DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI DATA PROTECTION

Competition Law, Consumer Law and Data Protection Law in the Digital Economy: A Comparison Between the *Bundeskartellamt* and the *Autorità Garante della Concorrenza e del Mercato* Decisions Against Facebook

Relatore

Pierluigi Congedo

Candidata

Claudia Martorelli

Mtr. 153913

Correlatore

Francesco Ricci

Anno accademico 2020/2021

Table of Contents

CHAPTER III - COMPETITION, DATA PROTECTION AND CONSUMER PROTECTION

CHAPTER IV - THE *BUNDESKARTELLAMT* DECISION

CHAPTER V - THE *AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO* DECISION

INTRODUCTION

In recent years, the importance of digital services and products in our everyday lives has grown exponentially. However, the market for digital services is populated by only a few dominant companies that have attained such economic power as to be equal to or perhaps even greater than that of a state. This situation poses risks to the fundamental freedoms of individuals, and to the very functioning of democracy.

This market structure has been formed over time, and is the result of a number of factors, which will be analysed in the course of this thesis, such as the intrinsic characteristics of digital platforms, or the inadequacy of classical competition law instruments.

Economies of scale and scope, ecosystems, network effects, and the role of data are only a few of the characteristics of the digital economy which call traditional competition approaches into question. In particular, the "consumer welfare" approach, developed by the Chicago School in the US and followed, to a certain extent, even in the EU, is claimed to be 'unequipped to capture the architecture of market power in the modern economy'.[1] According to the New Brandeis School, which shares with the Ordo-liberals a number of leading values, this lack of attention to the harm produced by unchallenged market power is caused mainly by the pursue of just one particular outcome through antitrust law: 'efficiency'.[2] Rather, the focus of competition law should be on the competitive process, and not on specific outcomes.[3]

Furthermore, 'price-based measures of competition are inadequate to capture market dynamics, particularly given the role and use of data'.[4] Due to the so-called "datafication", access to data is increasingly often a key factor for companies to compete and innovate. Access to data represents a competitive advantage which can contribute to the entrenchment of the dominant position of a firm, allowing the latter to collect even more personal data about its consumers.[5] This is why, from a competition law perspective data should be shared among companies as the more data are disseminated through the greatest number of firms, the stronger competition is going to be. Against this backdrop, it is clear that data protection law

[1] Lina Khan, 'Amazon's Antitrust Paradox' (2017) 3 The Yale Law Journal 710, 710.
[2] Lina Khan, 'The New Brandeis Movement: America's Antimonopoly Debate' (2018) 9 Journal of European Competition Law & Practice 131, 132.
[3] Khan (n 1) 738.
[4] Ibid 746.
[5] Miriam Caroline Buiten, 'Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law' (2020) Journal of Antitrust Enforcement, 1-2.

(and consequently, its interpretation and enforcement) plays a crucial role as it establishes how and to what extent data sharing among different actors is lawful.[6]

Given that consumers can benefit from services "paid" with their personal data (and, possibly with the data of the closest relatives, friend and acquaintances), abuse of a dominant position is likely to result in harm to consumer privacy rather than in "traditional" forms of harm linked to the dynamics of price and product quality or quantity.[7] In particular, the continuous harvesting of data has led to the 'age of surveillance capitalism': 'a form of tyranny that feeds on people but is not of the people'.[8] This surveillance is characterised by a strong asymmetry of power between centralised online operators and end-users, who 'are generally left in the dark with regard to the data collected, processed or inferred about them'.[9] The freedom of the individual – conceived as freedom from manipulation – and the right to privacy, are increasingly seen in danger by many commentators, in the Privacy, Constitutional, Private and Competition law fields.

As a result, many scholars have begun to question whether it is necessary and/or legitimate for competition law to take into account the way companies collect and process consumer data and to sanction disproportionate data collection by dominant firms as it were a form of abuse of market dominance.[10] Some of them believe that a more synergistic approach between the two disciplines is desirable and appropriate to meet the new challenges posed by the so-called "datafication", while others claim that it is not the case, mainly because there is no evidence of a link between more data collection and harm to consumers.

In this context, two recent decisions against Facebook[11] issued by the *Bundeskartellamt* (the German Competition Authority, "BKA" hereafter)[12] and by the *Autorità Garante della Concorrenza e del Mercato* (the Italian Competition Authority, "AGCM" hereafter)[13] acquire particular importance in the debate over the role of data in the application of competition and consumer law. In particular, they both assessed how Facebook collects its users' personal data, although they followed a complete different path: while the BKA adopted the GDPR

[6] Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, *Competition Policy for the digital era* (Publications Office of the European Union 2019), 76.
[7] Buiten (n 5) 14.
[8] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019), 513.
[9] Primavera De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies' [2016] Journal of Peer Production, 3.
[10] Buiten (n 5) 1-2.
[11] For ease of reference, I will use the expression "Facebook" to refer indifferently to Facebook Inc., Facebook Ireland Ltd. and Facebook Deutschland GmbH. In addition, please note that Facebook Inc. has changed name in "Meta Platforms Inc." on October 28, 2021. Still, in this thesis I will refer to it using the generic expression "Facebook" as already clarified.
[12] Bundeskartellamt, 6 February 2019, B6–22/16—Facebook.
[13] AGCM, decision No. 27432 of 2018.

violation as a benchmark to assess Facebook abuse of dominance, the AGCM applied the "traditional" tool of consumer protection law.

In my thesis, I will compare the two decisions, considering the two different approaches applied, the effectiveness of the measures adopted and their consequences, having regard to the broader context mentioned above.

Therefore, in Chapter I, I will present the main characteristics of digital markets from an economic perspective; the "consumer welfare" standard and the "preservation of the competitive process" as opposed approaches in the present debate over the objectives of competition law.

In Chapter II, I will focus on the impact of data protection law over digital markets.

In Chapter III, I will deal with the relationship between competition law, consumer protection law and data protection law, considering in particular the ongoing debate about their possible convergence. I will conclude with a brief overview of the latest regulation proposals from the European Commission to tackle the issues linked to the characteristics of the digital economy, mainly with reference to the so-called "gatekeepers".

In Chapter IV, I will discuss and analyse the BKA decision against Facebook in Germany.

In Chapter V, I will discuss and analyse the AGCM decision against Facebook in Italy.

In Chapter VI, I will carry out a comparison between the two.

The conclusions will summarise what is the state of play of European legislation and jurisprudence and how, *de jure condendo*, should be the evolution in my opinion.

CHAPTER I

DIGITAL MARKETS AND COMPETITION LAW

1. Introduction

Since the economic rise of digital platforms, the underenforcement of competition law has led to the formation of conglomerates whose power is comparable to that of states, a power that is even more worrying when one considers the business model based on data collection, which seriously threatens the fundamental freedoms of individuals.

In order to fully understand these risks, however, it is necessary to understand the dynamics that characterise these platforms. A central element in this analysis will therefore be the dynamics related to the collection and exploitation of user data. In particular, these mechanisms are useful in understanding how the freedoms of the individual are under threat, especially the freedom of self-determination and the right to be left alone. Major digital services are in fact designed to stimulate user engagement as much as possible so as to be able to extract more data from them and use them to affect their ability to make decisions without being conditioned. This obviously also translates into a massive risk for the privacy of people's lives.

Against this backdrop, it will be easier to understand how the "consumer welfare" standard pursued in the application of antitrust law is inadequate to meet the challenges posed by the digital economy and to ensure effective consumer welfare. In fact, not only the application of "traditional" antitrust tools, based on the pursuit of "efficiency" and linked to economic indicators (such as price, quantity, turnover) are inadequate to catch the dynamics underlying the platform economy, but this inadequacy has also led to a general situation of underenforcement. This is why it is important to present alternative approaches, which could address more properly the present situation.

Therefore, in this chapter, I will give an overview on the main characteristics of digital platforms and explain why they can raise competition concerns. I will then focus on the role of data in the digital economy. I will explain why the "consumer welfare" standard is inadequate to catch actual harms to competition and I will present the main critiques proposed by the New Brandeis movement.

2. Economic Characteristics of Digital Platforms

Online platforms are the protagonists of the digital economy. Facebook, Amazon, Apple, Netflix and Google (also known as "FAANG") are the 'most powerful players in the Internet'[14] of the Western hemisphere. Thus, the most influential companies in the digital economy are platforms and they all share some common characteristics.

Platforms act as intermediaries between two or more group of users, in two-sided or multi-sided markets.[15] Generally speaking, it is possible to identify two groups of platforms: aggregators and marketplaces.[16] Aggregators provide a valuable service to their users, but they also facilitate the interaction between users and other groups of costumers.[17] An example of aggregator is Facebook, in which users benefit from the interaction with their friends and, at the same time, are confronted with personalised content in order to facilitate their interaction with advertisers.[18] On the other hand, online marketplaces have the objective to efficiently match consumers and suppliers of goods. An example can be Uber, which matches people needing a ride with drivers through data collection and analytics.[19]

In the literature, there is a consensus over a number of economic characteristics of such platforms which tend to cause competition concerns, such as network effects, economics of scale and scope, data as a key input and as a by-product.[20] However, there are also other characteristics, which have been devoted with less attention, such as the presence of a 'kill zone', or the development of ecosystems, which determine problematic effects for competition as well. This convergence of features causes a general tendency towards market tipping; meaning that markets are inherently inclined to a single dominant player,[21] and therefore firms will compete to "win" (*i.e.*, capture) the whole market rather than compete within the market.

As said before, one of the key features of platform markets is the strong network effect they experiment. There are different types of network effects and different ways to classify

[14] Philip Marsden, Rupprecht Podszun, *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement* (Konrad-Adenauer-Stiftung e. V. 2020), 12.
[15] Bundeskartellamt, 'Market Power of Platforms and Networks' (2016), 8.
[16] Georgios Petropoulos, 'Competition Economics of Digital Ecosystems' (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020), 2. The expressions used to define these types of platforms may change, for example in Bundeskartellamt, 'Market Power of Platforms and Networks' the authority uses the terms 'transaction platforms' and 'audience providing platforms'.
[17] Petropoulos (n 16) 2.
[18] Ibid.
[19] Ibid.
[20] Amelia Fletcher, 'Digital competition policy: Are ecosystems different?' (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020), 2.
[21] Stigler Committee on Digital Platforms, 'Final Report' (2019), 7-8.

them.[22] For the sake of simplicity, in this thesis I will consider only direct and indirect network effects. Direct network effects take place when users in a side of the market benefit from more users of the same group joining the platform. Indirect network effects occur when the increasing in the number of users of one side of the market will cause the increasing in the benefits experimented by users on the other side of the market.[23] For instance, in social networks the greater the number of users, the greater the usefulness of the service for those users (direct network effect). At the same time, the greater the number of users, the more useful the service will become to advertisers (indirect network effect).

Network effects mean that the value of the platform increases as the number of its users increases. If everyone uses Facebook, it would not make any sense to use a different social media which no one uses. As a result, "crowded" platforms will draw more users than smaller ones, and an eventual fall in the number of users will determine a drop in the quality of the service.[24] This concentration process is likely to eliminate competitors, as their slimming platforms would become unattractive.[25]

Furthermore, direct network effects represent a powerful barrier to market entry: since the switching costs may be high, consumers incentive to switch provider is reduced. In particular, the user would have to convince other users to switch platform as well (and these users would have to do the same with their connections).[26]

In this context, it is of major importance to analyse whether users are 'single-homing' or 'multi-homing'. Single-home users use only one service or product for a particular activity. Whereas, they are multi-home users when they use more than one service or product for the same activity. An example of single-homing is the case in which an individual uses only WhatsApp as an instant messaging service, while an example of multi-homing is when an individual uses interchangeably WhatsApp, Telegram, Signal, etc. In general, the more multi-homing users are present in the market, the easier it will be for platforms to coexist in that particular market. On the contrary, when the number of single-homing users of a given platform is high, even if only with regard to one side of the market, not only the market will be prone to tipping, but that platform will also become a "gatekeeper" to accessing that group of users.[27] In this way, the platform will gain the so called "bottleneck" power, meaning, it

[22] Bundeskartellamt (n 15) 9-10.
[23] Digital Competition Expert Panel, *Unlocking digital competition* (March 2019), 35.
[24] Ibid.
[25] Bundeskartellamt (n 15) 100.
[26] Ibid.
[27] Fletcher (n 20) 3.

would be capable of charging users on the other side of the market high prices to access single-homing users.[28]

This leads to another characteristic of platforms: the non-neutrality of price structure. In particular, the free service offered to users of one side of the platform is part of a differentiated price strategy aiming at the internalisation of indirect network effects.[29] In this case the cost of the service is carried by the user group which gains more benefits from the interaction with and the increasing number of users of the other side of the platform. Furthermore, the non-paying user group supplies data to the operator, who uses it to increase the quality of the service provided and to increase the benefits that the paying group of user derivers from the platform.[30] An example can be the fact that Facebook's social network service is available to users without them having to pay any money, whereas advertisers are charged to access the users of the social network.

Digital services are usually produced at a significant fixed cost but no or little marginal costs. Since the costs incurred when more users use the services of the platforms (marginal costs) are very low or even equal to zero, a platform can benefit from massive economies of scale in a very short period of time.[31] This means that once established, digital firms could rapidly grow through the expansion of their operations to new users at minimum cost.[32] This also means that 'no firm, unless armed with a much superior and cheaper technology, would want to enter a market dominated by an incumbent, even when this incumbent is making large profits'.[33]

Digital platforms usually benefit from economies of scope, meaning that, once they are able to offer one service, it is likely that they will become more efficient at offering others.[34] Economies of scope can arise from a number of factors, such as, (i) the control over data (which could facilitate the development of new services and products), (ii) network externalities (which could enable the leveraging of existing user base), (iii) the re-use of technologies that have been successful in different areas.[35]

In particular, by collecting and analysing massive amounts of data, firms can improve their product, but also expand their activities in new areas. This is especially true when the "new"

[28] Ibid.
[29] Bundeskartellamt (n 15) 36; Oliver Budzinski, Marina Grusevaja, Victoriia Noskova, 'The Economics of the German Investigation of Facebook's Data Collection' (2020), 11.
[30] Crémer, Montjoye, Schweitzer (n 6) 44.
[31] Marsden, Podszun (n 14) 13.
[32] Petropoulos (n 16) 3.
[33] Crémer, Montjoye, Schweitzer (n 6) 20.
[34] Ibid 33.
[35] Ibid.

market is connected to the market in which firms already operate. An example can be the access of Facebook to the dating market through Facebook Dating, a service that relies on data collected from the social network.[36] In this way, data previously collected in one market facilitates the development of competitive products in a related market. This can lead to the situation in which 'specialists in connected markets may be unable to compete successfully with ecosystem firms if it requires access to the data from the primary market'.[37]

Economies of scope can exist both at the production process and at the product development stage. This is especially true for digital products, which usually involve a modular design. A modular design means that a product is made by a series of independent building blocks, or modules, whose interactions are standardised.[38] Digital products are composed of hardware and software units which can be mixed in different products and services due to their interoperability. Because of that, each component can be employed across different product lines.[39]

It would be wrong to generally assume that large platforms would be able to enter new markets at any time and be just as successful. This assumption will lead to the result of considering all platforms as actual competitors on all Internet markets, which of course is not the case. In fact, even if a platform may easily extends its services or products to neighbouring markets, it still has to start from "scratch" to reach a critical mass of users. The most obvious case being the attempt of Google to expand in the social network market with Google+, where not even its huge reach was able to ensure the establishment of a new service.[40]

The incentives digital platforms have to enter connected markets and to develop new complementary products, led to the creation of the so-called "ecosystems".

First, it is important to point out that the concept of "ecosystem" is used to refer to two different situations defined as "multi-actor" and "multi-product" ecosystems.[41] In multi-actor ecosystems independent parties work together to create value that a single firm could not create alone.[42] In multi-product ecosystems, to which digital-contexts literature often refers, the term ecosystem identifies the array of products offered by a single corporate organisation,

[36] Marc Bourreau, 'Some Economics of Digital Ecosystems' (Hearing on Competition Economics of Digital Ecosystems 3 December 2020), 4.
[37] Ibid, 8.
[38] Ibid, 4.
[39] Ibid.
[40] Bundeskartellamt (n 15) 43.
[41] Fletcher (n 20) 2.
[42] Ibid.

'often through a variety of separate divisions or businesses'.[43] In this work I will only take into account the latter definition.

A part from economies of scale and scope, which relates to the supply-side of a product, there are a number of factors relating to the demand-side which facilitates the creation of multi-product ecosystems as well.

First, the greater the range of services offered by a business within its ecosystem, the more consumers it will attract.[44] For example, Facebook started by allowing friends to keep in touch, but now its users value also other services it provides, such as its communication tools, or its marketplace.

Second, users may prefer to use a single operator for a number of different services. This tendency is strengthened by the possibility for users to use a single digital ID offered by a given operator on third party sites. In this way, users can access different products avoiding the struggle of having to recall all their usernames and passwords.[45] For instance, Facebook login is available on almost any website or service. When users log in through their Facebook accounts some of their data are shared with the third-party whose service they are accessing to, depending on the privacy policy adopted by the specific service to which the user has agreed. This means that while some services may require access only to the data of users' public profile, others may adopt a more invasive approach. At the same time, users' data concerning the use of the service are shared with Facebook. For instance, users can access the PayPal service using their Facebook account: PayPal will share with Facebook their transactions and Facebook will share with PayPal their data and use of the social network (and possibly also data pertaining to their friends and contacts).[46] Furthermore, there are cases in which users do not even have a real choice as to whether to link their account to other accounts they have on different services. For instance, Uber asks to its "Driver-partners" to confirm their identity connecting their Facebook account or one of their verified digital

[43] Ibid.
[44] Fletcher (n 20) 6.
[45] Ibid.
[46] According to PayPal's Privacy Statement (version of September 9, 2021), when a user logs in with a third party's service, such as Facebook, PayPal "*will use your contact list information (such as name, address, email address) to improve your experience when you use the Services*" or "*may receive information from the third-party about you and your use of the third-party's service. For example, if you connect your Account to a social media account, we will receive Personal Data from the social media provider via the account connection*." This information is available at https://www.paypal.com/va/webapps/mpp/ua/privacy-full#7 under section 3 'What Personal Data Do We Collect?' and section 7 'How Do We Work with Other Services and Platforms?', accessed 3 November 2021.

payment methods to their Uber account.[47] A part from cases such as these, where users may be (more or less) conscious about their data being shared through different services, empirical evidence has shown that, when using Facebook's log in option, it is possible that also third party's trackers may obtain the data from users' Facebook accounts even if not authorised.[48]

Third, if a user wanted to move to a different service, switching will become harder if the consumer is using a range of different services offered by the same operator and if changing operator would imply the need to switch away from all of them.[49]

Lastly, some products encompass a "gateway role", meaning that once the user chose to use them, the user will keep making choices nested within that initial decision.[50] For example, consumers choosing to buy an iPhone will probably chose to buy a Mac rather than a computer provided with a different operating system. So, when a product ecosystem generates "consumption synergies", consumers will have more benefits in joining the ecosystem rather than using the same products offered by different and independent providers, everything else being equal.[51]

It is therefore safe to say that next to a core service provided by a platform there are often a number of complementary or connected services which define a sort of "zone of interest"[52] covered by the activity of the platform.

This leads us to discuss the issue of the numerous acquisitions of successful start-ups carried out by big digital platforms.[53] Some have compared this type of acquisitions to the so-called "killer acquisitions" in the pharmaceutical industry. However, in a killer acquisition an incumbent acquires a potential competitor with the aim of eliminating the target's innovation so to avoid a potential replacement effect.[54] On the contrary, in the digital sector, the project

---

[47] "*Driver-partners are responsible for getting their rider from A to B safely, and we want to make sure they have as much information as possible to ensure a safe ride. You will need to confirm your identity by connecting your verified Facebook account or adding a verified form of a digital payment method*" in Uber Help for riders, 'Why do I need to verify my account using Facebook?' <https://help.uber.com/riders/article/why-do-i-need-to-verify-my-account-using-facebook?nodeId=fc267a07-2867-4d9f-add6-54639e9d6a67> accessed 3 November 2021.

[48] "*The researchers found that sometimes when users grant permission for a website to access their Facebook profile, third-party trackers embedded on the site are getting that data, too. That can include a user's name, email address, age, birthday, and other information, depending on what info the original site requested to access*" in Louise Matsakis, 'The Security Risks of Logging in With Facebook' (*Wired*, 20 April 2018) < https://www.wired.com/story/security-risks-of-logging-in-with-facebook/> accessed 3 November 2021.

[49] Fletcher (n 20) 6.

[50] Ibid.

[51] Bourreau (n 36) 4.

[52] Crémer, Montjoye, Schweitzer (n 6) 121.

[53] Geoffrey Parker, Georgios Petropoulos, Marshall Van Alstyne, 'Platform Mergers and Antitrust' (2021) Boston University Questrom School of Business Research Paper No. 376351, 8 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3763513> accessed 21 July 2021.

[54] Crémer, Montjoye, Schweitzer (n 6) 117.

of the start-up acquired by the incumbent is rather integrated in the incumbent's ecosystem.[55] Facebook's acquisitions of WhatsApp and Instagram are a good example of this. In both cases, the targets competed with Facebook in a segment of its ecosystem, which also constituted autonomous markets.[56]

Therefore, the "zone of interest" of an incumbent acquires the characteristics of a sort of a "kill zone" in which start-ups are not willing to enter and in which venture capital may not invest.[57] This is due not only to the concern start-ups may have that their successful innovation may be copied or bought by dominant platforms,[58] but also to the difficulty they may find in raising funds or convince investors to finance their project if they are going to "compete" with established platforms.[59]

Even if in many cases, such acquisitions may bring efficiencies, for example in cases where start-ups provide innovative ideas, and the incumbent provides skills and financial resources needed to further develop and commercialise them, the systematic pattern of such acquisitions by dominant firms will contribute to the entrenchment of the dominant position of the platform.[60]

In fact, the systematic acquisition of successful start-ups operating in the zone of interest of the dominant platform may act as a defensive barrier from potential competition in the core market in which the platform operates.[61] This is even more likely to happen when the dominant platform can identify trends in consumer consumption patterns at an early stage and act accordingly.[62] In these cases, the dominant position of the acquirer is further entrenched because the new service acquired will increase the value of the ecosystem to those users for which it is complementary and also because the acquisition will help retaining those users for which the platform is partial substitute.[63]

The concerns deriving from the tendency to monopolisation in digital markets are usually overcome by the reference to their great innovation potential and dynamic nature. In particular, the stability of the dominant position acquired by some businesses is questioned in view of the disruptive innovation which characterises the Internet and according to which the

[55] Ibid 117-118.
[56] Ibid.
[57] Sai Krishna Kamepalli, Raghuram G. Rajan, Luigi Zingales, 'Kill Zone' (2021) University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2020-19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555915> accessed 21 July 2021.
[58] Crémer, Montjoye, Schweitzer (n 6) 117.
[59] Petropoulos (n 16) 6.
[60] Crémer, Montjoye, Schweitzer (n 6) 111.
[61] Ibid 121.
[62] Ibid.
[63] Ibid.

innovative business model of new comers could replace apparently solid market positions of incumbents 'in an instant'.[64]

In this way, many commentators support the assumption according to which the position achieved by incumbents in digital market should be considered to be permanently at risk.[65] Often, reference is made to how Myspace was replaced by Facebook in only a few years. However, 'it is likely that large digital companies have learned lessons from the experience of the rivals they replaced'.[66]

In fact, even if the threat of competition could encourage incumbents to invest in research and development, such investments are likely to be directed to the development of technologies thanks to which they will be able to further solidify their position and possibly to make successful entry less likely.[67] It is true that future technological developments are unpredictable as well as their impact on incumbents, but it appears that established digital firms are the ones being in the best position to decide in which way this development has to go. This is especially true if we consider that most technological developments are based on machine learning and artificial intelligence powered by large datasets to which established digital platforms have greater access.[68]

In the following section, I will analyse in greater detail the importance of data in the digital economy.

3. Data In The Digital Economy

In the last decade, the "datafication" of our day-to-day activities allowed companies to gather massive amounts of data which, *inter alia*, has changed how markets function.[69] In fact, as already said in the previous section, in the era of digital markets, services are commonly provided to consumers at no monetary cost. This is possible because of the business model adopted by many companies, which allows them to generate revenue through advertising. Companies that are able to collect more data also tend to develop more accurate consumer profiles, which can then be used to identify the ads that are most likely to get consumers to adopt a certain behaviour. Thus, if more data is collected, the more effective

[64] Bundeskartellamt (n 15) 71.
[65] Ibid 72.
[66] Digital Competition Expert Panel (n 23) 40.
[67] Ibid.
[68] Ibid 41.
[69] Crémer, Montjoye, Schweitzer (n 6) 24.

advertising will be and the more advertisers will be willing to pay to acquire advertising space on the platform or through the platform.[70] In this way, users' data are monetized and transformed into revenues.[71] Since many platforms offer valuable services to consumers in exchange for their attention and time, they are considered to operate in the context of "attention markets".[72]

Given that one of the aims pursued by these providers it to keep users connected for as long as possible, they have modelled their services exploiting how our brain works. Similar to slot machines, social networks use the so-called "variable reward schedules" to keep users engaged and to make them develop new habits.[73] Social networks provide us with potentially infinite successful social interactions – for instance in the form of Facebook's likes, comments from other users – but also with unpredictability – for instance in the form of notifications. Successful social interactions and unpredictability stimulate the production of dopamine, which gives us a general feeling of wellness so that we are encouraged to repeat the actions that led to its production in order to have more. The more certain actions lead to a reward, *i.e.*, in the form of dopamine production, the more our neurons reinforce the pathway associated with that action, thus creating new habits.[74] It has been demonstrated that the most effective way of achieving this result, is through "variable reward schedules", that is, when we cannot predict when we are going to have a reward, but we are expecting it.[75] For this reason, social networks' algorithms release notifications at frequencies that we perceive as random: 'if we perceive a reward to be delivered at random, and if checking for the reward comes at little cost, we end up checking habitually (*e.g.* gambling addiction).'[76]

An interesting documentary produced by Netflix, called "The Social Dilemma"[77] clearly explains how all this process works. At the core of products such as social media, usually

---

[70] Competition & Market Authority, Information Commissioner's Office, 'Competition and Data Protection in Digital Markets: a Joint Statement Between the CMA and the ICO' (2021), 9.
[71] Buiten (n 5) 1-2.
[72] Digital Competition Expert Panel (n 23) 22.
[73] Trevor Haynes, 'Dopamine, Smartphones & You: A battle for your time' (*Harvard University Blog*, 1 May 2018) <https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/> accessed 6 November 2021.
[74] "*Social media provide users with a consistent supply of social rewards, with each and every suggestion of social connection or reputation enhancement. For example, Facebook users can receive positive feedback in the form of a 'like,' or social connections in the form of a 'friend' request. Even minimalistic cues of social success such as these may activate our brain's reward system, and keep us coming back to Facebook for more*" in Dar Mashi, Diana I. Tamir, Hauke R. Heekeren, 'The Emerging Neuroscience of Social Media' 19 Trends in Cognitive Sciences (2015), 774.
[75] Haynes (n 73).
[76] Ibid.
[77] Skyler Gisondo, Kara Hayward, Vincent Kartheiser, 'The Social Dilemma' (Netflix 2020). The documentary is structured on a double track, one made up of testimonies from former employees of big tech companies on the functioning of platforms such as Facebook, Google, Twitter; the other shows the life of a teenager who is an

there are three algorithms working together to keep users connected as long as possible, but each focused on a different area: one is to increase the "engagement" of the user with the platform, one is for increasing the "growth" of the platform, one is for advertising. According to the documentary, the very aim of those services is to be able to manipulate users' behaviour to make them take decisions they would not have taken otherwise (*i.e.*, buying the product advertised, spend more time connected or posting a content or a comment and so on). This manipulation is possible thanks to very detailed profiles that those services are able to develop about their users, allowing them to predict with a high level of accuracy the behaviour of each of them.

Zuboff gives a sharp description of this process (which is also illustrated in Figure 1):

> *Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to product or service improvement, the rest are declared as proprietary behavioural surplus, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into prediction products that anticipate what you will do now, soon, and later. […] Eventually, surveillance capitalists discovered that the most-predictive behavioral data come from intervening in the state of play in order to nudge, coax, tune, and herd behavior toward profitable outcomes.*[78]

unconscious victim of the mechanisms developed to influence his behaviour through these platforms. In general, the documentary highlights the social and moral implications of abusing these platforms, which are designed to *de facto* gain control over individuals. Space is also given to how these services can control public opinion and, as a consequence, delicate processes such as political elections, without individuals being aware of it. However, the fact that this documentary was sponsored by Netflix, which is in any case one of the too-big-to-fail companies populating digital markets – such as those denounced in the documentary – makes one wonder. The publication of the documentary in exclusive on Netflix could be a strategy to focus attention on the negative aspects related to the platforms that are the subject of the documentary and, at the same time, to enhance the value of services such as those offered by Netflix. However, even Netflix, with its algorithm, may favour the creation of a bubble that prevents users from opening their minds to opinions different from their own, and yet this was not discussed in the documentary.

[78] Zuboff (n 8) 8.

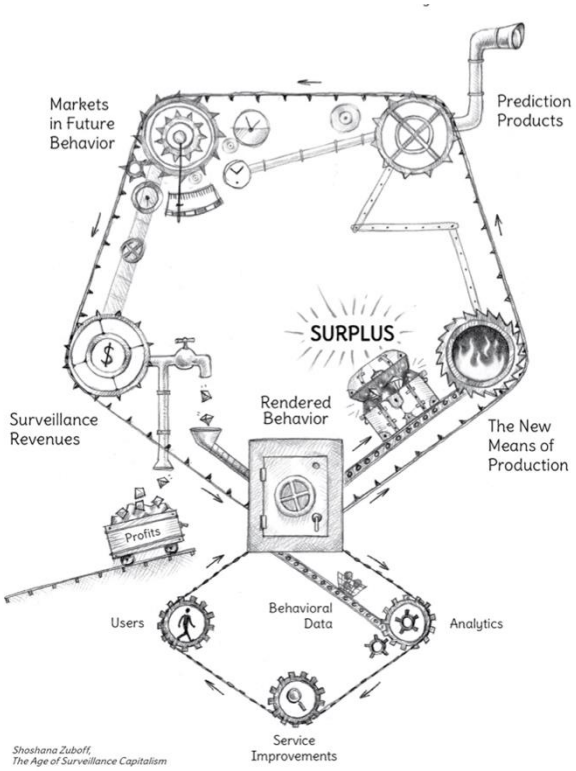

Figure 1 The Discovery of Behavioral Surplus, in Shoshanna Zuboff, The Age of Surveillance Capitalism (Profile Books 2019),97.

But, what is an algorithm? The most simple definition is "a sequence of instructions to achieve a given result". However, it has been acknowledged that there is no universal definition, as much depends on the context in which the algorithm is used. In the field of machine learning, an algorithm is a 'set of instructions a computer executes to learn from data.'[79] The aspect of learning and adapting is crucial in the field of social networks and digital platforms in general because the algorithm can learn how the user interacts with the service and can modify itself, and to a certain extent the service itself, to achieve a given goal.

Accordingly, the collection of user's data can also have positive implications, as, for example, a service may change to suit the user's needs; users could be able to find more easily services and products of interest thanks to targeted advertising; the analysis of large amounts of data can lead to efficiency and innovative new activities which could contribute to increased economic growth.[80]

However, massive data collection brings also risks for consumers. In fact, while consumers are usually fully aware of the price of the goods/services they consume, the level of privacy associated with the consumption of certain digital products or services constitutes one of the

[79] Kristian Lum, Rumman Chowdhury, 'What is an "algorithm"? It depends whom you ask' (*MIT Technology Review*, 26 February 2021) <https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/> accessed 6 November 2021.
[80] Competition & Markets Authority, 'The Commercial Use of Consumer Data' (2015), 2.

aspects that is probably less immediately perceptible and "quantifiable" by the consumer.[81] This information asymmetry also tends to produce effects within two different moments insofar as the release of data may give rise to an immediate benefit (e.g. improvement of the service) but, at a later stage, could have possible negative repercussions *vis-à-vis* the consumer. Indeed consumers are unable to evaluate pros and cons of giving away their data when deciding to use a given service and may not be aware of the consequences arising from the loss of control over their own data.[82]

Negative effects related to the use of digital platforms are not only those privacy-related, but can also take the form of psychiatric harms, such as anxiety, depression, diminished school performance.[83] A study has demonstrated that the very core of those social media which are based on the sharing of information about the individual, such as photos, videos and more generally highly curated content, can be particularly unhealthy for young adults as it encourages the so-called "social comparison", leading to a worsened perception of their life.[84]

A recent leak of Instagram's internal documents has shown that the social media is particularly addictive and harmful for the mental wellness of teenagers, especially girls: the focus of the social on "the perfect body" or "the perfect lifestyle", implemented through the content that the algorithm presents and highlights on the users' home feed, heavily promotes "social comparison" which makes teenage users feel worse about their body or their life, also leading to depression and/or food disorders.[85]

However, to properly understand the role of data in the digital economy, it is important firstly to understand which data are relevant in our discussion. Therefore, in the following sub-section, I will provide a brief classification of data and provide the definition of personal data as it emerges from relevant provisions of the General Data Protection Regulation ("GDPR" hereafter), the case law of the European Court of Justice ("CJEU" hereafter), and from the guidelines adopted by European institutions. Afterwards, I will focus on each of the

---

[81] Autorità Garante della Concorrenza e del Mercato (AGCM), Autorità per le Garanzie nelle Comunicazioni (AGCOM), Garante per la Protezione dei Dati Personali (GPDP), 'Indagine Conoscitiva sui Big Data' (2020), 90
[82] Ibid 88.
[83] James Niels Rosenquist, Fiona M. Scott Morton, Samuel N. Weinstein, 'Addictive Technology and Its Implication for Antitrust Enforcement' (2021) 100 North Carolina Law Review (forthcoming), 15-17 <Addictive Technology and Its Implications for Antitrust Enforcement by Niels J. Rosenquist, Fiona M. Scott Morton, Samuel Weinstein :: SSRN> accessed 6 November 2021.
[84] Luca Braghieri, Ro'ee Levy, Alexey Makarin, 'Social Media and Mental Health' (2021), 31 <Social Media and Mental Health by Luca Braghieri, Roee Levy, Alexey Makarin :: SSRN> accessed 5 November 2021.
[85] Georgia Wells, Jeff Horwitz, Deepa Seetharaman, 'Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show' (*The Wall Street Journal*, 14 September 2021) <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739> accessed 5 November 2021.

four steps acknowledged to be part of the "personal data value-chain",[86] meaning, (i) collection and access, (ii) storage and aggregation, (iii) analysis and distribution and (iv) usage of personal datasets. Finally, I will give an overview of the competitive dynamics linked to the availability of data to firms.

3.1. Data Classification

A first criterion of classification can be based on whether data are "structured" or not. This distinction is relevant in reference to their economic value. Indeed, for unstructured data to acquire commercial value, they need to be processed by state-of-the-art algorithms.[87] In fact, in situations where raw data is widely available and accessible to all, it is the development of particular proprietary algorithms, through investment and innovation, that is a source of competitive advantage.[88]

Data can be categorised on the basis of how they are collected. Data is often provided by users on voluntary basis (for example at the moment of registration), however they can be gathered also by 'tapping sources openly available on the internet or by observing user's behaviour, even without his or her knowledge'.[89] An example of how data can be collected by sources available to everyone is the so-called "crawling" carried out by search engines, a technique relying on systematic processing of all web pages available to the public.[90] An example of data collection through the observation of users' behaviour is the use of cookies thanks to which users can be tracked, *inter alia*, across webpages they visit.[91] The ways data are gathered by companies will be analysed deeper in the following sub-section.

