoudre ce problème spécifique lié au droit de la concurrence et à la protection des données personnelles. Ce travail de fin d'étude portera d'abord sur l'importance accordée par l'Union européenne à la protection des données à caractère personnel et au principe de libre concurrence. Nous poursuivrons avec l'analyse du Règlement Général sur la Protection des Données (RGPD) et sur le Digital Markets Act (DMA), en examinant leur impact international et leur interprétation par la Cour de justice de l'Union européenne.

REMERCIEMENTS

Merci au professeur Dirk Auer pour son encadrement et ses conseils,

Merci à mes parents dont l'affection et le support m'ont accompagnée lors de chaque examen,

Merci à Roro, Smile Popo et Samu, ils savent pourquoi,

Merci à Louis, mon amour, pour son soutien indéfectible,

Merci à Filou, mon chat pour toujours.

Table des matières

Introduction	3
1. Rappel historique de la montée en puissance des GAFAM	4
1.2. Mise en contexte	5
1.2.1. Institutionnalisation du marché interne européen	5
1.2.2. Article 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ..	7
2. Règlementation pertinente.....	9
2.1. Règlement général sur la protection des données	9
2.2. Digital Markets Act	11
2.3. Conclusion de l'analyse du RGPD et du DMA	14
3. Impact sur la scène internationale du Règlement général sur la protection des données et du Digital Markets Act.....	15
3.1. Le Brussels Effect	15
3.2. Le cas du RGPD	16
3.3. Le cas du DMA	18
3.4. Conclusions sur le <i>Brussels Effect</i>	20
4. L'interaction entre le droit de la protection des données personnelles et le droit de la concurrence	21
4.1. Arrêt <i>Meta</i> C-252/21	21
4.2. L'autorité de concurrence allemande.....	21
4.3. La décision de la Cour de justice de l'Union européenne.....	22
4.3.1. Prise en compte de la violation du RGPD par les autorités de concurrence ..	22
4.3.2. Coopération entre l'autorité de concurrence et l'autorité de protection des données	24
4.3.3. La notion de consentement dans le RGPD et le DMA	25
4.3.4. La réponse de Meta	26
4.4. Avis du Comité européen de la protection des données	27
4.5. Conclusion de l'affaire Meta	29
Conclusion finale	30
Bibliographie	33

Introduction

Si nous analysons l'histoire de l'humanité, nous constatons que le changement en est une composante essentielle. Il peut parfois paraître effrayant, notamment parce que nous ne pouvons pas toujours anticiper ses conséquences. La mondialisation et le développement des nouvelles technologies ont profondément transformé nos vies, en particulier dans la manière dont les opérations économiques sont réalisées. Avec l'essor d'Internet, l'échange de données est devenu rapide et aisé. Ces données sont accessibles au public mais surtout aux entreprises.

Leurs intentions ne sont pas toujours guidées par la bienveillance. Elles ont tendance à privilégier le profit au détriment d'autres considérations essentielles. Les données personnelles sont perçues comme un actif stratégique. Plus une entreprise accumule de données, plus elle acquiert de pouvoir sur le marché. En effet, les multinationales n'hésitent pas à collecter une immense quantité de données, parfois même sans toujours se préoccuper de la validité du consentement des consommateurs.

L'accumulation de données personnelles pose problème non seulement pour les consommateurs mais aussi en matière de droit de la concurrence, en favorisant la création de monopoles. Cette situation va à l'encontre du premier objectif de l'Union européenne : la création d'un marché libéral et concurrentiel. De plus, personne n'aurait pu prédire à quel point les grandes entreprises technologiques allaient évoluer et devenir si puissantes en termes de ressources et de capacités financières. Les autorités nationales ne sont pas en mesure, à elles seules, de les contraindre à respecter la législation. C'est la raison pour laquelle une intervention à l'échelle européenne s'est avérée nécessaire.

C'est dans ce contexte que le droit de la concurrence et le droit de la protection des données entrent en jeu. La Commission européenne et les autorités nationales tentent de suivre l'évolution rapide des technologies afin de mieux les réguler. En 2018, le Règlement général sur la protection des données (RGPD) est entré en vigueur. En matière de droit européen de la concurrence, le Digital Markets Act (DMA) est devenu pleinement applicable en 2024.

À première vue, la protection des données et le droit de la concurrence semblent être deux disciplines distinctes. Le droit de la concurrence est généralement interprété sous un prisme économique. Le droit de la protection des données, en revanche, est davantage axé sur la vulnérabilité des personnes physiques face aux grandes entreprises. Néanmoins, ce mémoire vise à démontrer qu'il existe un lien entre eux et qu'il est nécessaire de les considérer conjointement pour faire face aux enjeux soulevés par certains acteurs économiques. Ce travail de fin d'études se compose d'une étude comparative en quatre parties de ces deux législations. Dans un premier temps, une analyse historique sera réalisée afin de saisir la logique sous-jacente à ces deux domaines du droit. Nous analyserons ensuite les différentes législations en matière de protection des données et de droit de la concurrence.

Nous examinerons leur résonance à l'échelle mondiale et l'influence qu'elles exercent en dehors du territoire de l'Union européenne. Nous exposerons ensuite une analyse d'une décision fondamentale de la Cour de justice européenne concernant l'approche à adopter en matière de droit de la concurrence et de protection des données dans la pratique. Un autre aspect de ce mémoire concernera la notion de consentement des utilisateurs quant au traitement de leurs données personnelles. En effet, un service gratuit peut cacher un coût implicite. En conclusion, mon opinion personnelle sera présentée sur le sujet.

1. Rappel historique de la montée en puissance des GAFAM

En 2025, personne ne peut passer à côté du phénomène internet. Cet outil, créé vers la fin du XXe siècle, fait désormais partie intégrante de la vie courante et son usage est presque incontournable. La création du World Wide Web par Tim Berners-Lee en 1989¹, qui met en ligne sa première page web, donne une opportunité exceptionnelle aux sociétés actives dans le milieu du numérique pour se développer.

S'en suit la création d'entreprises qui, à l'origine, étaient bien différentes des multinationales que l'on connaît aujourd'hui. Tout commence en 1975 avec la création de Microsoft, qui s'est spécialisée dans la vente d'ordinateurs². Apple suit Microsoft de près en 1976, même si ce n'est qu'à partir de 1997 qu'elle commence réellement à se développer avec l'arrivée de Steve Jobs en tant que PDG³. Google fait également son apparition en 1998, en se développant principalement grâce aux droits de publicité⁴. Quelques années plus tard, le site de vente en ligne Cadabra, créé par Jeff Bezos et Mackenzie S. Tuttle commence à avoir du succès en rachetant des libraires en ligne⁵. Cette entreprise deviendra mondialement connue sous le nom d'Amazon. Enfin, Facebook est fondé en 2004 par Mark Zuckerberg et devient rapidement le géant de la communication mondiale⁶.

Ces entreprises américaines sont toutes liées au domaine numérique et se démarquent par leur prépondérance sur le marché informatique mondial et par leur capitalisation boursière⁷. Elles sont devenues tellement puissantes qu'elles sont définies par un acronyme bien connu : GAFAM. Cependant, d'autres sociétés émergentes provenant d'autres pays arrivent sur le marché et rivalisent avec ces géants du numérique. C'est le cas des BATHX⁸, les sociétés chinoises émergentes sur le marché mondial de la technologie. Ces acronymes peuvent évoluer rapidement en fonction des opérateurs économiques qui dominent le marché à un moment donné. Pour plus de clarté, l'acronyme GAFAM sera utilisé tout au long de ce travail.

Ces entreprises ont réussi à maintenir une telle position dominante que cela peut potentiellement porter atteinte au droit de la concurrence. En effet, grâce à leurs moyens et leur popularité exponentielle, celles que l'on appelle communément les *Big Tech* empêchent les petites entreprises de se développer et amassent de la sorte le plus de profit.

De plus, le non-respect des règles de concurrence n'est pas la seule chose qu'on reproche aux GAFAM/BATHX. Leur prospérité s'explique par la collecte et la vente des données personnelles de leurs utilisateurs. Ceci s'oppose aux droits fondamentaux comme le droit au respect à la vie privée et le droit à la protection des données personnelles.

¹ Bibliothèque nationale de France (BnF), « Naissance officielle d'Internet », *Passerelles.essentiels.bnf.fr*, [en ligne], <https://passerelles.essentiels.bnf.fr/fr/chronologie/article/a26aa768-a4b7-4fb3-823d-790c64b408a3-naissance-officielle-internet>, consulté le 7 mars 2025.

² R. Mourlada, « Une brève présentation des GAFAM », *Questions internationales*, N°5, 2021, p.17 et 18.

³ R. Mourlada, *Ibidem*, p.17 et 18.

⁴ R. Mourlada, *Ibidem*, p.17 et 18.

⁵ R. Mourlada, *Ibidem*, p.17 et 18.

⁶ R. Mourlada, *Ibidem*, p.17 et 18.

⁷ S. Sur, « De quoi les GAFAM sont-ils le nom ? », *Questions internationales*, N°5, 2021, spéc. p. 4 et 11.

⁸ Dans l'ordre suivant : Baidu, Alibaba, Tencent, Huawei et Xiaomi.

Le législateur européen a essayé à plusieurs reprises de réguler la puissance de ces entreprises. Que ce soit au niveau du droit de la protection des données à caractère personnel ou du droit de la concurrence, diverses législations dont le but est de maintenir un contrôle sont mises en place.

1.2. Mise en contexte

Cette partie consiste en une analyse de l'importance des principes régissant le droit de la protection des données personnelles et le droit de la concurrence européenne. Elle confirme la considération que leur accordent les institutions européennes dans sa politique interne et sur la scène internationale.

1.2.1. Institutionnalisation du marché interne européen

Il convient de rappeler brièvement les origines du droit de la concurrence européenne afin de comprendre sa mise en œuvre aujourd'hui. Ses premières traces remontent à la fin du XIXe siècle, sur le territoire des Etats-Unis où un petit nombre d'entreprises actives dans des secteurs clés de l'économie comme celui du pétrole, notamment la *Standard Oil Company*⁹ avaient acquis un quasi-monopole.

Afin de remédier à cette situation, le 2 juillet 1890 fut adopté le *Sherman antitrust Act*, du nom du sénateur américain dénonçant la position dominante de ces entreprises. Cette loi interdit la fixation des prix, le partage du marché et la collusion dans les appels d'offres publics¹⁰. L'idée d'un marché compétitif était déjà présente même si l'économie de cette époque était très différente de celle que nous connaissons aujourd'hui.

Après une période troublée par la montée du fascisme et la deuxième guerre mondiale, la volonté de mettre en place des mécanismes de coopération internationale se fait rapidement entendre. À cette période, le droit de la concurrence s'éloigne légèrement du modèle américain pour trouver son inspiration en Allemagne avec l'ordolibéralisme.

Selon cette école de pensée, les marchés ne peuvent fonctionner correctement et efficacement que si le gouvernement joue un rôle actif en soutenant la liberté contractuelle, la sécurité juridique et en garantissant une concurrence loyale¹¹. En effet, le but est de relancer l'activité économique et de favoriser la reprise des échanges commerciaux des pays européens après 5 années de conflit¹².

Deux principes majeurs émergent de ce modèle économique : l'établissement du marché commun et celui de la libre concurrence. Ils sont présents dans un des premiers traités portant sur une alliance économique en Europe. Le traité de la Communauté européenne du charbon

⁹ Britannica, The Editors of Encyclopaedia, "Standard Oil.", *Encyclopedia Britannica*, 9 mai 2025, disponible sur <https://www.britannica.com/money/Standard-Oil>, consulté le 11/05/2025.

¹⁰ Traduction libre de I. Bernaerts, « Geen doeltreffend industriebeleid zonder doortastend mededingingsbeleid – Hoe het EU-mededingingsbeleid mee evolueert met de tijd », *R.D.C.-T.B.H.*, 2023/6, p. 763.

¹¹ I. Bernaerts, *Ibidem*, p.764.

¹² X., « Premières organisations et coopérations dans l'Europe d'après-guerre », disponible sur <https://www.cvce.eu/education/unit-content/>, consulté le 17/03/25.

et de l'acier, où six états européens ont accepté de s'engager dans la voie de l'intégration, y fait déjà référence dans ses articles 66 et 67, en vigueur le 23 juillet 1952¹³.