In addition, data can be classified on the basis of whether they are generated from already existing data.[92] For example, data provided voluntarily can be combined with observed data and used as an input to algorithms so to allow online service providers to infer users' preferences[93] and develop accurate profiles.

Finally, a further criterion for classifying data is according to the information they provide. Large-scale datasets such as those available to digital platforms have favoured the emergence

[86] European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (2014), 6.
[87] Autorité de la Concurrence, Bundeskartellamt, 'Competition Law and Data' (2016), 6.
[88] AGCM, AGCOM, GPDP (n 81) 73.
[89] Autorité de la Concurrence, Bundeskartellamt (n 87) 7.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Petropoulos (n 16) 4.

of the expression "big data", which is commonly used to address datasets characterised by velocity, variety and volume (characteristics which give rise to the fourth "v", *i.e.* value).[94] Big data is more than personal data, since it embeds also anonymous data and aggregated data. However, even if many companies may regard their datasets to be mainly composed by non-personal data, this is unlikely to be the case for user-generated data.[95]

In fact, a significant share of the data generated is data on consumer behaviour,[96] *i.e.* data produced through the consumption of digital services (ranging from simply visiting a website to buying products online or using social networks and so forth). During their engagement with the service, which comprises their interactions with content and other users, users' actions and behaviour are observed.[97] Furthermore, at the moment of registration, users generally provide personal data on voluntary basis, such as, their name, age, gender, location email address, and so forth.

Understanding whether personal data are involved is important because in that case the GDPR applies to the operations carried out by companies.

Article 4 (1) defines personal data as

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

The concept of personal data has to be interpreted broadly, as suggested by the use of the expression "any information".[98] This definition covers any kind of statement about a living

[94] Marco Delmastro, Antonio Nicita, *Big Data: Come Stanno Cambiando il Nostro Mondo* (il Mulino 2019), 10. According to Gal and Rubinfeld, the characteristics of big data partially differ: "*Volume relates to the quantity of data points in the dataset. Velocity relates to the "freshness" of the data. Variety concerns the number of different sources from which the data are gathered, and veracity the accuracy of the data. The relative importance of each of these characteristics may differ among uses. For example, where old data can serve as a sufficiently effective input, velocity is unimportant.*" in Michal S. Gal, Daniel L. Rubinfeld 'Data Standardization' (2019) 94 New York University Law Review 737, 744.
[95] EDPS, 'Privacy and competitiveness in the age of big data' (n 86) 9.
[96] Crémer, Montjoye, Schweitzer (n 6) 77.
[97] Petropoulos (n 16) 4.
[98] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] EU:C:2017:994, para 34.

person, both objective and subjective, regardless of its correctness,[99] and of the format or the medium on which it is contained.[100]

Personal data relates to an identified or identifiable living person. A person is "identified" when he/she is distinguished from all other persons,[101] whereas he/she is "identifiable" when his/her identification is potentially achievable.[102] A person is directly identifiable when, in a given context, available identifiers are sufficient to single him/her out.[103] While he/she is indirectly identifiable when, in a given context, his/her identification could be possible combining available identifiers and other pieces of information, regardless of them being retained by the controller or by others.[104]

Even information which has undergone pseudonymisation is still personal data.[105] In fact, pseudonymisation is only a 'useful security measure',[106] used to prevent the attribution of the personal data being processed to the data subject in the absence of additional information.

Anonymous data is not personal data, therefore the processing of that kind of data is not subject to the GDPR. Anonymous data refer to information relating to a person whose identification is irreversibly prevented – the irreversibility has to be assessed considering all the means likely reasonably to be used either by the controller or by any other person. To ascertain which means are reasonably likely to be used, 'account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological development.'[107] This is a dynamic test, in which the controller has to consider the technological development that is likely to take place during the duration of the processing activity.[108]

To assess if an information is about a natural living person, at least one of these three elements should be present: content, purpose, effect.[109] The "content" element is present when the information is about a particular person.[110] The "purpose" element is present when the information is used or is likely to be used 'to evaluate, treat in a certain way or influence the

[99] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136 20 June 2017), 6.
[100] Ibid, 7.
[101] Ibid, 12.
[102] Ibid.
[103] Ibid, 13.
[104] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 48; WP29, 'Opinion 4/2007' (n 99) 13.
[105] Recital 26 GDPR.
[106] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP 216 10 April 2014), 3.
[107] Recital 26 GDPR.
[108] WP29, 'Opinion 4/2007' (n 99) 15.
[109] *Nowak* (n 98) [35].
[110] WP29, 'Opinion 4/2007' (n 99) 10.

status or behaviour of an individual.'[111] The "effect" element is present when the use of information is likely to have an impact on a certain person's rights and interests, being sufficient the mere possibility that the data subject will be treated differently from other persons as a result of the data processing.[112]

Most of the data processed by digital platforms are personal data. Even with regard to allegedly anonymous data, which are usually deployed by companies to carry out the profiling of their user base, it is possible to trace back the identity of a specific subject by crossing a series of databases.[113] Therefore, to the extent that data collected, or inferred, are related to an identified or identifiable natural living person residing in the European Union, the GDPR will apply. This means that companies' access to data will much depend on the way data protection law is interpreted and applied,[114] as we will see in Chapter 2.

3.2. Data Collection and Access

From the point of view of data acquisition, the advent of the digital era has amplified the material availability of publicly accessible personal data (through the information that users also voluntarily release on the Internet) and those that can be acquired on the market (for example from the so-called data brokers).[115] However, as we will see, the fact that data may be collected more easily than before does not imply that all types of data are substitute for one another,[116] or that they are actually accessible by firms.

Data is often collected directly from users as they make use of a product or a service. As pointed out by the AGCM, smartphones play a central role in the acquisition of user-generated data, as they can collect data from many sensors (such as motion, light, location), they are connected to the Internet and are used to carry out all kinds of activities. In this respect, the beneficiaries of the data generated through the use of smartphones are essentially the developers of the operating system used (*i.e.*, Apple or Google) and the developers of the apps installed on the device.[117]

Technically, the acquisition of user data is possible thanks to the use of specific tracking technologies that are now able to follow the user not only through different websites visited

[111] Ibid.
[112] Ibid 11.
[113] AGCM, AGCOM, GPDP (n 81) 24.
[114] Crémer, Montjoye, Schweitzer (n 6) 76.
[115] AGCM, AGCOM, GPDP (n 81) 85.
[116] Autorité de la Concurrence, Bundeskartellamt (n 87) 47.
[117] AGCM, AGCOM, GPDP (n 81) 13.

but also through different devices used. While some of these techniques may be easily avoided by users, others can be hard to escape.[118] An example can be the so-called "fingerprinting",[119] but there are many others, such as the so-called "zombie cookies".[120] With specific reference to web navigation, cookies are the most used tracking technologies, which are text files that collect preferences (e.g.: language, interface, geolocation, etc.) and information about the consumer (e.g.: pages visited, texts transmitted, etc.), allowing for precise profiling, which is updated on the occasion of each subsequent access to the same website.[121] In this regard, it should be noted that application and website developers usually outsource tracking technologies, relying on systems developed by large digital operators (such as Google Analytics and Facebook Business Suite), with the result that the data thus acquired are also available to the latter, which also acquire user data from the extremely popular operating systems and/or apps they offer.[122] The data collected from these sources can be combined up to the exact identification of the user.[123]

From the above it is clear that smaller businesses or new entrants which have a tighter user base will collect less first-party data (data collected directly from the customer) than larger and established counterparts. However, smaller companies may also buy and use third-party data (data collected by another entity). For example, data brokers aggregate consumer information from a variety of public sources and then sell it to other subjects. The possibility of sourcing data from external parties may be a way of compensating for the scarcity of first-party data, but in that case there are additional factors to be considered in order to define its actual utility, such as restrictions arising from data protection law or the actual usefulness of such data for the intended use.[124]

In fact, for many services, access to real-time data may be needed.[125] For example, retrospective data may be useful for analysing trends in consumer buying habits, but are completely useless for services that need constantly updated data, such as real-time bidding for ads or traffic data for services like Google Maps or search query data for search engines. In these latter cases, the data collected from the use of the service have a crucial relevance for

[118] Autorité de la Concurrence, Bundeskartellamt (n 87) 7.
[119] Geoffrey A. Fowler, 'Think you're anonymous online? A third of popular websites are 'fingerprinting' you.' (*The Washington Post* 31 October 2019) https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/ accessed 13 November 2021.
[120] The term is used to address those cookies that "respawn" after the user deletes them as they are generally stored in folders not used by the browser for that purpose.
[121] AGCM, AGCOM, GPDP (n 81) 13.
[122] Ibid 13-14.
[123] Ibid 78.
[124] Autorité de la Concurrence, Bundeskartellamt (n 87) 55-54.
[125] Crémer, Montjoye, Schweitzer (n 6) 104.

improving the service that cannot be compensated by the use of data purchased from external providers.[126] Thus, access to third-party data sets cannot always be useful to decrease discrepancies in data accessibility.

Moreover, a "knowledge asset" problem emerges. Data is a non-depreciating asset, since each single piece of data can be re-used. This means that firms know that a dataset might be valuable, but ascertaining its potential value (and how much it is convenient to invest in its collection and analysis) is difficult because they cannot preliminary assess how many times a piece of information can be re-used.[127]

Another way in which a company can increase the variety and volume of its databases is by acquiring or merging with a company that has the data it needs.[128]

Finally, there are data that can be acquired without having to interface with users or other firms, which are the so-called "open data", generally produced by public bodies and freely accessible to all.[129]

3.3. Data Storage and Aggregation & Data Analysis and Distribution

As rightly pointed out by the AGCM, when considered in isolation, data have little value, but they become valuable when they are organized. For this reason, a central role in the entire Big Data chain is played by the processing phase, which involves the organization of unstructured raw data into information that can be used for economic purposes. In this phase, knowledge can be extracted from large amounts of unstructured data, possibly in an easily interpretable format.[130]

The analysis of data is carried out using algorithms, tools capable of bringing out from raw unstructured data information susceptible of interpretation and practical use. The Italian Competition Authority, AGCM, distinguishes between algorithms of "interrogation" and algorithms of "learning". While the former aim to respond to precise requests from users, the

[126] CMA, ICO (n 70) 12; "*As reported by Google, 15 % of every day people's searches are new, implying that algorithms continuously need new data to be effective in providing the most relevant ranking of results to those new queries*" in Autorité de la Concurrence, Bundeskartellamt (n 87) 49.
[127] Nicolas Petit, David J. Teece, 'Taking Ecosystems Competition Seriously in the Digital Economy: A (Preliminary) Dynamic Competition/Capabilities Perspective' (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020), 7.
[128] Autorité de la Concurrence, Bundeskartellamt (n 87) 16.
[129] AGCM, AGCOM, GPDP (n 81) 14.
[130] Ibid 15.

latter aim to extract new knowledge using advanced techniques of Artificial Intelligence such as machine learning.[131]

The use of cutting-edge algorithms to analyse massive amounts of data is changing the process of knowledge extraction: in the so-called "data driven" model, data are not only used to confirm or verify hypotheses, but also and above all to discover new patterns and use these discoveries as a basis for developing new theories.[132] All this has determined a shift in the decision-making process of companies, which is also data-driven, in the sense that decisions can be taken directly on the basis of data, as well as on correlations between them, without the need for a complete prior understanding of the phenomenon being addressed.[133] Indeed, empirical evidence has shown that the productivity of companies relying on data-driven innovation increases faster than the one of companies not relying on this approach.[134]

It is worth remembering that high-quality data in larger quantities makes it possible to develop more efficient algorithms, so that in any case the problem of the inability, especially for small companies, to access user-generated data or sufficient data remains. Similarly, the larger the dataset the better.[135]

3.4. Usage of Datasets

Data is mainly used to offer personalised services to final users, to improve the quality of algorithms and artificial intelligence and therefore to improve the quality of services and products, and to extract useful knowledge to enter new markets.

Data are often used by enterprises to deliver highly personalized services to end users. For instance, e-commerce platforms can facilitate consumers' search by suggesting products that are most likely to meet their needs, thus reducing the searching time to the benefit of the consumer. The same method is adopted by on-demand content platforms, which suggest to the user content more akin to what he or she has liked in the past.[136] Examples include Amazon and Netflix. However, even if the benefit to the consumer is clear, a more subtle consideration is that in this way consumers risk slipping into so-called "bubbles" where products, content, but also opinions and more generally perspectives different from their own

[131] Ibid.
[132] Ibid 17.
[133] Ibid 18.
[134] Digital Competition Expert Panel (n 23) 23.
[135] Crémer, Montjoye, Schweitzer (n 6) 103.
[136] AGCM, AGCOM, GPDP (n 81) 103.

do not reach them, thus preventing them from changing their minds or engaging in constructive dialogue with people who have different opinions.[137]

Personalization involves profiling of users based on personal data, using machine learning, *i.e.* algorithms that adapt to the information they are fed. Profiling consists in the collection and processing of data relating to the users of a service, in order to segment them into groups according to their behaviour.[138] Usually, in order to profile the user, all data that can be traced back to the user, collected through its use of digital services, such as browsing history or search queries or location data, purchasing habits or data provided voluntarily, for example when registering for a service, such as name, age, sex, e-mail address, etc., are used. From this information it is possible to obtain a *precise profile of the user*, which can be used in different ways by companies, for instance, either to improve user experience or to offer new "contiguous" services, or even to personalise advertising communication and to practice differentiated prices according to estimated consumer spending capacities and price sensitivities.[139]

Online advertising based on the so-called "behavioural targeting" is an example of a business model which has become widely spread thanks to the technical developments described above, in which online ads are displayed to specific users on the basis of the profile generated thanks to the data collected about them.[140]

Regarding the improvement of products and services, the so-called "data feedback loop" plays a crucial role. The increasing quantity of available data, as well as of their quality, will help algorithms making better predictions, which will lead to better products and services. At the same time, data also plays a training function for algorithms, improving their quality through learning by doing. As a result, AI algorithms will become better at the tasks assigned to them.[141] It is therefore clear that for services where the user profile is the basis on which the product or service is developed, such as in the so-called "matching platforms" (as in online dating platforms), the quality/quantity of the data and the quality of the algorithms play a more important role in their development and improvement compared to different products and services.[142]

Lastly, data can also be re-purposed, making it possible for companies to explore new fields of business. In fact, data collected in connection to the provision of a given service can

[137] Budzinski, Grusevaja, Noskova (n 29) 12.
[138] AGCM, AGCOM, GPDP (n 81) 23.
[139] Ibid 86.
[140] Autorité de la Concurrence, Bundeskartellamt (n 87) 10-11.
[141] Petropoulos (n 16) 4.
[142] Autorité de la Concurrence, Bundeskartellamt (n 87) 10.

be used to gain a more efficient understanding of gaps in supply,[143] as well as to develop new services for which there is demand in a closely adjacent market.[144]

3.5. Competitive Dynamics

Access to data is now widely recognised as a competitive advantage. As we saw above, data is an essential resource for companies to offer competitive and cutting-edge products and services, which is why digital service providers in particular need to gain privileged access to data or develop better algorithms than their competitors.[145]

It is said that the broadest availability of data across the highest number of firms would ensure a healthier competition among companies.[146] As said earlier, there are different ways in which companies can acquire data, however, first-party data seems to be the most valuable in most cases. Therefore, the providers of the most popular services/products will have a privileged access to data which, in turn, will reinforce their position as they will have a higher chance to develop their products in accordance with future market trends than their competitors.[147]

However, the accumulation of large first-party datasets, essential to extract new knowledge, is subject to high fixed costs, easily absorbed by larger firms and not by new entrants or smaller firms. In any event, a prerequisite to the collection of first-party data remains the provision of a popular service, which can be difficult to achieve if significant investments are needed.[148]

The difficulties for smaller competitors to offer a competitive service due to restricted data access are likely to be self-reinforcing. In fact, more data makes possible the development of better services which can consequently attract more users – and, as a consequence, more data. *On the contrary, smaller companies may attract less users and, as a result, being able to collect less data*.[149]

[143] Digital Competition Expert Panel (n 23) 23.
[144] Petropoulos (n 16) 4.
[145] Autorité de la Concurrence, Bundeskartellamt (n 87) 15.
[146] Crémer, Montjoye, Schweitzer (n 6) 76.
[147] Petropoulos (n 16) 4.
[148] Autorité de la Concurrence, Bundeskartellamt (n 87) 38.
[149] Ibid 13

This is how data can act as a *barrier to entry* in digital markets. This mechanism is called "feedback loop" (a mechanism which I have already mentioned in the previous section concerning the improvement of products quality). There are two different forms of feedback loop: "user feedback loop" and "monetisation feedback loop". The former takes place when *data* collected by users is used to improve the quality of the product or service provided, which as a consequence attracts more users. The latter occurs when *revenues* generated from business users (such as advertisers in the case of targeted advertising) are reinvested in the improvement of the quality of the product/service provided, thus attracting even more users.[150]

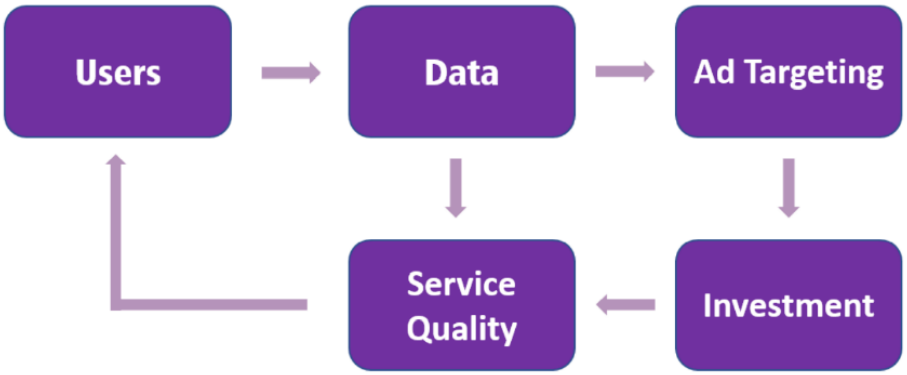

Figure 2. The left-hand loop represents user feedback, while the right-hand loop represent monetisation. Figure adapted from OECD, 'Big data: bringing competition policy to the digital era' (2016).

In this way, data access can foster network effects and further entrench the position of dominant firms. The combination of the access to a great amount of data and of subsequent network effect may, therefore, allow the first operators to enter the market (so-called "first movers") to benefit from a significant competitive advantage over potential new entrants.[151] This is especially true in zero-price markets where quality is practically the only dimension of competition. In fact, new entrants may not be able to provide a service/product of the same quality as those provided by incumbents and would not be able to compensate the lower quality by proposing lower prices.[152]

[150] Digital Competition Expert Panel (n 23) 33.
[151] AGCM, AGCOM, GPDP (n 81) 73.
[152] Autorité de la Concurrence, Bundeskartellamt (n 87) 29.

As a consequence, data-driven economies of scale and scope are particularly common when are determined by a privileged access to data relating to consumer behaviour[153] as it allows those "privileged" firms to develop their product and expand in neighbouring areas more easily than "non-privileged" ones.[154]

To conclude, it has to be highlighted that while consumers' data generally serve as a non-monetary form of consideration, their economics are very different from those of prices.[155] Indeed, the zero-price could still be a price too high to pay for consumers in comparison with the service/product they receive in exchange.[156] Furthermore, the value consumers place on certain services may not match the amount of data that is collected during their use. For instance, empirical studies suggest that consumers value email services 'almost 30 times more than access to social media, and yet they pay the same zero monetary price and may potentially give up more data in return in the latter case, suggesting they may not be getting such a good deal as they could'.[157] The two main factors which determine this market failure will be presented in more detail in Chapter 3.

For now it is enough to understand that in zero-price markets, the goals of competition law, data protection law and consumer law are increasingly difficult to separate, and that the traditional tools and approaches of competition law may not be adequate to address the new challenges brought by digital competition.

In the following sub-section, I will provide an overview of the "consumer welfare" standard of the Chicago School, which has constituted the leading approach in the application of competition law in the US and, only to a certain extent, also in the EU. I will also highlight the shortcomings of this approach when it comes to digital competition.

4. Consumer Welfare or Preservation of the Competitive Process?

To fully understand the decisions I will analyse in the following chapters, as well as the wider context of the present academic discourse about the interrelation between competition law and data protection law, it is necessary to provide a brief overview of the approaches followed in the application of competition rules. In order to do that, given the great influence

[153] Digital Competition Expert Panel (n 23) 32; Giovanni Pitruzzella, 'Big Data, Competition And Privacy: A Look From The Antitrust Perspective' (2016) 3 Concorrenza e Mercato, 19.
[154] Petropoulos (n 16) 3.
[155] Crémer, Montjoye, Schweitzer (n 6) 44.
[156] Digital Competition Expert Panel (n 23) 42.
[157] Ibid 42-43.

of the US approach over the EU one, I will start presenting the consumer welfare standard developed by the Chicago School in the 50ies and 60ies and how such a standard has influenced the EU approach. I will then focus on the Ordo-liberal perspective and on the critics moved by the so-called "Neo Brandeis School" to the consumer welfare standard.

Also relevant here the fact that the economic crisis of 2008 was a turning point to understand the risks linked to the underenforcement of antitrust laws. In fact, only at that moment the risks and consequences of the failure of too-big-to-fail companies became clear, especially with regard to the policies that would have to be adopted to save them, with unfair implications for taxpayers.[158] Since then, a number of criticisms have been directed at the Chicago School's approach,[159] culminating in the 2017 with the publication of Lina Khan's *Amazon Antitrust Paradox* and the prominence of the Neo-Brandeis school.

4.1. The Consumer Welfare Standard

The "consumer welfare" standard was developed in the context of the "law and economics" movement in Chicago, of which Aron Director was one of the major representatives. In a nutshell, this movement advocated for the application of economic analysis to law, so to assess its costs and potential economic efficiency. In particular, laws are included in the economic theory developed to explain the behaviour of economic actors.

A turning point in the rise of this movement was the foundation of the *Journal of Law and Economics* in 1958, of which Director was the first editor, then followed by Ronald Coase.[160] In 1960, Coase published an article, titled *The Problem of Social Costs*,[161] which is

[158] Jesse W. Markham Jr, 'Lessons for Competition Law from the Economic Crisis: The Prospect for Antitrust Responses to the "Too-big-to-fail" Phenomenon' (2011) 16 Fordham Journal of Corporate & Financial Law, 264.

[159] For an overview of those criticism, See John M. Newman, 'Reactionary Antitrust' (2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3454807> accessed 29 January 2022.

[160] Ejan Mackaay, 'History of Law and Economics' in *Encyclopedia of law and economics* (Edward Elgar Publishers 2000), 74.

[161] Robert Coase, 'The Problem of Social Cost' (1960) 3 The Journal of Law and Economics, in which the author analyses the role of transaction costs in facilitating or preventing private parties from negotiating for the resolution of conflicts. In particular, transaction cost are determined, *inter alia*, by laws: while high-quality laws keep transaction costs low, lo-quality rules increase transaction costs. For instance, when property rights are unclearly defined by law, private parties cannot bargain with each other and the number of disputes rises (being disputes a transaction cost). So, laws, transaction costs and property rights are key elements to determine the extent to which individuals can efficiently resolve conflicts among them.

considered to be a milestone in the evolution of the movement,[162] so much so that Hovenkamp describes it as the birth of the modern law and economics.[163]

However, the *laissez-faire* approach and the profit-maximisation paradigm together with the focus on simplistic price and profit dynamics, also stressed, later on, by Milton Friedman's 1970 *The Social Responsibility Of Business Is to Increase Its Profits*,[164] attracted a lot of criticism, especially following the 2008 economic crisis (which, as a recall, originated from the excessively risky behaviour held by some US banks in order to maximise their profits).

Aaron Director's works in the 1950's introduced the basic features of the Chicago School antitrust analysis, which were further developed by its students, most notably by Robert Bork.[165] Using price theory, Director criticised the Supreme Court case-law of being counterproductive with respect to "consumer welfare". In fact, the goal pursued by competition law, at that time, was the preservation of competition, which could result in the protection of less efficient companies at the expenses of consumers in terms of higher prices.

Two assumptions were at the basis of the Chicago School antitrust policy: the best tool to maximise economic efficiency is the neoclassical price theory model; the pursuit of economic efficiency[166] should be the sole objective of antitrust enforcement policy.[167] Antitrust enforcement should penalise conducts that are inefficient and tolerate and encourage those

[162] Robert Cooter, Thomas Ulen, *Law and Economics* (6th edn, Addison-Wesley 2012), 1.
[163] Herbert Hovenkamp, 'The First Great Law and Economics movement' (1990) 42 Standford Law Review, 994: "*The modern law & economics movement actually refers to the work of a group of economists and legal academics who carried economic analysis beyond explicitly regulatory subjects and into all areas of the law. The origin of the movement is sometimes identified with Ronald Coase's famous 1960 essay, The Problem of Social Cost […]*".
[164] Milton Friedman, 'The Social Responsibility Of Business Is to Increase Its Profits' (*The New York Times*, 13 September 1970).
[165] Richard A. Posner, 'The Chicago School of Antitrust Analysis' (1979) 127 University Of Pennsylvania Law Review 925, 925-926.
[166] The Chicago School predicated the maximisation of "allocative efficiency". According to Barak Y. Orbach "*Four concepts of efficiency also call for definition: static efficiency, productive efficiency, allocative efficiency, and dynamic efficiency. Static efficiency is optimization of production within present technologies to minimize deadweight loss. There are two forms of static efficiency: productive efficiency and allocative efficiency. Productive efficiency (or technical efficiency) describes the level of utilization of resources in the economy and is maximized with various combinations on the production possibility frontier of the economy. Put simply, optimal productive efficiency exists where the economy utilizes resources in the least expensive way possible. Allocative efficiency is focused on the consumer's willingness to pay. Maximum allocative efficiency is attained when the cost of resources used in production is equal to the consumer's willingness to pay. That is, allocative efficiency is maximized when market price is equal to marginal cost. Dynamic efficiency means increases in resources through investments in education and research and development*." from Barak Y. Orbach, 'The Antitrust Consumer Welfare Paradox' (2010) 7 Journal of Competition Law & Economics 133, 141.
[167] Herbert J. Hovenkamp, 'Antitrust Policy After Chicago' (1985) 84 Faculty Scholarship at Penn Law 213, 226.

that are efficient.[168] In any case, State intervention could be allowed only in exceptional cases.[169]

Director's theories began to spread mainly because of the works of Robert Bork and by the 80ies the consumer welfare standard of the Chicago School became the leading approach in the application of antitrust law.[170] This is due to three major reasons.

First of all, Bork argued that, according to a careful analysis of the *travaux préparatoires* of the Sherman Act, the maximisation of the consumer welfare was the overriding objective pursued by the Congress.[171] In fact, 'not only was consumer welfare the predominant goal expressed in Congress but the evidence strongly indicates that, in case of conflict, other values were to give way before it.'[172] As a result, when applying antitrust law, courts are required to distinguish between 'agreements or activities that increase wealth through efficiency and those that decrease it through restriction of output.'[173] In this way, Bork was able to prove that Directors' "consumer welfare" idea was not only an economist's perspective on what the law should do, but that it had been from the beginning the actual intent of the law.[174]

Secondly, Bork managed to depict the consumer welfare approach as a way to restrain the judicial. In fact, he argued that the variety of values pursued by antitrust law was too vague and it would promote judicial irresponsibility since 'often a court will apply a value in deciding a Sherman Act case without explaining either the selection of the value or the method of its application to the facts.'[175] Thus, according to Bork,

> *one is tempted, and perhaps occasionally entitled, to suspect that such a suddenly appearing of value is a deus ex machina by which the court rescues itself from the perplexing tasks of economic analysis and judgment that rigorous adherence to a consumer-welfare value premise would sometimes require.*[176]

Finally, Bork offered judges a rather simple way to deal with difficult cases. They could overcome all those complications implied by the application of antitrust law as they knew it

[168] Ibid 229.
[169] Ibid 231.
[170] Tim Wu, 'After Consumer Welfare, Now What? The "Protection of Competition" Standard in Practice' (2018) Columbia Public Law Research Paper No. 14-608, 1.
[171] Robert H. Bork, 'Legislative Intent and the Policy of the Sherman Act' (1966) 9 The Journal of Law & Economics 7, 7.
[172] Ibid, 10.
[173] Ibid, 7.
[174] Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (Columbia Global Reports, 2018), 87-88.
[175] Bork (n 171) 8.
[176] Bork (n 171) 8.

by adopting his 'disciplined and single-pointed theory that yielded straightforward answers.'[177]

The consumer welfare standard has been the main used metric in the application of antitrust law, even if its modern interpretation only considers *high output and low prices as the true goal of antitrust*, while efficiency is merely a means to achieve it.[178]

Over the 50ies the European Community adopted its own antitrust system, which was modelled over the American Sherman Act.[179] However, from the beginning, European competition law was dedicated to the protection of human freedom and democracy[180] and the "more economic approach" introduced later on by the Commission,[181] and subsequently followed also by other EU institutions, did not manage to fully overcome this commitment. The "European Consumer Welfare Standard" is not only about protecting consumers from price increases and restrictions of outputs, it is also about ensuring the conditions necessary for product quality and consumer choice to prosper for the sake of the whole society.[182]

Until the 90ies, the Commission remained bound by the values of the Ordo-liberal Freiburg School – which I will present in more details in the following section – and only after the adoption of the Merger Control Regulation 4064/89, it began a process of "Americanisation", where the Commission progressively developed its own version of the consumer welfare standard.[183] This process subsequently expanded also to the application of articles 81 and 82 EC Treaty (now articles 101 and 102 TFEU),[184] areas in which the European approach was

[177] Wu (n 174) 91.
[178] Herbert Hovenkamp, 'Is Antitrust's Consumer Welfare Principle Imperiled?' (2019) 45 Journal of Corporation Law 101, 125.
[179] Wu (n 174) 82.
[180] Ibid.
[181] The "more economic approach" was first introduced by former Commissioner for Competition Policy, Mario Monti, See Mario Monti, 'A Competition Policy for Today and Tomorrow' (2000) 23 Journal of World Competition.
[182] Agustín Reyna, 'The Shaping of a European Consumer Welfare Standard for the Digital Age' (2019) 10 Journal of European Competition Law & Practice, 1.
[183] Andreas Weitbrecht, 'From Freiburg to Chicago and Beyond – the First 50 Years of European Competition Law' (2008) 29 European Competition Law Review 81, 84-85.
[184] See Communication from the Commission — Notice — Guidelines on the application of Article 81(3) of the Treaty [2004] OJ C 101/98, para 21: "*Restrictions by object such as price fixing and market sharing reduce output and raise prices, leading to a misallocation of resources, because goods and services demanded by customers are not produced. They also lead to a reduction in consumer welfare, because consumers have to pay higher prices for the goods and services in question.*" See also Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/03, para 5: "*In applying Article 82 to exclusionary conduct by dominant undertakings, the Commission will focus on those types of conduct that are most harmful to consumers. Consumers benefit from competition through lower prices, better quality and a wider choice of new or improved goods and services. The Commission, therefore, will direct its enforcement to ensuring that markets function properly and that consumers benefit from the efficiency and productivity which result from effective competition between undertakings.*"

criticised 'for not being based on sound economic analysis and for protecting competitors rather than competition'.[185]

However, at first, this shift was not mirrored by the case law of the European Court of Justice (CJEU), which was rather focused on 'multiple goals, both economics based and non-economics based'.[186] In fact, the CJEU reiterated in several judgments that European competition law is about protecting competition as a means to ensure the EU wellbeing, the safeguard of the public interest as well as consumers' and competitors' interests.[187]

Eventually, the CJEU adopted some of the ideals advocated by Commission's more economic approach, especially the approach based on evaluating the actual effects of a conduct on the market before qualifying it as anticompetitive.[188] According to Witt, this shift of approach can be seen in a number of cases, such as, *inter alia*, *Post Danmark I*[189] and *Intel*.[190]

This shift in the approach of antitrust enforcement was not seen favourably by Germany, who opposed to this so-called "modernisation" of EU competition law.[191] In particular, Germany was the only European country to oppose both the procedural change (in which the Commission would play a central role in the enforcement of competition law) and the substantive change (*i.e.*, the application of classical economic theory to the enforcement of competition law) probably due to the fact that it was the only European country with a rather developed antitrust tradition.[192] Against this backdrop, the *Bundeskartellamt*'s decision

---

[185] Pinar Akman, 'Searching for the Long-Lost Soul of Article 82EC' (2009) 29 Oxford Journal of Legal Studies 267, 268.

[186] Roger D. Blair, D. Daniel Sokol, 'Welfare Standards in U.S. and E.U. Antitrust Enforcement' (2013) 81 Fordham Law Review 2497, 2512.

[187] See for instance Case C-8/08 *T-Mobile Netherlands BV, KPN Mobile NV, Orange Nederland NV, Vodafone Libertel NV v Raad van bestuur van de Nederlandse Mededingingsautoriteit* [2009] ECLI:EU:C:2009:343, para 38 "*Article 81 EC, like the other competition rules of the Treaty, is designed to protect not only the immediate interests of individual competitors or consumers but also to protect the structure of the market and thus competition as such*"; Case C-52/09 *Konkurrensverket v TeliaSonera Sverige AB* [2011] ECLI:EU:C:2011:83, paras 21-22 "*Article 102 TFEU is one of the competition rules referred to in Article 3(1)(b) TFEU which are necessary for the functioning of that internal market. The function of those rules is precisely to prevent competition from being distorted to the detriment of the public interest, individual undertakings and consumers, there-by ensuring the well-being of the European Union*".

[188] Anne C. Witt, 'The European Court of Justice and the More Economic Approach to EU Competition Law—Is the Tide Turning?' (2019) 64 The Antitrust Bulletin, 173.

[189] Case C-209/10, *Post Danmark A/S v Konkurrencerådet* [2012] ECLI:EU:C:2012:172, para 22: "*Thus, not every exclusionary effect is necessarily detrimental to competition (see, by analogy, TeliaSonera Sverige, paragraph 43). Competition on the merits may, by definition, lead to the departure from the market or the marginalisation of competitors that are less efficient and so less attractive to consumers from the point of view of, among other things, price, choice, quality or innovation*."

[190] Case C-413/14 P, *Intel Corporation Inc. v Commission* [2017] ECLI:EU:C:2017:632, para 134, where the Court reiterates the passage from Post Danmark cited above.

[191] David J. Gerber, 'Two Forms of Modernization in European Competition Law' (2008) 31 Fordam International Law Journal, 1260-1261.

[192] Ibid.

against Facebook may be seen as the breaking point with the approach followed by the European institutions.

According to Wu, Europe 'continues to enforce a law it borrowed from the United States in a manner more like America once did'; now it leads in the scrutiny of "big tech", and 'its leadership and willingness to bring big cases when competition is clearly under threat should serve as a model for American enforcers and for the rest of the world'.[193]

4.2. The Preservation of the Competitive Process

The debate over the objectives and legal standards of competition law has intensified with the rise of "digital competition" (to distinguish the new industry from the previous "hammer and bolts" industry).

On the one hand, non-interventionists argue that the threat of disruptive innovation pressures urges dominant firms to innovate and compete, therefore there is no need for Governments to intervene. On the other hand, others claim for more State intervention since while monopolies of the past might have forced consumers to accept higher prices and poorer quality products, abuses by big tech companies of today will affect also their privacy, wellbeing and democracy.[194]

In particular, over the past few years, and in the light of the inadequacy of price-based measures to address the competition issues brought by the development of big digital platforms, the values that once led antitrust enforcement prior to the Chicago School emerged again through the so-called "Neo-Brandeis" movement whose beliefs align closely to the Ordo-liberal's ones.[195]

The Neo-Brandeis School is named after Louis D. Brandeis, an American jurist who lived at the turn of the 19th and 20th centuries, appointed as a Supreme Court Justice in 1916 and regarded as the founding father of the right to privacy. Brandeis believed that any form of market concentration is a threat to democracy and to the social development of the individual.[196]

The Ordo-liberal movement or the Freiburg School founded by Walter Eucken, Franz Böhm and Hans Grossmann-Doerth and developed at Freiburg University in Germany

[193] Wu (n 174) 131.
[194] Ariel Ezrachi, Maurice E. Stucke, 'The Fight Over Antitrust's Soul' (2018) 9 Journal of European Competition Law & Practice 1, 1.
[195] Wu (n 174) 82.
[196] 'Mr. Justice Brandeis, Competition and Smallness: a Dilemma Re-examined' (1956) 66 The Yale Law Journal, 69.

between the 30ies and the 40ies considered that the law should protect market processes from distortion caused by the State public power or by the private economic power of large firms.[197] This position was a response to the fact that the Nazi government had been able to use private economic power in the iron and steel industry for its authoritarian purposes, thus translating the economic power of cartels and monopolies into political power. The leading purpose of Ordo-liberal competition policy is to achieve individual economic freedom, which could be done through the preservation of the competitive process and the control of economic power.[198] German competition law was considerably influenced by the Freiburg School and since Germany was the only European Member State which had a developed national competition law, German ideas become highly influential in EEC Competition law and policy for many years.[199]

The New Brandeis antitrust is a paradigm born in the US in response to the US antitrust enforcement attitude in the technology sector, which has led to the entrenchment of the dominant position of few companies to the detriment of competition, and possibly, of consumers. Scholars supporting this new approach argue that the main constraint of the consumer welfare paradigm is that 'it does not consider the social consequences of concentration, including wealth and income inequality, privacy intrusions, data security breaches as well as political corruption'.[200]

This lack of attention to the harms produced by undue market power is caused mainly by the fixation on promoting one particular outcome through antitrust law: 'efficiency'.[201] In particular, linking anticompetitive conducts to high prices or lower output, while disregarding whether and how market power is being acquired, undermines effective antitrust enforcement because intervention is restricted 'to the moment when a company has already acquired sufficient dominance to distort competition'.[202]

According to the New Brandeis School, antitrust law 'should focus on structures and processes of competition, not on outcome'.[203] In fact, using antitrust law to promote the achievement of social goals would replicate the mistake of the Chicago School, *i.e.*,

[197] Akman (n 185) 273.
[198] Liza Lovdahl Gormsen, 'The Conflict Between Economic Freedom and Consumer Welfare in the Modernisation of Article 82 EC' (2007) 3 European Competition Journal 329, 334.
[199] Weitbrecht (n 183) 82.
[200] Marco Botta, Silvia Solidoro, 'Fourth Annual Conference: Hipster Antitrust, the European Way?' (2020) Florence competition programme, 2.
[201] Khan, 'The New Brandeis Movement' (n 2) 132.
[202] Khan, 'Amazon's Antitrust Paradox' (n 1) 738.
[203] Khan, 'The New Brandeis Movement' (n 2) 132.

concentrating on a narrow set of outcomes rather than on processes and power inquiry.[204] Consequently, antitrust law should not encourage welfare, but rather competitive markets.[205] Antimonopoly is more than antitrust, and 'antitrust law is just one tool in the antimonopoly toolbox'.[206] This means that antimonopoly is a key tool to ensure democracy, to ensure that citizens can control and check private concentration of economic power, so that no man is allowed to be supreme over the law.[207] Therefore, 'antimonopoly aims to create a system of checks and balances in the commercial and economic sphere'.[208]

In particular, the rise of digital platforms has highlighted the shortcomings of the consumer welfare focus of antitrust law.[209] This is mainly because 'price-based measures of competition are inadequate to capture market dynamics, particularly given the role and use of data'.[210] Furthermore, long-term growth and scale strategies took the place of short-term revenue and profit maximization; firms are prone to engage in 'aggressive low-price strategies, leveraging across multiple lines of businesses, discrimination against digital complements, and defensive growth through predatory start-up acquisitions and M&A'.[211] In the digital economy, dominant tech platforms can use non-price strategies to suppress innovation brought by other firms, thus avoiding competition. They can do so, for instance through 'application cloning', or leveraging their massive datasets to predict consumer trends before other firms and 'identify and repress nascent competitive threats'.[212] When platforms supply their products for free to consumers, eventual abuses fall outside the radar of "traditional" antitrust law based on the consumer welfare standard as there is no price-related mechanism in place. For the same reason, the instruments traditionally used to identify the relevant market – based on the simulation of the effects of a price increase – are inadequate, too.[213]

5. Concluding Remarks

As we saw in the previous sections, many are the features of digital platforms which encourage the development of a market dominated by only a few large players. These

[204] Ibid.
[205] Khan, 'Amazon's Antitrust Paradox' (n 1) 737.
[206] Khan, 'The New Brandeis Movement' (n 2) 131.
[207] Ibid.
[208] Ibid.
[209] Khan, 'Amazon's Antitrust Paradox' (n 1) 738.
[210] Ibid 746.
[211] Douglas Melamed, Nicolas Petit, 'The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets' (2019) 54 Review of Industrial Organization 741, 743.
[212] Ibid 750-751.
[213] Ibid 752.

characteristics, and linked dynamics, are often traceable to the central role of data and not to economic indicators such as price, output or "efficiency".

From the analysis of the "personal data value-chain" has emerged how data is an essential element for undertakings to be able to improve their services and how the most useful kind of data for this purpose is the one gathered directly from users. This is why firms providing digital services are incentivised to develop ways to collect as much data as possible.

Data allow companies to improve their service and to generate revenues, giving rise to two different, yet self-reinforcing, kinds of feedback loops: on one hand, the improvement of their service will likely attract more users and as a consequence more data; on the other hand, more users and more data will attract more company users and consequently, more revenues.

Data are used to feed and improve algorithms and artificial intelligence. This is also causing a shift towards data-driven knowledge-extraction processes, so that firms with access to the largest amount of data also have an advantage in intercepting new trends before their competitors do.

Furthermore, the ways in which these platforms operate are often unknown by individuals, who ignore the extent of the invasiveness of the mechanisms developed to gather and infer as much data as possible from them. As a consequence, individuals also ignore that their right to self-determination is imperilled or that the use of these digital services may have negative consequences on their health. Users are not aware of the value of their data, nor of the risks linked to excessive data collection and cannot make informed decisions about digital services.

Against this backdrop, the enforcement of antitrust law based on economic analysis aimed at pursuing "efficiency" is not adequate to address the drawbacks of the platform economy. Suffice it to say that digital services are provided at zero monetary price and therefore they tend to be considered always advantageous for consumers. This approach overlooks the dangers linked to the concentration of economic power into the hands of only a few firms, even more so in digital economies where the massive collection and accumulation of data has far more serious implications for the exercise of fundamental rights.

In conclusion, antitrust law should focus on ensuring competitiveness of markets, rather than on efficiency. This change of approach is even more necessary in digital markets, where the lack of competition has led to an unprecedented concentration of power against which individuals (and possibly, society at large) are not adequately protected.

CHAPTER II

DATA PROTECTION LAW IN DIGITAL MARKETS

1. Introduction

In the previous chapter, we saw how crucial data is in digital markets. This leads us to the question of how data protection law influences firm's data accessibility. In fact, most of the data they process are personal data, whose processing is regulated by data protection law.

The underlying objective of data protection law is to strike a balance between the protection of the individual and the free circulation of data. However, many scholars have noted that the GDPR, with its (direct and indirect) compliance costs, may have the effect of discouraging the circulation of data, to the detriment of competition. The GDPR, as piece of European legislation directly enforceable in the EU Member States, has a heavy impact on (i) data accessibility as well as on (ii) "digital" competition more in general.

In particular, there are some GDPR principles which have (or should have) more influence than others over data accessibility. For instance, *inter alia*, the "lawfulness" principle provides that it is possible to collect and process data only if the processing can be based on one of the legal basis provided by law, thus restricting the cases in which companies are entitled to process users' personal data. As we will see, this principle indirectly encourages data sharing between companies of the same group, rather than data sharing between different players. In fact, users tend to consent to data sharing more often if the sharing takes place under the "roof" of the same company because they felt this is safer for their privacy.

The GDPR influences competition dynamics not only through its provisions, but also through the way it is interpreted and enforced by national authorities. The different degrees of severity that characterise GDPR enforcement by national authorities acquires even more importance because of the "one-stop-shop" principle, so that the major tech companies have their main establishments in countries where the GDPR is applied more loosely. This has a direct impact on firms' data accessibility and the compliance costs they have to bear.

In this chapter, I will provide a brief overview of the GDPR provisions which have the most significant role in shaping competition. I will then explain the dynamics they trigger and why they tend to favour data concentration. I will conclude with an overview of the enforcement-related differences between national data protection authorities.

2. The GDPR in short

From 1995 to 2018, Directive 95/46/EC[214] was the main EU legal data protection instrument.[215] Even if it provided a high level of harmonisation, Member States still had discretion in its national implementation and application. These differences could 'constitute an obstacle to the pursuit of economic activities at the level of the Union' and 'distort competition'.[216] The adoption of a more coherent legal framework for the protection of personal data was also needed due to the new challenges brought by technological developments and by globalisation, which increased the 'scale of the collection and sharing of personal data'.[217]

The GDPR was adopted in 2016 and became applicable from the 25th of May 2018,[218] repealing Directive 95/46/EC. Under EU law, regulations are directly applicable and there is no need for national implementation, therefore the GDPR provides a uniform legislative framework in the field of data protection across EU. However, there still exist differences on its interpretation among national Data Protection Authorities (DPAs) which have relevant repercussions on competition, due to the "one-stop-shop" mechanism, as I will explain.

The GDPR claims to be 'technologically neutral'.[219] This means that it can be applied regardless of the characteristics of a given technology. Such a "principle-based" design avoids discrimination between different technologies. It can be observed in a number of general overarching principles stated throughout it, that require to be applied to the specific data processing operation.

The main objectives pursued by the Regulation are 'the protection of natural persons with regard to the processing of personal data' and the 'free movement of personal data'.[220] To fulfil the first objective, it establishes the role of the "controller" – the main responsibility role in the Regulation – a natural or legal person determining the purposes and means of the

[214] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.
[215] European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), *Handbook on European data protection law* (Publications Office of the European Union 2018), 29.
[216] Recital 9 GDPR.
[217] Recitals 6 and 7 GDPR.
[218] Article 99 GDPR.
[219] Recital 15 GDPR.
[220] Article 1 GDPR.

processing;[221] as well as the overarching principle of the controller's accountability. In this way, it ensures that the processing of personal data is carried out in a responsible way through the introduction of a number of obligations that vary in accordance with the types of personal data being processed and with the level of risk entailed by the processing.

Article 5 GDPR[222] not only establishes the overarching accountability principle mentioned above, but provides also a number of principles that have to be complied with in each processing operation, which are thus relevant also from a competition law point of view. In particular, Article 5 requires that the processing of personal data shall be carried out in a lawful, fair and transparent manner, to achieve clearly determined purposes and using only the amount of data strictly necessary to achieve them. Data has to be accurate and up-to-date and can only be stored for the time necessary to achieve the purposes determined beforehand. The data controller has to ensure that the processed data is kept safe and in general, is responsible for and must be able to demonstrate compliance with all the mentioned requirements.

The 'data subject' is the natural living person whose personal data are being processed. Data subjects are granted a number of rights aimed at softening the information and power asymmetry between the data controller and the data subject.

3. Lawfulness

The lawfulness principle is likely to influence how and to what extent firms can access personal data. In fact, it requires the processing of personal data to be justified by at least one

[221] Article 4(7) GDPR.

[222] Article 5 GDPR reads as follow: "*1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*"

of the legal grounds provided by Article 6(1) GDPR: a) consent of the data subject; b) performance of a contract; c) compliance with a legal obligation to which the controller is subject; d) protection of the vital interests of the data subject or of another natural person; e) carrying out of a task in the public interest; f) legitimate interest of the controller or a third party.

Special categories of personal data cannot be processed, unless one of the exceptions provided by Article 9(2) GDPR applies. These data are personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or which consists in genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[223]

Article 9 (1) prohibits the processing of these categories of data, therefore the exceptions provided by Article 9 (2) are not to be considered as "regular" legal basis for processing. Since they provide exceptions to a general prohibition, they have to be interpreted strictly. This does not mean that in order to process special categories of data only the requirement provided by Article 9 have to be met. Rather, Article 6 has to be applied in a cumulative way with Article 9 to ensure that all relevant safeguards are complied with, and that the processing of special categories of data is carried out under a high level of protection.[224]

The principle of lawfulness aims at establishing boundaries to the possibility of a data controller to collect, and in general, process personal data. Therefore, it clearly influences how and to what extent firms can access consumers' personal data. This is why it is important to understand in which cases firms are allowed to collect users personal data and which requirements they have to comply with. Consequently, it is worth dwelling on the most commonly used legal basis, such as consent, performance of a contract and legitimate interest of the controller.

3.1. Consent and Explicit Consent

A major role is played by consent and by explicit consent given by data subjects as legal basis and as exception for processing their data.

Article 4(11) of the GDPR defines consent as:

[223] Article 9 (1) GDPR.
[224] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217 9 April 2014), 15.

> *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*.

Additional guidance as to how the controller must act to comply with the main elements of the consent requirements is provided in Article 7 and in Recitals 32, 33, 42, and 43.

Consent can be an appropriate basis for processing only when the data subject has control and an effective choice with regard to accepting or declining the terms offered or declining them without detriment.[225] The data subject has to be able to withdraw consent at any time,[226] and in the case she/he does, data has to be erased and must not be processed anymore, unless there is another purpose justifying the continued processing.[227]

Consent is "freely given" only when the data subject can choose to deny consent without suffering any detriment and in any case without being subjected to any unjustified pressure, otherwise the consent will be invalid.[228] For instance, when consent for processing is bundled to the acceptance of non-negotiable terms of services, consent will not be freely given.

According to Recital 43, consent is not deemed to be freely given also when a 'clear imbalance between the data subject and the controller' exists. Even if the provision only gives the example of the imbalance of power characterising the relationship between data subject and data controller when the latter is a public authority, the EDPB points out that imbalances of power may also occur in other situations, precisely when it translates into an element of compulsion, pressure or inability for the data subject to exercise free will.[229]

When assessing whether consent is freely given,

> *account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*[230]

[225] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020), para 3.
[226] Article 7(3) GDPR.
[227] Article 17(1)(b) GDPR.
[228] EDPB, 'Guidelines 05/2020' (n 225) [13].
[229] Ibid [24].
[230] Article 7(4) GDPR.

If consent is given in such a situation, it is presumed not to be freely given.[231] Thus, for consent to be valid, the service provider should offer data subjects also a service that does not imply consenting to processing of data for additional purposes which are not necessary to provide the service.[232]

Consent must be specific, meaning that data subjects should have the possibility to give consent in relation to one or more specific purposes for which data are processed and that a data subject has a choice with regard to each of them.[233] Therefore, a controller that seeks consent for different purposes should provide a separate opt-in for each purpose and specific information about the data that are processed. In this way, data subjects would have the possibility to understand the impact of the different choices they are going to make.[234]

Consent must be informed, meaning that data subjects have to be given enough information to make a choice, in an 'intelligible and easily accessible form, using clear and plain language'.[235] According to the EDPB, for consent to be informed, the data controller should provide, at least, information on its

> *identity, the purpose of each of the processing operation for which consent is sought, what data will be collected and used, the possibility to withdraw consent at any time, information about the use of data for automated decision-making (where relevant), and information about possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46 GDPR.*[236]

Consent must furthermore be unambiguous, meaning that it must always be given through an active motion or declaration by the data subject. Thus, the use of pre-ticked boxes is invalid as is silence or inactivity or merely proceeding to use a service.[237]

In any case, consent must be obtained prior to the beginning of the processing activity.[238]

Explicit consent is required for the processing of special categories of data, which are deemed to imply a higher risk of discrimination for the data subject and thus justify the

[231] Recital 43 GDPR.
[232] EDPB, 'Guidelines 05/2020' (n 225) [37].
[233] Article 6(1)(a) GDPR.
[234] EDPB, 'Guidelines 05/2020' (n 225) [60-61].
[235] Article 7(2) GDPR.
[236] EDPB, 'Guidelines 05/2020' (n 225) [64].
[237] Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801, para 65.
[238] EDPB, 'Guidelines 05/2020' (n 225) [90].

requirement of a higher level of control by the data subject.[239] As mentioned before, this is the case when special categories of personal data are at issue. Explicit consent requires an extra effort to be undertaken by the data controller than "regular" consent. The data subject must give an express statement of consent, for instance, a data controller can obtain explicit consent providing a text which clearly indicates the consent as well as the 'yes' and 'no' check boxes.[240]

Data subjects must be able to withdraw their consent at any time as easily as when it was given.[241] If consent is withdrawn, all data processing operations based on consent preceding the withdrawal remain lawful, however, the controller must stop the processing and, if there is no other lawful basis justifying the further processing of the data, data should be deleted.[242]

3.2. Performance of a Contract

Article 6 (1) (b) allows a data controller to process personal data to perform a contract of which the data subject is party or to carry out pre-contractual activities necessary to enter a contract requested by the data subject. To rely on this legal basis, the controller should be capable of demonstrating (i) the existence of a contract, (ii) the validity of the contract under the applicable contract law, (iii) the objective necessity of the processing for the performance of the contract.[243]

To assess if the processing is necessary to perform the contract, one has to identify the specific purpose that is going to be achieved through the processing itself.[244] If less intrusive alternatives are available, the processing cannot be considered as "necessary".[245] The "necessity" has to be assessed also from the perspective of 'an average data subject', therefore the data controller has to ensure that the processing constitutes a reasonable expectation of the data subject when entering into the contract.[246]

If a processing operation is based upon Article 6 (1) (b), when the contract is entirely performed and terminated, the processing of the data will no longer be necessary and the

[239] Ibid [91].
[240] According to Example 17 of the Guidelines provided by the EDPB a suitable sentence could be "*I, hereby, consent to the processing of my data*", while it would not provide explicit consent a statement such as "*It is clear to me that my data will be processed*." EDPB, 'Guidelines 05/2020' (n 225) [96].
[241] Article 7(3) GDPR.
[242] EDPB, 'Guidelines 05/2020' (n 225) [117].
[243] European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (2019), para 27.
[244] Ibid [24].
[245] Ibid [25].
[246] Ibid [32].

controller will need to stop processing.[247] However, if there are other purposes for processing, which are authorised under other legal grounds, and that were communicated clearly at the beginning of processing, it would still be possible to process personal data, even if the contract has been terminated.[248]

The necessity to perform a contract is not among the exceptions listed in Article 9 (2) for the processing of special categories of personal data. Therefore, if this type of data is needed to perform the contract, the processor has to obtain the explicit consent of the data subject, in accordance with the conditions for a valid consent.[249]

3.3. Legitimate Interest

Article 6 (1) (f) allows the data controller to process personal data when processing is necessary for the purposes of the legitimate interests pursued by the controller (or by a third party) given that such interests are not overridden by the interests or fundamental rights of the data subject. To rely on this legal basis, three cumulative conditions should be met: (i) the interest pursued must be legitimate, (ii) the processing must be necessary for the purpose of the legitimate interest pursued, (iii) the fundamental rights and freedoms of the data subject do not take precedence over the legitimate interest pursued.[250] The interest of the data controller and the rights and interests of the data subject have to be balanced. The outcome of the balancing test determines whether Article 6 (1) (f) can constitute a suitable legal basis for the processing.[251] It is important to highlight that the purpose of this test is not to avoid any negative impact on the data subject rights, but rather to prevent a disproportionate impact.[252]

In order to be considered as "legitimate", the interest of the controller has to be sufficiently specific, related to concrete and actual circumstances,[253] and in accordance with the law.[254] Furthermore, as in all the legal grounds listed in Article 6 (1), from (b) to (f), the processing has to be necessary for the purposes of the respective legal ground, in this case of the

[247] Article 17 (1) (a) GDPR.
[248] EDPB, 'Guidelines 2/2019' (n 243) [44].
[249] EDPB, 'Guidelines 05/2020' (n 225) [99].
[250] Case C-13/16 *Rīgas satiksme* [2017] EU:C:2017:336, para 28.
[251] WP29, 'Opinion 06/2014' (n 224) 9.
[252] Ibid 41.
[253] Case C-708/18 *Asociaţia de Proprietari bloc M5A-ScaraA* [2019] ECLI:EU:C:2019:1064, para 44; WP29, 'Opinion 06/2014' (n 224) 24.
[254] WP29, 'Opinion 06/2014' (n 224) 25.

legitimate interests pursued by the controller.[255] This means that there should not be any less invasive means to process data suitable to fulfil the legitimate interest of the controller.[256]

For instance, in the *Rīgas* case, the CJEU considered that Article 6 (1) (f) was an appropriate legal basis for the data controller to disclose a data subject's personal data to a third-party to allow the third-party to bring a legal action against the data subject to seek compensation for damaged it had caused.[257] In the *Asociaţia de Proprietari bloc M5A-ScaraA* case, the CJEU considered that the legitimate interest was a proper legal basis for the co-owners of a building to use surveillance cameras in order to prevent their property from being damaged and to ensure their safety, after other and less intrusive methods had proven ineffective.[258]

In the balancing test, the nature and the source of the legitimate interest, the impact on the data subject deriving from the processing, and eventual additional safeguards applied by the controller to prevent undue negative effects on the data subject, have to be assessed.[259] With regard to the nature and the source of the legitimate interest, it is important to verify if the legitimate interest can be linked to the exercise of the controller's fundamental rights,[260] or if it represents a public interest or an interest shared by the wider community,[261] or if it is an interest legally or culturally recognised.[262] As to the assessment of the impact of the

---

[255] Ibid 29.

[256] *Asociaţia de Proprietari bloc M5A-ScaraA* (n 253) [47]; A practical example, near to the cases we are going to analyse afterwards, and useful to understand how the legitimate interest works as a legal basis, is Example 26 of WP29 opinion on legitimate interest: "*An internet company providing various services including search engine, video sharing, social networking, develops a privacy policy which contains a clause that enables it 'to combine all personal information' collected on each of its users in relation to the different services they use, without defining any data retention period. According to the company, this is done in order to 'guarantee the best possible quality of service'. The company makes some tools available to different categories of users so that they can exercise their rights (e.g. deactivate targeted advertisement, oppose to the setting of a specific type of cookies). However, the tools available do not allow users to effectively control the processing of their data: users cannot control the specific combinations of their data across services and users cannot object to the combination of data about them. Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met.*"

[257] *Rīgas* (n 250) [35].

[258] *Asociaţia de Proprietari bloc M5A-ScaraA* (n 253) [61].

[259] WP29, 'Opinion 06/2014' (n 224) 33.

[260] Ibid 34.

[261] Ibid 35.

[262] Ibid 36; a further practical example which can be useful to understand the balancing activity implied by the legitimate interest is Example 1 of the WP29 opinion on legitimate interest: "*A public authority publishes - under a legal obligation (Article 7(c)) - expenses of members of parliament; a transparency NGO, in turn, analyses and re-publishes data in an accurate, proportionate, but more informative annotated version, contributing to further transparency and accountability. Assuming the NGO carries out the re-publication and annotation in an accurate and proportionate manner, adopts appropriate safeguards, and more broadly, respects the rights of the individuals concerned, it should be able to rely on Article 7(f) as a legal ground for the processing. Factors such as the nature of the legitimate interest (a fundamental right to freedom of expression or information), the interest of the public in transparency and accountability, and the fact that the data have*

processing on the data subject, one has to consider actual or potential, positive and negative consequences of the operation, the nature of the data processed, whether data is publicly available, how they are processed, the reasonable expectation of the data subject with regard to the use and disclosure of data, the status of the data subject and of the data controller.[263]

In addition, other issues often plays a crucial role in the context of Article 6 (1) (f), such as the right of the data subject to object to the processing[264] and the availability of an opt-out without the need for any justification; the extent to which data subjects are empowered through data portability and the possibly to access, modify, delete, transfer their own data.[265]

4. Purpose Limitation

Another principle which directly impacts firms' access to personal data is the purpose limitation principle, provided by Article 5(1)(b) GDPR. It requires that personal data be collected only for specified, explicit and legitimate purposes and further processed only so long as it is compatible with the purpose originally established. It aims to empower the data subject, allowing it to take informed choices and to exercise its right in the most effective way.[266]

The principle of purpose limitation encompasses two components: "purpose specification" and "compatible use". The former requires that personal data are collected for 'specified, explicit and legitimate purposes'; the latter, that they are 'not further processed in a manner that is incompatible with those purposes'.[267]

"Purpose specification" requires that, at the time of collection, the purposes of processing 'must be clearly revealed, explained or expressed in some intelligible form'.[268] As a consequence, the purpose pursued must be sufficiently specified as to allow a data subject to

---

already been published and concern (relatively less sensitive) personal data related to the activities of the individuals relevant to the exercise of their public functions, all weigh in favour of the legitimacy of the processing. The fact that the initial publication has been required by law, and that individuals should thus expect their data would be published, also contribute to the favourable assessment. On the other side of the balance, the impact on the individual may be significant, for example, because of public scrutiny, the personal integrity of some individuals may be questioned, and this may lead, for instance, to loss of elections, or in some cases to a criminal investigation for fraudulent activities. The factors above, taken together, however, show that on the balance, the controller's interests (and the interests of the public to whom the data are disclosed) override the interests of the data subjects."

[263] Ibid 37-39.

[264] Article 21 GDPR.

[265] WP29, 'Opinion 06/2014' (n 224) 43.

[266] Ibid 14.

[267] Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203 2 April 2013), 11.

[268] Ibid 17.

assess whether the processing activities carried out by the data controller are strictly necessary for the specified purposes or not.[269] Even the evaluation of whether a purpose is specific enough is highly contextual: purposes such as 'improving users' experience', 'marketing purposes' and the like, are deemed to be always too vague or general.[270] It is important to keep in mind that the processing of personal data for undefined or unlimited purposes, or just based on the consideration that data may be useful sometime in the future, is unlawful.[271]

In accordance with the general approach adopted by the GDPR, also with respect to the assessment of compliance with this principle it is important to look at factual evidence, as well as at the reasonable expectation of the data subjects. Therefore a processing activity will be in breach of the purpose limitation principle if it is unnecessary for the effective purposes of the processing.[272]

"Compatible use" requires that any processing following collection is compatible with the original purposes for collection, according to a ***substantive*** rather than formal assessment.[273] Key factors to consider are (i) the relationship between the original and the further processing purposes, (ii) 'the context in which the data were collected and the reasonable expectations of the data subject as to their further use', (iii) 'the nature of the data and the impact of the further processing on the data subject' also in light of (iv) 'the safeguards applied by the controller' to mitigate such impact.[274] In any case, as a general rule, processing is in breach of this principle if the data subject could not reasonably expect it on the basis of the purposes of the original processing, or if it is 'inappropriate' or 'objectionable'.[275] Therefore, every new purpose which is incompatible with the original one is considered a new, autonomous purpose which must have its own particular legal basis.[276]

For instance, even if not expressly based on the alleged violation of the principle of purpose limitation, several national DPAs (French, Dutch, German, Belgian, Spanish) investigated, and eventually sanctioned, Facebook's data processing following the announcement of amendment of its privacy policy in 2014. Among others, the DPAs considered that Facebook's processing of users' personal data for purposes not sufficiently

[269] Ibid 15.
[270] Ibid 16.
[271] FRA, CoE (n 215) 122-123.
[272] WP29, 'Opinion 03/2013' (n 267) 19.
[273] Ibid 21.
[274] Ibid 21-27.
[275] FRA, CoE (n 215) 123.
[276] Ibid.

illustrated and, in any way, not reasonably foreseeable by users – such as targeted advertising – was in violation of national data protection laws.[277]

Other practical examples of the application of the principle of purpose limitation are provided in the Guidelines of the WP29, for instance, according to Example 9, a store used fidelity cards to develop marketing strategies and offers tailored to the buying habits of their customers. However, this data was then also fed to an algorithm that could tell when a customer was pregnant based on their purchases. According to the WP29 this further processing is incompatible with the original purpose, especially because of the way it is carried out (*i.e.*, without informing users and combining different data which are then fed to an algorithm whose functioning is not clear). In any event, users cannot reasonably expect that having a fidelity card will allow the data controller to determine the existence of a state of pregnancy.[278]

5. Internal Data Collection

As explained above, to be GDPR-compliant the collection and the processing of personal data can take place only if justified under one of the legal basis provided by Article 6 and only for specific purposes. Due to these conditions, the most straightforward way to collect data is internally, i.e. by collecting data directly from the users of the service which the controller provides. In these cases, the most relied-upon legal basis to collect and process personal data is the consent of the data subject.

When data are collected internally by larger firms providing a diversified set of services, the data subject's consent to the collection of its data (generated while using those services) can be the channel through which economies of scale and scope are realised. In fact, the data collected across the different services/products offered by the same firm can be combined and merged into a single data pool, thanks to the user (in)voluntary consent, which, as said before,

[277] CNIL, 'Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium' (6 May 2017) <http://web.archive.org/web/20170520115539/https://www.cnil.fr/fr/node/23602> accessed 8 November 2021. According to Guido D'Ippolito, the purpose limitation principle has a scope that goes beyond the mere area of data protection, being potentially useful to prevent the exploitation of massive amounts of data by large companies for purposes not initially foreseen, such as the development of products or services in markets other than their core market; in Guido D'Ippolito, 'Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust' (2018) 6 Diritto dell'informazione e dell'informatica, 955.
[278] WP29, 'Opinion 03/2013' (n 267) 61.

will give an important competitive advantage to the firm, especially over smaller companies or those offering fewer services.[279]

For instance, Google can collect data from an entire package of services, not only the search engine or maps, available to all users even if they do not have a Google account, but also all services such as Gmail, Drive, Docs and so on, which are available free of charge to users who decide to create an account. Not to mention the data gathered through the service Google Analytics for business customers. The same goes for Facebook and its services (Facebook, Instagram, WhatsApp and so on).

Another reason large companies prefer to collect data internally is the way various national DPAs have enforced the GDPR so far. In fact, internal transfers have attracted less attention from national DPAs than data transfers between different companies. In particular, national authorities have generally overlooked how large digital platforms internally use and share data.[280] Furthermore, not all DPAs enforce the GDPR with the same severity: the Irish DPA, which is the lead authority for most of the larger digital operators, is notorious for its lax approach, which has further exacerbated the favourable position of those firms to the detriment of others. As we will see when dealing with the German BKA decision against Facebook, this defective and uneven enforcement of GDPR's lawfulness and purpose limitation principles poses a serious threat to user privacy and puts large, dominant platforms, in a further competitive advantage.[281]

This "internal data free-for-all" allows dominant platforms to create unique users' super-profiles on the basis of rather vague and numerous (pseudo) legal basis which are often different from those specifically provided by Article 6 GDPR.[282] The result of this practice, which imposes virtually no limits on the internal transfer of data between different units of the same large company, is that large platforms gain a considerable competitive advantage over companies that offer a limited number of services or that otherwise comply with the principle of purpose limitation.[283]

---

[279] Michal S. Gal, Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16 Journal of Competition Law & Economics 349, 363.
[280] Damien Geradin, Theano Karanikioti, Dimitrios Katsifis, 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech' (2020) TILEC Discussion Paper, 23.
[281] Ibid.
[282] According to Geradin, Karanikioti and Katsifis "*Google and Facebook use these data for a number of unspecific data processing activities. These platforms are indeed notorious for using vague terms in their privacy policies. In fact, a detailed examination of Google's numerous privacy-related sources and documents unveils that Google uses hundreds of purposes to justify its data processing activities instead of the six identified legal bases of Article 6(1) of the GDPR.*" in Ibid 25.
[283] Ibid.

Not to mention the fact that consent is not likely to be an adequate legal basis for data processing when the data controller is a dominant company, especially if the data subject's consent is a necessary condition for accessing the service offered. In this case, the positions of data subject/user and data controller/business are characterised by an excessive imbalance of power, the business being dominant and consent being a condition for accessing a service for which there may be few alternatives on the market. As a result, the data subject would not have an effective choice and would be subject to undue pressure.[284]

For instance, it is now clear that Facebook collects and combines users' data from all "Facebook Products" (*i.e.*, Instagram, Messenger, Oculus and more)[285] and from other Facebook-owned services, such as WhatsApp, Masquerade and more, which even if owned by Facebook, remain separate legal entities. Such activity is only recently being addressed by EU authorities[286] and still remains unknown to average users. This is probably due to the fact that these services usually have a very long and complex privacy policy, and to the fact that users, having no meaningful alternative, consider it unnecessary to read this information as they will use the service anyway.

6. Accountability

Article 5 (2) GDPR introduces the principle of accountability, which requires controllers to safeguard data protection in their processing activities, and establishes their responsibility for ensuring and demonstrating that the processing operations they carried out are in compliance with the law.[287] Consequently, two key elements can be singled out: first, this principle holds the controller responsible for complying with the GDPR; and second, the controller must be

[284] Gal, Aviv (n 279) 364.
[285] A list of "Facebook Products" is available at https://www.facebook.com/help/1561485474074139; According to Facebook's Privacy Policy available at https://www.facebook.com/about/privacy: "*We connect information about your activities on different Facebook Products and devices to provide a more tailored and consistent experience on all Facebook Products that you use, wherever you use them. For example, we can suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger.*"
[286] *See* EDPB, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (28 July 2021); also relevant here the warning issued by Indian Government against the new privacy policies of WhatsApp https://techcrunch.com/2021/05/19/india-tells-whatsapp-to-withdraw-its-new-policy-terms/ and the antitrust investigation opened on the same https://techcrunch.com/2021/03/24/india-antitrust-body-orders-investigation-into-whatsapp-privacy-policy-changes/ accessed 9 November 2021; and Garante Privacy, 'Whatsapp: Garante privacy, informativa agli utenti poco chiara. L'Autorità intenzionata ad intervenire anche in via d'urgenza' (14 January 2021) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9519943> accessed 9 November 2021.
[287] FRA, CoE (n 215) 134.

able to demonstrate compliance.[288] This principle thus requires controllers to 'actively and continuously' adopt measures to ensure compliance with data protection law, implying that controllers take a proactive approach.[289]

The principle of accountability is clearly linked to the controller responsibility role. The increasing complexity of data processing, which is ever more likely to comprise several different processes, and to involve numerous parties holding differing degrees of control, has led to the consideration that 'any interpretation which focuses on the existence of complete control over all aspects of data processing is likely to result in serious *lacunae* in the protection of personal data'.[290]

An important aspect to consider in our analysis is that the accountability principle holds accountable the single data controller for the "lawfulness" of the data it receives from third parties as well as for the subsequent processing of the data the controller may decide to transfers to third parties. This means that when a firm/data controller ("data receiver") buys or receives data from another firm/data controller ("data sender"), the data receiver has to check whether (i) those data were collected in accordance with the GDPR and (ii) whether data subjects were sufficiently informed of/gave their consent to the transfer.