L'article 67 prévoit expressément que si une action d'un état partie à ce traité est susceptible d'exercer une répercussion sensible sur les conditions de concurrence dans les industries du charbon, le gouvernement de l'état en question doit prévenir la Haute Autorité compétente¹⁴. Le concept d'état actif se situe au cœur de cette disposition, dans le sens où l'état lui-même doit surveiller les acteurs économiques présents sur le marché afin de préserver l'intégrité du marché intérieur.

Le principe de libre concurrence et l'établissement du marché commun continuent d'exister dans les différents traités et législations pris dans le contexte de l'instauration de ce qu'on connaît aujourd'hui comme l'Union européenne.

Ces principes se retrouvent à l'article 3 du Traité de l'Union européenne ainsi qu'à l'époque où le Traité de Rome était en vigueur, aux articles 85 et 86. La construction européenne se concrétise au fil des années pour aboutir au traité de Lisbonne, qui a mis en place le Traité sur le fonctionnement de l'Union européenne¹⁵ entré en vigueur le 1^{er} décembre 2009¹⁶.

L'article 119 du TFUE sur la politique économique et monétaire inclut expressément le principe de libre concurrence comme faisant partie des objectifs de l'instauration d'une politique économique fondée sur l'étroite coordination des politiques économiques des États membres¹⁷. Il est possible de constater qu'à travers ces différentes législations, ces deux principes sont une constante de la politique de l'Union européenne.

À côté de l'établissement du marché intérieur, un autre objectif du droit de la concurrence est le bien-être du consommateur. La commission européenne a fait plusieurs références à ce principe dans ses directives de communication¹⁸. Cette finalité du droit de la concurrence s'explique par le déséquilibre des rapports de force entre le simple consommateur et les entreprises, voire les multinationales, qui s'impose dans les relations commerciales.

En effet, les règles du droit de la concurrence ont pour objectif d'éviter que la concurrence ne soit faussée au détriment de l'intérêt général, des entreprises individuelles et des consommateurs¹⁹.

Un lien peut être effectué avec le droit de la protection des données personnelles, car son objectif est également de protéger les citoyens de l'Union face à l'exploitation de leurs données. Il est vrai que les consommateurs et plus largement les citoyens de l'Union européenne, n'ont pas les mêmes moyens que les multinationales pour imposer leur volonté

¹³ M. Maciejewski et R. Verdins, « Les traités initiaux », disponible sur <https://www.europarl.europa.eu/factsheets/fr/sheet/1/les-traites-initiaux>, consulté le 17/03/2025.

¹⁴ Article 67 du Traité instituant la Communauté économique européenne du charbon et de l'acier (CECA), signé à Paris le 18 avril 1951, (1951) JO C 24.

¹⁵ Ci-après « TFUE ».

¹⁶ Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, J.O.U.E, n°C 306.

¹⁷ Article 119 du Traité sur le fonctionnement de l'Union européenne (TFUE), signé le 13 décembre 2007, JO C 202 du 7.6.2016.

¹⁸ Par exemple, la communication de la commission sur les lignes directrices sur les restrictions verticales 2022/C 248/01, OJ C 248, 30.6.2022, paragraphe 15.

¹⁹ C.J.C.E., *Roquette Frères*, 22 octobre 2002, C-94/00, ECLI:EU:C:2002:603, point 42.

et faire valoir leurs droits. D'autant plus que ces dernières occupent une position dominante sur le marché, ce qui ne laisse pas vraiment aux consommateurs d'autre choix que de vendre leurs données pour accéder à certains services.

De plus, l'article 51 de la Charte des droits fondamentaux de l'Union européenne stipule que les états membres sont obligés de respecter les dispositions de la présente Charte lorsqu'ils appliquent le droit de l'Union européenne, comme les règles de droit de la concurrence²⁰. Ceci permet de renforcer la logique sous-jacente de protection du consommateur et le respect des droits fondamentaux lors de l'application de la législation européenne.

1.2.2. Article 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

La notion de protection des données n'a pas commencé à se développer avec le RGPD²¹ ou avec la directive 95/46, qui sont deux législations destinées spécifiquement à la protection des données à caractère personnel. En 1980, les données personnelles étaient déjà une préoccupation de l'OCDE²². Cette organisation internationale a pour but de promouvoir la croissance économique et le développement de l'économie mondiale²³.

À l'époque, les données personnelles représentaient déjà une opportunité d'échanges économiques entre les Etats, avec les risques d'atteinte à la vie privée qui en découlent. Par conséquent, cette organisation internationale a publié des lignes directrices afin de donner la marche à suivre pour la vente et le transfert des données personnelles.

Les recommandations de l'OCDE ont inspiré plusieurs éléments présents dans la directive 95/46 et par la suite, le RGPD. Par exemple, le concept de consentement se retrouve au paragraphe 10 du document, dans le sens où « les données personnelles ne doivent pas être divulguées, mise à disposition ou utilisées autrement que pour la finalité du traitement, sauf si l'entité dispose du consentement de la personne concernée ou qu'une autorité publique l'autorise »²⁴. Le paragraphe 7 s'inscrit dans la même logique que le paragraphe 10 en précisant que la personne concernée doit être informée de l'utilisation de ses données, avec sa connaissance ou son consentement²⁵.

Nous pouvons remarquer que la notion de consentement est déjà au centre de l'autorisation ou non du traitement des données à caractère personnel. Dans les faits, il est plus difficile de déterminer si un consentement est valide ou non. Cette notion sera analysée plus en profondeur dans la quatrième partie de ce travail.

Ensuite, cela démontre que la protection des données personnelles, bien qu'initialement abordée sous l'angle de la vie privée à travers l'article 8 de la Charte des droits fondamentaux

²⁰ Article 51 de la Charte des droits fondamentaux de l'Union européenne, JO C 326 du 26.10.2012.

²¹ Le Règlement Général sur la Protection des Données.

²² L'Organisation de coopération et de développement économique.

²³ Traduction libre de OECD (2002), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD Publishing, Paris, <https://doi.org/10.1787/9789264196391-en>, p.2.

²⁴ OECD, *Ibidem*, p.15.

²⁵ OECD, *Ibidem*, p.14.

de l'Union européenne, représentait déjà une préoccupation majeure sur la scène internationale.

Cette discipline nécessite donc une attention particulière ainsi que des ressources adéquates pour garantir son bon fonctionnement. Ces recommandations, bien que non contraignantes pour les états non-membres de l'OCDE, ont servi de base quant à l'adoption de droit dérivé spécifiquement consacré à la protection des données à caractère personnel, comme la directive 94/46 et le RGPD.

Pour aller plus loin, l'article 7 de la Charte des droits fondamentaux de l'Union européenne consacre le droit à la vie privée et à la vie familiale, tandis que l'article 8 énonce le droit à la protection des données à caractère personnel. Initialement, le droit à la protection des données personnelles était analysé sous le prisme du droit à la vie privée. Il ne constituait donc pas un droit à part entière mais une portion du droit à la vie privée. Lorsque que quelqu'un souhaitait invoquer l'article 8 de la Charte, il devait obligatoirement invoquer l'article 7.

De plus, lors de l'entrée en vigueur de la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en 1995, les nouvelles technologies commençaient seulement à faire partie du quotidien des citoyens de l'Union européenne, de sorte que seule cette directive suffisait. Il n'était donc pas nécessaire de consacrer le droit à la protection des données personnelles en un droit fondamental autonome.

Au fil du temps, les géants du numérique ont réussi à s'imposer sur le marché européen et à devenir de plus en plus intrusifs dans la vie privée des utilisateurs de plateforme. La Cour de justice de l'Union européenne²⁶ n'a pas tardé à réagir afin de donner plus d'importance à l'article 8 de la charte des droits fondamentaux de l'Union Européenne, en devenant une notion indépendante de l'article 7 de la Charte.

Dans son arrêt *Google Spain*, La Cour affirme à maintes reprises le caractère autonome du droit de la protection des données. En effet, au paragraphe 80 du présent arrêt concernant un traitement de données à caractère personnel, la Cour énonce : « susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel²⁷ ».

En s'exprimant ainsi, la Cour met au même niveau le droit à la vie privée et le droit de la protection des données personnelles. Ces deux dispositions sont d'ailleurs invoquées ensemble dans l'arrêt *Google Spain*²⁸.

De fait, elles poursuivent le même objectif, qui est de protéger les informations concernant les citoyens de l'Union européenne. L'article 7 bénéficie d'une interprétation large et couvre de manière générale le domaine de la vie privée. Cependant, comme énoncé précédemment, afin de limiter l'exploitation des données personnelles par les entreprises dominantes du numérique, il est nécessaire de prévoir un droit spécifique pour la protection des données.

²⁶ Ci-après « la Cour ».

²⁷ C.J., *Google Spain*, 13 mai 2014, C-131/12, EU:C:2014:317, point 80.

²⁸ C.J., *Ibidem*, point 74.

C'est pour cette raison spécifique que la Cour consacre le droit de la protection des données personnelles comme droit fondamental autonome. Cela révèle l'intention de la Cour de s'adapter aux réalités contemporaines ainsi que sa volonté de placer la protection des données personnelles au premier plan. Le point de vue de la Cour a d'ailleurs été suivi par le législateur européen dans le Règlement général sur la protection des données²⁹ dans son considérant numéro un.

Ce considérant affirme mot pour mot que « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental »³⁰. Le choix des différentes institutions européennes d'emprunter cette voie témoigne de leur revendication d'accorder de l'importance à la réglementation sur l'exploitation des données.

Cette brève évolution historique souligne les enjeux des organisations internationales et des Etats concernant la protection des données personnelles et leurs conséquences. Celles-ci constituent en effet des opportunités commerciales internationales significatives, pouvant influencer la position de l'Europe sur la scène mondiale et affecter le droit de la concurrence.

2. Réglementation pertinente

Cette partie consiste en une analyse des principales réglementations européennes sur la protection des données personnelles et le droit de la concurrence dans le domaine du numérique. Elle illustre la volonté de l'Union européenne de s'adapter à l'évolution du fonctionnement de l'économie et aux nouveaux défis posés aux droits fondamentaux.

2.1. Le Règlement général sur la protection des données

Ce règlement a été adopté le 27 avril 2016 à la suite de l'obsolescence de la directive 95/46 du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Cette directive est entrée en vigueur en 1995 et n'était dès lors pas adaptée au marché numérique et à l'exploitation des données que l'on connaît aujourd'hui. En effet, à cette date, les GAFAM commençaient seulement à prendre de l'ampleur³¹, de sorte que la quantité de données traitées et leur circulation étaient beaucoup plus limitées. À l'heure actuelle, des milliards de données sont échangées par jour, de sorte qu'une mise à jour était nécessaire pour mieux encadrer ce traitement et en assurer un meilleur contrôle.

Par exemple, un des éléments importants de la directive 95/46 était le remplissage de formalités obligatoires concernant le traitement des données personnelles. Ce système n'était

²⁹ Ci-après « le RGPD ».

³⁰ Considérant n° 1 du règlement UE n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE, n° L 119 du 4 mai 2016.

³¹ Voy. Supra section 1.

plus suffisant pour assurer une protection effective des personnes physiques dans l'ensemble de l'Union européenne³².

L'article 18 de la directive 95/46 prévoyait également que le responsable de traitement devait en principe prévenir l'autorité de contrôle mise en place par l'état membre de l'Union européenne lorsqu'il effectuait un traitement partiellement ou complètement automatisé³³. Il est évident qu'un tel système constitue une perte de temps et d'argent pour les états membres de l'Union européenne étant donné la quantité de données circulant à travers le monde.

Ce principe a été remplacé dans le RGPD par un mécanisme permettant de cibler certains types de traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques³⁴. Ceci témoigne de la volonté du législateur européen de s'adapter aux enjeux contemporains en rendant l'application de la législation européenne plus efficace et concise, afin de promouvoir et d'encadrer les échanges économiques liés aux données à caractère personnel.

Un des principaux objectifs du RGPD est de renforcer le cadre de protection des données pour le rendre plus solide et plus cohérent, compte tenu de l'intensification des échanges de données à caractère personnel entre acteurs publics et privés³⁵. Cet objectif sert indirectement au développement du marché numérique européen, qui sert également le droit de la concurrence.

Comme exposé plus haut³⁶, les dispositions concernant le droit de la concurrence doivent permettre d'aboutir à l'établissement d'un marché commun européen, afin d'avoir du poids sur la scène internationale. Le RGPD peut dès lors être utile afin de limiter l'expansion rapide des GAFAM, qui est largement facilitée par la législation en leur faveur dans le pays où se trouve leur siège social. D'autant plus que la politique américaine est très différente en matière de traitement des données que celle mise en place par l'Union européenne via le RGPD³⁷.