Likewise, when the data sender transfers data to a third party, it must ensure that the data receiver is processing such data only for the purposes and in the manner of which the data subjects were informed at the time of the collection of consent. This sort of extension of the scope of application of the accountability principle is intended to ensure that data subjects retain greater control over their data and can exercise their rights more easily.

For the data controller, on the other hand, this extension of the scope of application of the accountability principle entails a twofold cost. A direct cost arising from the obligation to verify the due diligence of the entities with which he or she undertakes data transfers, and an indirect cost arising from the non-usability of data that may have been acquired but cannot be used because it was collected or transferred in breach of the GDPR (e.g. because the data subjects were not sufficiently informed of the transfer or did not express valid consent to it).[291]

---

[288] Information Commissioner's Office, 'Accountability and Governance' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 8 June 2021.
[289] FRA, CoE (n 215) 134.
[290] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C:2018:388, Opinion of AG Bot, para 62.
[291] Geradin, Karanikioti, Katsifis (n 280) 12.

A serious example of accountability failure is the Cambridge Analytica ("CA") case, in which CA, a UK-based company, was able to access the data of millions of users (around 87 million) without their knowledge and use it to send targeted political ads.[292] In fact, between 2007 and 2014, the applications available on the Facebook social network or which allowed access via Facebook login (including thisisyourdigitalife, the app used by CA), could access not only the data of the users using them, but also that of their Facebook friends without adequate information being given, let alone obtaining their consent to the processing.[293] This data was then used to develop precise models of Facebook users in order to identify the type of message that would be most likely to successfully influence their political choices. Users could not reasonably expect that their data were going to be used for purposes of political ad-targeting.

Despite the serious violations of the then applicable Data Protection Act, the Information Commissioner's Office (the English DPA – "ICO") was unable to impose any sanction on CA because, by the time the violation was established,[294] CA had gone into administration and therefore the ICO considered that the application of the sanction would have harmed CA's creditors more than the company itself.[295]

More generally, even if the GDPR has addressed some of the shortcomings of the previous data protection legal framework, such as the centralisation of the accountability principle, the major problem has not being addressed: no regulatory framework was introduced to mitigate the aggressive political ad-targeting and to protect the legitimacy of the electoral process. The most widely used platforms for political discourse offer a single ad targeting service for both commercial and political purposes, making no distinction according to whether the customer is a business or a political party.[296] The ICO has therefore highlighted the risk this poses to democracy and recommended that the government regulates the use of personal data in political campaigns.[297]

---

[292] Information Commissioner's Office, 'Investigation into the use of data analytics in political campaigns' (2018), 26.

[293] Ibid 38-39.

[294] According to the investigation report cited, the ICO had to analyse around '*700 terabytes of data, equivalent to 52.5 billion pages*'. Cases as complicated as CA's bring to the surface the limitations of the data protection enforcement system such as the one-stop-shop mechanism. In cases such as these, it would be advisable to consider the possibility for the lead authority to obtain assistance from other authorities or support at European level.

[295] Ibid 37.

[296] Information Commissioner's Office, 'Democracy Disrupted? Personal information and political influence' (2018), 41.

[297] This is particularly evident in Italy, where detailed legislation regulates political communication through the "traditional" media in order to ensure that each candidate has the same space and therefore equal opportunities to convince voters to vote for him/her as for other candidates. Detailed legislation such as law no. 28/2000 seems a

7. Data Transfers

GDPR is said to reduce the 'economic incentives of firms to share any data collected'.[298] This is caused by a number of reasons. One is that, as explained above, firms which share data are still accountable for ensuring that the firm(s) receiving the data ("data receiver") processes them in compliance with GDPR. Such obligation stems from the accountability principle, which also implies that the data controller is responsible to the data subject for ensuring that he/she can meaningfully exercise his/her rights also *vis-à-vis* the data receiver. As a consequence, data sharing increases the level of risk the data provider faces, as the data provider may not have control over the recipient.

Another factor that may increase the risk of a violation of the accountability principle by the data sender is the fact that the data sender will hardly be able to obtain a clear perspective of the composition of the data set of the data receiver and may never be able to exclude with certainty that, thanks to the data it will transfer to the data receiver, the latter will not be able to infer sensitive information with respect to the data subjects.[299] For example, if a data controller intends to transfer data subjects' data to third parties, he must also obtain the data subjects' consent for this activity, specifying for which purposes the data receiver will use their data. If the data receiver already has a large database, it is possible that with the data provided by the original controller it will also be able to infer sensitive information of data subjects for which stricter rules apply (e.g. consent for the processing of special categories of data must be explicit). In such cases it could be difficult for the original data controller to verify to what extent this is the case and to act accordingly.

At the same time, data receivers must also ensure that the data they obtain is collected and processed in compliance with the GDPR.[300]

The virality of non-compliant data is another deterrent to data sharing. In fact, if non-compliant data received from an external provider is combined with the recipient dataset, the entire dataset will be considered non-compliant. Furthermore, when datasets contain personal

---

paradox because it only regulates, perhaps in too much detail, the tip of the iceberg. In fact, most political communication now takes place via social networks, where the voter is the recipient of announcements and content without being fully aware of its political nature and without sufficient space being given to opinions different from the one deemed to be the user's political opinion. For an in-dept analysis of this phenomenon *see* Autorità per le Garanzie nelle Comunicazioni (AGCOM) 'News vs. Fake Nel Sistema dell'Informazione' (2018).

[298] Gal, Aviv (n 279) 353.

[299] Ibid 367.

[300] Ibid 366.

and non-personal data, the obligations imposed by GDPR apply also to non-personal data, thus indirectly influencing also the free flow of such type of data.[301] According to Gal and Aviv

> *Virality may affect all types of data included in the dataset, including nonpersonal data, so long as it is combined with—and cannot be easily separated from—the noncompliant personal data. Furthermore, and potentially more troubling, even if the datasets can be separated ex post, any learning by an algorithm based on the combined dataset cannot be easily reversed, especially if such learning was already translated into products or services.*[302]

For instance, in Decision No. 267 of 2020, the Italian DPA declared unlawful the processing of data acquired from third parties' databases by a company without prior verification of their compliance with applicable law (in particular, the company had not verified whether the data had been collected and sold on the basis of the valid consent of the data subjects).[303]

The result of these dynamics is that (i) the overall cost of data transfers has increased and that (ii) the number of data controllers willing to share collected data has decreased. As a consequence, competition in data-based markets has decreased, as due to the above mentioned risks, larger firms which can afford to collect internally a sufficient amount of data prefer not to engage in risky transfers, but rather to collect data directly from their users.[304] This will cause firms to try to control all products and services in a relevant ecosystem. Generally speaking, the greater the difficulties linked to data sharing, the stronger the incentives for firms to expand the range of services offered.[305]

As the principle of accountability has effects that go beyond the boundaries of the data controller's business, the GDPR also influences firms decisions on possible mergers or data

---

[301] Ibid 355.
[302] Ibid 354.
[303] Autorità Garante per la Protezione dei Dati Personali, decision n. 267 of December 10, 2020, available at <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9557571>. With reference to this case, the Italian DPA also pointed out in the Annual Report of 2020 "*The need to carry out appropriate evaluations of compliance with the legislation in case of acquisition of databases has been reiterated, since such acquisition does not relieve the data controller from the duty to verify and document the presence of appropriate consent of the data subjects (see in this sense already decision of 29 May 2003 on spam as well as the more recent decision of 18 April 2019, no. 96, doc. web n. 9105201, on electoral propaganda). In view of the repercussions of the unlawfulness of the collection on further processing, it was therefore necessary to prohibit the further use of the data acquired in the absence of appropriate consent, as well as to censure the failure to inform the data subjects*" in Autorità Garante per la Protezione dei Dati Personali, 'Relazione Annuale 2020' (2020), 150.
[304] Gal, Aviv (n 279) 354.
[305] Ibid 372.

suppliers. All else being equal, a firm will likely chose to merge with/buy data from a firm whose compliance with the GDPR can be easily verified or whose compliance has been already verified. Accordingly, data suppliers which have already being vetted could be advantaged over other firms, as well as reputable data supplier over unknown ones, or larger data suppliers over smaller ones.[306]

Lastly, the uncertainty linked to the correct interpretation of the GDPR, due to both its principle-based nature and to its uneven enforcement by national DPAs, could favour the strategic use of it to the benefit of large technology firms. As pointed out by some scholars, after the introduction of the GDPR some of these firms decreased the frequency with which they transferred data to third parties in ways which 'go far beyond what is needed to comply with the GDPR'.[307] Some have referred to this practice as the "weaponization" of GDPR.[308]

8. Data Portability

According to Article 20 GDPR, the data subject has the right to receive the personal data concerning him/her which he/she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller. This right is only recognised when (i) the data has been collected on the basis of the consent of the data subject or to perform a contract and when (ii) the processing is carried out by automated means.

The right to data portability aims to empower data subjects with respect to their data, as it enables them not only to receive a subset of their data for their personal use, but also to move their data from one IT environment to another. To this end, Recital 68 recommends to data controllers to develop interoperable formats that would allow data portability but without introducing an obligation for controllers to adopt or maintain processing systems that are technically compatible. As well as being a tool to avoid user lock-in, the right to data portability is also expected to enhance innovation and the sharing of personal data between controllers under the control of the data subject.[309]

---

[306] Ibid.
[307] Ibid 374.
[308] According to Geradin, Karanikioti and Katsifis "*Google has used the GDPR – or privacy concerns more generally – as an excuse to engage in practices that have strengthened its control on the ad tech ecosystem to the detriment of advertisers, publishers and smaller rivals. This could be referred to as the "weaponization" of the GDPR, i.e. the use of the GDPR by Google as a strategic tool to strengthen its grip on the ad tech market.*" in Geradin, Karanikioti, Katsifis (n 280) 6.
[309] Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (WP 242 rev.01 5 April 2017), 5.

A data subject has the right to obtain his/her data or to have them transferred to another data controller only with regard to personal data concerning him/her or to personal data the data subject provided to the controller. According to the WP29, the category of data "provided by" the data subject also includes data observed form the activities of users, whereas data created by the data controller, such as the profile of the user created by the controller on the basis of collected and inferred data, are excluded.[310] Thus, any further data resulting from the analysis of the user's behaviour is not subject to the right of data portability.[311]

Finally, once a data controller has transmitted the data in accordance with the data subject's request, it is no longer responsible for the fact that such data are further processed in compliance with the GDPR or not. In particular, if the data subject has requested the transfer of its data to another controller, the sender is not responsible for the compliance of the receiver as, unlike in the case of the accountability principle applied to data transfers, in this case the transfer takes place at the will of the data subject. As for the data controller receiving the data, it still has the responsibility to accept and process only the data 'necessary and relevant to the service being provided'.[312] In any event, receiving data controllers are not obliged to accept data transmitted as a result of a data portability request.[313]

9. Misplaced Trust in Data Portability

In literature, the right to data portability was recognised as 'one of the instruments that can keep markets open'[314] or which could 'help individuals to avoid being locked into web-based services'.[315] However, its actual impact has been rather limited. Although the GDPR has been

[310] Ibid 9-10.
[311] Ibid 10.
[312] Ibid 7.
[313] Ibid 6.
[314] Crémer, Montjoye, Schweitzer (n 6) 16.
[315] EDPS, 'Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016), 14. See also Digital Competition Expert Panel (n 23) 79; according to Colangelo and Maggiolino the right to data portability would allow unsatisfied users to switch from a provider to another, thus enhancing competition based on service quality, in Giuseppe Colangelo, Mariateresa Maggiolino, 'Data Protection in Attention Markets: Protecting Privacy through Competition?' (2017) 8 Journal of European Competition Law & Practice 363, 368-369; according to D'Ippolito, data portability could be used (i) to prevent dominant firms from abusing their market power through technology-based user lock-in; (ii) to facilitate market entry by new players, thus increasing consumers' choice, in D'Ippolito (n 277) 978.

in force for more than three years, there has been only one decision of a national DPA fining a controller for not having granted the right to data portability to a data subject.[316]

Furthermore, it is difficult to assess to what extent the exercise of this right is actually granted in practice. Even if according to the guidelines to data portability the concept of personal data is to be interpreted broadly, including observed data,[317] it is problematic to assess whether a data controller has provided all observed data about a data subject, as a data subject may very well be unaware of how much observed data a service provider ultimately tracks about its users.

However, a study has shown that controllers providing the most popular services usually provide observed data as well as inferred data significantly more often that other service providers in response to a data portability request.[318] The same study has shown that competitors to those market leading services offer consumers significantly fewer data import possibilities.[319] As a consequence, consumers may not be able to smoothly move from popular service providers to less popular ones.

Article 20 (2) GDPR provides that, when technically feasible, a data subject shall have the right to have the personal data transmitted directly from one controller to another, however, there is no functioning infrastructure for direct transfer of data between online services yet.[320] Given this *status quo*, the economic impact of the GDPR's right to data portability is naturally limited.

10. The One-Stop-Shop Principle

The GDPR establishes a decentralized enforcement system, in which each Member State provides for one or more independent public authorities to be responsible for monitoring the application of the GDPR.[321] Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the GDPR.[322]

---

[316] Autorité de protection des données, 'Décision quant au fond n° 02/2021 du 12 janvier 2021' (2021) in which the Belgian DPA fined Facebook for not having transferred the data related to a page to the data subject entitled to have it.
[317] WP29, 'Guidelines on the right to data portability' (n 309) 9-10.
[318] Emmanuel Syrmoudis and Others, 'Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20' (2021) 3 Proceedings on Privacy Enhancing Technologies 351, 361.
[319] Ibid 352.
[320] Ibid 364.
[321] Article 51(1) GDPR.
[322] Article 55(1) GDPR.

When cross-border processing takes place, Article 56 GDPR provides the one-stop-shop system ("OSS" hereafter), according to which the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor.

Therefore, the OSS mechanism applies only when a cross-border processing is taking place. According to Article 4(3) GDPR, this will be the case when the processing (i) is carried out in the context of the activities of establishments in more than one Member State, or (ii) is taking place in the context of the activities of a single establishment of a controller or processor in the Union, but it substantially affects, or is likely to affect data subjects in more than one Member State. In the latter case, the test of "substantial effect" must consider a number of factors, such as whether 'the processing causes or is likely to cause damage, loss or distress to individuals'; whether it 'leaves individuals open to discrimination or unfair treatment'; or it 'involves the analysis of the special categories of personal data'.[323]

To identify the leading supervisory authority, one has to determine the location of the controller's or processor's main establishment in the European Union. Article 4(6) GDPR defines the "main establishment" as the 'place where the decisions on the purposes and means of the processing are taken'. As regards a processor main establishment, one has to identify the place of its central administration in the Union or the establishment where the main processing activities occur. However, Recital 36 provides that in cases involving both a controller and a processor, the lead supervisory authority remains the one of the Member State where the controller has its main establishment.

The purpose of the OSS is to facilitate companies operating in several MSs in complying with the GDPR. In particular, thanks to this mechanism, they can interface with a single DPA and adapt to its way of applying the Regulation. In addition, the risk that the same conduct is investigated and sanctioned by different DPAs is reduced. Nonetheless, each national DPA can handle a complaint or investigate over a possible GDPR infringement, if the complaint or the violating conduct (i) concerns only the establishment of the firm in its Member State or (ii) it substantially affects data subjects only in its Member State.[324] However, this can only be

[323] Others elements to consider are listed in Article 29 Data Protection Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (WP 244 rev.01 5 April 2017), 4.
[324] Article 56(2) GDPR.

done if the national DPA informs the lead DPA and the latter decides not to handle the case.[325]

The GDPR does not allow "forum shopping". Also in this case to evaluate how the GDPR has to be enforced it is necessary to carry out a substantive, rather than a formal assessment. This means that if a firm holds that its main establishment is in a given Member State, but in reality no decision-making activity is carried out in that establishment, the relevant supervisory authorities (or eventually the EDPB) will decide which is the actual main establishment of the firms and accordingly, which supervisory authority is the "lead", on the basis of factual evidence.[326]

The GDPR's OSS mechanism is only applicable if a controller has an establishment, or establishments, within the European Union. If a controller has only appointed a representative within the Union, the OSS system does not apply. As a consequence, in the latter case, the controller, through its local representative, will have to deal with local supervisory authorities in every Member State in which it is active.[327]

11. Uneven Degrees of DPAs' Severity

As previously explained, the OSS mechanism established by the GDPR provides that companies have to deal only with the DPA of their single or main establishment. This implies that, when it comes to firms operating in digital markets, some DPAs may have more power than others with regard to GDPR enforcement. A new report from the Irish Council for Civil Liberties ("ICCL")[328] has shown that the DPAs of Ireland, Spain, Germany, Netherlands, France, Sweden and Luxemburg are the one receiving almost the 72% of all complaints linked to tech firms due to the OSS mechanism (Figure 3).

[325] Article 56(3) and (5) GDPR.
[326] WP29, 'Guidelines on lead supervisory authority' (n 323) 8.
[327] Ibid 10.
[328] Irish Council for Civil Liberties, 'Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities' (2021).

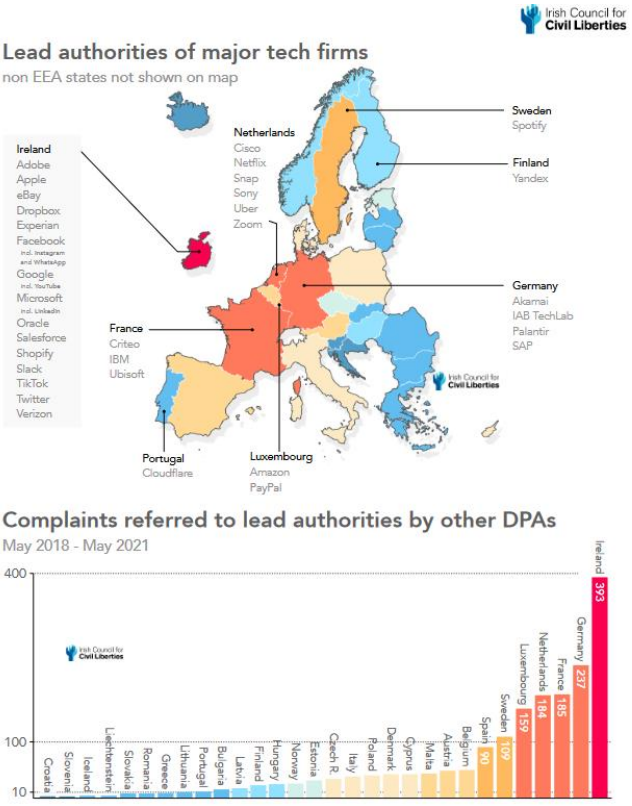

Figure 3 Lead DPAs for major tech firms & percentage of complaints referred to them under the OSS mechanism. Taken from Irish Council for Civil Liberties, 'Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities' (2021), 4.

In particular, it is well known that all major tech firms have their European headquarters in Ireland. This creates serious bottlenecks resulting in big tech platforms being able to avoid rigorous supervision and, eventually, liability.[329]

The Data Protection Commissioner, the Irish DPA ("DPC" hereafter), has long been blamed of being accommodating to the firms it is meant to supervise, by not actively monitoring their compliance with the GDPR and by not imposing 'effective, proportionate and dissuasive' fines for GDPR violations.[330] The report from the ICCL has shown that the DPC is the authority before which are pending the highest number of cross-border cases and the authority which has issued the smallest number of draft decisions since the entry into force of the GDPR (precisely, only four, thus leaving almost 98% of the cases unaddressed – see Figure 3). The DPC is thus addressed as 'the big EU bottleneck' whose failure to enforce the GDPR against big tech companies is paralysing the enforcement of the GDPR in Europe.

[329] Geradin, Karanikioti, Katsifis (n 280), 18.
[330] Ibid 19.

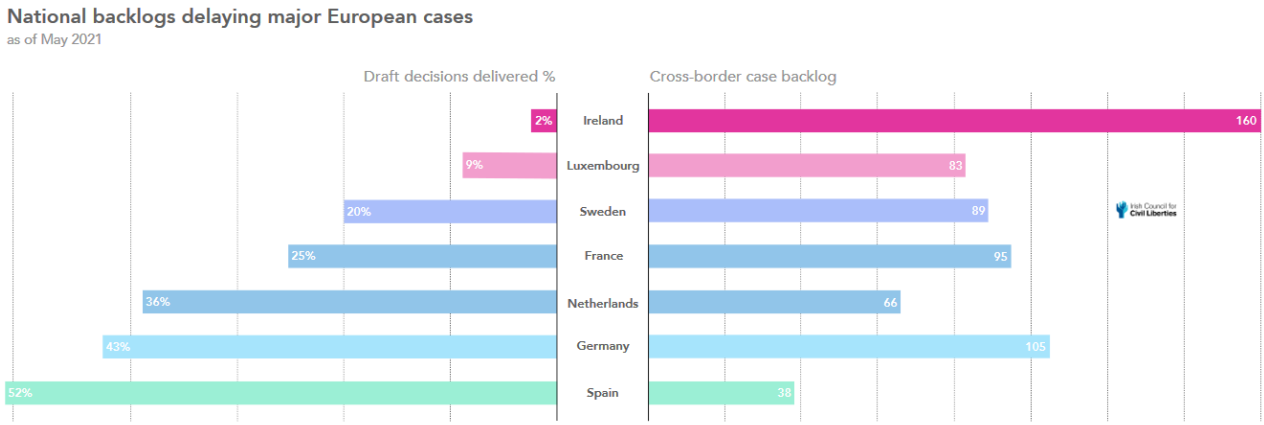

Figure 4 The percentage of draft decisions handed over on cross-border cases & the number of cross-border cases which remain unresolved. Taken from Irish Council for Civil Liberties, 'Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities' (2021), 5.

Furthermore, the DPC has been criticised also for the almost insignificant fines imposed so far. In particular, this has been the case for the draft decisions about Twitter's data breach[331] and the most recent decision about WhatsApp,[332] which have led to the issuing of two binding decisions by the EDPB according to Article 65 GDPR.[333] In both cases, other concerned DPAs objected, among other things, the amount of the fines proposed by the DPC (in the Twitter case the proposed fine was between 150,000 and 300,000 USD;[334] in the WhatsApp case it was between 30 million and 50 million euro).[335]

It has to be highlighted that even if the dispute resolution mechanism provided by Article 65 may counterweight the light touch of the DPC in the GDPR enforcement, this procedure has delayed the issuing of the final decisions of around half a year. Therefore, this is not a viable solution to solve the "bottleneck" issue.

Some have argued that this is not only a matter of the DPC being overwhelmed by pending cases, but also a matter of economic dependency existing between Ireland and big tech companies which have their headquarters there.[336] According to some scholars, this economic dependency should explain why the DPC generally avoids on-site inspections and imposes light sanctions.[337]

---

[331] A summary of the facts is available at https://techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/.
[332] A summary of the facts is available at https://techcrunch.com/2021/09/02/whatsapp-faces-267m-fine-for-breaching-europes-gdpr/.
[333] European Data Protection Board, 'Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR' (9 November 2020); and EDPB, 'Binding decision 1/2021' (n 286).
[334] EDPB, 'Decision 01/2020' (n 333) [165].
[335] EDPB, 'Binding decision 1/2021' (n 286) [340].
[336] Geradin, Karanikioti, Katsifis (n 280) 20.
[337] Ibid.

At the same time, some DPAs across Europe have adopted a more severe approach than others. This emerges also when looking at how national DPAs have interpreted the requirements for valid consent with regard to consent banners. While most DPAs requires users to be allowed to express refusal as easily as consent, the DPC allows to place the "refuse" button also in the second layer of a consent banner (Figure 4). As a result, data subjects are more likely to accept cookies by firms regulated by the DPC than by firms regulated by the other DPAs.

Stakeholders	Positioning regarding the "balanced banner" requirement
CJEU's Advocate General[162]	emphasized the need that actions, "*optically in particular, be presented on an equal footing*"
French DPA[163]	Parag. 39. 'interfaces should not use potentially misleading design practices, such as the use of visual grammar that might lead the user to think that consent is required to continue browsing or that visually emphasizes the possibility of accepting rather than refusing. Parag. 40. The user may also have the choice between two buttons presented at the *same level and in the same format*, with "accept" and "refuse", "allow" and "forbid", or "consent" and "do not consent", or any other equivalent wording that is sufficiently clear to the user. Parag. 51. Thus, this mechanism should not involve potentially misleading design practices, such as the use of visual grammar that impedes the user's understanding of the nature of his or her choice.
Danish DPA[164]	"users are given the option to accept or decline cookies either by an "accept" or "reject" button, or by toggles to accept or reject specific cookie purposes. The option to decline cookies is as *easy as* it is to accept cookies".
UK DPA[165]	refusal of trackers should be at the *same level* as the "accept" button. "[A] consent mechanism that emphasizes "agree" or "allow" over "reject" or "block" represents a non-compliant approach, as the online service is influencing users towards the "accept" option".
Greek DPA[166]	Parag. 4: The user must be able, with the same number of actions ("click") and from the *same level*, to either accept the use of trackers (those for which consent is required) or to reject it, either all or each category separately. Parag. 7: "To ensure that the user is not affected by website designs favoring the option to consent vis-à-vis the option to decline, buttons of the *same size, tone and color* ought to be used, so as to provide the same ease of reading to the attention of the user". Parag. 6: "The size and colour of the "accept" or "consent" button strongly urges the user to choose, e.g. is very large and / or in bold and / or is pre-ticked."
Irish DPA[167]	"no use of an interface that "nudges" a user into accepting cookies over rejecting them. Therefore, if you use a button on the banner with an "accept" option, you must give *equal prominence* to an option which allows the user to "reject" cookies, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them do that, by cookie type and purpose.

Figure 5 The position of different DPAs on the requirements of consent banners to be compliant with GDPR. Taken from Cristiana Santos, Nataliia Bielova, Célestin Matte, 'Are cookie banners indeed compliant with the law?' (2020) Technology and Regulation 91, 117.

In conclusion, as a result of the inconsistency in the interpretation and enforcement of the GDPR among different DPAs, some firms which adopted a data-centric business model, may experiment a competitive advantage over others established in Member States where the GDPR is applied in a stricter way. In addition, while for large digital operators the imposition of the fines established by the GDPR would not significantly impact their business, for smaller firms it can be enough to drive them out of the market.[338]

12. Concluding remarks

In this chapter, we saw how the principles of the GDPR impact firms' data accessibility. In particular, the "lawfulness" principle allows the processing only if this activity can be based

[338] Ibid 23.

on one of the legal basis provided by article 6 GDPR. Even more stricter requirements apply for the processing of special categories of data, which is generally prohibited, unless one of the provided exceptions are met.

One of the most relied upon legal basis for the processing of data is consent from the data subject. However, consent has to be specific, informed, freely given and unambiguous. This requirements are meant to protect users right to self-determination, however, oftentimes these requirements translate into mere formal guarantees (especially when consent is a condition to access a service provided by a dominant undertaking, for which no substitutes exist on the market).

Furthermore, users tend to give consent more easily to the sharing of data between firms of the same group, which added to the fact that national authorities have generally overlooked how large digital platforms internally use and share data, gave rise to the so-called "internal data free-for-all", to the detriment of smaller firms.

Other legal basis can be relied upon only if the processing is strictly necessary to achieve the purposes of the respective legal ground, meaning that there should be no less invasive means to process data than the one envisaged. However, firms, especially big tech firms, tend to improperly use such legal basis, extending their scope of application to cases they do not cover.

Another principle which shapes the extent to which users data can be processed is the "purpose limitation" principle, according to which data can be processed only for specific purposes communicated at the time of collection and for further "compatible" use, also on the basis of what users can reasonably expect. However, firms usually adopt long and complex data policies, also using too vague descriptions of the purposes they intend to achieve, preventing users from making informed choices.

Also the accountability principle impacts firms data accessibility, which requires data controllers to comply, and be able to prove compliance, with the GDPR. This principle has effects that go beyond the boundaries of the data controller's business as, in the data-sharing chain, a controller has to ensure that data it receives from third parties were collected in compliance with the GDPR and that they could be lawfully shared. This has discouraged data sharing between different firms, and encouraged companies to develop and offer a diversified package of as many services as possible on their own (the so-called "ecosystems" we saw in the first chapter), so that they could accumulate more first-party data, without the need to buy them from third parties.

To conclude, we saw how the one-stop-shop principle, united with the uneven degrees of data protection national authorities severity, favours those big tech companies which have their main establishments in countries where data protection laws are applied more loosely, such as Ireland.

All these dynamics have an important role in shaping competition on digital markets, as well as on firms' choice of adopting a business model rather than others. Overall, GDPR provisions, their interpretation and enforcement, seem to favour market concentration and the further entrenchment of the dominant position of already dominant firms.

CHAPTER III

COMPETITION, DATA PROTECTION AND CONSUMER PROTECTION

1. Introduction

Now that the effects that the enforcement of competition and data protection law have on digital markets have been singled out, it is proper to analyse whether a more synergetic enforcement between the policies that necessarily overlap in digital markets (namely, competition, data protection and consumer protection laws) may remedy digital markets typical shortcomings.

For the sake of simplicity, these shortcomings may be traced to two macro-categories, namely information asymmetry and lack of competition. These two issues are at the basis of a market failure where consumers do not have the possibility to choose whether to provide data or money in exchange for digital services or products, nor they are able to provide less data for less valuable services.

As we will see, a heated debate has flourished among scholars, authorities and institutions over the opportunity (or not) to pursue a more integrated approach in the enforcement of competition, data protection and consumer protection laws in digital markets, so to address the issues abovementioned. This debate has brough to light both potential benefits and drawbacks which are worth highlighting so to gain a more in-dept understanding of the decisions I will analyse in the following chapters. In fact, both the AGCM's and the BKA's decisions may be placed within this overarching discourse, therefore it is useful to analyse the main themes it tackles.

In this chapter, I will thus focus on the issues causing the described market failure in digital markets; then, I will present the opposing views which populate the debate over the need to adopt a synergetic enforcement approach of the overlapping policies in digital markets, concluding with a brief overview of the new regulatory tools developed by the European Union to address such issues.

2. Do We Need a More Integrated Approach?

First of all, it is important to specify that even if data protection and privacy may overlap, they represent distinct concepts. In fact, data protection refers to an active obligation related to informational privacy, which includes a number of other rights such as rights of access to data, data security, data portability and so on. Privacy implies a negative obligation, *i.e.* not to interfere with the private sphere of individuals, which is recognised as an essential element to guarantee personal development. For ease of reference, in the following paragraphs, with the expression "data protection", I will refer to both the "active" and the "negative" obligations outlined above.

An ongoing debate is taking place among scholars and authorities about whether competition law should take into account data protection concerns in zero-price markets. This is due to the fundamental role played by data in the business model of digital service providers,[339] and in particular to the fact that consumers can access services without the need to pay any monetary price, providing their personal data as a form of consideration. Consequently, in these markets, consumer harm is likely to manifest itself as privacy harm rather than in "traditional" forms linked to price/quality/quantity variations. As a consequence, it is becoming more and more challenging to separate the scope of application of competition law, data protection law and consumer protection law.[340]

Data harvesting in the digital environment covers different areas of law, inclusive of data protection, consumer protection and competition law. Its transversal character brings out the fragmentation of the legislative framework which could address the abuses linked to this activity.[341] This fragmentation is said to be the reason why the challenges posed by the platform economy are not efficiently dealt with, therefore, some scholars and authorities advocate for a more comprehensive approach where privacy-related issues are embedded in

[339] CMA, ICO (n 70) 7.
[340] Buiten (n 5) 14.
[341] Viktoria H.S.E. Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2019), 9 <Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data by Viktoria H.S.E. Robertson :: SSRN> accessed 24 August 2021.

the assessment carried out during the enforcement of antitrust law.[342] On the other hand, others voice concerns over such an inclusion.[343]

To understand these different perspectives it is necessary to first analyse which issues underlying the markets failure of the digital sector they try to address. In particular, they can be linked to two major areas: (i) weak competition, and (ii) information asymmetry. In markets where only a few dominant firms operate, it is easier to impose abusive privacy policies on consumers and to stifle competition on privacy-friendly services. At the same time, consumers' choice is imperilled due to lack of transparency over the real costs of using a service "for free", while providing their own personal data. Furthermore, as rightly pointed out by Wolfgang Kerber, these two issues are self-reinforcing since

> *weak competition between platforms can reduce the competitive pressure to disclose information about the collection and use of data, and, vice versa, the lack of transparency and lack of information for consumers can dampen the intensity of competition due to a lack of comparability.*[344]

2.1. Market Dominance and Weak Competition

Weak competition derived from the presence of only a restricted number of very large firms in digital markets is said to lead to an excessive collection of users' data and to an insufficient provision of privacy-differentiated services and products for satisfying the privacy preferences of users.[345]

---

[342] Among others, see CMA, ICO (n 70); Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16 European Competition Journal 628; Francisco Costa-Cabral, Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 Common Market Law Review 11; Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11 Journal of Intellectual Property Law & Practice 856; EDPS, 'Opinion 8/2016' (n 315); Autorité de la Concurrence, Bundeskartellamt (n 87).

[343] Among others, see Buiten (n 5); Eugene Kimmelman, Harold Feld, Agustìn Rossi, 'The limits of antitrust in privacy protection' (2018) 8 International Data Privacy Law 270; Colangelo, Maggiolino (n 315); D. Daniel Sokol, Roisin Comerford, 'Does Antitrust Have A Role to Play in Regulating Big Data?' in Roger D. Blair and D. Daniel Sokol (eds), *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech* (Oxford University Press 2017); Maureen K. Ohlhausen, Alexander P. Okuliar, 'Competition, Consumer Protection, and the Right (Approach) to Privacy' (2015) <Competition, Consumer Protection, and the Right (Approach) to Privacy by Maureen K. Ohlhausen, Alexander Okuliar :: SSRN> accessed 22 August 2021.

[344] Kerber (n 342) 862.

[345] Marco Botta, Klaus Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey' (2019) 64 The Antitrust Bulletin 428, 432; Kerber (n 342) 859.

In particular, the structural characteristics of digital markets, as outlined in Chapter 1, such as network effect, ecosystems and user lock-in, favour market concentration and reduce consumer choice, thus segregating the individual's online experience into a limited number of 'walled gardens'.[346] The social and professional costs of opting out of many web-based services has increased due to lack of interoperability and to the fact that available choices often only offer low-level privacy protections. Accordingly, it has been observed that today, it is nearly 'impossible to choose not to be tracked while consuming digital services'.[347]

Undertakings exercise 'their market power to foment consumers' supposed lack of interest for data protection' and to suppress 'competition on this parameter'.[348] For instance, whit specific reference to Facebook, Dina Srinivasan interestingly depicts how this company has used users' privacy concerns to gain popularity and to subsequently downgrade the general level of privacy granted in digital services.[349]

More in general, by concealing data practices behind complex and oftentimes misleading privacy policies, incumbents impede the development of competition on privacy-enhancing services. In fact, consumers are not put in a position to evaluate and compare the diverse levels of privacy protection offered by different services as they can do for other attributes of a product or service, such as its material or its overall quality. In the market for digital services consumer are able to directly experience and evaluate only the efficiency of a service and its monetary cost. Given that providers who want to develop a privacy-enhancing product could not rely on the revenue of targeted advertising, they would have to offer a less efficient product or charge a monetary price on consumers (as a recall, this is due to the fact that they will not experiment the user or the monetisation feedback-loop). Given that consumers will not pay for a service which is generally provided free of charge, or chose a less efficient service than those available on the market, to avoid a cost (such as the detriment of their privacy) which they cannot assess, it is likely that they will continue to use less privacy-friendly products, thus discouraging the emergence of competition in the provision of privacy-enhancing products/services. [350]

Against this backdrop, in which the dominant position of big platforms is far from being under threat, big platforms are in a position to set the standards on the degree of intrusiveness

[346] EDPS, 'Opinion 8/2016' (n 315) 6.
[347] Ibid.
[348] Costa-Cabral, Lynskey (n 342) 28.
[349] Dina Srinivasan, 'The Antitrust Case Against Facebook: a Monopolist's Journey towards Pervasive Surveillance in spite of Consumers' Preference for Privacy' (2019) 16 Berkeley Business Law Journal 39.
[350] Kemp (n 342) 660.

and the level of data a digital service can afford to harvest. The consequence is that 'the data dynamics of online markets may drive a "race to the bottom" in privacy quality'.[351]

Only recently firms are beginning to consider higher level of privacy protection as a way to differentiate their product and to fill in the supply gap left open with respect to the consumer share which would like to use more privacy-friendly products.[352] Sadly, all this only confirms that change is only possible when it is undertaken and nurtured by already dominant companies, rather than by consumers.

2.2. Information Asymmetry

A second issue concerns the lack of transparency users face about the collection and use of their data, as well as of their real value, which prevents them from making 'informed rational decisions about their privacy behaviour on the internet, leading to failures caused by information asymmetry and behavioural biases'.[353] In fact, users cannot fully understand the value of their data nor the objective costs deriving from excessive data collection or dissemination. The *real* problem is that even if they were diligent and concerned, users would still be prevented from making informed choices.[354] This is due to a number of reasons.

First of all, online operators tend to adopt privacy policies which provide weak privacy protections, and present them in a misleading way, so that consumers cannot fully understand the 'extent of those terms, the resultant data practices and their consequences'.[355] These terms commonly allow or ask the user to consent to excessive data collection in comparison to the data effectively needed to provide the service and often also go beyond what consumer could reasonably expect.[356] Here the problem is that digital operators have an interest in preventing

---

[351] Ibid 661.

[352] In particular, Apple and Google are trying to offer more privacy-friendly services. These developments have already caught the attention of Antitrust authorities as these practices risk entrenching even more the dominant positions of these firms by denying access to data to their competitors in the targeted advertising sector. *See* Laura Kayali, Thibault Larger, Giorgio Leali, 'Apple's new privacy feature backed by French competition watchdog' (*Politico* 17 March 2021) <https://www.politico.eu/article/french-competition-watchdog-backs-apple-privacy-push/> accessed 25 September 2021; Natasha Lomas, 'Google's plan to replace tracking cookies goes under UK antitrust probe' (*Techcrunch* 8 January 2021) <https://techcrunch.com/2021/01/08/googles-plan-to-replace-tracking-cookies-goes-under-uk-antitrust-probe/> accessed 25 September 2021.

[353] AGCM, AGCOM, GPDP (n 81) 94; Botta, Wiedemann (n 345) 432; Kerber (n 342) 859-860.

[354] Botta, Wiedemann (n 345) 432.

[355] Kemp (n 342) 637.

[356] Ibid. As also pointed out by Khan and Pozen with regard to Facebook's users: '*Most Facebook users, … rely on the platform to communicate with other Facebook users. According to a recent Pew Research Center survey, seventy-four percent of them do not know that the platform collects data to classify their interests and traits. Other surveys have found that an overwhelming majority of Facebook users do not want to be exposed to any targeted political or commercial advertisements, reflecting a "resounding consumer rejection of surveillance-based ads and content." As a rule, it appears that Facebook users tend to be deeply ignorant of the ways the*

users from reading and understanding the privacy policy of their services and act accordingly.[357] Consequently, consumers do not read/understand the privacy policies of the services they use and are unable to compare or consider this aspect of digital services while making their choices.[358]

Furthermore, consumers are not able to carry out a rational evaluation of costs and benefits when deciding whether to use an online service. This is due to the inability of consumers to assess the economic value of their data and to the inability to properly evaluate the costs associated with sharing them.

This asymmetry of information tends, moreover, to have an intertemporal dimension insofar as the release of data may give rise to an immediate benefit (for example, improvement of service), but may subsequently have future negative repercussions for the consumer.[359] In fact, as rightly pointed out by Kemp, weak data practices impose on consumers objective and future costs, such as

> *increased risks of data breach, identity theft, hacking and fraud; exposure of sensitive information the consumer would not wish to disclose through unanticipated collection and tracking; exposure to manipulation-based marketing, profiling, segmenting or scoring which can lead to a series of negative consequences for the consumer.*[360]

The amount of data collected, the storage period and the extent to which it is disseminated and shared with third parties are some of the elements that have to be considered when evaluating the quality of a digital service, as they could imply an aggravation of the risk of misuse of the data, to the detriment of consumers.[361] This risk is even less perceivable from

---

company serves (or disserves) them, and deeply unnerved when they find out. This is not just an unusually stark asymmetry of information. It is an elaborate system of social control whose terms are more imposed than chosen." in Lina M. Khan, David E. Pozen, 'A Skeptical View of Information Fiduciduciaries' (2019) 133 Harvard Law Review 497, 519–520.

[357] An interesting TED Talk on the topic, held by Finn Lützow-Holm Myrstad, a member of the Norwegian Consumer Council, in which he explains that together with his colleagues, they printed the privacy policies of the apps which are most likely to be found on average smartphones and they resulted in more than 900 pages and that it took them 31 hours, 49 minutes and 11 seconds to read them. The talk is available at https://www.ted.com/talks/finn_lutzow_holm_myrstad_how_tech_companies_deceive_you_into_giving_up_your_data_and_privacy accessed 14 November 2021; the Norwegian Consumer Council also published a report on how consumer are exploited by digital operators: Forbrukerrådet, 'Out of control: How Consumers are exploited by the Online Advertising Industry' (2020) available at https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

[358] Kemp (n 342) 664.

[359] AGCM, AGCOM, GPDP (n 81) 88.

[360] Kemp (n 342) 654-655.

[361] Ibid 644.

consumers who are generally only aware of the information they voluntarily provide, which may seem harmless if taken alone. However, the reality is that this information is likely to be combined also with information the consumer provided in different contexts (and maybe even believing that he/she was doing so on an anonymous basis) thus also allowing the reidentification of sensitive data.[362]

Data collected about a consumer's online and offline behaviour without their knowledge can also be used to their detriment, for instance to make unfavourable assumptions about their creditworthiness or to apply price discrimination charging higher prices:

> *it may mean, for example, that the consumer is charged higher interest rates or insurance premiums; shown more expensive search results; quoted higher prices for the same product; or completely excluded from certain offers*.[363]

Moreover, while consumers are usually fully aware of the price of the goods/services they consume, the level of privacy associated with the consumption of certain goods/services is one of the aspects that is probably less immediately perceptible and quantifiable by the consumer.[364] Users may not even be aware of the extent to which third-party trackers are able to scoop up personal data related to them, and are therefore not informed about the extent of the counter-performance that a certain privacy policy requires from them.[365]

The Italian Competition Authority has pointed out that information used for the profiling of users for commercial use and for marketing purposes, acquires, by reason of such use, an economic value that clearly constitutes the counter-performance of the service provided by the platform in the absence of monetary consideration.[366]

It has been suggested that consumers tend to over-value the services offered by digital platforms while placing less value than they should on the personal data they provide in return.[367] The user is generally not able to attribute an economic value to his personal data, and therefore is not able to identify the relative "transfer price".[368] This is also due to the fact that online services are provided for zero monetary price, which also reflect the perceived

[362] Ibid, 647-648; Wolfgang Kerber, Karsten K. Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2021), 14, according to who more data collection implies that consumers bear objective costs.
[363] Kemp (n 342) 647-649.
[364] AGCM, AGCOM, GPDP (n 81) 90.
[365] Robertson (n 341) 11.
[366] AGCM, AGCOM, GPDP (n 81) 89.
[367] Robertson (n 341) 11.
[368] AGCM, AGCOM, GPDP (n 81) 96.

value of data. However, the personal data collected may be worth far more than the cost of providing the "free" service, so that users are not fairly compensated for their data.[369]

The difficulty in properly estimating the value of data is caused by a number of factors.

One is the fact that this value is formed in a sequence of transfers of property and uses that the user is not able to foresee *ex ante*.[370]

In addition, it is not clear which parameters should be considered:

> *should the reference point be the price one would accept to give away their data, or the amount they would pay to protect it? Or, should it be the expected cost the data subject may suffer if her data is exposed, or the expected profit the data holder can generate from acquiring her personal information?*[371]

Usually, these questions are solved by market dynamics, but there is still no recognised market for personal data which also involves data subjects.[372] Furthermore, data subjects have even more difficulty in putting a value on their data because they do not know at what price their data is marketed by digital service providers,[373] and also because this ignorance prevents them from developing expertise in transactions involving their data (which, on the contrary, happens on a daily basis with respect to monetary transactions, which allows consumers to understand when a price is too high with respect to a service offered).[374]

This information asymmetry leads to behavioural biases, such as the so called "privacy paradox" and "free effect". Privacy paradox is about the discrepancy between individuals' intention to protect their privacy and how they actually behave in the market.[375] Although consumers are very interested in privacy and see it as an important factor in the quality of a service, they do not, however, seem to make consumption choices consistent with this stated preference. This is the case, for example, when a user will not give up a free service, even if it provides a very low level of privacy protection, and other services on the market offer greater protection of personal data for a positive price.[376]

---

[369] Maurice E Stucke, 'Should We Be Concerned About Data-Opolies?' (2018) 2 Georgetown Law Technology Review 275, 294–295.
[370] AGCM, AGCOM, GPDP (n 81) 96.
[371] Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature 442, 447–448.
[372] Ibid.
[373] Nicholas Economides, Ioannis Lianos, 'Data, networks, and platforms: What effects on economic development? Antitrust and restrictions on privacy in the digital economy' (2020) 2 Concurrences Review, 28.
[374] Budzinski, Grusevaja, Noskova (n 29) 9.
[375] Patricia A. Norberg, Daniel R. Horne, David A. Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (2007) 41 The Journal of Consumer Affairs 100, 101.
[376] AGCM, AGCOM, GPDP (n 81) 94.

Another distortion that is found in consumers behaviour in relation to digital services is the so-called "free effect". It relates to the fact that the perceived utility of free services tends to be disproportionate in the evaluation of the entailed costs and benefits. In fact, the user values the usefulness of a service offered free of charge in a much more positive way. This implies that a reduction of the price impacts the utility of the consumer in a non-constant way, peaking in correspondence of the moment in which a service passes from having a positive price to being offered for free.

Such effect introduces a series of implications on competition for privacy-enhancing services. In fact, even a small price increase that exponentially improves the quality of the service by a potential entrant may not be sufficient to allow him to enter the market.[377] Thus, presenting services to consumers as "free" is unfair because consumers will not perceive the actual costs of those services and because their behaviour is therefore distorted by a misleading presentation of the reality.[378]

To conclude, consumers finally accept the privacy terms of digital services without even reading them because they feel powerless. In such circumstances it is legitimate to ask to what extent it is correct to speak of "freely given" and "informed" consent and to what extent such consent does not end up being reduced to a sterile formal requirement,[379] even more so when the data controller is a dominant undertaking, providing a service for which there is high demand and scarce alternatives are available on the market.[380]

As rightly pointed out by Kemp,

> *effective competition is competition which drives innovation and is responsive to consumers. Effective competition depends on consumers having access to accurate information and the ability to bargain for, and switch to, a better deal*.[381]

The present situation cannot be further from Kemp's words, since at present, consumers are unable to "reward" the best service through the rational exercise of their power of choice. If consumers were given back the possibility to make informed and rational choices among a variety of services including more privacy-friendly ones, privacy preservation itself could

[377] Ibid 95.
[378] EDPS, 'Privacy and Competitiveness in the Age of Big Data' (n 86) 31-32.
[379] Botta, Wiedemann (n 345) 433; EDPS, 'Privacy and Competitiveness in the Age of Big Data' (n 86) 35.
[380] EDPS, 'Privacy and Competitiveness in the Age of Big Data' (n 86) 35.
[381] Kemp (n 342) 663.

become an area where companies compete to attract more consumers and this could also encourage the development of 'privacy-protective business models'.[382]

2.3. Opposing Views

As anticipated before, in response to the outlined market failures, some scholars and authorities advocate for a more comprehensive approach where privacy-related issues are taken into account in the application of antitrust law, while others do not.

According to the first group, data protection law 'should act as a normative benchmark for competition law, and the two policies should be applied in a holistic manner when their material scope intersects'.[383] This could be the case in a number of situations, for instance with respect to privacy policies adopted by dominant firms which have a data-centric business model;[384] or when the dominance of the firms is strongly linked to its privileged access to data.[385]

This assumption is strengthen by the fact that according to some, competition law, consumer protection law and data protection law pursue the same goals: protecting the consumer and rebalancing relationships characterised by an excessive imbalance of power.[386] Their intersection is even more evident when the market dominance of firms depends on their access to data.[387] However, these three disciplines intervene 'at different ends of the same spectrum': while data protection law and consumer protection law tackle the information asymmetry and the power asymmetry between the data subject/consumer and the controller/trader, thus protecting the individual during the decision-making process, competition law addresses the imbalances of market power and protects the individual from the undue exercise of that power.

In this context, the protection of personal data is considered as one qualitative dimension, among many, of a service: all else being equal, (properly informed) consumers should tend to choose the service that guarantees the lowest possible provision of data or, in any case, a higher control over their own data.[388]

---

[382] CMA, ICO (n 70) 20.
[383] Ibid 21; Costa-Cabral, Lynskey (n 342) 21; Autorité de la Concurrence, Bundeskartellamt (n 87) 23-25.
[384] Autorité de la Concurrence, Bundeskartellamt (n 87) 23-24.
[385] Ibid 25.
[386] Costa-Cabral, Lynskey (n 342) 21.
[387] Ibid 15.
[388] AGCM, AGCOM, GPDP (n 81) 90.

More generally, it is possible to identify a variety of dimensions related to the processing of personal data that may be relevant not only under the GDPR, but also when assessing data protection as an element of the quality of a service. In fact, one can have regard to: i) the type and volume of data collected; ii) the purpose of collection and processing; iii) the duration of processing; iv) the possible sharing of data with third parties; v) the degree of control users have over their data; vi) the link between the type of service and the amount of data collected; vii) the transparency of data collection and processing practices.[389]

The AGCM has noted that considering privacy as a quality component is still consistent with the approach that sees the consumer attributing an economic value to the protection of personal data: as with other qualitative characteristics, a higher level of privacy, other things being equal, should correspond to a greater utility for the consumer.[390]

Considering the degree of use of personal data as an aspect of the price consumers pay for a good/service, or as a qualitative dimension of the latter, is a useful element to analyse the link between competition and the exploitation of personal data.[391] In fact, in this case it is possible to apply the tools developed in the application of competition law to assess firms' data collection practices.[392]

In particular, it is argued that privacy policies imposing excessive data collection on consumers can be qualified as exploitative abuses under Article 102 TFUE.[393] This is said to be especially the case 'when an incumbent collects data by clearly breaching data protection law and when there is a strong interplay between the data collection and the undertaking's market position'.[394] Thus, data protection law is considered as an appropriate benchmark for

---

[389] Ibid.
[390] Ibid.
[391] Ibid 91.
[392] Kerber (n 342) 860.
[393] Consolidated version of the Treaty on the Functioning of the European Union [2008] OJ C 115/13. Article 102 reads as follows: "*Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.*
Such abuse may, in particular, consist in:
(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts."
This thesis is held by a number of authors and authorities, among others, see Giulia Schneider, 'Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook' (2018) 9 Journal of European Competition Law & Practice 213, 221; AGCM, AGCOM, GPDP (n 81) 102; Kemp (n 342) 657; Buiten (n 5) 7; Costa-Cabral, Lynskey (n 342) 34; Autorité de la Concurrence, Bundeskartellamt (n 87) 25.
[394] Autorité de la Concurrence, Bundeskartellamt (n 87) 25.

assessing in which cases privacy policies adopted by dominant companies, assimilated to standard contractual clauses, can be deemed to be exploitative.[395]

While the difficulty of equating excessive data collection to excessive price is unanimously recognised, there is a consensus over the viability of equating privacy policies imposing excessive data collection on consumers as unfair trading conditions.

In order to bring excessive data collection within the scope of overpricing, it would be necessary to have a clear perception of the value of the data in terms of its possible uses, but also of the data-related practices of other companies in similar sectors.[396] As discussed above, it is rather difficult to properly establish the value of data, and even more difficult to place an absolute value on it, as on the corporate side, some individuals' data may be more valuable than others, while on the consumer side, some consumers may place more importance on protecting their data than others.[397] However, Facebook has been recently sued in a class action lawsuit on the basis of the alleged violation of UK's Competition Act. In particular, Facebook has been accused of having charged an unfair price on its consumers as they were not properly compensated for the data they gave up upon registration and following use of the service.[398]

In *United Brands*,[399] the CJEU developed a two-step test for assessing whether a conduct falls within the excessive prices abuse: the first step consists in determining 'whether the difference between the costs actually incurred and the price actually charged is excessive.'[400] If this is the case, then the second step consists in determining 'whether a price has been imposed which is either unfair in itself or when compared to competing products.'[401]

Therefore, in order to apply this test to data-related practices, it is first necessary to assess how much data is collected by a service and then to evaluate whether this data is proportional

[395] Ibid.
[396] However, Botta and Wiedemann considered the application of the criterion adopted by the CJEU in case C-177/16 (Latvian Copyright Society), which consists in the comparison of the amount of data collected by a firm to provide a given service with the amount of data that competitors generally require to provide similar services. Even this approach is problematic to apply given the lack of transparency that characterises the privacy policies and the actual extent of data collection in digital services. *See* Marco Botta, Klaus Wiedemann, 'Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision' (2019) 10 Journal of European Competition Law & Practice 465, 467.
[397] Buiten (n 5) 7. Here https://ig.ft.com/how-much-is-your-personal-data-worth/ you can have a glimpse of how much your personal data is worth.
[398] Dan Milmo, 'Meta sued for £2.3bn over claim Facebook users in UK were exploited' (*The Guardian*, 14 January 2022) <https://www.theguardian.com/technology/2022/jan/14/meta-sued-for-23bn-over-claim-facebook-users-in-uk-were-exploited> accessed 15 January 2022.
[399] Case C-27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1976] ECLI:EU:C:1978:22.
[400] Ibid [252].
[401] Ibid.

to the service the consumer receives in return.[402] To carry out this assessment one should be able to clearly determine the value of data, which is rather problematic, not to mention that the value of the service may differ from user to user. In a second step, it has to be assessed whether the amount of data gathered is 'unfair in itself or when compared to competing products.' Applying this second step is even more challenging,[403] given the lack of transparency which characterises data collection practices and in any case, given the widespread tendency to collect more data than is strictly essential to provide the service, this comparison may not necessarily be the right tool for detecting abusive behaviour.

While qualifying data-related practices as excessive pricing abuse tends to be difficult, this is not the case for qualifying the privacy notices of such services as abusive terms of service in the meaning of Article 102(a) TFEU. In fact, also in view of the central role of data in the provision of digital services, privacy notices can be qualified as 'unfair trading conditions'[404] if they impose on the consumer counter-performances that are disproportionate to the object of the contract,[405] or if they breach data protection laws.[406]

The CJEU case law demonstrated that the infringement of a different branch of law can be taken into account for competition law enforcement purposes.[407] Furthermore, according to the CJEU case law, trading conditions are unfair pursuant to Article 102 TFEU, when they are (i) 'disproportionate', (ii) 'not necessary for the objectives the undertaking is meant to purse', and (iii) 'misleading in terms of information rendered to the contracting parties'.[408] Therefore,

---

[402] Robertson (n 341) 10-11.
[403] Ibid 11.
[404] Schneider (n 393) 221.
[405] Buiten (n 5) 7.
[406] Costa-Cabral, Lynskey (n 342) 33; Autorité de la Concurrence, Bundeskartellamt (n 87) 25.
[407] According to Schneider, "*In* Allianz Hungária*, for example, it was expressly affirmed that the impairment of objectives pursued by another set of rules could be taken into consideration for the purposes of competition assessments. Moreover, with respect to exploitative conducts under art. 102 TFEU, the European Court of Justice took into consideration breaches of – or better said the distortive use of rights provided by – intellectual property law, in both the* DSD *case and in the well-known* Astrazeneca *case. As commentators observed with respect to the latter case, the relevance of intellectual property for competition law assessments reflects the fact that competition law itself does not have sufficient tools for the assessment of the unfairness of an allegedly abusive conduct. In some cases, thus, external parameters may be borrowed from other legal regimes.*" in Schneider (n 393) 221.
[408] As pointed out by Scheider "Belgische Radio en Televisie vs. SABAM *clarified how the unfairness of terms and conditions imposed by a collecting society onto the original right-holders originated from the fact that obligations borne by its members were 'not necessary for the attainment of its objects'. Such terms were found to 'unfairly' impair a member's freedom to exercise his copyright and were thus deemed by the Court to constitute an abuse of the dominant position held by the company. Thus, as acknowledged also by the literature, at the core of the judgment of exploitative abuses lies the assessment of the necessity and the proportionality of the limitation determined by the trading condition and suffered by the users' right in exchange of a given service. In the same vein, another useful parameter of unfairness of trading conditions is to be drawn from the already cited* Astrazeneca *case, where the European Court of Justice found the company's conduct consisting in 'deliberate' and 'consistent' 'misleading representations' and 'misleading information' to be an abuse of dominant position. Thus, in the court's view, the 'objectively wrong representation' made by the dominant*

privacy policies that require the collection of an excessive amount of data with respect to what is actually needed to provide the service, or that in any case impose processing operations that are not necessary for the provision of the service and that do not clearly explain all this, may be considered abusive under Article 102 TFEU when adopted by a dominant undertaking.

It could be pointed out that principles governing the assessment of unfairness under competition law, *i.e.* necessity, proportionality and transparency, are the same principles taken into account in the assessment of unlawfulness processing under the GDPR.[409] However, for competition law enforcement purposes, it should be the dominant position of the company adopting such policies the one element that allows it to breach data protection law. [410]

Therefore, data protection law can provide a normative benchmark to assess whether a dominant operator is imposing unfair trading terms. According to this line of though, this does not entail an instrumentalization of competition law to achieve data protection law objectives, since

> *the "internal" role proposed for data protection is compatible with the aims of competition law and, indeed, merely helps competition law to achieve these aims in circumstances where price is not the only relevant competitive parameter.*[411]

On the other hand, some authors argued that competition law is not the appropriate legal instrument to sanction unfair clauses imposed by online platforms on final users. According to them, these clauses should instead be sanctioned either via consumer or data protection law.

In particular, it has been argued that 'it is the task of consumer policy to remedy market failures caused by information asymmetries and behavioural biases'.[412] In fact, even if the level of data protection provided by a good/service is to be taken into account while evaluating the quality of that good/service, also other characteristics of a product such as its safety or efficiency, which are types of non-price competition as well, are mainly monitored by consumer/data protection law authorities rather than by antitrust agencies.[413]

---

company, causing the violation of regulatory procedures, constituted an abuse of dominant position." in Schneider (n 393) 222.

[409] Namely, Article 5(1)(a) GDPR provides that "*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*"; Schneider (n 393) 223.

[410] Ibid 224.

[411] Costa-Cabral, Lynskey (n 342) 31.

[412] Kerber (n 342) 861.

[413] Sokol, Comerford (n 343) 311.

Furthermore, market failures such as these, stemming from information asymmetries, will not be solved increasing competition because regardless of the number of firms competing in the market, all firms could keep providing services offering poor levels of data protection.[414]

Finally, consumer and data protection law are usually the tools through which firms adopting misleading and unfair terms able to harm consumers' free choice are sanctioned, not competition law.[415]

Another reason put forward to justify avoiding a more integrated approach in the enforcement of competition law and data protection law is to preserve their legitimacy. To do that, it is necessary to use legal instruments only for their intended purposes.[416] Therefore, in order to preserve the legitimacy of competition law, its scope should not be unexpectedly extended to protect interests that do not generally fall within its scope of application: 'Using it as an 'all-purpose' enforcement tool would undermine legal certainty and the legitimacy of competition law',[417] indeed the role of competition law 'is not to fill gaps in the privacy laws'.[418] The same applies to breaches of data protection law, which must always be treated as such and not as violations of competition law only in certain circumstances.[419]

It is also said that the remedies offered by competition law, in addition to failing to adequately address privacy issues, may even be harmful in certain cases. As also said before, competition law applies only if a certain behaviour distorts competition and is therefore not suitable to properly address conducts harming consumers' privacy as privacy harms are usually carried out by firms of all sizes and are usually not able to distort competition.[420] As a consequence, the merging of privacy and competition law to address privacy harms to consumers risks leading to a lack of protection. Furthermore, this approach risks unfairly limiting data-driven innovation even for those consumers who prefer to have more efficient services/products at the expense of their privacy.[421] Finally, given that the more data are shared between firms, the more competition is enhanced, remedies which could be beneficial under a competition law perspective could be detrimental for consumers' privacy. This could happen if a dominant company would be required to share its data with competing firms even if consumers did not consent to this data sharing.[422]

[414] Buiten (n 5) 16.
[415] Botta, Wiedemann (n 345) 435.
[416] Buiten (n 5) 17.
[417] Ibid.
[418] Sokol, Comerford (n 343) 311.
[419] Buiten (n 5) 18.
[420] Kimmelman, Feld, Rossi (n 343) 271.
[421] Ohlhausen, Okuliar (n 343) 38.
[422] Sokol, Comerford (n 343) 311-312.

Additionally, taking data protection law into account in the application of competition law would lead to a departure from the economic method developed to delimit its scope of application, also 'shifting its focus away from efficiency'.[423] It has thus been commented that following a more integrated approach would imply that other elements besides efficiency should also be taken into account in the analysis made when assessing the application of competition law, which are usually impossible to define universally and unambiguously. In fact, privacy is said to be 'conceptually unsettled', so that, 'depending on who one asks, it could include also other rights, such as property rights or human dignity'.[424]

Consequently, considering the level of privacy offered by a good/service as an element of the quality of that good/service it is harder than it looks. In fact, privacy is said to be 'subjective, contextual',[425] or even a 'squishy concept' which is not comparable to an 'attribute of goods or services', nor to a 'feature of the market', but is 'rather a consumer preference'.[426] Accordingly, different people are said to have different degrees of tolerance with regard to the privacy intrusiveness of a service, depending on several factors, such as 'age, background, and personal sensitiveness to privacy issues'.[427] Some consumers may perceive that they get more value from services offered for no monetary cost but more intrusive in terms of data collected, than from paid services that collect less data: 'more privacy-friendly terms may not automatically determine a consumer perception of superior quality'.[428] Moreover, it has been pointed out that to date there is no empirical study proving that even those consumers who claim to value their privacy would in fact chose more expensive or less efficient services/products but more respectful of their privacy.[429] Rather, most empirical studies have proved the contrary: 'the majority of consumers value privacy quite a bit less than other product attributes, including price'.[430]

Lastly, the exact point at which privacy degradation should justify the intervention of the authority is hard to determine in cases where, regardless of this degradation, the undertaking offers a product that is nevertheless of higher quality overall. In fact, even if it has been long recognised that anticompetitive effects may manifest through non-price terms and conditions

[423] Ohlhausen, Okuliar (n 343) 40-44.
[424] Ibid 40.
[425] Ibid 36.
[426] Allen P. Grunes, 'Another Look At Privacy' (2013) 20 George Mason Law Review 1107, 1113.
[427] Vera Pozzato, '2014 Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law' (2014) 5 Journal of European Competition Law & Practice 468, 469.
[428] EDPS, 'Privacy and Competitiveness in the Age of Big Data' (n 363), 34.
[429] Colangelo, Maggiolino (n 315) 368.
[430] Geoffrey A. Manne, R. Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (2015) 2 CPI Antitrust Chronicle, 5.

that adversely affect consumers, product quality effects are still rather difficult to distinguish from price effects.[431] Thus, proving a product-quality case without relying on prices would mean to engage in an evaluation that has to balance different non-objective an imprecise dimensions. As pointed out by Manne and Sperry:

> *A watch's quality lies in both its ability to tell time as well as how nice it looks on your wrist. […] Thus, for example, a smaller watch battery may improve its aesthetics, but also reduce its reliability. Any such analysis would necessarily involve a complex and imprecise comparison of the relative magnitudes of harm/benefit to consumers who prefer one type of quality to another.*[432]

What is more, besides the great difficulty of carrying out such an analysis, it is said to be 'extraordinary unlikely' that harms to consumers would outweigh the benefits on net, since 'there is no obvious reason why monopolists would have an incentive to degrade privacy' and 'there is also no likely connection between more data collection and use and harm to consumer welfare'.[433] According to this perspective, an antitrust authority carrying out an investigation based on the above-mentioned risks to consumer privacy would in fact be limited to a simple comparison between

> *the harms to what appears to be a small group of privacy-sensitive consumers (who have not otherwise protected themselves by use of marketplace tools like track-blockers or by use of the opt-out options provided by major ad networks and data brokers) to the benefits of the majority of less privacy-sensitive consumers.*[434]

In this context, it is important concluding with a brief overview of the forthcoming regulatory tools that the European Union will adopt in the context of the so-called "European digital strategy" to address the issues highlighted thus far.

[431] Ibid 3.
[432] Ibid.
[433] Ibid 6.
[434] Ibid.

3. Digital Markets Act

The proposed Digital Markets Act (DMA)[435] is a Proposal of Regulation aimed at introducing 'harmonised rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present'.[436]

The DMA is an *ex-ante ad hoc* regulation proposal which condenses in a single act the knowledge gathered in recent years about large digital platforms thus reacting to the difficulties emerged in addressing their *modus operandi* through a classic antitrust investigation, with the aim to align this knowledge among MSs and to speed up the enforcement process.[437]

It covers eight categories of core platform services (which could be expanded following a market investigation by the Commission pursuant to Article 17 DMA): 'online intermediation services'; 'online search engines'; 'online social networking services'; 'video-sharing platform services'; 'number-independent interpersonal communication services'; 'operating systems'; 'cloud computing services'; 'advertising services'.[438]

Concentrating on "core platform services" will enable the DMA to keep a closer watch on those digital services which usually act as so-called "choke points" where gatekeeper positions are more likely to form with a major impact on businesses and consumers.[439]

It introduces a number of criteria to ascertain whether a large online platform can be qualified as a "gatekeeper". In particular, a gatekeeper is a company which (i) has 'a strong economic position', 'a significant impact on the internal market' and is 'active in multiple EU

[435] Proposal for a Regulation Of The European Parliament And Of The Council on contestable and fair markets in the digital sector (DMA) [2020] COM/2020/842 final. To further deepen the topic, with a focus on critical analyses of the proposed regulation, See Alexandre De Streel, Pierre Larouche, 'The European Digital Markets Act Proposal: How to Improve a Regulatory Revolution' (2021) 2 Concurrences; Pablo Ibáñez Colomo, 'The Draft Digital Markets Act: A Legal and Institutional Analysis' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790276> accessed 10 August 2021; Giorgio Monti, 'The Digital Markets Act: Improving Its Institutional Design' (2021) 5 European Competition and Regulatory Law Review; Rupprecht Podszun, Philipp Bongartz, Sarah Langenstein, 'Proposals On How To Improve The Digital Markets Act' (*Competition Policy International*, 11 March 2021) <https://www.competitionpolicyinternational.com/proposals-on-how-to-improve-the-digital-markets-act/> accessed 3 February 2022; Simonetta Vezzoso, 'The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772724> accessed 3 February 2022.
[436] Art. 1(1) DMA.
[437] Nicolas Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' (2021) Journal of European Competition Law & Practice, 4.
[438] Article 2(2) DMA.
[439] Petit (n 437) 4.

countries'; (ii) has a 'strong intermediation position' between users and businesses; (iii) has or is about to have an 'entrenched and durable position in the market'.[440]

These thresholds are practically designed to capture the FAANG big tech and possibly a few more.[441] A firm can be qualified as a gatekeeper even after a market investigation based on indicators such as 'high growth rate', 'entry barriers' derived from 'network effects' and 'data driven advantages', 'economies of scale and scope', 'user lock-in'.[442] This investigation resemble a market power analysis, without the need to define the relevant market beforehand.[443]

Gatekeepers are subject to a number of obligations listed in Articles 5 and 6 DMA which address behaviours considered to be '*per se* harmful' regardless of whether companies can justify such conduct with possible efficiencies: 'companies which qualify as gatekeepers under the DMA will have to integrate all its provisions in their business models'.[444] Such obligations can be classified in four groups which account for the most abusive conduct witnessed in the digital economy:[445] 'opaque and asymmetric access to data';[446] 'obstacles to interoperability';[447] 'conditions for obtaining access to end-users';[448] 'end-user empowerment'.[449]

Article 12 DMA introduces an obligation for gatekeepers to notify the Commission of any planned acquisitions in the digital sector irrespective of potential parallel application of merger control rules, so that it can have a full picture of the areas in which gatekeepers are extending.[450]

Finally, Article 13 DMA introduces the obligation to periodically submit to the Commission an independently audited description of any techniques for profiling consumers that the gatekeeper applies to or across its core platform services. This obligation aims to

---

[440] European Commission, 'The Digital Markets Act: ensuring fair and open digital markets' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en#new-rules-in-a-nutshell> accessed 10 August 2021.
[441] Luís Cabral and Others, *The EU Digital Markets Act* (Publications Office of the European Union 2021), 9.
[442] Article 3(6) DMA.
[443] Petit (n 437), 5.
[444] Filomena Chirico, 'Digital Markets Act: A Regulatory Perspective' (2021) Journal of European Competition Law & Practice, 3.
[445] Ibid.
[446] In particular the practices described in Articles 5(a), 5(g), 6(1)(a), 6(1)(g), 6(1)(i), 6(1)(j).
[447] In particular the practices described in Articles 5(e), 6(1)(c), 6(1)(e), 6(1)(h).
[448] In particular the practices described in Articles 5(b), 5(c), 5(f), 6(1)(d), 6(1)(k).
[449] In particular the practices described in Articles 6(1)(b), 6(1)(e), 6(1)(f).
[450] Chirico (n 444) 3.

make the use of user data by these operators more transparent, so that consumers can make informed choices.[451]

Of particular relevance is the obligation introduced by Article 5(a) DMA, which requires gatekeepers offering multiple core platform services to

> *refrain from combining personal data sourced from these services with personal data from any other services offered or with personal data from third-party services unless the end user has been presented with the specific choice and provided consent according to Regulation 2016/679.*

The DMA thus addresses the conduct of Facebook that gave rise to the German BKA decision which I will analyse deeper in Chapter 4. The purpose of this provision is to address consumer exploitation through the massive collection of personal data and heavy profiling, obliging gatekeepers to give them a choice as to the extent of such practices.[452] A second objective pursued by Article 5(a) DMA is the limitation of data-driven economies of scope, which are likely to take place on the supply side through the combination of personal data, so 'to improve contestability conditions for new entrants in the core platform service and adjacent markets'.[453]

Furthermore, the DMA proposal introduces some provisions which may tackle the lock-in issues. In particular, gatekeepers will have to 'provide effective portability of data through the activity of business user or end user'.[454] Gatekeepers will also have to provide business users with 'effective, high-quality, continuous and real-time access and use' of data generated during the use of their services available on the platform.[455]

Since the DMA provides for conducts that are always prohibited, the discretion of antitrust authorities in applying the law is limited. Indeed, certain conducts are prohibited irrespective of whether or not they constitute an abuse of power.[456] Therefore, the DMA can be qualified as 'a no fault and a *per se* prescription and proscription system'.[457]

Even if the DMA is an *ex-ante* form of regulation and it does not need to be applied only after an harmful conduct has been detected, there are still a number of decisions to be taken

[451] Ibid.
[452] Petit (n 437) 8.
[453] Ibid.
[454] Article 6(1)(h) DMA proposal.
[455] Article 6(1)(i) DMA proposal.
[456] Petit (n 437) 4.
[457] Ibid 4.