Le second objectif du RGPD est d'ajuster le cadre de la protection des données personnelles au sein de l'Union, mais aussi dans ses rapports avec les acteurs privés en dehors de l'Union³⁸. En effet, les données personnelles de ses citoyens circulent de manière quasiment automatique à la suite de la mondialisation du marché numérique. De nombreuses données personnelles quittent le territoire européen pour se trouver hors du champ

³² R. Perray, « Les outils de la conformité au RGPD : des outils de valorisation », *Rev. Aff. Eur.*, 2021/1, p. 35-47.

³³ Article 18 de la directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

³⁴ Règlement (UE) n° 2016/679 du 27 avril 2016, précité, considérant n°6.

³⁵ C. Castets-Renard, « Le règlement général de protection des données : quel bilan cinq après son adoption ? », *Rev. Aff. Eur.*, 2021/1, p. 9-13.

³⁶ Voy. *Supra* section 2.1.

³⁷ Voir en ce sens : A-T. Norodom, « La comparaison des modèles normatifs européen, américain et chinois en matière de protection des données à caractère personnel : une illustration de l'utilisation stratégique du droit » in Bertrand, B. (dir.), *La politique européenne du numérique*, 1^{re} édition, Bruxelles, Bruylant, 2022, p. 175-207.

³⁸ C. Castets-Renard, *op. cit.*, p. 9-13.

d'application territorial du RGPD. Il est donc nécessaire de mettre en place des mesures de protection et de clarifier leur statut lorsqu'elles quittent le territoire européen.

C'est pour cette raison que l'article 3 du RGPD fixe le champ d'application territorial de ce règlement. Cette disposition affirme que le RGPD s'applique à des responsables de traitement ou des sous-traitant ne se trouvant pas sur le territoire de l'Union tant que le traitement des données concerne des personnes se trouvant dans un état où le RGPD s'applique³⁹.

De cette manière, même si les données faisant l'objet d'un traitement quittent le territoire européen, le responsable de traitement est tenu par les obligations contenues dans le RGPD. Il devra respecter le droit fondamental de la protection des données personnelles des citoyens de l'Union européenne. Le but initial et historique du législateur européen se manifeste ici en renforçant la législation européenne afin de servir au mieux les intérêts de l'Union européenne, à savoir la libéralisation du marché et la protection des droits fondamentaux.

Ce principe d'extraterritorialité régule le transfert des données personnelles entre l'Union et les pays tiers. Ce qui a également un impact sur le droit de la concurrence, vu que les pays tiers sont obligés de se conformer au RGPD lorsqu'ils réalisent des échanges économiques. Le RGPD sert donc indirectement la politique de droit de la concurrence de l'Union européenne en régulant a priori un secteur qui ne relève pas du droit de la concurrence mais qui lui permet d'imposer des modalités de commercialisation sur le marché.

2.2. Le Digital Markets Act⁴⁰

Face à l'économie numérique, le législateur européen se voit confronté à de nouveaux défis. Les *Big data* et plus spécifiquement le transfert de données massives, constituent le carburant de l'économie numérique⁴¹. Les *Big Tech*, c'est-à-dire les entreprises qui œuvrent dans le domaine numérique, ont profité de ce marché émergent pour en devenir les acteurs principaux et développer leurs propres écosystèmes numériques⁴².

En effet, en amassant une quantité considérable de données, elles ferment l'entrée du marché à d'autres acteurs économiques qui ne peuvent pas les concurrencer, n'ayant pas accès à ces données pour cibler les consommateurs potentiels. Ce problème structurel porte atteinte au droit de la concurrence. Premièrement, en limitant l'innovation vu qu'il n'existe pas d'autres entreprises pouvant les concurrencer et deuxièmement, en diminuant la possibilité de choix des consommateurs⁴³.

³⁹ Règlement (UE) 2016/679 du 27 avril 2016, précité, article 3.

⁴⁰ Le *Digital Markets Act* se traduit en français par « la législation sur les marchés numériques ». Pour une meilleure compréhension, ce terme ne sera pas traduit, car il est également utilisé dans la langue française comme tel.

⁴¹ Traduction libre de S. OLIVEIRA PAIS, "Big data and big databases between privacy and competition", in J. CANNATACI, V. FALCE and O. POLLICINO (dir.), *Legal challenges of Big data*, Cheltenham, Edward Elgar Publishing Limited, 2020, p.15.

⁴² Traduction libre de V. DEHAECK, « Het voorstel van de (Europese) Wet Digitale Markten (Digital Market Act). Ex ante regels voor digitale poortwachters: grenzen aan het rijk van Amazon? » in *Eerlijke en vrije mededinging: wijsheid is maat*, 1^e editie, Bruxelles, Intersentia, 2021, p.42.

⁴³ Traduction libre de S. OLIVEIRA PAIS, *op. cit.*, p. 16.

Une législation spécifique est donc nécessaire afin de rétablir une économie numérique équitable et compétitive⁴⁴. C'est alors que le règlement européen 2022/1925, appelé le Digital Markets Act⁴⁵, est applicable depuis le 2 mai 2023. Ce règlement a été instauré afin de doter le marché numérique d'une législation adaptée à ses particularités et de combler les lacunes des textes précédents qui n'étaient pas conçus pour ce secteur.

Le premier constat à observer par rapport aux autres législations est son champ d'application restreint. En effet, le DMA s'applique exclusivement aux entreprises agissant dans le secteur numérique au sein de l'Union européenne, plus particulièrement aux « *gatekeepers* », qui se traduit par contrôleurs d'accès en français⁴⁶.

Les articles 2 et 3 du DMA définissent les contrôleurs d'accès comme étant une entreprise fournissant des services de plateforme essentiels qui constituent un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux. Elle possède également un poids important sur le marché intérieur, elle jouit d'une position solide et durable dans le cadre de ses activités ou en jouira dans un avenir proche⁴⁷.

Ce règlement vise donc une problématique où un type d'entreprises se trouve dans une situation spécifique qui ne peut pas être réglé par l'application de règles de droit de la concurrence classiques. Son champ d'application s'explique par le fonctionnement des entreprises agissant dans le domaine du numérique. Celles-ci proposent des services gratuits à leurs utilisateurs en échange généralement de leurs données personnelles. Ces données leur permettent d'avoir un avantage concurrentiel considérable qu'elles ne vont bien évidemment pas partager. Elles acquièrent ainsi rapidement une position dominante sur le marché numérique qui se distingue par sa rapidité d'innovation et d'expansion.

Les mécanismes classiques du droit de la concurrence ne correspondent pas forcément aux caractéristiques intrinsèques des marchés numériques. En effet, ce type de marché se caractérise par leur rapidité d'évolution, de sorte que les procédures classiques de droit de la concurrence *ex post* ne sont pas adaptées à ce type de marché⁴⁸. Un contrôle a posteriori de l'établissement d'une entreprise agissant dans le domaine du numérique intervient trop tard pour limiter les effets néfastes que celle-ci peut avoir sur le marché.

Pour remédier à cette situation, l'article 3, paragraphes 1 et 2, du DMA définit des critères qualitatifs et quantitatifs établissant une présomption réfragable selon laquelle les contrôleurs d'accès sont automatiquement considérés comme tels. Ces critères portent sur leur chiffre d'affaires annuel et leur nombre d'utilisateurs atteints au cours d'une période donnée.

Si ces critères sont remplis, le contrôleur d'accès en question devra impérativement se conformer à une série d'obligations qui se trouve dans le DMA dans les six mois après sa

⁴⁴ Traduction libre de V. DEHAECK, *op. cit.*, p.40.

⁴⁵ Ci-après « DMA ».

⁴⁶ Article 1 du Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés numériques et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828, J.O.U.E., L 265, 12 octobre 2022.

⁴⁷ Règlement (UE) 2022/1925, *Ibidem*, articles 2 et 3.

⁴⁸ Traduction libre de V. DEHAECK, *op. cit.*, p.43.

désignation en tant que « *gatekeeper* »⁴⁹. Ce contrôle *ex ante* oblige les entreprises concernées à se conformer à la législation en vigueur sans que la commission européenne ou les autorités nationales de concurrence ne doivent prouver le dommage causé par ces entreprises. Cela permet un déplacement de la charge de travail de l'autorité de concurrence vers l'entreprise concernée elle-même⁵⁰.

Un rôle plus actif des entreprises est cité également à l'article 3 paragraphe 5 du DMA. Si l'entreprise fournissant des services de plateformes souhaite échapper à la qualification de « *gatekeeper* », elle doit démontrer elle-même que malgré qu'elle remplisse les seuils fixés à l'article 3 paragraphe 2 du DMA, elle ne satisfait pas aux exigences fournies au paragraphe 1 du même article⁵¹.

Cette condition les oblige à se rendre compte de l'impact qu'elles peuvent avoir sur le marché en ayant un nombre élevé d'utilisateurs qui leur permettent de toucher par conséquent une multitude de consommateurs. Cette présomption réfragable fait également passer la charge de la preuve de l'autorité de surveillance et de la Commission européenne à l'entreprise concernée⁵².

Cela renforce l'efficacité de l'application de la législation européenne et le fait d'opérer un contrôle plus ferme sur son application. De fait, le marché numérique est assez vaste et dense, de sorte qu'examiner au cas par cas chaque entité sans les critères quantitatifs établis par le DMA serait inefficace. Le temps que ces vérifications s'opèrent, l'entreprise en question aura déjà eu le temps de se développer et d'occuper une place importante sur le marché numérique, voir une position dominante, ceci au détriment de l'Union européenne et des consommateurs.

Après avoir été désignée comme contrôleur d'accès, l'entreprise en question devra se conformer aux obligations de l'article 5, 6 et 7 du DMA. Cette approche se différencie des règles de droit de la concurrence classique notamment avec les articles 101 et 102 du TFUE caractérisées par un contrôle *ex post* de la part de la Commission européenne et des autorités de concurrence nationales⁵³. En effet, le DMA impose aux entreprises concernées de prendre leurs propres mesures et de démontrer leur application pour se conformer aux dispositions précitées⁵⁴.

Ces articles ne seront pas analysés en détail dans ce travail de fin d'étude afin de ne pas dépasser le cadre de la recherche. Cependant, il est important de soulever qu'ils contiennent des obligations qui s'adressent spécifiquement au fonctionnement des fournisseurs de plateforme. L'article 5 du DMA impose aux contrôleurs d'accès des restrictions dans le traitement et le transfert des données des utilisateurs.

⁴⁹ Règlement (UE) 2022/1925 du 14 septembre 2022, précité, article 3 paragraphe 10.

⁵⁰ Traduction libre de V. DEHAECK, *op. cit.*, p.43.

⁵¹ Règlement (UE) 2022/1925 du 14 septembre 2022, précité, article 3 paragraphe 5.

⁵² Traduction libre de V. DEHAECK, *op. cit.*, p.46.

⁵³ X., « Mettre en œuvre les règles de concurrence de l'UE : l'application des articles 101 et 102 du TFUE », synthèse de la législation, Eur-lex, [en ligne], disponible à l'adresse : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3A12609>, consulté le 30/04/2025.

⁵⁴ Traduction libre de V. DEHAECK, *op. cit.*, p.48.

Ces derniers ne peuvent notamment pas combiner les données à caractère personnel provenant du service de plateforme avec celles provenant de tout autre service de plateforme fourni par le contrôleur d'accès ou provenant de services tiers⁵⁵. En effet, ce mécanisme permet de collecter rapidement d'autres données des utilisateurs auxquelles les fournisseurs de services n'avaient pas accès au départ, ce qui renforce encore plus leur position dominante sur le marché numérique.

Cet article énonce cependant que le contrôleur d'accès peut procéder à de telles manœuvres si l'utilisateur a donné son consentement. L'article renvoie expressément au RGPD quant à sa définition. Voici qui confirme l'intérêt du législateur européen pour le bien être du consommateur et le respect de ses droits fondamentaux. Ce lien entre le RGPD et le DMA sera analysé plus tard dans ce travail.

Certaines critiques ont été formulées à l'égard de cette législation, arguant que les entreprises concernées doivent investir pour se conformer au DMA, ce qui pourrait être perçu comme une perte de temps et d'argent pouvant être alloués à d'autres initiatives. Toutefois, il convient de noter que ces entreprises ont bénéficié d'un délai suffisant pour se développer, ce qui les place à l'heure actuelle en position dominante sur le marché et leur permet de disposer des moyens nécessaires pour se conformer à la législation européenne tout en continuant à innover.