(such as the designation of a firm as a gatekeeper[458] or the determination that a given conduct amounts to a violation of the DMA).[459] In this regard, the Commission, assisted by a committee of Member States' representatives (the Digital Markets Advisory Committee), is designated as the competent authority to supervise the compliance with the DMA throughout the internal market.

The DMA procedural rules recall the rules on the enforcement of EU competition law,[460] with regard to 'the opening of proceedings for market investigations as well as the Commission's powers to gather the necessary information', 'to impose interim measures', 'to accept commitments', 'to monitor implementation and compliance'.[461]

The DMA has the objective of complementing the existing *ex post* application of competition rules with regard to those practices that either escape the reach of "traditional" antitrust laws or that cannot be precisely framed and successfully handled by them.[462] In fact, the DMA adopts a completely different approach in addressing specific *per se* harmful conducts, irrespective of the market boundaries in which the gatekeepers operates and of its position in it.[463]

4. Concluding Remarks

In this chapter, we saw how the two issues of information asymmetry and weak competition self-reinforce in digital markets. In fact, the absence of meaningful competitive pressure due to the presence of only a few dominant firms on the market, discourages those firms from revealing in a clear and accessible way the data practices they carry out. This lack of transparency prevents users from carrying out informed consumption choices on the basis of a comparison between the characteristics of the services offered.

In particular, we saw how weak competition leads to the collection of excessive data from users and prevents the developing and offering of more privacy-friendly services, also causing a supply-gap in which the demand for more privacy-friendly services is not satisfied.

As for information asymmetry, not only users are prevented from clearly understanding the extent to which their data are collected and whether or not this is justified for the provision of

[458] Article 3(4) DMA.
[459] Article 25 DMA.
[460] Regulation No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1.
[461] Chirico (n 444) 3.
[462] Ibid 4.
[463] Ibid.

the service they request, but they are also unaware of the risks they bear because of this excessive data collection. Furthermore, they cannot perceive the actual value of their data. As a result, their behaviour is biased, so that they overvalue the fact that services are provided at zero monetary costs and underestimate the value of their data. Firms take advantage of this biased behaviour to claim that there is no need to provide less privacy-invasive services as there is no proof users will actually prefer them.

In this context, some scholars, institutions and authorities advocated for a more integrated enforcement approach between competition, data protection and consumer protection laws. This is mainly justified by the central role of data in digital markets which determines the overlap between their spheres of application. In particular, the level of privacy ensured by a service can be assessed as an element of the quality of the product; also, privacy policies can be considered as unfair trading conditions, and in this case data protection law can be used as a benchmark to assess unfairness.

On the other hand, some authors advocate for a separate and autonomous application of those policies, so that information asymmetry can be tackled with consumer or data protection law, while competition law has to be applied without taking into account privacy considerations. This latter consideration is even more justified by the need to preserve the economic method guiding the application of competition law.

Regardless of the potential overlap between different areas of law, the applicable law should be chosen also on the basis of the type of harm being addressed and of the effectiveness of the remedies available.[464] As we saw in Section 3.1. and following, the market failure caused by the information asymmetry between users and firms is inextricably tied to the weak competition over the level of privacy protection offered in digital markets. In particular, it is clear that the GDPR and available consumer law remedies alone are not adequate to properly address them as in this case weak competition is also a factor which prevents consumers from making informed choices.

As discussed above, in the digital economy the overlap between competition, consumer and data protection law is inevitable for the reasons already explained at length. It would be wrong to see this overlap as an obstacle in law enforcement as it would lead to paralysis. Instead, support should be given to a more synergetic application of the three disciplines, whereby even in the event of overlapping, action can be taken where there is reason and opportunity to do so.[465]

[464] Ohlhausen, Okuliar (n 343) 39.
[465] Botta, Wiedemann (n 345) 439.

These considerations seems to have been taken into account by the proposed DMA, which in a number of provisions addresses the way in which gatekeepers may or may not use data. However, the centralised model of enforcement it provides may limit national authorities contributions in finding ways to intervene in digital markets.

In the following chapters I will present and discuss the BKA and the AGCM decisions against Facebook, which are emblematic of the current position of national authorities with regard to abusive practices in data-related markets.

CHAPTER IV

THE *BUNDESKARTELLAMT* DECISION

1. Introduction

In this chapter, I will first provide a summary of the decisions issued by the *Bundeskartellamt*, the Higher Regional Court in Düsseldorf and the Federal Court of Justice. Afterwards, I will present the legal context in which the *Bundeskartellamt* decision was adopted so to allow a more in dept analysis of its approach and of its effectiveness and further consequences.

2. An Overview

On 6 February 2019 the *Bundeskartellamt* ("BKA" hereafter) issued a decision against Facebook based on Section 19 German Competition Act[466] (which can be considered as the German equivalent of Article 102 TFEU). The decision was adopted at the end of an administrative proceeding, therefore the BKA did not imposed a fine on Facebook.[467]

The BKA found that Facebook is dominant on the German market for social networks, and that it abused its position by imposing exploitative terms of service to its users. Through these terms of service, which had to be accepted in order to use the social network, Facebook was able to collect users' data outside the social network and to assign them to the individual user account thus developing very detailed profiles of each user, without a valid consent. In particular, Facebook was able to collect data from company-owned services (like WhatsApp, Instagram, Oculus and Masquerade), and from third party websites and apps (mainly through Facebook Business Tools, such as the Like Button, Facebook Login or Facebook Analytics).

The BKA argued that Facebook terms of service were abusive because they caused users to lose control over their personal data, and because they harmed competition allowing Facebook to entrench further its dominant position.

---

[466] Bundeskartellamt, 6 February 2019, B6–22/16—Facebook.

[467] According to the BKA, '*Administrative proceedings are more appropriate for complex cases that raise difficult legal and economic questions, and for pilot proceedings to clarify the interpretation of the law in a (new) case constellation. The main objective of such proceedings is not to impose a fine but to re-establish pro-competitive conditions as fast as possible*', in Bundeskartellamt, 'Background information on the Facebook proceeding' (19 December 2017), 1.

The BKA prohibited Facebook to keep the supply of the social network for private users residing in Germany conditional on the acceptance of the abusive terms of service.

2.1. The Decision of the Higher Regional Court in Düsseldorf

Facebook appealed the BKA decision before the Düsseldorf Higher Regional Court asking for an interim relief. On 26 August 2019, the Court granted the suspensive effect of the appeal against the BKA decision due to serious doubts as to its legality, pursuant to Section 65(3) GWB.[468]

The Court argued that, because data can be duplicated and users can make them available to any third party, users did not experience any economic weakening. They do not lose control over their data because, at the moment of registration, they can autonomously assess the advantages and disadvantages of using a free advertising-financed social network. The Court argued that users not taking notice of Facebook terms of service is not based on Facebook's market power, but on the indifference or convenience of users.

Furthermore, whether the exploitative terms are set by a dominant or non-dominant undertaking is irrelevant for the burden on the consumer. Not any abusive conduct performed by a dominant undertaking can be addressed under Section 19 (1) GWB, but only the ones that are possible *because of* its dominant position. In this case, The BKA did not prove that Facebook was able to unduly influence the behaviour of consumers because of its dominant position. Rather, the user could make a choice autonomously and without being subject to any abusive influence, in accordance with its own values and preferences. As a consequence, users' right to self-determination was not violated.

Furthermore, the Court did not found any exclusionary abuse to the detriment of Facebook's competitors. The collection and combination of data across Facebook-owned services and third party's services do not increase barriers to entry.

In any event, according to the Court, the order issued by the BKA is not suitable to put an end to the assumed abuses, because it does not prohibit the abusive behaviour *per se*, meaning collecting, bundling and using the data in question, but it makes it conditional to the valid consent of users.

[468] Düsseldorf Higher Regional Court, 26 August 2019, VI-Kart 1/19(V)—Facebook I, Juris.

2.2. The Decision of the Federal Court of Justice

The BKA challenged this decision before the Federal Court of Justice (FCJ), which overruled it, deciding that the BKA's order against Facebook could be enforced while pending a final judgment in the main proceedings.[469]

The FCJ uphold that Facebook abuses its dominant position through the terms of services prohibited by the BKA, however it is not relevant whether these terms violate the GDPR. The important aspect is rather that these terms deprive Facebook's users of any choice as to whether they prefer to use the service with a level of personalisation which is based only on data they themselves share on Facebook, or also on data gathered from different sources so to have a more personalised service. This lack of choice is possible because competition is no longer capable of exercising its controlling function over Facebook. In fact, if competition on the market for social networks was effective, such an option could be expected to be available and users who wished to disclose less personal data could switch to other alternatives.

The Court recognised that access to data is an essential competition parameter in both the markets of advertising and social networks. Facebook's terms of service can impede competition because Facebook's access to data, thus gained, increases the 'lock-in effects' on the user side, and enhances the possibilities to finance the social network using the profits generated from advertising contracts, which also depend on the scope and quality of the available data.

2.3. The Request for a Preliminary Ruling

On April 2021, the Higher Regional Court, before which the main proceedings are still pending, referred a preliminary ruling to the European Court of Justice, asking seven questions.[470]

In the first question, the Court asked whether it is in breach of the GDPR the fact that an antitrust authority has ordered Facebook, which has its main establishment in another Member State, to stop carrying out a processing which is deemed to be in violation of the GDPR. Furthermore, the Court asked whether the fact that the Irish DPA (the lead DPA for

[469] Federal Court of Justice, 23 June 2020, KVR 69/19—Facebook, Juris.
[470] Request for a Preliminary Ruling, Case C-252/21 *Facebook Inc. and Others v Bundeskartellamt*.

Facebook) opened an investigation into the same contractual terms could be compatible with Article 4 (3) TEU.[471]

With the second question the Court asked whether the fact that Facebook collects and combines from third-parties' services data related to the criteria of Article 9(1) GDPR implies the processing of special categories of personal data, and if this is the case, whether an active action of the user (such as clicking on buttons integrated in these services provided by Facebook ('like', 'share' etc.), implies that the user is manifestly making public such information pursuant to Article 9(2)(e) GDPR.

With the third question, the Court asked whether the collection and bundling of data across Facebook-owned services and third party's services is a processing activity which could rely on Article 6(1)(b) GDPR (namely, whether this activity could be deemed necessary for the performance of the contract concluded by Facebook and the user) or on Article 6(1)(f) GDPR (namely, whether this activity could be considered to be aimed at pursuing the legitimate interest of the controller).

With the fourth question, the Court listed a number of specific purposes (such as the improvement of products, research and innovation for social good, etc.) and asked whether all these purposes could be pursued on the basis of Facebook's legitimate interest through the collection and bundling of data across Facebook owned services and third-party's services.

With the fifth question, the Court asked whether these processing activities could be justified under other legal bases, such as the compliance with a legal obligation of the controller (Article 6 (1) (c)), or the protection of the vital interests of the data subject or another person (Article 6 (1) (d)), or the performance of a task in the public interest (Article 6 (1) (e)).

With the sixth question, the Court asked whether the consent given to a dominant undertaking such as Facebook, can be deemed valid pursuant to the requirements set by the GDPR.

With the last question, the Court asked whether the BKA, while assessing the legality of the terms of service related to the processing of personal data, can determine that such terms violate the GDPR, and if this is the case, whether this is permissible under Article 4 (3) TEU when the Irish DPA is also investigating the same terms.

---

[471] Article 4(3) TEU provides that "*Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.*
The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.
The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives."

3. The BKA Decision

In the following sections, I will present the BKA decision in more details, providing the legal framework and the relevant case law on which the BKA relied upon to adopt its decision, as well as its main findings, an analysis of its approach and of its effectiveness.

3.1. Legislative Framework and Case Law

The BKA's decision is based on Article 19 (1) GWB[472] as interpreted by the Federal Court of Justice (FCJ). This is a rather generic provision, as it states that 'any abuse of a dominant position by one or several undertakings is prohibited'. However, the FCJ elaborated specific criteria defining the scope of application of this norm.

To assess whether an undertaking is dominant, the BKA has to consider the elements set forth in Article 18 GWB. The BKA found that Facebook has a dominant position in the German market for social networks pursuant to Article 18(1) in conjunction with (3) and (3a) GWB.[473]

Before the beginning of the investigation into Facebook's conduct, the GWB underwent the 9th amendment, which recognised more power to the BKA in the field of consumer protection[474] and introduced a number of changes especially aimed at digital markets.[475] For instance, Article 18 (2a) provides that a market can be defined even when a service is provided at zero monetary price; Article 18 (3a) is a clear reference to digital platforms, according to which, in order to determine the market share in multi-sided markets and networks the following elements have to be considered: the existence and extent of direct and indirect network effects; whether users multi-home; the economies of scale experimented by the undertaking in connection with the network effect; the extent to which the undertaking has access to data relevant for competition; whether there is any competitive pressure arising from innovation.

---

[472] The English version is available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/GWB.

[473] Bundeskartellamt, 6 February 2019, B6–22/16—Facebook (English version), para 374.

[474] Irene Lorenzo-Rego, 'The Perspective of the Bundeskartellamt in the Evaluation of Facebook's Behaviour: Prior Considerations and Possible Impact' (2019) 3 European Competition and Regulatory Law Review 100, 101.

[475] Schneider (n 393) 218; Anne C. Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021) 66 The Antitrust Bulletin 276, 283.

Through Section 18 (3a) GWB, the BKA was able to take a vivid picture of Facebook's dominant position and of the dynamics at the basis of it. In fact, this provision considers all the elements typical of multi-sided digital markets, as also outlined in previous sections, which are usually difficult to address using "traditional" tools of competition law.

Once the BKA established that Facebook held a dominant position in the national market for social network, it then focused on the evaluation of the abusive conduct. In this respect, the BKA relied on the general clause of Section 19 (1) GWB and on the case law of the Federal Court of Justice.

In the *Entega II* judgment,[476] the FCJ stated that Section 19 (1) GWB can be used also as a tool to protect consumers.[477] In the *VBL-Genenwert* cases,[478] the FCJ stated that Section 19 (1) GWB can be relied upon to address an abusive practice in which a dominant firm has adopted general business terms that (i) are inadmissible under the legal principles of Sections 307 and following of the German Civil Code (regulating unfair business terms), and (ii) represent a manifestation of market power or superior market power.[479] In the *Pechstein* case,[480] the FCJ clarified that when constitutionally protected legal positions are threaten in the context of unbalanced negotiations, it is necessary to carry out a balancing of interests through the application of general clauses, such as Section 19 GWB, so that the constitutional rights of all parties are maintained as far as possible.[481]

According to the BKA, through this case law the FCJ developed the principle of 'appropriateness' requiring that an appropriate balance of interests is reached in unbalanced negotiations where the bargaining power of one party is able to unduly compress the right to self-determination of the other.[482] In this balancing test, a predominant role is covered by the legislation on unfair contractual terms, so that if a conduct is deemed abusive under these provisions, the same conduct will be considered abusive under Section 19 GWB if a sufficient degree of market power is involved.[483]

---

[476] Federal Court of Justice, judgment of 07.12.2010 – KZR 5/10 – *Entega II*, WuW/E DE-R 3145, 3155f., para. 24.
[477] Bundeskartellamt (n 473) [525].
[478] Federal Court of Justice, judgment of 6 November 2013, file KZR 58/11,VBL Gegenwert I, para. 65; Federal Court of Justice, judgment of 24 January 2017, file KZR 47/14, VBL Gegenwert II, para.35.
[479] Bundeskartellamt (n 473) [527].
[480] Federal Court of Justice, judgment of 7 June 2016, file KZR 6/15, Pechstein, para. 55 – 57.
[481] Bundeskartellamt (n 473) [527].
[482] Ibid 528, in reference to Federal Constitutional Court, decision of 7 September 2010, file ref. 1 BvR 2160/09, Gasag, para 34.
[483] Ibid, in reference to Federal Court of Justice, decision of 6 November 2013 – KZR 58/11, VBL Gegenwert I; Federal Court of Justice, decision of 24 January 2017 – KZR 47/14 – VBL Gegenwert II.

Even if this case law was developed to take into account the principles of Section 307 and following of the German Civil Code in the application of Section 19 (1) GWB, the BKA argues that the same mechanism can be applied with any principle of legal provisions provided that the conduct under scrutiny (i) is put in place by a dominant firm and that (ii) it concerns unbalanced negotiations.[484]

Accordingly, in data-driven industries the goal of data protection law is to address the power asymmetries between the parties involved, so to preserve the contractual freedom of the consumer in relation to the collection and processing of its personal data. The BKA thus argued that conditions which violate the principles of data protection law as well as those on unfair contractual terms constitute an abuse of a dominant position under Section 19 (1) GWB if a sufficient degree of market power is involved.[485]

This approach was subsequently sustained by a legislative proposal to amend the GWB published on October 2019, only after a month the Higher Regional Court in Düsseldorf took down the BKA's decision.[486] In January 2021 the amendment was enacted.

The most significant change is the introduction of Section 19a 'Abusive Conduct of Undertakings of Paramount Significance for Competition Across Markets', which recalls the 'gatekeeper' concept of the DSA, and addresses conducts typically held by large digital platforms. In particular, Section 19a (2) no. 4 allows the BKA to prohibit an undertaking, which has been declared of paramount significance for competition across markets pursuant to Section 19a (1), to adopt terms and conditions which would allow it to collect data in a way that impairs competition. According to Section 19a (2) no. 4(2) this would be the case when an undertaking makes the use of a service conditional to users' consent to collect and combine data across different services provided by the same undertaking or by third parties. However, it has been observed that it is not clear what would be an acceptable range of choice that an undertaking has to provide to consumers in order to comply with such a provision, nor it is clear which legal standard should be considered when carrying out such evaluation.[487]

Finally, the amended GWB simplifies the proceeding to challenge the decisions issued by the BKA pursuant to Section 19a which will be brought directly before the FCJ, thus bypassing the Düsseldorf Court.

---

[484] Bundeskartellamt (n 473) [529].
[485] Ibid [532].
[486] Witt (n 475) 296.
[487] "*It is also not clear, from which normative criterion such a minimum standard of choice is ultimately derived: Is it derived from privacy protection and informational self-determination (as in the BKA or Federal Court of Justice decisions) or from contestability and fairness (as in the DMA proposal), from the objective of consumer empowerment (consumer policy), or from an autonomy-basedconcept of freedom of choice (or a combination of them)?*" in Kerber, Zolna (n 362) 24.

3.2. Market Definition

The BKA held that Facebook.com is an advertising-financed network, which as a result forms a multi-sided market, composed by private users, advertisers, publishers and developers.[488] According to the BKA, private users and advertisers are the key user groups.[489]

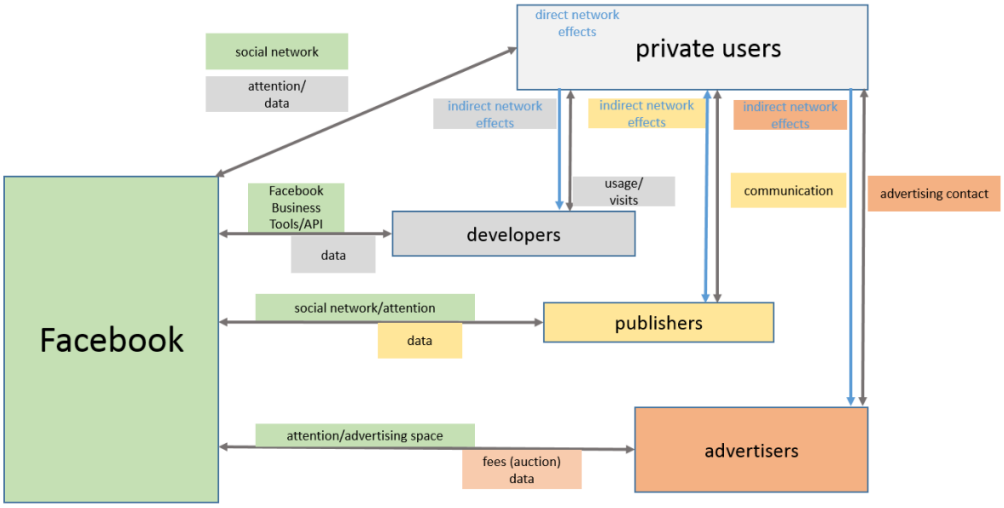

Figure 6 Involved market sides in Facebook's social network service, in Bundeskartellamt, Case Summary B6-22/16 (2019), 4.

The BKA defined the product market based on the criterion of demand-side substitution from the perspective of private users. Social networks respond to specific demand private users have, therefore they constitute a specific market in the context of social media. The BKA argued that only StudiVZ, Jappy and Google+ can be included in the market, whereas all other services (like professional networks or services like Snapchat, Youtube, Twitter, Instagram, Pinterest) were excluded from the relevant market as represent competition from substitutes.[490]

According to the BKA, the purpose of social networks is to allow users to find and network with people they already know, and 'to exchange on a daily basis experiences, opinions and contents among specific contacts which the users define based on identity.'[491] The competitors of Facebook included in the relevant market fulfil this same purpose, despite

[488] Bundeskartellamt (n 473) [213-229].
[489] Ibid [216].
[490] Ibid [230].
[491] Ibid [249].

the limited scope for substitutability, due to the direct network effect which characterises the Facebook service.[492]

As for the relevant geographic market, the BKA found that the use of social networks is mostly limited to national borders, due to the identity-based network effect mentioned above.[493] In fact, the BKA's surveys showed that the vast majority of Facebook users in Germany uses the social network to connect with users who reside in Germany.[494]

3.3. Market Dominance

The BKA found that Facebook is dominant on the national market for social network for private users, pursuant to the assessment of the factors listed in Section 18(1) in conjunction with (3) and (3a) GWB.

The BKA relied on Article 18 (2a) GWB to justify the analysis of the dominant position of Facebook, specifying that the distortion of the competition due to the presence of a dominant position in a market where users are charged no monetary price can be assessed considering other elements than price dynamics:

> *In particular in the case of advertising-funded internet platforms, where direct monetary payments by users of the services are replaced by attention marketing and the marketing of user data to advertisers in the form of targeted advertising, the scope for processing user data which users cannot avoid because of the services' market power, is also a relevant factor in defining market power. This applies irrespective of the question of whether the user data themselves are to be considered as payment for a service or as a contractual condition serving to maintain a price of zero. Besides, the extent of data processing can also be seen as an element of the quality of the service*.[495]

The BKA relied on the Article 18 (3a) GWB to assess whether Facebook held a dominant position in the relevant market[496] finding that: (i) Facebook benefitted from identity-based direct network effect on the users' market side and indirect network effect with regard to the

[492] Ibid [264-265].
[493] Ibid [345-347].
[494] Ibid [347].
[495] Ibid [379].
[496] Ibid [422] and ff.

advertising market side;[497] (ii) users did not multi-home and experimented a high lock-in effect mainly because of the identity-based direct network effect and of the lack of interoperability of the Facebook service with other services;[498] (iii) Facebook benefitted from economies of scale due to the very low marginal cost for any additional user and to the ease of absorbing fixed costs;[499] (iv) Facebook had a superior access to users' data due to its massive user base and to its variegated data sources;[500] and (v) Facebook's position was not restrained by any innovation-driven competitive pressure.[501]

The network effects from which Facebook benefits are 'identity based' since the most important element for private users is not the number of Facebook's users, rather, their identity: 'the network's value for individual consumers increases with an increasing number of people from their social context who join the network.'[502] Consequently, users experiment a powerful lock-in effect due to the difficulty of switching networks, as friends (and friends of friends, etc.) would have to be persuaded to switch as well.[503]

To assess Facebook's market share, the BKA relied on the number of daily active users,[504] holding that this criterion was much more relevant to grasp the actual market share of a digital platform than the volume of its turnover, as the services in one or several market sides were provided free of any monetary charge.[505] In particular, the BKA specified that 'the number of daily active users is the primary indicator of the value of a network and its market success', considering that social networks such as Facebook.com are aimed at allowing users to share content on daily basis with other users.[506]

Furthermore, the number of daily active users is also the most relevant factor to assess the monetisation potential of the social network service from a targeted advertising perspective:[507] the collection of massive amounts of data on a daily basis improves the accuracy of targeting and the value of the advertising service.

Accordingly, on the basis of daily active users, Facebook was found to have a market share of more than 90% since 2012 'with an upward trend'.[508]

---

[497] Ibid [449-451].
[498] Ibid [452].
[499] Ibid [477] and ff.
[500] Ibid [481].
[501] Ibid [501] and ff.
[502] Ibid [273].
[503] Ibid [276].
[504] Ibid [400].
[505] Ibid [404].
[506] Ibid [407].
[507] Ibid [410].
[508] Ibid [413].

3.4. Abusive Data Policy as Abusive Business Terms Pursuant to Section 19 (1) GWB

According to the BKA, Facebook's terms of service

> *constitutes an abuse of a dominant position on the market for social networks for private users in the form of abusive business terms pursuant to the general clause of Section 19(1) GWB because, as a manifestation of market power, these terms violate the principles of the GDPR.*[509]

As previously explained, the BKA relied on the FCJ case law to hold that principles of the legal system that regulate the appropriateness of conditions in unbalanced negotiations can be taken as a benchmark when assessing whether terms and conditions are abusive under Section 19(1) GWB. Consequently, as the principles of GDPR address power imbalances in data-driven industries, the GDPR can be used as a standard to assess the 'appropriateness' of the data processing conditions of a dominant company.[510] The BKA argued that the protection ensured by data protection law and the one ensured by provisions prohibiting unfair contractual terms are very similar, also because they address similar kinds of violations: violations of data protection law are often committed through the adoption of violating privacy policies, which consist in pre-formulated contractual terms imposed on the consumer.[511]

Consequently, the BKA focused on assessing whether Facebook's privacy policy violated the GDPR and found that the processing activity under scrutiny could not be justified under any of the legal bases provided by the GDPR.[512]

In particular, the BKA argued that the consent obtained from users was not freely given, specific, informed and unambiguous, as required by the GDPR: agreeing to terms of service in order to be able to use the service does not constitute a voluntary consent, even more so because Facebook has a dominant position.[513]

The BKA refers to Article 7 (4) GDPR, according to which consent is not freely given when is conditional to the provision of a service for which said processing is not necessary; and to Recital 43 according to which consent given by the data subject is not freely given

[509] Ibid [523].
[510] Ibid [526].
[511] Ibid [532-534].
[512] Ibid [629].
[513] Ibid [640-643].

when a ‘clear imbalance’ exists between the data controller and the data subject. According to the BKA, the processing activities under its scrutiny were not necessary to the provision of the social network service and yet, their acceptance was conditional to use it; furthermore, Facebook is in a dominant position and a ‘clear imbalance’ exists between the firm and its users.

Finally, the BKA mentioned Recital 42, according to which consent should not be considered freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. According to the BKA the choice between accepting the conditions or not being able to use the service is not a ‘genuine choice’.

In any case, no such explicit consent, as required by Article 9 (2) (a) GDPR, is given from users for the processing of special categories of data. If anything, an explicit consent can only be deemed to exist for data users voluntarily provide at the moment of creation of the profile, but not for the information derived from the combination and use of data from Facebook-owned services and Facebook Business Tools.[514]

The BKA argued that the processing was not necessary for the performance of the contract between Facebook and its users, therefore Facebook improperly relied on Article 6 (1) (b) GDPR. According to the BKA, there is no contractual link between all Facebook products that could allow the combination of data across them, also because separate contracts regulate the provision of each of the Facebook products and independent registration processes are required for each Facebook-owned service.[515] In any case, data processing from all sources is not necessary for the claimed contractual purposes, namely ‘the provision of personalised services and the display of personalised advertising.’[516] In fact, the necessity has to be assessed with respect to a narrowly-defined main purpose of the contract, according to which not all data processing that is merely useful can be deemed necessary.

With regard to Article 6 (1) (c), which allows the processing of data if necessary for the controller to comply with legal requests and obligations, the BKA argued that the data processing consisting in the collection from Facebook-owned services and Facebook Business Tools and/or data being combined with Facebook user accounts, is not even mentioned in Facebook’s Terms of Service, ‘which deals with data access, storage and transfer to the authorities, but not with the collection and combination of data.’[517]

[514] Ibid [647-650].
[515] Ibid [680].
[516] Ibid [667-670].
[517] Ibid [718].

The same is true for the legal ground provided by Article 6 (1) (d), which allows the processing in order to protect the vital interests of the data subject or of another person. The BKA claimed that this legal basis can be relied upon only in situations in which there is a 'concrete risk for life' in which the data subject is incapable of expressing its consent while it does not justify processing operations aimed at anticipating the occurrence of such situations.[518]

The BKA argued that there is no evidence which could justify the application of the legal basis provided by Article 6 (1) (e), which allows the processing to take place when is necessary to carry out tasks in the public interest.[519]

Finally, the BKA found that not even Article 6 (1) (f) could justify the processing at stake. Article 6 (1) (f) allows the processing if necessary for the purposes of the legitimate interests pursued by the controller, and if such interests are not overridden by the interests or fundamental rights and freedoms of the data subject. With regard to the processing operations assessed by the BKA, the Authority argued that there is a significant imbalance between Facebook's interests and the protection of users' fundamental rights, therefore Article 6 (1) (f) cannot be invoked as a legal basis for the processing of data collected and combined from Facebook-owned services or Facebook Business Tools.[520]

3.5. Abusive Data Policy as a Manifestation of Market Power

The BKA recalls the case law of the Federal Court of Justice, according to which the fact that the violation of legal adequacy provisions has taken place as a manifestation of market power is a sufficient causal link to substantiate a violation of antitrust laws. The BKA rejects the necessity of a strict causality between the conduct and market power, meaning that it is not necessary to prove that Facebook's data policy could be formulated in such a way only because of Facebook's market power. Rather, a normative causality is deemed to be enough, meaning that it is sufficient to prove that the conduct is 'anticompetitive as a result of market dominance'.[521]

According to the BKA, a normative-causal connection exists between Facebook's market power and the violation of data protection laws. In fact, the infringement of data protection rules is determined by the fact that Facebook's dominant position makes possible the

[518] Ibid [722].
[519] Ibid [723].
[520] Ibid [870].
[521] Ibid [872-873].

restriction of private users' right to self-determination as users only accept its data processing conditions because otherwise they could not access the service[522] and they would also have little or no possibility of switching to a different provider to avoid the dominant undertaking's data policy.[523] Therefore, according to the BKA, the violation of data protection laws is 'a manifestation of Facebook's market power'.[524]

Furthermore, the BKA deemed Facebook's conduct to be detrimental not only for private users, but also for competitors. The BKA stated that there is a causal relationship between Facebook's unlawful data processing and market dominance 'with regard to the actual and potential impediment effects to the detriment of competitors'.[525] In particular, the risk of transferring market power is especially high with regard to the market of targeted advertising, and to the markets in which other Facebook-owned services operate.[526] Furthermore, Facebook's data processing increases the barriers to market entry in the market for social networks, and puts competitors, who have lawfully processed data in the past, at a competitive disadvantage.[527]

4. BKA's Approach

The BKA's approach is said to be innovative at least for three reasons: (i) it is the first time a competition authority finds an exploitative abuse, rather than an exclusionary one, with regard to a digital platform;[528] (ii) the BKA applied German law rather than Article 102 TFEU;[529] (iii) data protection law was used as a benchmark to assess the unfairness of the conduct.[530]

This approach has been widely criticised mainly because, according to some scholars, there was room to apply European law rather than the GWB and because data protection law was improperly used.

[522] Ibid [876].
[523] Ibid [883].
[524] Ibid [879].
[525] Ibid [885].
[526] Ibid [886-887].
[527] Ibid [888].
[528] Botta, Wiedemann (n 345) 429; Schneider (n 393) 215.
[529] Botta, Wiedemann (n 345) 440.
[530] Witt (n 475) 281; Kerber, Zolna (n 362) 21.

Some scholars argue that the BKA should have applied Article 102 TFEU rather than national law.[531] In fact, not only Facebook's conduct is not limited to Germany and it impacts the EU internal market, but it also meets the requirements for an abuse under Article 102 (a) and/or (b) TFEU.

As for Article 102 (a), according to the CJEU case law, an exploitative abuse takes place when a dominant undertaking imposes contractual clauses which are unjustifiably unrelated to the purpose of the contract, or unnecessarily limit the freedom of the parties, or are disproportionate, unilaterally imposed or seriously opaque. Therefore it is argued that the BKA could have applied Article 102 (a) as Facebook's terms providing the combination of users' personal data are disproportionate, unilaterally imposed and seriously opaque.[532] In fact, there is room to argue that (i) the extent to which this practice invades users' privacy is disproportionate in comparison to the value of the service offered, (ii) users cannot decide to decline these terms if they want to use the social network and (iii) the extent of the combination of users' data is insufficiently explained in Facebook's privacy policy.

As for Article 102 (b), it has been argued that Facebook's conduct has a foreclosure effect towards its competitors in the advertising market. In particular, this conduct would fall within the definition of exclusionary abuse provided by the CJEU in *Post Danmark I*:[533]

> *the conduct of a dominant undertaking that, through recourse to methods different from those governing normal competition on the basis of the performance of commercial operators, has the effect, to the detriment of consumers, of hindering the maintenance of the degree of competition existing in the market or the growth of that competition.*[534]

Facebook's collection and combination of users' personal data in violation of the GDPR is considered a method 'different from those governing normal competition' which has the effect of hindering the competition on the markets for privacy-friendly social networks and

[531] Wouter P.J. Wils, 'The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the Facebook Decision of the Bundeskartellamt' (2019) King's College London Law School Research Paper Forthcoming, 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3424592> accessed 29 September 2021; Botta, Wiedemann (n 345) 441.
[532] Giuseppe Colangelo, Mariateresa Maggiolino, 'Antitrust Über Alles. Whither Competition Law after Facebook?' (2019), 15 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362428> accessed 2 June 2021.
[533] Renato Nazzini, 'Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision' (2019) Competition Policy International, 5.
[534] Case C-209/10 *Post Danmark A/S v. Konkurrencerådet* [2012] ECLI:EU:C:2012:172, para 24.

for advertising, to the detriment of consumers.[535] As a result, the BKA has been criticised because it did not focus on the foreclosure effect of Facebook conduct as an autonomous abusive conduct, but it used it to substantiate the thesis of the exploitative abuse derived from users' loss of control on their data.[536]

However, to apply such provisions the BKA should have demonstrated that Facebook competitors collect less personal data from their users to provide the same service, or that Facebook is able to do that only because of its dominant position, while any non-dominant firm could have done the same. The same goes for the exclusionary abuse, in which the BKA should have proved that other firms could not gather the same amount of personal data as Facebook because of Facebook's conduct, which is not the case, given that any firm is potentially able to track users on the Internet regardless of Facebook's conduct.

Therefore, the BKA applied national law because it provided the necessary tools to address an abusive conduct that could only be difficultly addressed under EU law, under which, in any event, there is no such approach as the one developed by the FCJ and under which data protection law cannot be used as a benchmark to assess a violation of competition law.[537] The decision to rely on national law is completely in line with Article 3(2) of Regulation 1/2003, according to which Member States are not precluded from adopting or applying stricter national provisions in their territory in order to prevent or punish unilateral actions by undertakings.

As for the alleged improper use of data protection law, since the BKA found that Facebook's privacy policies amounted to an exploitative abuse as they violated GDPR requirements for valid consent, it has been pointed out that following this approach any violation of data protection law could amount to a violation of competition law. Taking this reasoning to the extreme, some scholars have even argued that any violation of the law by a dominant undertaking may have as a result to give it an unjust edge over its competitors and thus amount to a violation of competition law. Thus, by following the BKA's approach, competition authorities risk becoming an 'all-purpose enforcement institutions' and competition law a gap-filler for the shortcomings of other fields of law.[538]

[535] Mario Midiri, 'Le Piattaforme e il Potere dei Dati (Facebook non passa il Reno)" (2021) 2 Il Diritto dell'Informazione e dell'Informatica, 125.
[536] Nazzini (n 533) 5.
[537] Buiten (n 5) 8, under reference to Case C-238/05 *Asnef-Equifax* [2006] ECLI:EU:C:2006:734, para 63; *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision of 3 October 2014, para 164.
[538] Buiten (n 5) 13; Thomas Höppner, Philipp Westerhof, 'Abrupt End to "Hipster Antitrust"? Tackling Facebook's Expansion Following the First Court Ruling in Germany' (2019) Hausfeld Competition Bulletin, 5.

These critics mainly stem from an erroneous reading of the context surrounding the BKA decision and from a superficial analysis of the approach followed by the BKA. First of all, it is clear that not any violation of data protection law could result in an abuse of dominant position. It can be argued that only the provisions of the GDPR regulating the relationship between a data controller and a data subject can fit in the analysis undertaken by the BKA. Under Article 19 (1) GWB, as interpreted by the FCJ, only provisions regulating 'unbalanced negotiations' can be considered as a benchmark to assess abusive behaviours.[539] Therefore the relevant data protection provisions can only be those regulating and protecting the bargaining power of data subjects in terms of their right to self-determination. Furthermore, the violation of these provisions has to take place 'as a manifestation market power or a great superiority of power.'[540] As a consequence, the approach of the BKA can be applied only when these two requirements are met, namely, when in the context of a contractual negotiation, (i) the user's position is not in line with the safe environment created by the legislative framework that it was meant to restore the balance in unbalanced negotiations; and when (ii) the individual is prevented from doing so because, due to the dominant position of the counterparty, no meaningful alternatives are available.

Secondly, it is not even clear why some argue that the BKA decision would be 'rooted in the idea that virtually *every legal infringement* by a dominant firm could amount to an antitrust violation'[541] or why the BKA's approach should be potentially applicable to '*all* sorts of features [that] are "essential for the market position" of firms.'[542] In fact this is obviously not the case.

These positions unjustly widen the scope of application of the BKA's approach as they overlook that, in any case, (i) the conduct has to breach the balance restored by the law in unbalanced negotiations; and that (ii) the foreclosure effect and the following unjust competitive edge referred to by the BKA are only the last part of the reasoning, in which the BKA is assessing the *outcome* of the abuse. In fact, the BKA stated that there has to be a normative or an outcome link between 'the norm addressee status' and 'the infringement'.[543]

---

[539] Bundeskartellamt (n 473) [526].
[540] Ibid [872].
[541] Colangelo, Maggiolino (n 532) 13.
[542] Geoffrey Manne, 'Doing double damage: The German competition authority's Facebook decision manages to undermine both antitrust and data protection law' (*Truth on the Market*, 8 February 2019) <https://truthonthemarket.com/2019/02/08/doing-double-damage-bundeskartellamt-facebook/> accessed 24 October 2021.
[543] '*It is sufficient to determine that the two aspects are linked by a causality which is either based on normative aspects or the outcome. Both aspects can be assumed to be fulfilled in this case'* in Bundeskartellamt, Case B6-22/16, Case Summary (2019), 11.

As a consequence, the foreclosure effect alone is not enough for a conduct to be addressed under Article 19 (1) GWB, but it has to be the consequence of the violation of laws aiming at restoring the balance between parties with different levels of bargain power so to protect the right to self-determination of the weaker party. For example, a breach of the rules governing companies' environmental obligations would not be punishable under the BKA's approach, although it is likely to give a competitive advantage to the responsible company. The same would apply in the case of tax evasion or in the case of violation of any other discipline not intended to protect the freedom of self-determination of a weaker contracting party.

Against this backdrop, also the claim that competition law risks becoming a 'gap-filler' for the shortcomings in other fields of law does not stand. The BKA has detected a violation of Article 19 (1) GWB whose required elements happen to be linked to data protection law.[544] Such a result is not surprising if one thinks about the strong interlink between competition and the collection and use of data in digital markets. Also, this provision has always been interpreted as an instrument to protect consumers.[545] As correctly affirmed by Botta and Wiedemann, in markets as the one populated by digital platforms, which are characterised by heavy intersections of different fields of law, antitrust authorities should be free to address conducts which harm competition even if the same conduct could be relevant under other fields of law.[546]

In this way the BKA correctly addressed the challenges posed by the platform economy, in which the shift from price to data had the consequence of paralysing the enforcement of antitrust law to the detriment of the competitive process.

The BKA explored the boundaries of competition law in order to find a remedy to address dynamics which are detrimental for the competitive process and, as a result, to end users and for democracy.[547] If we think that the goal of competition law, as it was born in Germany, was to ensure that no man or undertaking could live above the law, it is clear that with the Facebook case the BKA got back on track.

Finally, even if the BKA's decision will be overruled in the end, the abusive conduct it addressed, as well as the normative causal link, are now explicitly recognised as such/adopted by the new Section 19a GWB and by the DMA. This is a further demonstration that the BKA

[544] A similar reasoning is developed by Schneider with reference to the need to rely on disciplines other than competition law to give substance to the concept of unfairness in the context of 'unfair trading conditions' under Article 102 TFEU, in Schneider (n 393) 216-217.
[545] Bundeskartellamt (n 473) [525].
[546] Botta, Wiedemann (n 345) 439.
[547] Rupprecht Podszun, 'After Facebook: What to Expect from Germany' (2019) 10 Journal of European Competition Law & Practice 69, 69; Schneider (n 393) 214.

decision was a suitable approach to address the market failures typical of the digital economy, which it was also subsequently embraced at legislative level.

5. Effectiveness

After having explained why Facebook abused its dominant position in the German market for social network, the BKA prohibits Facebook from combining users' personal data collected from its services and third parties websites without users' valid consent.

As a consequence, the BKA ordered Facebook to give users residing in Germany the opportunity to choose to use the Facebook.com service without having their personal data combined with data gathered from other Facebook-owned services or from third party websites. In this way, the BKA ordered the internal unbundling of data, thus forcing Facebook to provide different levels of privacy for the same service. To comply with this order, Facebook will have to provide at least three different options, from the most privacy-friendly to the most privacy-invasive: one in which personal data are gathered and processed only in the context of the social network Facebook.com; one in which users personal data are combined across the different products of Facebook, namely, Facebook.com, Instagram, WhatsApp, Oculus, Masquerade; one in which users' personal data are combined also with data gathered from third party websites.

It has been argued that even if this remedy increases the choices available to users, it is not enough to address the issues causing the market failures typical of digital markets, namely, the lack of meaningful competition and the information asymmetry between consumers and firms.[548] For instance, Kerber and Zonla argue that relying on the need of obtaining the 'valid consent' from users is not as effective as it would have been the utter prohibition of the bundling of data to address the superior data advantage of Facebook: users can still be nudged to give consent.[549]

Furthermore, it has been suggested that the BKA decision will have the result of strengthening the dominant position of Facebook, as it will help the company retaining and/or

[548] '*It is, however, still an open question whether this remedy offers sufficient choice options, e.g., for protecting the constitutionally protected right of privacy and informational self-determination. However the main problem of this remedy of granting a choice is that we still have the additional information and behavioral market failure problem, which is not solved by this remedy. If many users of the Facebook services do not understand the impact of this additional consent, also due to intransparency and unawareness of the large amount of collected data through third-party websites, online-tracking, and other sources, then they can be in a similar way overwhelmed by this additional option as they are in many other situations where they face "notice and consent" solutions.*' in Kerber, Zolna (n 362) 26.
[549] Ibid 25.

acquiring those users more concerned about their privacy who did not use the service due to the lack of more privacy-friendly versions of it.[550]

However, the imposition of such a remedy will surely draw more attention and encourage more critical thinking than the imposition of yet another sanction.[551] As explained in previous sections, one of the problems at the basis of information asymmetries and the lack of competition is the concealed data practices which are typical of data-centric business models. Following the implementation of the remedy imposed by the BKA, Facebook.com's users will be presented with a choice and with something different from what they have been experiencing until that moment. This could be a chance for users to try and appreciate more privacy-friendly services and to start asking for them increasingly often.

Furthermore, as explained before, even if there is a chance that this remedy is going to further entrench the dominant position of Facebook, the remedy of internal unbundling would give a chance also to smaller competitors to offer more privacy enhancing services and to stop the so-called "race to the bottom" led by dominant businesses when it comes to the preservation of users' privacy.

The BKA's decision is useful also because it addressed another problem typical of data-centric businesses, which is the internal free-for-all approach according to which data processing and transfers between companies of the same group take place with much less safeguards and tends to be less subject to authorities' scrutiny than external transfers.[552] As we have seen in previous sections, this is another phenomenon causing market concentration. By ordering the internal unbundling of data, the BKA has made Facebook 'less attractive for advertisers'.[553]

In conclusion, the adoption of a behavioural remedy rather than the adoption of a fine is a suitable solution to properly address both information asymmetries and the lack of meaningful competition in the social network market and possibly, of digital markets in general. In particular, the BKA's decision gives an alternative approach to effectively address the market failures typical of digital markets, which were not properly being dealt with through the traditional separate enforcement of data protection law and competition law.[554] The BKA has found an innovative solution to new challenges brought with the platform economy which due

[550] Carsten Koenig, 'Exploit to Exclude: Federal Court of Justice Considers Facebook's Data Policy to Violate Competition Law' (2020) 4 European Competition & Regulatory Law Review 294, 298.
[551] Christoph Becher, 'Germany: A Closer Look at the BKA's Facebook Decision' (2019) 3 European Competition and Regulatory Law Review 116, 121.
[552] Geradin, Karanikioti, Katsifis (n 275) 26.
[553] Colangelo, Maggiolino (n 532) 4.
[554] Kerber, Zolna (n 362) 2-3.

to the prominent role of data and the zero price policy inevitably mixes consumer law, data protection law and competition law and inevitably requires a more integrated enforcement approach.

CHAPTER V

THE *AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO* DECISION

1. Introduction

In this chapter, I will first provide a summary of the decisions issued by the *Autorità Garante della Concorrenza e del Mercato,* the Administrative Regional Court in Rome and the *Consiglio di Stato*. Afterwards, I will present the legal context in which the AGCM decision was adopted so to allow a more in dept analysis of its approach and of its effectiveness and further consequences.

2. An Overview

On November 29, 2018, the AGCM fined Facebook for the violation of articles 21, 22, 24, 25 of the Italian Consumer Code[555] ("ICC"). According to the AGCM, Facebook has engaged in two unfair commercial practices: (i) claiming that the Facebook.com service "it's free and always will be" without providing clear information about how user's data is going to be used for commercial purposes thus misleading consumers and causing them to make transactional decisions they would not otherwise have made (*i.e.*, signing in to the Facebook service, or continuing using it), in violation of articles 21 and 22 ICC ("commercial practice A"); (ii) registered users were subject to undue pressure by Facebook with regard to the extent to which their data were shared between Facebook and third parties, in violation of articles 24 and 25 ICC. In particular, the default setting allowed the wider data sharing between Facebook and third parties thanks to a pre-selected box. In addition, if the user tried to change this setting, it would have faced a message warning that serious limitation of the services offered by both Facebook and third parties might have followed ("commercial practice B").

According to the AGCM, the conducts addressed with its decision are relevant under consumer protection law because of the economic exploitation of users' data carried out by Facebook. In fact, precisely because of the economic value of consumers' personal data, their

[555] AGCM, decision No. 27432 of 2018.

provision can be considered a form of counter performance for the social network service. As a result, consumer protection law is applicable even if no monetary price is paid by consumers.

As a consequence, the AGCM affirms its competence to address conducts which, according to Facebook should be addressed under data protection law, not only because the economic value of data implies that the choices linked to the registration or use of the social network are economic choices, but also because the applicability of data protection law does not exclude the applicability of consumer law to conducts which fall within its field of application.

As a result, the AGCM imposed a fine of five million for each of the abusive conduct, for a total of ten million, and due to the significant effects of the censured practices on consumers, required the publication of a corrective statement on the Facebook.com website and application.[556]

2.1. The T.A.R. Lazio's Judgment(s)

Facebook appealed the AGCM decision before the T.A.R. of Lazio (which is the regional administrative court before which AGCM's decisions can be appealed) and based the appeal on several grounds, among which the most interesting for the subject matter of this thesis are: (i) the AGCM lacked competence to adopt the at-issue decision as the conduct under scrutiny cannot be qualified as a commercial practice due to lack of any monetary consideration required from the consumer (and as a result, lack of any economic interest to be protected), and in any event, (ii) the AGCM ruled on a subject matter covered by data protection law; (iii) the AGCM applied the law in violation of the principle of legality as established by Article 7 of the European Convention on Human Rights ("ECHR") and Article 25 of the Italian Constitution.

[556] The corrective statement is attached to the decision and reads as follows: "*Facebook Inc. and Facebook Ireland Ltd. did not adequately and immediately inform consumers, when activating their accounts, of the collection of the data provided by them for commercial purposes. In this way, they induced consumers to register on the Facebook platform, also emphasising the fact that the service was free of charge. In addition, they have unduly influenced registered consumers, who are subjected, without their prior and explicit consent, to the transmission and use of their data by Facebook and third parties for commercial purposes. The undue influence arises from Facebook's pre-selection of the options on the consent to the transmission of their data to and from third parties, in particular by automatically activating the "active platform" function, together with the prospect, following the deactivation of that platform, of significant limitations on the use of the social network and third-party websites/apps, which are broader and more pervasive than those actually applied. These practices have been assessed as unfair, pursuant to Articles 21, 22, 24 and 25 of Legislative Decree no. 206/2005 (Consumer Code). The Authority has ordered the publication of this corrective statement pursuant to article 27, paragraph 8, of the Consumer Code*" (free translation from Italian).

With judgments No. 260 and 261 of 2020,[557] the T.A.R. recognised that personal data can constitute an "asset" which can be economically exploited and which, as a result, can be also a form of consideration in a contractual relationship: the "commodification" of personal data thus requires digital operators to comply with the informational duties provided by consumer law.[558]

According to the Court, personal data have a dual nature: they can be the expression of a fundamental right of the individual, but they can also be an economic resource. This dual nature justifies the applicability of both data protection law (when necessary to protect personal data as an expression of a fundamental right of the individual) and consumer law (when necessary to safeguard the economic interest of the individual).[559]

As for the relation between the two different sets of provisions, the T.A.R. concluded that data protection law and consumer law complements each other, imposing different information duties aimed, in one case, at protecting consumers' personal data as expression of a fundamental right and, in the other case, at allowing consumers to take informed economic decisions.[560]

As a consequence the AGCM approach does not risk violating the *ne bis in idem* principle: while consumer protection authorities would assess the completeness and transparency of information provided on the exploitation of data for commercial purposes, data protection authorities would rather assess the completeness and transparency of information relating to the proper processing of data in relation to the use of the platform.[561]

The Court also affirmed that, contrary to Facebook's view, the application of consumer law to the conducts under scrutiny cannot be described as an innovative approach that would violate the principle of legality. This is because both the recognition of the economic value of data and the need to protect the consumer are concepts that have been repeatedly affirmed at both European and national level. In this regard, the T.A.R. recalls a number of examples provided by the AGCM in its decision: (i) in the Commission's guidance on the

[557] The AGCM fined both Facebook Ireland and Facebook Inc., which filed two autonomous appeals before the T.A.R.; the substance of these appeals is pretty much identical, except for a further ground of appeal set forth by Facebook Inc. according to which the AGCM erroneously applied the principle of parental liability (*i.e.*, the presumption that the parent company is liable for the conduct of its subsidiaries if it can be shown to have exercised a decisive influence on their market conduct) as the Facebook service is provided to European users by Facebook Ireland only. However, with judgment No. 261 of 2020, the T.A.R. upheld the AGCM decision as, according to the Court, Facebook Inc. not only benefited financially from Facebook Ireland's conduct, but was also responsible for its own conduct in that it did not ensure that the subsidiary acted in compliance with the law (so-called *culpa in vigilando*).
[558] T.A.R. Lazio, Roma, n. 260 of 2020, para 6; T.A.R. Lazio, Roma, n. 261 of 2020, para 6.
[559] Ibid.
[560] Ibid [8].
[561] Ibid [9].

implementation of Directive 2005/29/EC on unfair commercial practices,[562] the Commission affirmed that users' personal data and in general user-generated content have economic value; (ii) the AGCM already recognised the economic value of consumers' personal data, as well as the applicability of consumer law to digital services not requiring monetary payment for their use in the WhatsApp decision;[563] (iii) the European Commission recognised the economic value of users' personal data in the Facebook/WhatsApp merger decision;[564] (iv) the Consumer Protection Cooperation Network affirmed that Directive 93/13/ECC is applicable to all contracts concluded between consumers and professionals, including those in which the collection of the consumers' personal data represents the consideration.[565]

As for the first conduct sanctioned by the AGCM, Commercial Practice A, the Court upholds the AGCM position, concluding that the economic value of users' data requires the trader to inform the consumer of the commercial purposes pursued through their use: in the absence of adequate information, or in the case of misleading statements, the practice put in place can therefore be qualified as misleading.[566]

As for the second conduct sanctioned by the AGCM, Commercial Practice B, according to which registered users were subject to an undue pressure to keep the wider data transfer between Facebook and third parties, the T.A.R. affirmed that the AGCM's reconstruction of the way the transfer should take place was erroneous and as a result, so was the application of the law. The Court stated that, according to the exhibits submitted by Facebook, the transfer of data takes place only after several further passages in which the user is required to give his/her consent to the transfer, pre-selection allowing potentially the sharing of data between Facebook and third parties not being a sufficient condition for the transfer to take place automatically.

---

[562] European Commission, 'Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices' (2016) available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0163&from=IT, where the Commission points out that "*Personal data, consumer preferences and other user generated content, have a "de facto" economic value and are being sold to third parties. Consequently, under Article 7(2) and No 22 of Annex I UCPD if the trader does not inform a consumer that the data he is required to provide to the trader in order to access the service will be used for commercial purposes, this could be considered a misleading omission of material information. Depending on the circumstances, this could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data*".

[563] AGCM, decision No. 26597 of May 11, 2017, which I will analyse in further details in the following sections.

[564] European Commission, Case M.7217 – Facebook/ WhatsApp (2014).

[565] T.A.R. Lazio (n 569) [7].

[566] Ibid [10].

In addition, according to the Court, the warning to users on the diminished functionality of Facebook's and third parties' services in case of deselection is not qualifiable as an aggressive practice, as there are indeed negative consequences in the event of deactivation.

The Court points out that, in any event,

> *any dispute as to whether the processing of user data is irrelevant or excessive in relation to the purpose of the processing itself would fall within the competence of the Data Protection Authority, since these profiles do not affect the freedom of choice of the consumer.*[567]

As a consequence, the T.A.R. overturns the AGCM measure in so far as it fines the conduct at issue and consequently reduces the total amount of the fine to five million.

In these evaluations, the T.A.R. seems to adopt the "average consumer" benchmark[568] (or maybe more properly, an average user benchmark): a consumer who takes its decisions being aware of the consequences in terms of profiling and not being influenced by warnings about a decrease in the functionality of the service (an approach which has been criticized for being too distant from reality).[569]

2.2. The *Consiglio di Stato* decisions

Both the AGCM and Facebook appealed the T.A.R. decisions before the *Consiglio di Stato* ("CDS" – which is the court of last instance in the administrative justice).

According to the AGCM, the T.A.R. failed to consider that not only the Commercial Practice B was aggressive because of the default wider users' data sharing, but also and most importantly because of the opt-out mechanism repeatedly used in the following passages in which the user has to decide whether to allow the data sharing between Facebook and third parties. The AGCM points out that in this way Facebook is making the choice instead of users, thus putting them under undue pressure:

> *the user/consumer is never put in a position to make an active and direct choice, having to make an effort – <u>provided that he is able to grasp the existence of such</u>*

[567] Ibid [16].
[568] The average consumer benchmark was elaborated by the CJEU case law: in the *Gut Springenheide* judgment (Case C-210/96) the CJEU clarified that the average consumer is "*reasonably well informed and reasonably observant and circumspect*". More information on this standard and on how it is applied in Italian case law will be provided in the following sections.
[569] Mario Midiri, 'Privacy e antitrust: una risposta ordinamentale ai Tech Giants' (2020) 14 federalismi.it, 228.

> *preselection* – *to deactivate the sharing of the data that he does not wish to provide for commercial purposes and which the professional has "chosen" to share in his place.*[570] (emphasis added)

It is clear that, contrary to the T.A.R. approach, the AGCM is less inclined to apply the standard of the average consumer to the (probably most insidious) practices found in the digital environment.

Facebook reiterates, in essence, the grounds of appeal already raised before the T.A.R., also pointing out that the AGCM had wrongfully found that information about the further exploitation of consumers' data for commercial purposes were insufficient because, as allowed by data protection law (Article 12 (8) GDPR and WP29 guidelines on automated individual decision-making and profiling) Facebook provided all relevant information on different layers of the privacy notice.

The CDS rejected the appeal of both Facebook and the AGCM.[571] In particular the CDS considered that given the very broad notion of "processing" provided by Article 4 GDPR, which extends the applicability of data protection law to virtually any activity affecting personal data, it is unreasonable to assume that the applicability of data protection law excludes the applicability of other disciplines that are otherwise relevant to a specific situation, as this would lead to the exclusion of the applicability of any other legal discipline. Therefore, in cases where data processing affects situations governed by other legal sources protecting different legal interests, the applicability of data protection law does not exclude the applicability of these other relevant laws. In the present case, contrary to Facebook's assertion, even if the conduct sanctioned by the authority may be relevant from the perspective of data protection law, this does not exclude the applicability of consumer law.[572]

Furthermore, the CDS confirmed that, contrary to Facebook's view, data protection law and consumer law have different scopes of operation, with non-overlapping sanctioning regimes: the former concerns the violation of the rules on the processing of personal data and the latter, the conditioning of the awareness of the user. In the at-issue case, only the latter is relevant, since the user is not previously and adequately informed that in order to obtain the benefits described as free of charge, he has to give up personal data that will not be used

[570] *Consiglio di Stato*, judgment of March 29, 2021, No. 2631, para 5, explaining AGCM's grounds of appeal.
[571] Even in this case, Facebook Inc. and Facebook Ireland filed two autonomous appeals before the CDS, which were both rejected in judgments of March 29, 2021, No. 2630 and No. 2631. As these two decisions follow an identical reasoning, for ease of reference I will refer only to judgment No. 2631.
[572] *Consiglio di Stato* (n 570) [8].

exclusively to obtain the services to which he aspires, but will constitute a profiling tool for commercial purposes. The CDS recognised that the provision of users' personal data represents consideration for the service, which cannot therefore be regarded as free of charge.[573]

In this context, the CDS affirmed that the conduct has the elements of a misleading commercial practice in that, at the time of registration (which must be considered to be an economic choice of the user), Facebook did not provide sufficient information for the user to make an informed decision, also in view of the failure to make a clear distinction between the functional use of the users' personal data (necessary for the provision of the service) and the use of such data for advertising purposes.[574]

In particular, the CDS pointed out that:

> *In the face of the promise of a free service, the user was induced to access it in order to obtain the 'immaterial' advantages of joining and being involved in a social network following registration on the platform by making available his personal data, which were thus involved in profiling for commercial purposes without the user having been effectively informed of the exact scope of such use, which could only be interrupted, with revocation of consent, at a later date [...] and in the face of a comprehensive indication of the disadvantages that would ensue.*[575]

As for the AGCM's ground of appeal, the CDS confirmed the findings of the court of first instance, holding that AGCM's factual reconstruction of the mechanism by which Facebook would transfer data to third parties is contradictory and thus precludes the demonstration that such mechanism actually impedes users from making a free choice.[576]

2.3. The AGCM's Non-compliance Proceeding against Facebook

On February 9, 2021 the AGCM imposed another sanction of seven million on Facebook for failure to comply with the order to terminate the misleading practice and to publish on the

[573] Ibid [9].
[574] Ibid [10].
[575] Ibid.
[576] Ibid [15].

social network website and app the corrective statement attached to the decision of November 29, 2018, as modified following the T.A.R. rulings.[577]

In particular, the AGCM sustained that even if the claim "it's free and always will be" had been removed from the home page of the social network, Facebook still did not provide sufficient information about the commercial use of consumers' personal data at the time of creation of a new account, thus still perpetrating the conduct that the AGCM had prohibited. According to the Authority, the presence of a link to the terms and privacy policy of the service near the "sign in" button was irrelevant and not sufficient to remedy the at-issue conduct, as information related to the consideration due in exchange of a service is essential for the consumer to take an informed decision and must be provided in a clear manner and in conjunction with the sign in button.[578]

As a result, Facebook added this phrase above the sign in button "*Finanziamo i nostri servizi utilizzando i tuoi dati personali per mostrarti inserzioni*"[579] as showed in Figure 7, and on April 8, 2021 published the corrective statement on the social network website and app.[580]

Figure 7 Screenshot from the sign in form of Facebook.com, emphasis added.

[577] AGCM, decision No. 28562 of February 9, 2021.
[578] Ibid [37-38].
[579] "*We finance our services by using your personal data to show you advertisements*" (free translation from Italian).
[580] Gustavo Olivieri, 'Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali', Orizzonti del Diritto Commerciale, 366.

3. The AGCM decision

In the following sections, I will present the AGCM decision in more details, providing the legal framework on which the AGCM relied upon to adopt its decision, as well its previous and following decisions from which is possible to observe a consolidated approach. Finally, I will assess the effectiveness of the AGCM approach.

3.1. Legislative framework

According to the AGCM, Facebook's conduct with regard to the lack of information about the economic exploitation of consumers' data would constitute a misleading commercial practice, in breach of articles 21 and 22 ICC, while the opt-out mechanism with regard to the sharing of users' data between Facebook and third parties would constitute an aggressive commercial practice, in breach of articles 24 and 25 ICC.

The Articles from 18 to 27 of the ICC were modified by Legislative Decree No. 146 of 2007, implementing Directive 2005/29/CE on unfair commercial practices ("UCPD") in the Italian legislative framework. The legislative framework on commercial practices applies to unfair commercial practices between professionals and consumers before, during and after a commercial activity relating to a product.[581]

In this context, "commercial practice" means any act, omission, conduct or representation, commercial communication including the advertising and marketing of the product, by a trader in relation to the promotion, sale or supply of a product to consumers.[582]

A commercial practice is unfair when it is (i) contrary to professional diligence and (ii) it is likely to distort to an appreciable extent the economic behaviour of the average consumer.[583] In order to have an unfair practice it is not necessary that such practice actually distorts consumer behaviour, but it suffices that it is likely to produce such a result.

Like the UCPD, the ICC also divides unfair commercial practices into two macro categories: misleading commercial practices and aggressive commercial practices.

A commercial practice is misleading when it misleads or is likely to mislead the average consumer (i) through false or misleading information[584] or (ii) through the omission of essential information which the consumer needs to make an informed choice.[585]

[581] Article 19 ICC.
[582] Article 18 (1)(d) ICC.
[583] Article 20 ICC.
[584] Article 21 ICC.

A commercial practice is aggressive when it restricts or is likely to considerably restrict the average consumer's freedom of choice or behaviour in relation to a given product, including through the use of violence, coercion or undue influence.[586]

Although AGCM's decision is based on Italian law, the ICC provisions taken into account in that decision reproduce almost identically the UCPD provisions, respectively Articles 6 and 7 for misleading practices and Articles 8 and 9 for aggressive practices. Therefore, AGCM's approach could well be replicated outside the Italian borders and in other Member States, also depending on the "average consumer" benchmark adopted by national courts.

In fact, a relevant role in the definition of the scope of applicability of the UCPD, and consumer protection law more in general, is played by the identification of the average consumer, which has been usually defined as 'reasonably well informed and reasonably observant and circumspect' by the CJEU case law (for instance in Case C-303/97 *Sektkellerei Kessler*,[587] Case C-220/98 *Lifting*).[588] This standard was subsequently transposed in recital 18 of Directive 2005/29/EC on unfair commercial practices (which was implemented in the Italian Consumer Code through, *inter alia*, articles 20, 21, 22, 24, 25). In this way, it is assumed that the average consumer is a rational decision maker, meaning that he is expected to favour logic and analysis over subjectivity when making choices between alternative goods.

The average consumer standard was primarily elaborated by the CJEU to challenge Member States' consumer law, that was considered overprotective and therefore an obstacle to the smooth functioning of the Single Market. In fact, by imposing a certain level of responsibility on the consumer for his economic choices, the CJEU established a balance between clashing interests, those held by consumers on one side, and the free movement of goods, on the other.

The assumption that the average consumer is a rational decision maker is in line with the "information paradigm" that informs the consumer protection policy of the European Union and with the "labelling doctrine" elaborated in the case-law of the CJEU (for instance in Case C-51/94, *Commission v Germany*,[589] and Case C-120/78, *Cassis de Dijon*).[590] According to

---

[585] Article 22 ICC.
[586] Article 24 ICC.
[587] Case C-303/97, *Verbraucherschutzverein eV v Sektkellerei G.C. Kessler GmbH und Co*. [1999] ECLI:EU:C:1999:35.
[588] Case C-220/98, *Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH* [2000] ECLI:EU:C:2000:8.
[589] Case C-51/94, *Commission of the European Communities v Federal Republic of Germany* [1995] ECLI:EU:C:1995:352.
[590] Case C-120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* [1979] ECLI:EU:C:1979:42.

the information paradigm the consumer is sufficiently protected when he has been provided with all the information needed to take an informed decision. This approach is evident when looking at the numerous provisions in the Secondary EU law providing duties of information in many different sectors.

However, the benchmark elaborated by the CJEU case law is generally perceived to be too distant from reality, in which consumers usually are not such rational decision-makers, especially in the online world.[591]

As for Italian administrative courts, they tend to adopt an average consumer benchmark adapted to the context of a given practice, rather than a single standard applicable in all circumstances, which takes into account the information asymmetry and the difficulty a consumer may encounter with respect to services/economic sectors whose mechanisms are likely to be beyond his/her understanding[592] (such as consumer credit,[593] telecommunications[594] or sectors with a high degree of technological development).[595] Italian administrative courts, in fact, do not pretend the consumer to behave rationally or to critically evaluate the information a trader provides. On the contrary, a great deal of responsibility is

[591] Alessandra Cervone, 'Unfair Contract Terms and Sharing of Data with Facebook, Towards a Better Protection of Social Media Users: The WhatsApp Cases' (2017) 2 Rivista Italiana di Antitrust, 214.
[592] Bram B. Duivenvoorde, *The Consumer Benchmarks in the Unfair Commercial Practices Directive* (Springer 2015), 135-136.
[593] T.A.R. Lazio, Sez. I, 19 May 2010, No. 12364, in which the Court affirms that "*In the appeal, the idea seems to be that, since consumer credit is now an extremely widespread experience among the public, the asymmetry of information in this area that is known to exist has been eroded, overlooking, however, that the sector in question is in fact characterised by the offer of increasingly refined and complex products, as well as involving a very large number of potential consumers, within which a high and widespread degree of information cannot reasonably be expected. The reference to the model of the average consumer, when placed in relation to the peculiarities of the sector in question, does not exclude, therefore, that adequate protection must also be ensured to less knowledgeable consumers, since presumably, they are precisely the "average" users of the services covered by the practice*" (free translation from Italian.
[594] T.A.R. Lazio, Sez. I, 29 March 2010, No. 4931, where the Court affirmed that: "*The identification of such a model [...] cannot be the result of an assessment carried out in merely statistical or empirical terms, since social, cultural and economic factors must be taken into consideration, among which, in particular, the economic and market context in which the consumer finds himself acting must be analysed. From this point of view, it cannot be denied that the sector in question is not only extremely complex and characterised by a continuous technological evolution (so much so as to require frequent interventions by the Autorithy for the Guarantees in Communications, in order to safeguard the competition between operators and users' rights), but above all it 'impacts' on a very large number of potential consumers, within which a high and widespread degree of information is not reasonably predictable"* (free translation from Italian).
[595] T.A.R. Lazio, Sez. I, 9 September 2015, No. 11122, where the Court affirmed that: "*The qualification of the average consumer must also be related to the context in which the messages are disseminated, and to the type of product. Therefore, particularly in sectors with a high level of technological evolution and in the context of new and diversified services, consumers may not be equipped with the specific skills needed to detect and deal with the existence of risks connected with their use*" (freee translation from Italian).

placed on traders who are required to always provide clear and complete information, especially in sectors characterised by strong information asymmetry.[596]

3.2. On the AGCM Competence

The Authority addresses the question of its competence to assess the practices at issue, in response to the objection of lack of competence raised by Facebook during the investigation on the grounds of possible overlaps with data protection law.

According to AGCM, the fact that the conduct examined is also relevant in relation to data protection law does not exempt Facebook from complying with other legislative provisions which are in any event relevant to its conduct. In the present case, therefore, the potential relevance of the conduct from a data protection point of view does not exclude the applicability of the consumer protection law. This is further confirmed by the different interests protected by the two areas of law: while data protection law aims to ensure the proper processing of personal data as the expression of an inalienable right of the individual, the provisions prohibiting unfair commercial practices aim to ensure the freedom of choice of the consumer.[597]

The Authority states that although both conducts assessed in the decision concern the collection and transfer of users' data, they were assessed from the point of view of their impact on users' economic choices. Moreover, such conducts are not taken into consideration, let alone prohibited, by any legislation on the protection of personal data applicable in Italy (namely, Legislative Decree No. 196 of 2003, the "Privacy Code", and the GDPR).[598]

Therefore, even if the practices in question were privacy-compliant, this would not exclude their potential to constitute a breach of consumer protection law. For this reason, Facebook's allegations that the Irish DPA considered that the practices sanctioned in the decision were GDPR-compliant are deemed to be completely irrelevant by the AGCM.[599]

[596] Duivenvoorde (n 592), 138. *See ex multis* Consiglio di Stato, Sez. VI, 19 September 2017, No. 4378; Consiglio di Stato, sez. VI, 17 February 2012, No. 853; Consiglio di Stato, sez. VI, 22 June 2011, No. 3763; T.A.R. Lazio, sez. I, 24 September 2021, No. 9903; T.A.R. Lazio, sez. I, 08 November 2021, No. 11419.
[597] AGCM, decision No. 27432 of 2018, paras 45-46.
[598] Ibid [47].
[599] Ibid [48].