2.3. Conclusion de l'analyse du RGPD et du DMA

La responsabilisation des entreprises par le biais de la législation peut constituer une approche positive. L'entrée en vigueur du RGPD a servi d'avertissement aux entreprises, leur indiquant qu'elles ne pouvaient plus gérer les données de leurs utilisateurs comme elles l'entendaient. Cette législation représente une mise à jour essentielle en matière de protection des données à caractère personnel, adaptée à une époque où des milliards de données circulent à travers le monde chaque seconde.

Elle envoie un message clair aux entreprises extérieures à l'Union européenne : la possession de ressources considérables ne les exonère pas du respect des lois en vigueur. Il leur incombe de se conformer à la législation et non l'inverse. Il ne revient pas à l'Union européenne d'adopter une politique de laissez-faire sous couvert d'un libéralisme excessif.

Même si certains remettent en question l'efficacité à long terme du DMA, nous considérons qu'il responsabilise également les entreprises grâce à son approche *ex ante*. Cette législation permet de cibler des entreprises qui, sans nécessairement enfreindre le droit européen de la concurrence au sens des articles 101 et 102 du TFUE, se trouvent en position dominante sur le marché.

Grâce au DMA, la Commission européenne et les autorités de concurrence nationales disposent d'un nouvel outil pour évaluer leur manière d'opérer sur le marché et pour les contraindre à adopter les mesures nécessaires, compte tenu de leur mode de fonctionnement

⁵⁵ Règlement (UE) 2022/1925 du 14 septembre 2022, précité, article 5 paragraphe 2.

spécifique dans le cadre de l'économie du marché numérique qui nécessite une approche particulière.

3. Impact sur la scène internationale du Règlement général sur la protection des données et du Digital Markets Act

Le chapitre précédent, dédié à l'analyse du RGPD et du DMA, montre que ces deux législations ont un impact sur le commerce international en raison de leur champ d'application et de la nature des échanges commerciaux. Par conséquent, les entreprises souhaitant exercer sur le marché européen doivent se conformer à la législation en vigueur pour pouvoir y accéder.

Cette influence de l'Union européenne à travers sa législation sur le monde a été théorisée par Anu Bradford, dans son livre « *The Brussels effect : How the european Union rules the world* ». Cette partie présentera brièvement les conditions du *Brussels Effect*, puis analysera son application confirmée dans le cadre du RGPD, tout en s'interrogeant sur la possibilité d'un effet similaire avec le DMA.

3.1. Le Brussels Effect

Le *Brussels Effect* fait référence au pouvoir unilatéral de l'Union européenne de réglementer les marchés mondiaux⁵⁶. La particularité de cette influence européenne réside dans sa capacité à imposer ses standards sans recourir à la coercition ni à la nécessité de la coopération des États tiers à l'Union européenne⁵⁷.

L'Union européenne oblige indirectement les entreprises tierces à adopter un comportement conforme à sa législation afin d'accéder à son marché qui représente une part importante de leurs bénéfices. Par souci d'économie d'échelle, ces entreprises appliquent souvent ce même modèle de gestion dans d'autres territoires. Cela influence également les États tiers, car, par le biais du lobbying, ces entreprises cherchent à les inciter à adopter une législation similaire à celle de l'Union européenne.

Il est évident qu'un type de législation comme le RGPD ou le DMA a un effet extraterritorial, en ciblant les entreprises qui ont des interactions avec les consommateurs européens, même si leur établissement principal ne se situe pas sur le territoire de l'Union européenne.

Cet effet extraterritorial leur impose d'ajuster leur modèle de gestion en fonction des standards européens sur d'autres territoires ayant un système juridique distinct de celui de l'Union européenne, ou encore a pour effet que d'autres états adoptent une législation sur le même sujet que celui règlementé par l'Union européenne⁵⁸.

⁵⁶ Traduction libre de A. Bradford, "Introduction: The Brussels Effect", *The Brussels Effect: How the European Union Rules the World* (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), p. xiii-xx.

⁵⁷ A. Bradford, *Ibidem*, p.14.

⁵⁸ Traduction libre de Drewes, Helena and Kirk, Alexander, "Extraterritorial Effects of the Digital Markets Act - The 'Elusive Long Arm' of European Digital Regulation", 18 mars 2024, p.4.

Il devient donc un standard international dans un certain domaine régulé par de la législation, comme celui de la protection des données personnelles, qui sera analysé dans la section suivante.

Anu Bradford a établi cinq critères permettant de déterminer si la résultante d'une législation particulière peut s'apparenter au *Brussels Effect*. Le premier énonce que le marché réglementé doit être suffisamment large et attractif pour inciter les entreprises à se conformer à la législation du territoire en question afin de commercialiser leurs produits⁵⁹. Le deuxième se nomme « *the regulatory capacity* ». Il signifie la capacité d'une institution, comme l'Union européenne, à faire appliquer des règles et à influencer d'autres états à en faire autant⁶⁰. Le troisième énonce que ces règles doivent également être strictes et répondre à des normes exigeantes.

Le quatrième affirme que la réglementation doit viser des entreprises ou des produits sur un marché qui ne peuvent pas faire autrement que de respecter la législation mise en place par l'état ou l'ensemble d'états afin de vendre leurs produits ou leurs services⁶¹. Par exemple, une part importante de la vente des produits ou services des entreprises visées par la législation se matérialise sur le territoire où la législation est implantée, de sorte que les entreprises ne peuvent pas ignorer ce marché.

Le cinquième critère est celui de « la non-divisibilité » : les entreprises adaptent le même modèle de gestion pour tous les systèmes juridiques dans lesquels elles commercialisent des produits ou des services y compris ceux dont les standards de régulation sont moins élevés.

Il est vrai que l'importance du marché régulé est telle que ces dernières ne peuvent pas simplement délocaliser leur business ailleurs pour échapper au champ d'application de la réglementation stricte. Elles appliquent donc un standard uniforme pour l'entièreté de leurs transactions et pour leurs ventes de services ou de produits⁶², pour des questions d'économie d'échelle.

3.2. Le cas du RGPD

Une partie de la doctrine affirme que le RGPD bénéficie du *Brussels Effect*. En effet, les conditions établies par Anu Bradford sont remplies par le RGPD. En ce qui concerne le premier critère de marché attractif, les entreprises comme Meta ou encore Google ne peuvent pas se permettre d'ignorer un continent avec une population de plus de 700 000 000 habitants⁶³.

Par exemple, rien qu'en 2024, la valeur économique des flux de données sur le cloud est estimée à 77 millions d'euros⁶⁴. L'harmonisation du marché européen autour d'un espace économique unifié renforce son attractivité, en offrant aux entreprises un accès direct à un

⁵⁹ Drewes, Helena and Kirk, Alexander, *Ibidem*, p.6.

⁶⁰ Traduction libre de A. Bradford, *op. cit.*, p.30 et 31.

⁶¹ A. Bradford, *Ibidem*, p.48.

⁶² A. Bradford, *Ibidem*, p.54.

⁶³ X., « population mondiale par continent », disponible sur <https://populationtoday.com/fr/>, consulté le 28/03/2025.

⁶⁴ Commission européenne, "Data Flow and Economic Value EU Framework: Modelling Update and Data Collection", disponible sur <https://digital-strategy.ec.europa.eu/en/library/data-flow-and-economic-value-eu-framework-modelling-update-and-data-collection>, consulté le 28 mars 2025.

vaste territoire intégré, facilitant ainsi les échanges commerciaux à l'échelle internationale. Ce marché est donc suffisamment large pour attirer les entreprises et leur donner envie de se conformer au RGPD afin de vendre leurs produits et services sur le continent.

Ensuite, par ses institutions, l'Union européenne peut imposer ses règles aux acteurs économiques et les rendre contraignantes. Notamment avec la Commission européenne, qui peut accepter ou refuser l'entrée d'un acteur économique sur le marché européen et qui peut également imposer des amendes conséquentes sur la base du chiffre d'affaires de l'entreprise en question⁶⁵. La Commission est également en collaboration avec les autorités de protection des données de chaque États membre afin d'exercer un meilleur contrôle sur la circulation des données personnelles par pays et de s'assurer que la supervision du marché s'effectue correctement.

La Cour de justice de l'Union européenne se porte également garant de la bonne interprétation de la législation européenne et s'assure que les intérêts des citoyens européens soient respectés. Par exemple, dans son arrêt *Schrems I*, la Cour a invalidé le transfert des données personnelles de l'Union européenne vers les Etats-Unis. Elle a fait valoir que le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données à caractère personnel des citoyens de l'Union européenne conservées sur son territoire⁶⁶, de sorte que la décision d'adéquation entre les Etats-Unis et l'Union européenne sur le transfert des données est invalide.

La Cour impose donc aux entreprises ayant des activités économiques sur le territoire européen à adhérer au RGPD. Les moyens mis en place par les institutions européennes confirment donc leur capacité à contraindre les acteurs économiques à respecter la législation européenne.

Le règlement général sur la protection des données peut également être considéré comme une législation mettant en place des standards élevés. Ce n'est pas la première fois que le législateur européen se montre exigeant en termes de protection de ses intérêts et particulièrement envers ses citoyens⁶⁷. Le RGPD contient différentes obligations envers le responsable de traitement des données concernant leur transfert, ce qui n'est pas le cas dans toutes les autres législations sur la protection des données.

De plus, le RGPD a été considéré comme une législation rigoureuse et de qualité. Une étude empirique a été réalisée auprès de personnalités de différents pays ayant exercé une influence sur l'adoption d'une législation sur la protection des données personnelles dans leur pays, cette législation s'inspirant elle-même du RGPD européen. Selon cette étude, 46.2% des personnes interviewées citent ce critère pour expliquer le *Brussels Effect* du RGPD⁶⁸.

⁶⁵ Traduction libre de J. Tamim, « The Brussels Effect and the GDPR: EU Institutions as Catalysts for Global Data Protection Norms », ResearchGate, 2024, p. 15.

⁶⁶ C.J., *Schrems II*, 16 juillet 2020, C-311/18, ECLI:EU:C:2020:559, point 52.

⁶⁷ Directive (UE) 2019/2161 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de protection des consommateurs dans l'Union, JO L 328, 18.12.2019.

⁶⁸ Traduction libre de G.V. Cervi, "Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws." *DISO* 1, 2022, p.18.

Ce chiffre ne représente peut-être pas l'opinion d'une petite moitié des participants, mais il confirme l'importance des moyens mis en œuvre par les institutions européennes qui permettent de produire des textes législatifs devenus des références internationales. Une des premières raisons d'utilisation du RGPD européen comme modèle de législation est bien évidemment l'intérêt économique.

La quatrième condition du *Brussels Effect*, « l'inélasticité de l'entité concernée par la législation⁶⁹ », est aussi remplie. En effet, compte tenu du champ d'application extraterritorial défini à l'article 3 du RGPD, tant que ce sont des données personnelles des citoyens européens de l'Union qui sont traitées, le RGPD s'applique peu importe l'établissement du responsable de traitement.

Ce règlement s'applique dès lors aux entreprises situées en dehors de l'Union européenne, qui n'ont que le choix de se conformer au RGPD si elles veulent exploiter les données personnelles des citoyens de l'Union européenne, celles-ci étant peu enclines à se délocaliser complètement en dehors du territoire de l'Union.

En ce qui concerne le critère de la non-divisibilité, la nature du commerce des données personnelles implique que ces données changent de lieu très rapidement. Dès lors, le produit principal, la donnée personnelle, doit pouvoir circuler dans et en dehors de l'Union européenne en s'assurant de respecter la législation en vigueur là où elle passe⁷⁰.

Il est donc plus avantageux d'adopter le même modèle de gestion pour tous les ordres juridiques dans lesquels les données passent que de prévoir plusieurs systèmes pour les différents ordres juridiques, même si certains d'entre eux sont moins stricts que le RGPD⁷¹. En effet, comme expliqué précédemment, le marché européen ne peut pas être ignoré par les entreprises compte tenu de sa valeur et du flux important de données qui y circule.

3.3. Le cas du DMA

Le marché unique européen constitue un argument de taille pour remplir la première condition du *Brussels Effect*. En effet, comme démontré plus haut, le marché européen est d'une taille assez large pour être très attractif. Le poids de l'Union européenne réside dans la collaboration de ses États membres à former une union économique. Par conséquent, il est impossible d'entrer sur le marché d'un seul état membre de manière isolée, l'Union européenne est vue comme un tout, qui lui permet d'être un acteur économique majeur sur la scène internationale.

L'Union européenne possède également la capacité à imposer sa législation aux acteurs économiques exerçant sur son territoire. En effet, la commission européenne collabore avec les autorités de concurrence nationales afin de surveiller les comportements potentiellement anticoncurrentiels des acteurs économiques.

⁶⁹ Ce passage en français est mis entre guillemets compte tenu de la difficulté de sa traduction depuis l'anglais qui est : « *inelastic regulatory target* ».

⁷⁰ Traduction libre de J. Tamim, *op. cit.*, p.7.

⁷¹ J. Tamim, *Ibidem*, p.7.

De plus, même si ce ne sont pas exactement les mêmes législations, la proposition législative du DMA a eu comme effet sur d'autres états de prendre aussi les mesures nécessaires pour encadrer les dénommés « *gatekeepers* ».

De fait, le Royaume-Uni a récemment adopté une loi sur le fonctionnement du marché numérique⁷². D'autres pays ont également montré de l'intérêt quant à la régulation de ces plateformes numériques comme le Brésil⁷³, les Etats-Unis⁷⁴ ou encore l'Australie⁷⁵. Même si ces législations et ces enquêtes de marché ne reposent pas toutes sur les mêmes principes et mécanismes que le DMA européen, nous pouvons constater que celui-ci a provoqué un déclic international concernant la réglementation sur les fournisseurs de plateforme et plus largement sur les marchés numériques.

Le DMA a donc eu un impact sur les États qui n'étaient initialement pas concernés par cette législation. Il les a alertés sur la problématique de la régulation des marchés numériques, sur l'ampleur de ces derniers et sur les conséquences potentielles sur la liberté de concurrence.

Le Digital Markets Act s'adresse aux problèmes d'accès au marché qui peuvent se produire lorsque se créent des effets anticoncurrentiels. Pour contrer cette problématique, le DMA impose certaines obligations⁷⁶ aux entreprises concernées de manière automatique, afin d'essayer de rétablir une concurrence juste et équitable. Le DMA se démarque également des autres législations sur le droit de la concurrence avec son mécanisme *ex ante*, ce qui diffère du mécanisme classique du droit de la concurrence.

En d'autres mots, imposer aux acteurs concernés certaines contraintes simplement parce que ceux-ci remplissent des conditions quantitatives et qualitatives nécessite une vigilance supplémentaire de leur part. Ces caractéristiques confèrent au DMA le statut de législation stricte, ce qui remplit la troisième condition d'Anu Bradford concernant le *Brussels Effect*.

Ensuite, concernant le critère « d'inélasticité de l'entité concernée », il a été démontré *supra* que le DMA possède un effet extraterritorial, tout comme le RGPD. Il est possible d'avancer que le DMA essaye de réguler les effets anticoncurrentiels qui portent atteinte aux choix des consommateurs, mais également aux autres entités économiques qui souhaitent exercer une activité dans le marché numérique⁷⁷. Il suffirait donc que le comportement d'une entreprise porte atteinte aux autres opérateurs économiques pour que le DMA intervienne, sans avoir besoin de porter atteinte aux consommateurs finaux.

⁷² Digital Markets, Competition and Consumers Act 2024, c.13, disponible sur <https://www.legislation.gov.uk/ukpga/2024/13/enacted>, consulté le 1/04/2025.

⁷³ Proposition de loi 2768/2022 (Brésil), 2022, disponible sur <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417&fichaAmigavel=nao>, consulté le 1/04/2025.

⁷⁴ American Innovation and Choice Online Act." *Congress.gov*, Library of Congress, 2 mars 2022, S.2992 - 117th Congress (2021-2022) disponible sur <https://www.congress.gov/bill/117th-congress/senate-bill/2992/text>, consulté le 1/04/2025.

⁷⁵ Australian Digital advertising services inquiry, *Australian competition and consumers commission*, 2021, disponible sur <https://www.accc.gov.au/system/files/Digital>, consulté le 1/04/2025.

⁷⁶ Article 5, 6 et 7 du règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés numériques et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828, J.O.U.E., L 265, 12 octobre 2022.

⁷⁷ Traduction libre de J. Blockx, "The Digital Markets Act: Fostering Innovation 'Made in Europe'?", 31 mai 2023, p.9.

Par exemple, l'article 6 paragraphe 5 du DMA interdit au contrôleur d'accès d'accorder un traitement plus favorable en termes de classement à ses propres services qu'aux services et produits similaires d'un tiers⁷⁸. Cette disposition ne s'adresse pas aux consommateurs finaux qui ne sont même pas au courant de la différence de classement entre les produits, mais aux entreprises tierces situées sur le territoire de l'Union européenne qui veulent concurrencer le contrôleur d'accès.

Les contrôleurs d'accès en question sont donc tenus de respecter la législation européenne lorsqu'ils sont en contact avec des consommateurs européens mais également lorsqu'ils ont des interactions commerciales avec d'autres opérateurs économiques situés sur le territoire de l'Union. Cela renforce le concept d'inélasticité, dans le sens où il existe encore plus de possibilités pour le contrôleur d'accès d'être lié au territoire de l'Union européenne.

Pour terminer, le cinquième critère du *Brussels Effect*, celui de la non-divisibilité, fait l'objet d'un débat plus approfondi. Le marché numérique est en constance évolution, de sorte les analyses précédentes du *Brussels Effect*, comme avec le RGPD, ne s'appliquent pas forcément aux marchés numériques⁷⁹. Nous pouvons constater une fragmentation du marché numérique dans le monde.

Par exemple, les consommateurs chinois n'ont pas accès à certains sites européens, il est par conséquent impossible pour le DMA de s'y appliquer. Différents territoires sont chacun dominés par des géants de l'internet⁸⁰, sans possibilité qu'ils soient mis en concurrence sur un même ordre juridique.

Cela limite fortement l'impact du DMA sur la scène internationale car les autres ordres juridiques ne s'inspireront pas nécessairement de la législation européenne, étant donné qu'elle ne s'appliquera pas à leurs opérateurs économiques nationaux.

Un autre facteur susceptible de limiter le *Brussels Effect* du DMA est la considération accordée à cette législation. Même avant son entrée en vigueur, le DMA faisait déjà l'objet de critiques. Des questions se posent notamment sur la procédure entre la Commission européenne et les autorités de concurrence nationales, ainsi que sur son efficacité. À cause de ces critiques, les Etats tiers à l'Union européenne ont tendance à s'orienter vers une approche juridique différente de celle du DMA quant à l'encadrement des marchés numériques.

3.4. Conclusion sur le *Brussels Effect*

Il est évident que le RGPD et le DMA sont différents sur plusieurs points. Cependant, grâce à cette analyse, nous pouvons constater que ces deux législations possèdent un impact significatif sur la scène internationale. Bien qu'à première vue, la récente adoption du DMA semble avoir un impact moindre que celui du RGPD, nous pourrions tirer des conclusions plus définitives dans quelques années, une fois que son application aura été analysée sur le long terme.

⁷⁸ Règlement (UE) 2022/1925 du 14 septembre 2022, précité, article 6 paragraphe 5.

⁷⁹ Traduction libre de J. Blockx, *op. cit.*, p.11.

⁸⁰ J. Blockx, *Ibidem*, p.11.

De plus, une des conséquences notables du RGPD et du DMA est la prise de conscience des États tiers à l'Union européenne sur la nécessité de réguler le marché numérique. Le RGPD a exercé une influence internationale significative en matière de protection des données personnelles. Cette législation a agi comme un signal d'alerte, mettant en évidence l'impact potentiel des GAFAM sur les droits fondamentaux des citoyens et sur l'économie nationale des États concernant le transfert des données à caractère personnel et leur valeur économique.

Quant au DMA, bien qu'il ait eu un impact moins notable que le RGPD, il a également servi de catalyseur pour d'autres États. Ces derniers ont reconnu l'importance d'allouer des ressources supplémentaires afin de tenter de rétablir une concurrence loyale entre les opérateurs économiques, celle-ci étant essentielle pour le bon fonctionnement de leur économie nationale.

4. L'interaction entre le droit de la protection des données personnelles et le droit de la concurrence

Les parties précédentes de ce travail de fin d'études ont servi à démontrer l'importance qu'accorde l'Union européenne aux problématiques actuelles, notamment la concurrence déloyale avec le DMA et la protection des données personnelles avec le RGPD. Ces deux législations ont comme point commun leur dimension et leur impact international, notamment sur les entreprises numériques telles que les GAFAM.

La portabilité des données personnelles constitue une source de revenus importante pour les entreprises ciblées par ces législations. Cette partie constitue une analyse de la jurisprudence sur les interactions entre le droit de la protection des données et le droit de la concurrence, malgré leurs intérêts opposés à première vue.

4.1. Arrêt *Meta* C-252/21

Le Digital Markets Act est une législation récente. L'analyse de celle-ci par la jurisprudence, notamment par la Cour de justice de l'Union européenne, a toute son importance car elle donne la marche à suivre dans l'application de cette nouvelle législation.

Le 4 juillet 2023, la Cour de justice de l'Union européenne a rendu un arrêt dénommé *Meta*, qui a suscité beaucoup de commentaires en doctrine. Cette partie reprend le bref contexte de la décision de l'autorité de concurrence nationale allemande, le *Bundeskartellamt*⁸¹, suivi d'une analyse de l'arrêt de la Cour de justice de l'Union européenne et de ce que l'on peut en retirer.

4.2. L'autorité de concurrence allemande

Le 6 février 2019, l'autorité de concurrence allemande, appelée aussi le BKA, a rendu une décision interdisant à l'entreprise Meta, anciennement Facebook, de combiner les données

⁸¹ Ci-après le « BKA ».

des utilisateurs provenant de différentes sources sans leur consentement⁸². Selon cet office, le fonctionnement de Meta en ce qui concerne les données personnelles ne respecte pas la section 19(a)⁸³ de la législation allemande sur le droit de la concurrence, qui correspond à l'équivalent national de l'article 102 du TFUE.

La particularité de cette affaire réside dans le fait que le BKA a utilisé la non-conformité de Meta au RGPD, qui touche à la protection des données personnelles, pour justifier l'abus de position dominante de cette entreprise. Meta a décidé de faire appel de cette décision et de fil en aiguille, cette affaire arrive devant la Cour fédérale de justice allemande qui a décidé de poser plusieurs questions préjudicielles à la Cour de Justice de l'Union européenne.

4.3. La décision de la Cour de justice de l'Union européenne

Trois questions pertinentes se posent quant à cette affaire et quant aux potentielles interactions entre le droit de la protection des données personnelles et le droit de la concurrence.

Premièrement, est-ce qu'une autorité de concurrence est apte à prendre en compte une violation d'une disposition concernant le droit de la protection des données personnelles pour apprécier un abus de position dominante de la part d'une entreprise au sens de l'article 102 du TFUE⁸⁴ ?

La deuxième question pertinente pour ce travail est relative à la coopération entre l'autorité de protection des données et l'autorité de concurrence. La troisième question porte sur la notion de consentement qui, même si elle provient du RGPD, a une importance non négligeable en droit de la concurrence.

4.3.1. Prise en compte de la violation du RGPD par les autorités de concurrence

Dans son arrêt Meta, la Cour commence par rappeler que l'accès aux données à caractère personnel et leur exploitation revêtent une importance majeure dans le cadre de l'économie numérique⁸⁵.

En effet, les fournisseurs de plateforme se financent principalement par la publicité ciblée en ligne, qui nécessite la vente des données des utilisateurs. En accumulant la possession de ces données, les entreprises comme Meta renforcent leur position dominante sur le marché en

⁸² Traduction libre de Bundeskartellamt, « Facebook Proceedings concluded », *communiqué de presse*, 10 octobre 2024, disponible sur : https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html, consulté le 4/04/2025.

⁸³ Traduction libre de Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 6 des Gesetzes vom 5. Dezember 2024 (BGBl. 2024 I Nr. 400) geändert worden ist., disponible sur : <https://www.gesetze-im-internet.de/>, consulté le 4/04/2025.

⁸⁴ C.J., *Meta Platforms*, 4 juillet 2023, C-252/21, ECLI:EU:C:2023:537, point 35.

⁸⁵ C.J., *Ibidem*, point 50.

refusant l'accès à ces données aux potentiels nouveaux concurrents qui souhaitent exercer sur le marché.

En tenant compte de la spécificité du marché numérique, il va de soi que les données personnelles représentent des ressources importantes pour les entreprises. La conformité ou non d'un comportement d'une entreprise aux dispositions du RGPD peut constituer un indice important pour établir ou non un abus de position dominante⁸⁶.

Ce paramètre doit donc être pris en compte par les autorités de concurrence étatiques lorsqu'il y a lieu d'examiner si une entreprise abuse de sa position dominante. Le respect ou non du RGPD peut dès lors rendre plus facile la constatation d'une infraction en droit de la concurrence. De fait, dans les circonstances de l'espèce, la capacité d'accéder à des données à caractère personnel et à les traiter peut être vu comme un avantage concurrentiel en droit de la concurrence dans le cadre de l'économie numérique⁸⁷.

La Cour affirme ce principe dans l'arrêt *Meta*, en précisant qu'il peut s'avérer nécessaire qu'une autorité de concurrence d'un état membre examine la conformité du comportement de cette entreprise à des normes autres que celles relevant du droit de la concurrence, telles que des règles en matière de protection des données comme le RGPD⁸⁸.

Par ailleurs, une autorité de concurrence peut constater la violation d'une disposition, *in casu* du RGPD, qui ne relève pas initialement de son domaine de compétence, lorsque ce constat est nécessaire pour établir un abus de position dominante⁸⁹. Même si la protection des données en droit de la concurrence reste incidente, cette adaptation permet en premier lieu de renforcer l'efficacité des règles de droit de la concurrence et d'imposer des obligations à ces entreprises numériques.

Ce mécanisme permet indirectement d'imposer le respect des dispositions du RGPD en tant qu'obligation concurrentielle⁹⁰. Encore une fois, le lien entre la protection des données et le droit de la concurrence est indéniable.

La Cour met ainsi un terme aux doutes portant sur la possibilité de mobiliser le RGPD par les autorités de concurrence⁹¹. En effet, dans l'économie numérique, le droit de la protection des données personnelles et le droit de la concurrence doivent s'analyser de manière conjointe pour en assurer le respect de leur application.

⁸⁶ C.J., *Ibidem*, point 48.

⁸⁷ Traduction libre de A. GOREKA, "On the interplay between competition law and privacy: the impact of *Meta Platforms case*", *European Competition Journal*, 7 mars 2024, p.5.

⁸⁸ C.J., *Meta Platforms*, 4 juillet 2023, C-252/21, ECLI:EU:C:2023:537, point 48.

⁸⁹ C.J., *Ibidem*, point 63.

⁹⁰ L. Walz, « Abus de position dominante et RGPD : les combiner pour renforcer l'autonomie stratégique de l'UE (CJUE, 4 juillet 2023, *Meta Platforms e.a.*, aff. C-252/21, EU:C:2023:537) » in Arcelin, L. (dir.), *Les régulations européennes du numérique et le droit du marché*, 1e édition, Bruxelles, Bruylant, 2024, p. 97.

⁹¹ L. Walz, *Ibidem*, p. 95.

4.3.2. Coopération entre l'autorité de concurrence et l'autorité de protection des données

En principe, les différentes autorités administratives des États membres règlent leurs matières respectives comme elles l'entendent, de sorte que par exemple, l'autorité de concurrence n'est pas amenée à analyser une matière qui ne relève pas du droit de la concurrence. Ce principe s'applique à toutes les autorités administratives.

Cependant la Cour a affirmé et ce, de manière tout à fait raisonnée, qu'exclure les règles en matière de protection des données à caractère personnel du cadre juridique à prendre en compte par les autorités de concurrence lors de l'examen d'un abus de position dominante peut porter atteinte à l'effectivité du droit de la concurrence au sein de l'Union⁹².

Il est vrai que le mode de fonctionnement de l'économie numérique repose sur la vente et le transfert de données à caractère personnel, notamment pour la publicité ciblée. Ignorer ce paramètre en droit de la concurrence reviendrait à passer à côté de l'analyse d'un bon nombre de cas d'abus de position dominante, vu que l'accumulation de données personnelles demeure un indice majeur afin d'évaluer un abus.

Afin de lutter contre l'hégémonie des GAFAM, les différentes autorités nationales sont tenues par le principe de coopération loyale, en vertu de l'article 4, paragraphe 3 du TUE⁹³. Mettre en œuvre les objectifs de l'Union européenne nécessite de la part des états et, par extension, de la part de leurs autorités administratives, une assistance mutuelle et un partage d'informations.

Cette coopération loyale implique que les autorités administratives nationales peuvent demander une communication d'informations nécessaires à leur enquête, sans empiéter sur leurs compétences respectives.

Cependant, les autorités nationales de concurrence ou de protection des données ne doivent pas empiéter sur les compétences de l'une ou l'autre. Si le BKA avait directement appliqué le RGPD à cette affaire, sans considérer d'autres facteurs pour évaluer l'abus de position dominante de Meta, la réponse de la Cour quant à l'analyse du RGPD par une autorité de concurrence aurait été différente.

Le communiqué de presse de la CJUE précise que les autorités nationales doivent prendre en considération toute décision ou enquête de l'autorité de contrôle compétente en vertu du règlement en question⁹⁴. Cela signifie que si une autorité de protection des données a rendu une décision similaire que dans le cas auquel l'autorité de concurrence fait face, celle-ci ne peut pas l'ignorer et s'en écarter. L'autorité en question reste cependant indépendante et peut appliquer cette décision en fonction du droit de la concurrence.

⁹² C.J., *Meta Platforms*, 4 juillet 2023, C-252/21, ECLI:EU:C:2023:537, point 51.

⁹³ C.J., *Ibidem*, point 53.

⁹⁴ Comm. UE, communiqué de presse, 4 juill. 2023, n° 113/23, aff. C-252/21, *Meta Platforms*, disponible sur : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-07/cp230113fr.pdf>, consulté le 10/04/2025.

La Cour affirme donc que l'examen du RGPD par un office national comme le BKA est permis dans le concept plus large d'analyse de pratiques anticoncurrentielles⁹⁵, afin de permettre une coopération loyale et efficace entre les différentes autorités nationales.

4.3.3. La notion de consentement dans le RGPD et le DMA

Le consentement est la clé de voute du traitement des données à caractère personnel : si le responsable de traitement choisi le consentement comme base légale, il doit s'assurer que celui-ci a été exprimé de manière claire et univoque dans le chef des utilisateurs, afin de procéder audit traitement. Cependant, les GAFAM et autres fournisseurs de plateforme ont la réputation d'utiliser l'ambiguïté d'un texte juridique en leur faveur, au détriment des utilisateurs et à des fins financières.

Le consentement constitue une base légale fréquemment utilisée par les GAFAM car les utilisateurs prêtent rarement attention à la fenêtre pop-up qui s'affiche lors du lancement d'une application.

Ce manque de vigilance ou cette insouciance s'explique par une méconnaissance des implications réelles de l'acquisition et de la transmission de leurs données personnelles et par la volonté d'accéder directement au service sans prendre le temps de lire les conditions d'utilisation de l'application. Ces circonstances permettent aux GAFAM d'imposer leurs conditions contractuelles de manière unilatérale aux utilisateurs.

Le consentement est défini à l'article 4, paragraphe 11 du RGPD comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement⁹⁶. Il constitue une base légale afin d'obtenir la licéité du traitement qui permet *in fine* au responsable de traitement d'effectuer ledit traitement.

Cette notion est également présente dans le DMA à son article 5, qui interdit tout une série de comportements aux contrôleurs d'accès, notamment l'exploitation de données à caractère personnel, sauf si lesdits utilisateurs donnent leur consentement. Le dernier alinéa de l'article 5, paragraphe 2 fait expressément référence à l'article 4, paragraphe 11 du RGPD, pour définir la notion de consentement.

Le respect du consentement des utilisateurs s'applique donc tant aux responsables de traitement en cas de violation du RGPD, qu'aux contrôleurs d'accès, appelés aussi « *gatekeepers* », s'il existe une infraction dans le cadre du DMA et plus largement, en droit de la concurrence.

Il est également possible que le responsable de traitement et le contrôleur d'accès soient la même personne physique ou morale. Cette entité devra s'acquitter des obligations provenant de chaque législation qui s'applique à lui.

⁹⁵ Traduction libre de A. GOREKA, "On the interplay between competition law and privacy: the impact of Meta Platforms case", *European Competition Journal*, 7 mars 2024, p.5.

⁹⁶ Règlement (UE) 2016/679 du 27 avril 2016, précité, article 4 paragraphe 11.

La Cour de justice de l'Union européenne fournit une interprétation restrictive de la notion de consentement parce que cette notion représente une possibilité pour les utilisateurs de contrôler ce qu'il advient de leurs données, en refusant par exemple leur traitement. Elle rappelle d'ailleurs les propos du considérant 2 du RGPD, qui énonce que le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou encore de retirer son consentement sans subir de préjudice⁹⁷.

Il convient de comprendre à travers le raisonnement de la Cour, qu'afin de prouver que les utilisateurs bénéficient d'une véritable liberté de choix, une alternative au service initial doit être proposée. La Cour semble insinuer que cette alternative puisse être payante et plus précisément que lesdits utilisateurs se voient proposer, le cas échéant contre une rémunération appropriée, une alternative équivalente non accompagnée de telles opérations de traitement de données⁹⁸. La Cour fait uniquement référence au caractère payant de l'alternative dans ce paragraphe, ce qui laisse de la place pour l'interprétation et n'apporte pas une solution claire et précise au problème initial.

4.3.4. La réponse de Meta

Fin 2024, afin de remédier à la violation du respect du consentement de ses utilisateurs, Meta a proposé une solution spécifique à destination des citoyens européens.

Pour les réseaux sociaux tels que Facebook et Instagram, deux versions des applications sont proposées. D'une part, si les utilisateurs refusent de donner leur consentement pour l'exploitation de leurs données, qui ne permet donc pas à Meta de mettre en œuvre une stratégie de publicité ciblée, une version payante des réseaux sociaux est proposée. D'autre part, une version gratuite des réseaux sociaux reste disponible, avec l'obligation d'accepter de faire l'objet de la publicité ciblée.

La solution adoptée par l'entreprise Meta illustre la capacité contraignante de l'Union européenne à inciter les acteurs du numérique à adapter leur mode de fonctionnement en fonction de l'évolution de la législation européenne, afin de continuer d'exercer sur le marché européen⁹⁹.

Cette décision a fait l'objet de plusieurs critiques. En effet, l'ambiguïté créée par la Cour a donné la possibilité à Meta de pouvoir proposer ce système de deux types d'applications avec la version payante ou non. Ce choix économique pour se conformer à la législation européenne pose plusieurs questions sur la validité du consentement des citoyens européens.

⁹⁷ Règlement (UE) 2016/679 du 27 avril 2016, précité, considérant 42.

⁹⁸ C.J., *Meta Platforms*, 4 juillet 2023, C-252/21, ECLI:EU:C:2023:537, point 150.

⁹⁹ Traduction libre de A. SATARIANO et C. HAUSER, "In Europe, Meta Offers Ad-Free Versions of Facebook and Instagram for First Time", in *The New York Times*, 30 octobre 2023, disponible sur <https://www.nytimes.com/2023/10/30/technology/facebook-meta-subscription-europe.html>, consulté le 7/04/2025.

Premièrement, la question du déséquilibre des rapports de force entre le responsable du traitement ou contrôleur d'accès et les utilisateurs se posent, notamment en ce qui concerne le pouvoir effectif des utilisateurs à donner valablement leur consentement.

Le considérant 43 du RGPD rappelle que le consentement ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable de traitement¹⁰⁰. À ce stade de cette analyse, il est impossible de nier la position dominante des GAFAM sur le marché.

Elle est non négligeable parce que l'utilisation d'un réseau social comme Facebook ou Instagram est devenu incontournable. Ces entreprises bénéficient également du « *network effect* », c'est-à-dire un principe économique qui développe l'idée que plus des personnes utilisent un produit ou un service, plus sa valeur augmente¹⁰¹.

Ce principe constitue le mode de fonctionnement des réseaux sociaux, dans le sens où plus un réseau social devient populaire, plus les utilisateurs publient du contenu qui alimente cette plateforme, ce qui augmente l'intérêt des utilisateurs et par conséquent leur nombre sur la plateforme.

Ce mécanisme rend difficile la possibilité pour les utilisateurs de changer de plateforme et en même temps renforce leur dépendance vis-à-vis de celle-ci¹⁰². Il va de soi que personne n'a envie de quitter un réseau social ou changer de moteur de recherche quand tout le monde l'utilise et qu'il fonctionne correctement.

En outre, grâce à leur position dominante, ces plateformes disposent du temps et des moyens de se développer afin de devenir de plus en plus efficaces et innovantes, ce qui les maintient à distance de leurs potentiels concurrents.

Cette situation renforce encore une fois leur position dominante, ce qui empêche les concurrents d'entrer sur le marché et influence en leur faveur le choix des consommateurs.

L'ensemble de ces facteurs leur permettent d'imposer unilatéralement les conditions du contrat qu'ils passent avec leurs utilisateurs. En effet, ceux-ci ne peuvent qu'accepter leurs conditions d'utilisations vu qu'il n'existe pas d'autre plateforme attractive qui propose des services équivalents à ceux des GAFAM.

4.4. Avis du Comité européen de la protection des données

Suite à la demande des autorités de protection des données à caractère personnel néerlandaise, norvégienne et allemande, le Comité européen de la protection des données¹⁰³ a rendu un avis adopté le 17 avril 2024 sur les circonstances et les conditions dans lesquelles les modèles « consentir ou payer » mis en place par les grandes plateformes en ligne dans le

¹⁰⁰ Règlement (UE) 2016/679 du 27 avril 2016, précité, considérant 43.

¹⁰¹ Traduction libre de X., "What is the network effect?", in *Wharton Online*, 17 janvier 2023, disponible sur <https://online.wharton.upenn.edu/blog/what-is-the-network-effect/>, consulté le 7/04/2025.

¹⁰² Traduction libre de A. D'AMICO, D. PELEKIS, C. TEIXEIRA SANTOS et B. DUIVENVOORDE, « Meta's Pay-or-Okay Model », *Technology and Regulation*, 2024, p. 258.

¹⁰³ Ci-après : le CEPD.

cadre de la publicité comportementale peuvent l'être d'une manière qui constitue un consentement valable et en particulier un consentement donné librement, en tenant compte également de l'arrêt Meta rendu par la Cour de justice de l'Union européenne¹⁰⁴.

Cet avis fait suite à la solution proposée par Meta après de l'arrêt de la Cour. Le CEPD commence par rappeler les principes essentiels d'un traitement de données à caractère personnel présents à l'article 5 du RGPD, tels que le principe de minimisation des données, de transparence, de loyauté et de proportionnalité. Le CEPD rappelle que même si le traitement est fondé sur le consentement, il ne justifie pas la collecte de données à caractère personnel au-delà de ce qui est nécessaire à la finalité spécifique ou d'une manière qui soit déloyale à l'égard des personnes concernées¹⁰⁵.

En effet, la manière dont le traitement s'opère doit être suffisamment claire pour les utilisateurs afin qu'ils puissent comprendre ce qu'il advient de leurs données personnelles, afin de leur permettre d'évaluer plus efficacement la validité de leur consentement. Si le responsable de traitement parvient à prouver qu'il remplit les critères établis par le RGPD concernant le traitement des données concernées, les utilisateurs sont mieux informés et peuvent donner leur consentement en toute connaissance de cause.

En ce qui concerne l'alternative payante au service initial, qui ne contiendrait donc pas de publicité ciblée en échange d'une rémunération, le CEPD souligne que ce n'est pas la meilleure voie à suivre. En effet, la personne qui refuse de donner son consentement à des fins de publicité comportementale n'a pas d'autre alternative que de payer afin de continuer à bénéficier du service, ce qui lui cause inévitablement un préjudice financier.

Le CEPD précise que plus la version alternative diffère de la version avec publicité comportementale, moins il est probable que la version alternative soit considérée comme réellement équivalente, bien que cela reste une appréciation au cas par cas¹⁰⁶.

Dans la situation de Meta et des citoyens européens, l'alternative payante s'éloigne fortement de la version gratuite avec la publicité ciblée, dans le sens où, si un citoyen européen veut continuer à bénéficier d'un service qui était gratuit dès le départ, il est obligé de consentir à l'exploitation de ses données sous peine de subir un préjudice financier.

Pour un citoyen lambda qui ne saisit pas pleinement les implications des traitements de données à caractère personnel sur sa vie privée, il est logique pour lui de privilégier la version gratuite. Son choix lui permet de continuer à accéder au service initial sans avoir à passer en revue des conditions générales d'utilisation longues et complexes, que peu de personnes prennent le temps de lire. Nous pensons donc que ce système ne permet ni d'obtenir ni d'évaluer un consentement libre de la part des utilisateurs.

Le CEPD suggère de proposer une autre version gratuite qui n'utilise pas la publicité comportementale. Les opérateurs économiques concernés pourraient par exemple, proposer une version du service assortie d'une autre forme de publicité impliquant le traitement d'un nombre réduit de données à caractère personnel, par exemple de la publicité contextuelle ou

¹⁰⁴ Avis 08/2024 du Comité européen de la protection des données sur la validité du consentement dans le cadre des modèles « consentir ou payer » mis en place par les grandes plateformes en ligne, 17 avril 2024.

¹⁰⁵ Avis 08/2024 du Comité européen de la protection des données, *Ibidem*, p.20-21.

¹⁰⁶ Avis 08/2024 du Comité européen de la protection des données, *Ibidem*, p.35.

générale ou de la publicité fondée sur des thèmes que la personne concernée a sélectionnés dans une liste de sujets d'intérêt¹⁰⁷. Cela respecterait également le principe de minimisation des données, dans le sens où seules les données nécessaires à l'objet du contrat feraient l'objet d'un traitement.

Cette solution semble fonctionner en théorie. Cependant, à moins que les opérateurs économiques ne soient contraints d'adopter ce mode de fonctionnement, ils ne vont probablement jamais l'adopter d'eux-mêmes.

En effet, une publicité générale, donc moins ciblée sur les préférences spécifiques des consommateurs, serait beaucoup moins avantageuse financièrement car les données personnelles des utilisateurs seraient moins précises et par conséquent diminueraient drastiquement de valeur. Ce mode de fonctionnement serait contraire à celui du business model de Meta, dont le but est d'engranger un maximum de profit.

De surcroît, ces entreprises n'ont aucune raison d'adopter de telles mesures, étant donné que les avis du CEPD ne sont pas contraignants. Bien que ces mesures soient fréquemment suivies par les États, il n'existe pas d'incitation directe à les mettre en œuvre, à moins que ce ne soit pour éviter des poursuites. De plus, il n'est pas garanti que les États optent pour cette approche, vu le manque d'attrait économique pour eux de se conformer aux recommandations de ces mesures de *soft law*.

4.5. Conclusion de l'affaire Meta

Tout d'abord, la Cour tranche la controverse sur l'étanchéité des compétences quant à l'application de la législation. En effet, il est maintenant clair qu'une discipline juridique peut servir de fondement pour démontrer un abus, *in casu* un abus de position dominante, dans une autre discipline juridique. Cette approche permet de se rapprocher de la réalité du terrain, qui n'était pas initialement prévue par le législateur.

Il faut noter que les nouvelles technologies évoluent plus rapidement que la législation. Ce phénomène est en quelque sorte normal si l'on veut s'assurer qu'un processus législatif démocratique soit respecté. Par conséquent, les entreprises privées comme les GAFAM, bénéficient d'un avantage concurrentiel, dans le sens où elles ont le temps et les ressources nécessaires pour se développer sur le marché sans être soumises à trop de contraintes législatives, ce qui leur permet de consolider leur position dominante.

La Cour devient très utile dans ce genre de situation, en donnant la ligne à suivre en termes d'interprétation de la législation. La manière d'interpréter celle-ci permet aux États membres d'être plus efficaces dans sa mise en œuvre. Dans le cas de l'affaire Meta, la Cour offre la possibilité de prendre en considération certains critères qui, de base ne relèvent pas du champ d'application des autorités nationales de concurrence. La Cour s'adapte à l'évolution du marché numérique afin d'assurer la réalisation des objectifs de l'Union européenne.

En ce qui concerne la problématique du consentement des utilisateurs, nous pensons que cette question ne sera pas résolue aisément. La Cour de justice est restée évasive sur la

¹⁰⁷ Avis 08/2024 du Comité européen de la protection des données, *Ibidem*, p.36.

question de savoir si une version payante équivaut à une version gratuite avec publicité ciblée, ce qui laisse place à différentes interprétations et complique la recherche de solutions concrètes.

Bien que l'avis du CEPD soit pertinent et puisse offrir une voie pour garantir le respect des droits fondamentaux des citoyens et des dispositions du RGPD, il est illusoire de croire que les opérateurs économiques adopteront ce mode de fonctionnement de leur propre initiative, car cela entraînerait une perte financière pour eux. Le principe de consentement reste donc bafoué par de nombreux acteurs économiques. Il est donc nécessaire que des mesures fermes et contraignantes soient mises en place au niveau européen pour que les recommandations du CEPD aient un réel impact concret généralisé.

Conclusion finale

L'objet de ce travail de fin d'études a pour but de comparer deux législations mises en place pour remédier aux potentiels problèmes qui peuvent survenir sur le marché numérique. Le législateur européen procède à une mise en balance de deux objectifs a priori contradictoires de l'Union européenne : d'une part, la préservation de la libre concurrence sur le marché européen et d'autre part et d'une manière plus générale, la protection des droits fondamentaux des citoyens.

À l'issue de ce travail, nous pensons que l'approche conjointe de la protection des données personnelles et du droit de la concurrence est nécessaire pour faire face au phénomène des GAFAM tel que nous le connaissons aujourd'hui. Bien que cela n'ait pas été prévu initialement aujourd'hui car les nouvelles technologies évoluent rapidement et de manière inattendue. Par conséquent, une adaptation constante de la part de l'Union européenne est cruciale afin de rester en adéquation avec ses objectifs. Il est donc plus judicieux pour les institutions européennes et les états membres de mettre en commun ses compétences et ses connaissances pour d'appréhender ce phénomène au mieux.

Il est possible que la réaction de l'Union européenne ait été quelque peu tardive lors de la mise en œuvre d'une législation comme le Digital Markets Act. Il est clair que l'élaboration de cette législation constitue un processus démocratique qui, par essence, requiert un certain délai. Durant ce laps de temps, ces entreprises ont saisi l'opportunité de se développer et de consolider leur position dominante sur le marché.

Des amendes d'un montant non négligeable peuvent être imposées aux entreprises qui entravent l'accès au marché pour leurs concurrents ou qui imposent des conditions contractuelles inéquitables aux consommateurs. Cependant, elles demeurent des acteurs économiques puissants et continuent d'exercer des rapports de pouvoir inégaux envers les consommateurs.

En effet, elles possèdent les ressources économiques nécessaires pour couvrir le montant de ces amendes infligées par la Commission européenne ou par les autorités de concurrence nationales. Cela soulève des préoccupations quant au respect du principe de libre concurrence

et du droit fondamental à la protection des données, qui ne sont manifestement pas réglées par le DMA ou le RGPD.

Il est toutefois facile de critiquer l'Union européenne alors qu'elle s'efforce de résoudre un problème existant depuis des années. Nous considérons qu'il est essentiel de maintenir un regard critique en toutes circonstances, quelle que soit la situation. Cependant, nous ne pouvons pas reprocher à l'Union européenne de tenter une nouvelle approche afin de résoudre cette problématique.

De plus, le DMA n'est entré en vigueur qu'en 2023, de sorte qu'évaluer de manière définitive son efficacité nous semble un peu prématuré. Même si des problèmes de procédure semblent exister entre les autorités de concurrence nationales et la Commission européenne, rien ne permet d'affirmer qu'ils ne puissent pas être résolus. Les effets concrets du DMA doivent être analysés sur une période plus longue que deux ans.

La question de l'innovation fait couler beaucoup d'encre au sein de la doctrine. Il est évident que des législations comme le RGPD ou le DMA ne devraient pas freiner le développement des entreprises et l'innovation de manière plus générale. De nombreuses sociétés ont déjà traversé des procès majeurs en droit de la concurrence¹⁰⁸ et elles n'ont pas manqué de se plaindre du fait qu'ils avaient provoqué des retards de développement et d'énormes coûts. Pourtant, elles continuent de générer des milliards en exploitant les données des citoyens européens. Il est donc peu probable qu'elles rencontrent des difficultés quant à leur croissance.

Certains¹⁰⁹ affirment que les entreprises européennes sont à la traîne par rapport à leurs concurrentes internationales. Celles-ci pourraient se développer plus rapidement si elles ne devaient pas se conformer à la législation stricte de l'Union européenne. Cependant, cette assertion nous semble nuancée.

En effet, les entreprises américaines, par exemple, doivent également s'adapter au DMA pour opérer sur le territoire européen, ce qui les oblige à fournir des efforts qui pourraient limiter leur propre innovation. Certes, celles-ci n'opèrent pas uniquement sur le marché européen. Cela étant, leur puissance actuelle leur garantit une position dominante, indépendamment des défis réglementaires.

Enfin, il est essentiel de trouver un équilibre entre la course à l'innovation et la protection des droits fondamentaux. Comme l'illustre l'arrêt *Meta*, le droit à la protection des données personnelles et le droit de la concurrence sont intrinsèquement liés et mis en œuvre dans le même domaine. Le fait que ces entreprises soient en position dominante leur permet d'exploiter les données des utilisateurs à leur guise, ce qui peut constituer une atteinte au droit fondamental à la protection des données.

Ce sont également ces mêmes données qui leur ont permis d'atteindre cette position dominante, compte tenu de ce qu'elles représentent en matière d'échanges économiques

¹⁰⁸ Commission européenne, « Antitrust : la Commission inflige à Microsoft une astreinte de 899 millions d'euros pour non-respect de la décision de mars 2004 », *Communiqué de presse*, 27 février 2008, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_08_318, consulté le 11/05/2025.

¹⁰⁹ Voir en ce sens : M. DRAGHI, "The future of European competitiveness", in *Commission européenne*, 2024, disponible sur https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059, consulté le 10/05/2025.

internationaux. L'abus de position dominante et le transfert de données sont, dans ce cas, des vases communicants.

L'arrêt Meta souligne que le non-respect des droits fondamentaux peut être un indicateur de position dominante. Ainsi, une législation comme le DMA, bien que critiquée pour ses effets potentiellement limitants sur l'innovation, peut également jouer un rôle crucial, même de manière indirecte, dans la protection des droits des citoyens de l'Union européenne, notamment en matière de vie privée et de protection des données. Même si l'Europe semble en retard sur ce plan, d'autres paramètres doivent être pris en compte, ce qui relativise ce manque d'innovation.

En conclusion, nous pensons que le RGPD et le DMA peuvent grandement contribuer au bon fonctionnement de l'Union européenne face aux défis qu'elle rencontre. Il est impératif que l'Union européenne reste vigilante face aux évolutions du marché et aux dynamiques opérationnelles des entreprises afin de garantir une transition adéquate aux changements et de s'adapter aux transformations sociétales en cours.

Bien qu'aucune solution ne soit parfaite, une collaboration entre la Cour de justice européenne, les institutions européennes et les États nationaux pourrait permettre de promouvoir les intérêts de l'Union en faveur de la prospérité économique des États membres et du respect des droits fondamentaux des citoyens.

Bibliographie

1. Doctrine :

1.2. Ouvrages

Bradford A., "Introduction: The Brussels Effect", *The Brussels Effect: How the European Union Rules the World*, New York, 2020; online edn, Oxford Academic, 19 Dec. 2019, p. 1-404.

DEHAECK V., « Het voorstel van de (Europese) Wet Digitale Markten (Digital Market Act). Ex ante regels voor digitale poortwachters: grenzen aan het rijk van Amazon? » in *Eerlijke en vrije mededinging: wijsheid is maat*, 1^e editie, Bruxelles, Intersentia, 2021 p.35-41.

OLIVEIRA PAIS S., "Big data and big databases between privacy and competition", in J. CANNATAI, V. FALCE and O. POLLICINO (dir.), *Legal challenges of Big data*, Cheltenham, Edward Elgar Publishing Limited, 2020, p. 15-45.

Norodom, A.-T., « La comparaison des modèles normatifs européen, américain et chinois en matière de protection des données à caractère personnel : une illustration de l'utilisation stratégique du droit » in Bertrand, B. (dir.), *La politique européenne du numérique*, 1^e édition, Bruxelles, Bruylant, 2022, p. 175-207.

Walz, L., « Abus de position dominante et RGPD : les combiner pour renforcer l'autonomie stratégique de l'UE (CJUE, 4 juillet 2023, Meta Platforms e.a., aff. C-252/21, EU:C:2023:537) » in Arcelin, L. (dir.), *Les régulations européennes du numérique et le droit du marché*, 1^e édition, Bruxelles, Bruylant, 2024, p. 1-254.

1.3. Articles de revue

Bernaerts I., « Geen doeltreffend industriebeleid zonder doortastend mededingingsbeleid – Hoe het EU-mededingingsbeleid mee evolueert met de tijd », *R.D.C.-T.B.H.*, 2023/6, p. 762-775.

Castets-Renard C., « Le règlement général de protection des données : quel bilan cinq après son adoption ? », *Rev. Aff. Eur.*, 2021/1, p. 1-110.

D'AMICO A., PELEKIS D., TEIXEIRA SANTOS C. et DUIVENVOORDE B., « Meta's Pay-or-Okay Model », *Technology and Regulation*, 2024, p. 255-252.

GORECKA A., « On the interplay between competition law and privacy: the impact of Meta Platforms case », *European Competition Journal*, 7 mars 2024, p. 1-22.

Mourtada R., « Une brève présentation des GAFAM », *Questions internationales*, N°5, 2021, p.17 et 18.

Perray R., « Les outils de la conformité au RGPD : des outils de valorisation », *Rev. Aff. Eur.*, 2021/1, p. 35-47.

Sur S., « De quoi les GAFAM sont-ils le nom ? », *Questions internationales*, N°5, 2021, spéc. p. 4-11.

1.4. Recherches scientifiques et rapports

Blockx J., “The Digital Markets Act: Fostering Innovation ‘Made in Europe’?”, 31 mai 2023, p. 1-13, disponible sur SSRN: <https://ssrn.com/abstract=4487366> or <http://dx.doi.org/10.2139/ssrn.4487366>, consulté le 15/04/2025.

Cervi G.V., “Why and How Does the EU Rule Global Digital Policy: an Empirical Analysis of EU Regulatory Influence in Data Protection Laws.” *DISO* 1, 2022, p. 1-18, disponible sur <https://doi.org/10.1007/s44206-022-00005-3>, consulté le 16/04/2025.

Drewes, Helena and Kirk, Alexander, “Extraterritorial Effects of the Digital Markets Act - The ‘Elusive Long Arm’ of European Digital Regulation”, 18 mars 2024, p. 1-20, disponible sur SSRN: <https://ssrn.com/abstract=4763361> or <http://dx.doi.org/10.2139/ssrn.4763361>, consulté le 5/04/2025.

Tamim J., « The Brussels Effect and the GDPR: EU Institutions as Catalysts for Global Data Protection Norms », ResearchGate, 2024, p. 1-16, disponible sur : <https://www.researchgate.net/...>, consulté le 28/03/2025.

1.5. Recherches académiques

Bibliothèque nationale de France (BnF), « Naissance officielle d’Internet », *Passerelles.essentiels.bnf.fr*, [en ligne], disponible à l’adresse : <https://passerelles.essentiels.bnf.fr/fr/chronologie/article/a26aa768-a4b7-4fb3-823d-790c64b408a3-naissance-officielle-internet>, consulté le 7 mars 2025.

2. Jurisprudence de la Cour de justice de l’Union européenne :

C.J.C.E., arrêt C-94/00, *Roquette Frères*, 22 octobre 2002, ECLI:EU:C:2002:603.

C.J., arrêt C-131/12, *Google Spain*, 13 mai 2014, EU:C:2014:317.

C.J., arrêt C-311/18, *Schrems II*, 16 juillet 2020, ECLI:EU:C:2020:559.

C.J., arrêt C-252/21, *Meta Platforms*, 4 juillet 2023, ECLI:EU:C:2023:537.

3. Législation européenne :

Charte des droits fondamentaux de l’Union européenne, JO C 326 du 26.10.2012.

Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Directive (UE) n° 2019/2161 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de protection des consommateurs dans l'Union, JO L 328, 18.12.2019.

Règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE, n° L 119 du 4 mai 2016.

Règlement (UE) n° 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés numériques et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828, J.O.U.E., L 265, 12 octobre 2022.

Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, J.O.U.E, n°C 306.

Traité instituant la Communauté économique européenne du charbon et de l'acier (CECA), signé à Paris le 18 avril 1951, (1951) JO C 24.

Traité sur le fonctionnement de l'Union européenne (TFUE), signé le 13 décembre 2007, JO C 202 du 7.6.2016.

4. Législation internationale :

American Innovation and Choice Online Act." *Congress.gov*, Library of Congress, 2 mars 2022, S.2992 - 117th Congress (2021-2022) disponible sur <https://www.congress.gov/bill/117th-congress/senate-bill/2992/text>, consulté le 1/04/2025.

Australian Digital advertising services inquiry, *Australian competition and consumers commission*, 2021, disponible sur <https://www.accc.gov.au/system/files/Digital>, consulté le 1/04/2025.

Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 6 des Gesetzes vom 5. Dezember 2024 (BGBl. 2024 I Nr. 400) geändert worden ist., disponible sur : <https://www.gesetze-im-internet.de/>, consulté le 4/04/2025.

Digital Markets, Competition and Consumers Act 2024, c.13, disponible sur <https://www.legislation.gov.uk/ukpga/2024/13/enacted>, consulté le 1/04/2025.

Proposition de loi 2768/2022 (Brésil), 2022, disponible sur <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417&fichaAmigavel=nao>, consulté le 1/04/2025.

5. Sites internet :

Britannica, The Editors of Encyclopaedia, "Standard Oil.", *Encyclopedia Britannica*, 9 mai 2025, disponible sur <https://www.britannica.com/money/Standard-Oil>, consulté le 11/05/2025.

Commission européenne, "Data Flow and Economic Value EU Framework: Modelling Update and Data Collection", disponible sur <https://digital-strategy.ec.europa.eu/en/library/data-flow-and-economic-value-eu-framework-modelling-update-and-data-collection>, consulté le 28 mars 2025.

Maciejewski M. et Verdins R., « Les traités initiaux », disponible sur <https://www.europarl.europa.eu/factsheets/fr/sheet/1/les-traites-initiaux>, consulté le 17/03/2025.

SATARIANO A. et HAUSER C., "In Europe, Meta Offers Ad-Free Versions of Facebook and Instagram for First Time", in *The New York Time*, 30 octobre 2023, disponible sur <https://www.nytimes.com/2023/10/30/technology/facebook-meta-subscription-europe.html>, consulté le 7/04/2025.

X., « Mettre en œuvre les règles de concurrence de l'UE : l'application des articles 101 et 102 du TFUE », synthèse de la législation, Eur-lex, [en ligne], disponible à l'adresse : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3A12609>, consulté le 30/04/2025.

X., « population mondiale par continent », disponible sur <https://populationtoday.com/fr/>, consulté le 28/03/2025.

X., « Premières organisations et coopérations dans l'Europe d'après-guerre », disponible sur <https://www.cvce.eu/education/unit-content/>, consulté le 17/03/25.

X., "What is the network effect?", in *Wharton Online*, 17 janvier 2023, disponible sur <https://online.wharton.upenn.edu/blog/what-is-the-network-effect/>, consulté le 7/04/2025.

6. Soft Law :

Avis 08/2024 du Comité européen de la protection des données sur la validité du consentement dans le cadre des modèles « consentir ou payer » mis en place par les grandes plateformes en ligne, 17 avril 2024.

Bundeskartellamt, « Facebook Proceedings concluded », *communiqué de presse*, 10 octobre 2024, disponible sur : https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html, consulté le 4/04/2025.

Commission européenne, « Antitrust : la Commission inflige à Microsoft une astreinte de 899 millions d'euros pour non-respect de la décision de mars 2004 », *Communiqué de presse*,

27 février 2008, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_08_318, consulté le 11/05/2025.

Commission européenne, *Communiqué de presse n° 113/23 du 4 juillet 2023, affaire C-252/21, Meta Platforms*, disponible sur : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-07/cp230113fr.pdf>, consulté le 10/04/2025.

Communication de la Commission sur les lignes directrices sur les restrictions verticales 2022/C 248/01, OJ C 248, 30.6.2022.

DRAGHI M., “The future of European competitiveness”, in *Commission européenne*, 2024, disponible sur https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059, consulté le 10/05/2025.

OECD (2002), “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, OECD Publishing, Paris.