3.3. On the Applicability of the Consumer Code to Facebook's Practices

According to the AGCM, the ICC is applicable to the conduct at issue as users' data acquire an economic value so long as they are used for commercial purposes (in the Facebook case, for marketing purposes). The economic value of users' data is what triggers applicability of the ICC to the relationship between Facebook and its users, even if no monetary compensation is required for the provision of the social network service. This economic value is enough to qualify the choices made by consumers as "economic choices".[600]

3.4. Commercial Practice A

According to the AGCM Facebook did not provide enough information about the commercial use of personal data of users at the moment of registration to the social network, thus preventing consumers from making informed decisions and even misleading them because of the claim "it's free and always will be" found near the registration form, as highlighted in Figure 8.

[600] For an analysis of the economic value of personal data, see Antonio Leo Tarasco, Michele Giaccaglia, 'Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo' (2020) 2 Il diritto dell'economia.

Figure 8 Facebook's registration form at the time of AGCM investigation.

In particular, this exaltation of the free nature of the service was not accompanied by any information on the economic exploitation of the user's data, which, by virtue of their economic value, represented the counter-performance demanded in exchange for the provision of the service. Therefore, while the statement on the gratuity of the service was highlighted, the information on the economic exploitation of the user's data was included only in the conditions of use and in the privacy and cookies policies, accessible through hyperlinks placed right above the button "create account" (which, according to the Authority, are documents whose consultation is merely possible before registration), together with numerous other pieces of information and, moreover, written in a complicated and too technical language for consumers to fully understand their meaning.[601]

As a result, the AGCM concluded that Facebook misled consumers-users to register on the platform by failing to inform them clearly and immediately upon registration of the remunerative purposes underlying the provision of the service.

[601] AGCM, decision No. 27432 of 2018, paras 18-19.

3.5. Commercial Practice B

According to the AGCM, Facebook allegedly exerted undue pressure on its users by means of pre-setting consent for the integration between the social network and third-party websites and apps, whereby user data are transmitted from the platform to third parties and *vice versa* without the prior express consent of users. That coercion is further aggravated by the penalising consequences which Facebook envisaged for the user upon deactivating the integration (in the form of diminished efficiency and restricted accessibility to the social network, as well as to third parties services).[602]

In particular, the setting through which the data exchange between Facebook and third parties would take place was active by default, and users had the possibility to reverse the choice already made by Facebook by clicking on the "modify" option and accessing a further informative page. In this page, before the "deactivate" button, however, a number of negative effects that would result from deactivation were reported,[603] which according to the AGCM, would be exacerbated in order to induce the user to keep the integration active.[604]

Moreover, according to the AGCM, there was a concrete possibility that users could never realise that the integration had been enabled and that she/he was entitled to make a choice other than the one made, without her/his knowledge and on her/his behalf, by Facebook, given the absence of any warning of that fact upon registration or when surfing on the social network.[605]

Due to this opt-out mechanism, there would be also a lock-in effect to the detriment of registered users, which may increase over time. In fact, users may only realise after a long time that Facebook.com had been integrated with a significant number of third-party websites, apps and games and would be prevented from deactivating the integration because of the

---

[602] Ibid [5].
[603] At para 23 the AGCM reports the list of such negative effects, which consisted in: "*If you deactivate the apps on the Platform:*
- You will not be able to access websites or apps using Facebook.
- You will not be able to access games or mobile apps using Facebook.
- Your friends will not be able to interact with you and share items using apps and websites.
- Instant personalisation will also be disabled.
- Apps you have previously installed may still have information you have shared with them. Contact these apps for information on how to remove this data.
- Apps that you have signed in to (via Facebook or anonymously) will be removed.
- App posts will be removed from your profile" (translated from Italian).
[604] Ibid [61].
[605] Ibid [59].

significant limitations envisaged, including the risk of losing data generated during the use of various websites, apps and games.[606]

As regards the functioning of this mechanism, the activation of the integration would allow Facebook to decide autonomously which data (both strictly necessary and not) to share with third parties when accessing third parties' websites/apps via the Facebook login. Through a further opt-out mechanism, the user would have to prohibit the sharing of data that are not essential to use the service and which Facebook, however, according to its own proportionality judgment, had decided to share with third parties. According to the AGCM, in that way Facebook would not allow the user to make choices on his own initiative but only to de-select the choices already made by Facebook.[607]

With specific reference to third-party games accessible through the social network, even if the user were to deselect the data that she/he did not intend to share with third parties, the user would be required to deselect them at every log-in because at each new navigation Facebook would reset the default settings as if consent had been given to the transfer of all the data it had selected according to its own proportionality assessment.[608]

Furthermore, according to the AGCM, the default activation of the integration would allow a general authorisation to the sharing of users' data, even if users did not use any of the Facebook plug-ins or the Facebook login service.[609]

Finally, the AGCM also noted that in addition to pre-activating the integration, Facebook also pre-set the choice available to the user regarding advertisements, pre-selecting the user's consent to view the advertisements "profiled" according to her/his online interests.[610]

The at-issue practice is thus deemed to be aggressive by the AGCM, as it would allow Facebook to exercise an undue pressure on its users, making them choosing to allow the sharing of their data between Facebook and third parties.

4. The AGCM Approach

In a nutshell, the AGCM has adopted an approach according to which also those practices that could be addressed from a data protection standpoint are considered "commercial

[606] Ibid [62].
[607] Ibid [27].
[608] Ibid [29].
[609] Ibid [30].
[610] Ibid [32].

practices" under consumer law when they are put in place between a trader-data controller and a consumer-data subject.

This approach has been adopted by the AGCM in other decisions before and after the one analysed in this thesis.

In the Samsung decision,[611] the Authority has ascertained an aggressive commercial practice linked to the collection of Samsung customers' personal data for marketing purposes. In particular, once a consumer had purchased a product subject to a promotion, Samsung required, as mandatory conditions for participating in the promotion, (i) registration on the Samsung People platform and (ii) consent to the use of consumer's personal data also for marketing purposes. According to the AGCM, it was not sufficient to inform the consumer of these further requirements only after the purchase of the product, since the consumer, who had purchased the promoted product with a view to obtaining a prize/refund/gift, could not at that point refrain from (i) providing personal data that went beyond what needed to take part to the promotion, and (ii) consenting to the processing of the same for marketing purposes.[612]

In the WhatsApp decision,[613] issued in 2017, the AGCM qualified as an aggressive commercial practice the way in which WhatsApp sought to obtain the consent of its users to the change of its terms of service, in particular with regard to the intended sharing of data with Facebook for profiling and marketing purposes.

According to the Authority, by envisaging the interruption of the service for those users who did not accept its terms, WhatsApp exerted undue influence over them by taking advantage of their position with regard to the service offered (which they probably could not do without as it was used as a substitute for regular mobile phone services).[614] The conduct appears to be even more unfair if one considers that the non-acceptance of the terms would not actually have led to the interruption of the service, and that users also had the possibility to deny data sharing between WhatsApp and Facebook. In fact, on opening the second layer of information, accessed by clicking on the link to read the terms and privacy policy, the user discovered that there was a pre-ticked box authorising WhatsApp to share its data with Facebook. Moreover, users who only realised after accepting the terms in their entirety that they could have refused consent to data sharing would have to follow a more complicated route than that proposed for initial acceptance to reverse this choice.

[611] AGCM, decision no. 26387 of January 25, 2017.
[612] Ibid [123].
[613] AGCM, decision no. 26597 of May 11, 2017.
[614] Ibid [63].

Therefore, according to the Authority, the practice in question would be aggressive because: (i) the user could have continued to use the service even without accepting the new terms (contrary to what WhatsApp had threatened); (ii) WhatsApp had pre-selected consent to the transfer of data to Facebook without the user's knowledge and (iii) the procedure to be followed to reverse this choice was more complicated than the initial one.

In this decision the AGCM addressed the issues regarding its competence, the applicability of the Consumer Code and the nature of non-monetary consideration of the data transferred by users.[615] As also argued in the decision against Facebook, the Authority stated that the applicability of data protection law to WhatsApp's conduct did not exclude its relevance also under consumer protection law.[616]

In the Telepass decision,[617] the AGCM deemed to be a misleading commercial practice the failure to inform users about the further processing for marketing purposes of the data collected to estimate the most advantageous insurance premium among those offered by a number of Telepass' partner insurance companies. In particular, according to the Authority, Telepass should have stated this clearly upon initiating the process, not being enough the mere reference to the privacy policy (in which, in any case, this further purpose was made clear).[618]

More recently, the AGCM sanctioned Apple and Google for unfair commercial practices related to the collection and processing of consumers' personal data.

In the Apple decision,[619] the AGCM considered that Apple's failure to inform its users of the commercial use of data collected through the creation of an Apple ID was misleading.[620] The AGCM also considered that the opt-out method by which Apple obtained consent to the use of user data for commercial purposes was aggressive, *i.e.* it did not provide the consumers with the possibility of making a choice regarding the transfer of their data, the possibility of acquiring which was pre-set from the stage of creation of the Apple ID.[621]

In this decision, the AGCM once again affirmed the applicability of the Consumer Code to conducts which could be relevant also under data protection law as the latter's aim is to protect personal data as an expression of a fundamental right, whereas consumer protection law aims to protect consumers from economic choices induced by misleading and aggressive

[615] Ibid [54]
[616] Ibid [50]. WhatsApp has not appealed the decision, so there are no further rulings to help define a legal stance on the matter.
[617] AGCM, decision No. 28601of March 9, 2021.
[618] Ibid [52].
[619] AGCM, decision No. 29888 of November 9, 2021.
[620] Ibid [86-87].
[621] Ibid [102-103].

practices: data protection law and the ICC therefore have a different scope of application and pursue distinct interests, while complementing each other.[622]

Finally, the same approach has been adopted in the Google decision,[623] where the Authority sanctioned identical conducts to that at issue in the Apple decision: Google's failure to inform users of the commercial use of their data upon creation of a Google account was deemed to be a misleading commercial practice;[624] while the opt-out mechanism through which the consent to such processing was collected was deemed to be an aggressive commercial practice.[625]

From the above, it is clear that the AGCM bases its competence to deal with conduct relating to the processing of consumer data on the distinction between personal data as the expression of a fundamental right and personal data as an economic asset.[626] In this way, the conditions of application of the data protection legislation (applicable in the first case) and that of consumer protection (applicable in the second) are differentiated, and a certain scope of applicability is carved out in favour of the latter with respect to conducts which would otherwise be outside its scope.[627]

It has been pointed out that the use of the term "counter-performance" rather than "price" to indicate the provision of data in exchange for the use of a digital service strikes a fair balance between two perspectives that lie at the extremes of the discussion on the qualification of data (*i.e.*, one that recognises exclusively the nature of a fundamental right and the other that recognises it as a commodity), acknowledging that the provision of data is not only part of the individual's right to freedom of self-determination, but also an economic activity whose transparency has to be ensured to guarantee free competition and preserve the social function of the market.[628]

This approach thus clearly admits that individuals may contractually dispose of their personal data, overcoming the obstacle linked to the non-availability of the right to data

[622] Ibid [64].
[623] AGCM, decision No. 29890 of November 16, 2021.
[624] Ibid [54].
[625] Ibid [63-64].
[626] Francesco Midiri, 'Proteggere i dati personali con le tutele del consumatore' (2021) 5 Giornale di diritto amministrativo, 611.
[627] Thobani describes the relationship between the data protection framework and the consumer one in a slightly different way: while the former provides a substantial regulation of the data market, establishing when a given data processing operation is lawful or not, the latter regulates how a given operation has to be carried out in terms of transparency and remedies usually guaranteed to consumers. *See* Shaira Thobani, 'Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente' (2019) 3 Rivista di diritto dei media, 146.
[628] Ilenia Maria Alagna, Niccolò Centofanti, 'La consumerizzazione della privacy tra California Consumer Privacy Act e GDPR' in *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven* (Giuffrè Francis Lefebvre 2021), 130.

protection inasmuch as it is a fundamental right.[629] However, this approach seems not to be in line with the EDPB's opinion on the matter, according to which data subjects 'cannot trade away their fundamental rights' through a contract.[630] Also the Italian DPA itself has referred the issue to the EDPB with reference to the Weople case.[631]

It is also worth citing the recently published European Commission's Guidance on the interpretation and application of the UCPD, which is in line with the AGCM's approach, and in which the Commission claims that opaque information on the processing of personal data may constitute an unfair commercial practice:

> *under Article 7(2) and No 22 of Annex I UCPD, if the trader does not inform a consumer that the data provided will be used for commercial purposes, this could be considered a* ***misleading omission of material information****, as well as a breach of transparency and other requirements under Articles 12 to 14 of the GDPR.*[632]

The Commission also discusses the fact that online products and services are often presented as "free". In this regard, the Commission sustains that a misleading commercial practice is put in place when the provider of the product/service does not inform adequately the consumer on the commercial use of the personal data collected through the product/service offered:

> *The marketing of such products as 'free' without adequately explaining to consumers how their preferences, personal data and user-generated content are*

[629] Carla Solinas, 'Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette' (2021) 2 Giurisprudenza Italiana, 324-326.
[630] EDPB, 'Guidelines 2/2019' (n 243), [54]. The EDPB has also discouraged the qualification of the provision of personal data in exchange for the fruition of a digital service/product as "counter-performace", see EDPB, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' (2017), paras 11-34.
[631] Weople is an application that acts as an intermediary between data subjects and large companies and aims to ensure that data subjects get paid for their data. In this respect, the Italian DPA asked to the EDPB to express an opinion on the admissibility of such "merchantability" of the data. Garante Privacy, 'Lettera del Presidente del Garante al Presidente dell'EDPB - Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità' (2019) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126725#ENGLISH> accessed 27 December 2021.
[632] European Commission, 'Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market' (2021), 22-23.

going to be used could be considered a misleading practice in addition to possible breaches of data protection legislation.[633]

More in general, the Commission states that when assessing the overall unfairness of a given commercial practice, it should also be taken into account whether the practice infringes data protection legislation, thus advocating for a more integrated approach between the two frameworks.[634]

Finally, even the most recent European legislation on consumer protection takes into account the provision of personal data in exchange for digital products and services, extending to such cases the guarantees usually recognised to consumers.[635]

5. Effectiveness

Overall, the AGCM approach has been praised by scholars because it adopts an innovative concept of commercial practice, which includes activities which are typically dealt with under data protection law.[636] For instance, according to Solinas, the AGCM has found a way to integrate two different legislative frameworks in a way in which individuals can benefit from a more effective protection before the ever growing exploitation of their data.[637]

It has also been pointed out that the AGCM approach refuses to deny the economic value of data and, as a result, the applicability of all the guarantees usually linked to economic

[633] Ibid 84. In this section, the Commission also brings the AGCM decision against Facebook as a practical example to illustrate this convergence between the UCPD and the GDPR.
[634] Ibid 22.
[635] For instance, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, at Recital 24 provides that: "*Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data*". Another example is Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules which, *inter alia*, by adding to it Article 3(1a), extends the applicability of Directive 2011/83/EU also to contracts between a trader and a consumer where "*the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader*".
[636] D'Ippolito (n 277) 971; Nicolo Zingales, 'Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law' (2017) 33 Computer Law & Security Review, 557.
[637] Solinas (n 629) 333.

relationships, thus avoiding an unnecessary and unrealistic reading of the reality and the resulting diminished protection of the individual.[638]

The Authority has contributed to raise the awareness of consumers on the existence of unfair commercial practices even in the provision of social media services, as they often do not realise that when using a digital service/product, such as a social networks, they are 'subscribing a contract with the service provider', to which the consumer framework applies.[639]

However, it has also been observed that accepting this coordination between the two different sets of rules would limit the scope of application of the GDPR beyond what can reasonably be inferred from its own provisions. In particular, the approach followed by the AGCM denies that data protection legislation is meant to regulate all those processing activities affecting the economic sphere of individuals. This reading would be a way to remedy the ineffectiveness of data protection legislation in protecting individuals from mass exploitation of personal data;[640] but it does not take into account the fact that several provisions of the GDPR refer precisely to the economic sphere of data processing (such as, for example, the requirements of consent, aimed at protecting the bargaining freedom of the weaker party) and that this regulatory system is the result of a balancing of interests carried out by the European legislator to allow a sustainable circulation of data in an economy increasingly based on such resources. Thus, according to Midiri, the replacement of that system by consumer law, which focuses on the protection of the individual only, would fail to take into account the greater good which society at large obtains from the circulation of data.[641]

A further concern has been raised on the risk that this new interpretation of consumer law, and the following reinterpretation of the scope of application of the GDPR, may violate the principle of the *ne bis in idem*, thus increasing firms' uncertainty and compliance costs. In fact, it has been argued that applying consumer law to the same conducts regulated by data protection law in order to pursue the same legal interests, such as the protection of economic and commercial freedoms, would mean duplicating not only the obligations but also the sanctions provided for the same legal acts.[642] In this way, the same company risks being

[638] Tarasco, Giaccaglia (n 600) 302.
[639] Cervone (n 591) 207.
[640] Midiri (n 626) 612.
[641] Ibid 614-618.
[642] Ibid 618.

called to account for the same conduct by several authorities, even within the same national jurisdiction.[643]

Nonetheless, these concerns do not consider that, a part from data protection law, there are also other regulations setting specific transparency requirements whose application do not exclude the applicability of consumer law. From the moment the UCPD was transposed into the ICC, Italian administrative courts have always held that the ICC complements other sectoral rules, so that (i) the existence of specific sectoral rules does not exhaust every possible rule of conduct required of the undertakings themselves in order to protect the consumer's freedom of choice and self-determination; and (ii) when different authorities are competent to protect consumers' freedom of self-determination, they do so in a complementary manner.[644] Therefore, the fact of having adopted all the necessary measures to be compliant with data protection law does not exempt undertakings from adopting all the necessary measures to be in compliance with consumer law as well.

It also follows from the above that such a coordination of different laws cannot lead to a breach of the *ne bis in idem* principle. This principle prohibits the punishment of the same historical fact twice, but it does not rule out the possibility that the same historical fact may be relevant to more than one legislative framework, even more so if these different frameworks aim to protect different legal interests.

According to the CJEU case law, the *ne bis in idem* is violated only if three cumulative requirements are met: (i) identity of the facts, (ii) unity of the offender, and (iii) unity of the legal interest protected.[645] In this case, data protection law and consumer law protect different legal interests, as the former protects the fundamental right to data protection (which also encompasses the protection of the individual freedom of choice and self-determination) while the latter protects consumers' freedom of choice and self-determination in their economic choices and through that also the preservation of competitive markets. *A contrario*, if these sets of rules were to protect the same legal interest, their applicability should be triggered by the same facts, which is not the case (for instance, data protection law is applicable to the

[643] Sara Gobbato, 'Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo' (2019) 3 Rivista di diritto dei media, 160.

[644] *Ex multis* T.A.R. Lazio, Sez. I, 19 May 2010, No. 12364, in which the Court analysed the relationship between the ICC and Legislative Decree No. 385 of 1st September 1993 (the Italian Banking Code); T.A.R. Lazio, Sez. I, 8 September 2009, No. 8399, in which the Court analysed the relationship between the ICC and a regulation issued by the Authority for Electricity gas and water system.

[645] Case C-17/10, *Toshiba Corporation and Others v Úřad pro ochranu hospodářské soutěže,* [2012] ECLI:EU:C:2012:72, para 97; Joined cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P *Aalborg Portland and Others* v *Commission* [2004] ECLI:EU:C:2004:6, para 338.

processing of personal data of patients of a healthcare facility for healthcare purposes, but this operation will not trigger the application of consumer law).

In conclusion, the AGCM, by requiring further transparency from undertakings also in connection to commercial practices consisting in data processing operations, has contributed to raising consumers' awareness on the economic dynamics hiding behind the use of digital services and products. This approach is thus potentially suitable to address the deep information asymmetry between online operators and consumers, as singled out in Chapter 3, with regard to the risks and costs entailed in the provision of large amounts of personal data.

In the following chapter, I will compare the BKA and AGCM decisions analysed.

CHAPTER VI
COMPETITION LAW, CONSUMER LAW, DATA PROTECTION LAW IN DIGITAL MARKETS

1. Introduction

As we saw in the first part of this thesis, digital platforms possess a number of intrinsic characteristics which allow them to accumulate an increasing number of users, to expand their range of services and to gain more and more market share. On the other hand, we also saw how data protection laws encourage to a certain extent this concentration of power and how the "traditional" tools of competition law are unsuitable to effectively catch and address the market distortions deriving from it. Furthermore, the fact that the same conduct may fall into areas covered by different disciplines has *de facto* paralysed the application of competition and consumer law in favour of data protection law, which however, due to the mechanisms envisaged to facilitate companies operating in several European countries, has not been applied with the necessary degree of diligence, especially with regard to large digital platforms.

The two decisions analysed in previous chapters are representative of how national authorities are now trying to remedy the enforcement gap experienced in the past years with respect to the conduct of major digital platforms. Both decisions are emblematic of how data-related conducts can be addressed through the application of different sets of laws. However, each set has its own strength and weaknesses that make it more or less appropriate for the resolution of a given issue.

Therefore, in this last Chapter, I will compare different elements of the decisions analysed, highlighting their strengths and weaknesses in the wider context of the markets of digital services and products. I will then conclude with some observations on the wider European context.

2. The Regulatory Dilemma

What both decisions have in common, is that they tried to overcome the regulatory *lacunae* derived from the lack of coordination between consumer, competition and data protection law needed to address typical issues of digital markets – which may potentially fall within the scope of application of all of them, but that, at enforcement level, fail to be addressed by any of them. Botta and Wiedemann define this situation as the "regulatory dilemma".[646]

In fact, what is new in these markets is the main role of data, whose economic exploitation makes data-related activities relevant not only from a data protection point of view but also from a consumer and competition law point of view. Due to the fundamental role of data, data protection law has "invaded" the areas that consumer and competition law have always covered, an invasion that has paralysed the enforcement of the latter two disciplines with respect to practices that in other (less data-driven) contexts are peacefully recognised to fall within their scope of application. This is because when a practice has to do with data there is a tendency to think that it can only be regulated by data protection legislation, disregarding its value in the wider context. Thus, for example, it does not seem obvious that information on how consumer data will be used is essential for consumers to make an economic decision, yet it is if we consider the costs borne by consumers when they give up data. Similarly, it is not obvious that the imposition of a privacy policy that exploits users can be an abuse of dominant position, and yet it becomes so when one considers how this imposition is made possible by the absence of competitors in the market.

However, this underenforcement with respect to data-related conducts was only the first reaction to the new convergence of different policies. In fact, in the last few years, the number of decisions taken against digital platforms has drastically increased.[647]

The Italian and the German competition authorities addressed different Facebook's conducts in their decisions, which coincide only to a certain extent. In fact, only the AGCM considered the lack of transparency with regard to the economic exploitation of users' personal data. Whereas both the AGCM and the BKA considered Facebook's sharing of its users' personal data outside the Facebook.com service "regardless" of the actual will of the user. However, even in this case, the conduct under scrutiny is reconstructed and addressed differently because of the different sets of rules applied: while the AGCM evaluates to what

[646] Botta, Wiedemann (n 345) 444.
[647] Only the BKA, following the 10th amendment of the BWG has opened six proceeding against major digital platforms. The BKA has published the list of proceedings initiated, which is available at List_proceedings_digital_companies.pdf (bundeskartellamt.de).

extent the user is conditioned *within* the Facebook.com service, the BKA investigates *why* such conditioning is even possible in the first place; while the AGCM has imposed a fine and the publication of a statement, the BKA has imposed a behavioural remedy. This raises the question as to which of the two sets of laws, as applied by the two authorities in the decisions examined, is best suited to overcome the issues leading to market failures in digital markets.

As a recall, one issue is the information asymmetry between users-consumers and firms, in which the former do not perceive the value of their data, nor the costs linked to their provision, while the latter keep adopting "concealed data practices" so that it stays that way. The other is linked to market dominance of very few incumbents, which are thus able to set the standards when it comes to the level of privacy ensured by digital products and services, favouring a so-called "race to the bottom" in the preservation of users' privacy.

3. Strengths and Weaknesses

Many elements should be considered to assess the effectiveness of the decisions analysed, and yet due to the novelty of the subject matter, it is inevitable that some of the "unseen effects"[648] would only reveal themselves over time.

A first group of elements is linked to the different legal frameworks applied, which brought to different outcomes, remedies envisaged, reach, and time taken to issue the decisions. Generally speaking, while competition law allows a more in-dept analysis of the functioning of a given market and the adoption of remedies tailored to a specific situation as well as the imposition of higher fines, consumer law allows the issuance of a decision in a shorter time frame, so as to provide a quick response to a given situation.

By applying competition law, the BKA could adopt a structural remedy, which once put into practice, should have the effect of widening the choices available to consumers, and as a consequence, hopefully their awareness. Whereas, the AGCM by imposing a fine and the publication of a corrective statement, provided a less persuasive solution. In fact, taken alone, the decision of the AGCM was not as effective in terms of increasing the awareness of consumers when it comes to the economic exploitation of their data: as we saw in previous sections, what has changed is that now, upon registration, users can read below the "sign in"

[648] According to Frédéric Bastiat, the same choices that cause many positive economic effects also cause negative effects that are not as obvious as the positive ones, but in fact end up cancelling them out. *See* Frédéric Bastiat, *That Which is Seen, and That Which is Not Seen: Bastiat and the Broken Window* (1853).

button that their data are used to show them personalised advertisements, so to finance the Facebook.com service.

By applying competition law, the BKA could explain *why* Facebook managed to impose exploitative terms on its users, contributing to the clarification of the mechanisms underlying the provision of digital services and products through digital platforms. However, the in-dept analysis of the market, needed to correctly apply competition law, required the BKA to focus on the Facebook decision for three years. Whereas, in only two years, the AGCM issued at least three decisions in which it applied consumer law to practices related to the economic exploitation of consumers' personal data.

The real benefit of applying consumer law is rather the quick response it allows to undertake, so that in a relatively short period of time the AGCM was able to develop a consistent approach to firms' concealed data practices. So, while the AGCM's *decision* may not be as effective as the BKA's decision in terms of increasing consumers' awareness, the AGCM's *approach* could work as a deterrent for firms: even if fines under consumer law are not as high as to constitute an actual deterrent in most cases, the *certainty* that adopting a misleading commercial practice with regard to consumers' data will be sanctioned (also, and maybe more effectively, through the imposition of a corrective statement) is something that firms will have to consider.

The AGCM's approach could also be easily adopted by authorities in other Member States, as it was based on the UCPD, a directive requiring a high level of harmonisation, whose provisions were thus likely implemented in a similar way among Member States. On the other hand, the BKA's decision was based on national law and is unlikely that other European competition authorities will try to adopt the same approach.

Another difference worthy of note is about how the BKA and the AGCM described the relationship between the sets of law applied and data protection law: while the BKA used data protection law to assess whether the conditions imposed on users were exploitative, the AGCM based its competence and the applicability of consumer law on the fact that consumer and data protection law pursue different scopes and impose cumulative transparency requirements on firms.

While the BKA's approach may avoid discrepancies between the enforcement of data protection law and competition law (thus promoting a more integrated application of the two), it also risks perpetuating the same shortcomings of data protection law. A hint of that can be seen in the decision under scrutiny in this thesis: the BKA found that Facebook breached the GWB because it had obtained invalid consents from its users, however, as explained in

previous section, consumers can be easily nudged into giving consent.[649] As a result, if Facebook had provided the possibility for users to use the service without combining their data, the conduct would not have infringed competition law, regardless of whether users had been induced to choose the least privacy-preserving form of the service.

4. Concluding Remarks

As clearly emerged from the previous section, there are pros and cons for both decisions. However, the BKA seems to provide a more structured answer to the problem and a more comprehensive protection for society at large. In fact, while the AGCM approach may increase consumers' awareness over time, it is unable to give them a meaningful choice. In fact, consumers will become more aware of how their data are exploited and, potentially, of the costs they have to bear to use ad-financed services, but they will not have the possibility to use a less privacy-invasive service due to the lack of supply. The BKA's approach, on the other hand, will provide a solution, a concrete choice, also for informed consumers who do not wish to give up more data than necessary.

Generally speaking, if consumer law is about ensuring that consumers are able to take informed economic decision, it is clear that everything else being equal, we will end up having informed consumers who can consciously decide to use the service and give up their data or not to use it. In this scenario, Chicagoans would likely say that the decrease in demand for privacy weakening services would stimulate the offering of more privacy-friendly services, however this is unlikely to happen because the very majority of digital services is not privacy friendly and consumers will be forced to use them in order not to be cut out of society. For this reason, competition law's remedies, such as the one adopted by the BKA, are more likely to succeed.

In fact, this becomes clearer applying the "exit" and "voice" concepts presented by Albert Hirshman in his book *Exit, Voice and Loyalty*.[650] In his book, Hirshman uses these concepts to describe how an individual can express dissatisfaction with respect to a given group of which it is part, thus exerting an endogenous force capable of restoring balance in situations of "inefficiency". In particular, an example of "exit" is the individual deciding to stop buying a given product:

[649] Kerber, Zolna (n 362) 25.
[650] Albert O. Hirschman, *Exit, Voice and Loyalty. Responses to Decline in Firms, Organisations, and States* (Harvard University Press 1970).

> *The customer who, dissatisfied with the product of one firm, shifts to that of another, uses the market to defend his welfare or to improve his position; and he also sets in motion market forces which may induce recovery on the part of the firm that has declined in comparative performance.*
> *This is the sort of mechanism economics thrives on.*[651]

According to the author, "voice" is the attempt of the individual to change things from the inside:

> *Voice is here defined as any attempt at all to change, rather than to escape from, an objectionable state of affairs, whether through individual or collective petition to the management directly in charge, through appeal to a higher authority with the intention of forcing a change in management, or through various types of actions and protests, including those that are meant to mobilize public opinion.*[652]

With regard to the level of privacy ensured by major digital services and products (and, as a consequence, also by less known ones), individual are *de facto* deprived of any significant "exit" power. Indeed, an individual can chose not to use Facebook.com or WhatsApp or any other digital service, but this will only result in that individual being cut off of society. The exit power is meaningful only where users can comprehend the drawbacks linked to the use of a service, and where users have an alternative to which they can turn to. In digital markets this two requirements are absent, and this alone explains why the tool of antitrust law is more effective than consumer law in cases as the one examined.

In digital markets, it is also questionable whether users have and effective "voice" left. In fact, one can easily imagine the futility of a complaint made to Facebook (or any other big tech firm) by an individual about the unsatisfactory degree of privacy of the service offered.

But even more worrying is the fact that the authorities themselves lack the power to ensure that users' "voice" preserves a minimum of usefulness; and if we consider that Hirshman thought "voice" to be the impersonation of politics, and we may deduce of democracy as well, we also understand how this situation is harming the fundamental values of our traditions. In fact, generally speaking, the decisions issued thus far did not prove very successful: despite

[651] Ibid 15.
[652] Ibid 30.

all the sanctions imposed, large digital platforms continue to retain a disproportionate amount of power that allows them to be *de facto* entities above the law.

In an attempt to restore some sort of balance, national authorities have tried to devise innovative solutions to protect individuals, and the competitiveness of markets at large, of which the cases examined in this thesis are emblematic, leading to a situation of over-enforcement and fragmentation.[653] Similarly, also at the regulatory level,[654] attempts are being made to find a solution to the only real problem at the root of the current situation: nobody knows which tools are the best to deal with the power, the business model and the consequent strategic role of large digital platforms.

However, the proposed Digital Market Act is likely to change the actual enforcement scenario in Europe. In fact, we are heading toward a centralisation model at both regulatory and institutional level, which in the foreseeable future risks undermining the efforts made by national authorities to apply competition law to large digital platforms. Indeed, the DMA is a form of ex-ante regulation, which will determine a shift from the lengthy in-dept investigations carried out case by case, to a form of regulatory approach to the dynamics of

[653] In addition to the already cited six new proceedings opened by the BKA in 2021 alone (to which must be added another three proceedings opened before the reform of the GWB), the AGCM has issued a number of decisions against digital platforms, such as the one against Amazon, in which the Authority has imposed a fine of over one billion euro, (decision No. 29925 of 30 November 2021), the one against Google (decision No. 29645 of 27 April 2021), the one against Apple and Amazon (decision No. 29889 of 16 November 2021). The UK Competition Authority opened an investigation into Google's Privacy changes (https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes?utm_medium=email&utm_campaign=govuk-notifications&utm_source=4e17cb10-a818-46ca-a4c9-e959ec65e945&utm_content=immediate) and into Apple's terms and condition for app developers (https://www.gov.uk/government/news/cma-investigates-apple-over-suspected-anti-competitive-behaviour) and into Facebook's use of users' personal data (https://www.gov.uk/cma-cases/investigation-into-facebooks-use-of-data). The French Competition Authority adopted a decision against Google (https://www.autoritedelaconcurrence.fr/en/article/autorite-de-la-concurrence-hands-out-eu220-millions-fine-google-favouring-its-own-services) and Apple (https://www.autoritedelaconcurrence.fr/en/article/fines-handed-down-apple-tech-data-and-ingram-micro). This list of cases is not intended to be exhaustive, but only serves to give an idea of the current situation.

[654] An example can be the 10th amendment of the GWB in Germany, viewed favourably by the AGCM, which proposed to adopt a similar approach in the Italian legal framework: "*the Authority advocates the introduction of a specific provision, modelled on the German example, establishing the possibility of qualifying certain undertakings as undertakings of major importance for competition in several markets, which may be prohibited from certain competition-distorting conduct, unless the undertaking proves that its conduct is objectively justified*". See AGCM, 'Proposte di riforma concorrenziale, ai fini della Legg Annuale per il Mercato e la Concorrenza' (2021), 97. The German GWB reform has been looked upon also by other Member State with the aim of amending their own legislative framework, such as, Austria (an overview is available at https://www.lexology.com/library/detail.aspx?g=fcf46df4-4694-4f10-b11b-67564a824470) and Grece (http://www.opengov.gr/ypoian/?p=12356). Finally, it is worth mentioning the UK Competition Authority's code of conduct regulating "gatekeeper" digital platforms, See Competition and Markets Authority, 'A new pro-competition regime for digital markets. Advice of the Digital Markets Taskforce' (2020) < Digital Markets Taskforce – GOV.UK (www.gov.uk)> accessed 1st February 2022.

competition between large digital platforms;[655] additionally, the DMA establishes the Commission as the single competent authority to apply the proposed regulation to these companies.

Although the adoption of a tailor-made regulation for large digital platforms is to be welcomed, especially by virtue of the introduction of a homogeneous approach to problems that have so far been answered in the most disparate ways by the authorities of different member states,[656] the concentration of enforcement powers on the Commission alone has given rise to legitimate concerns. In particular, besides the fact that the Commission risks becoming a bottleneck, this centralised approach is likely to considerably limit the input of national authorities in detecting harmful conduct and developing innovative solutions, thus reducing the options that can be assessed in order to find the best approach.[657]

[655] This shift is criticised by Borgogno and Colangelo, who advocate for the need to maintain an *ex post* enforcement approach. See Oscar Borgogno, Giuseppe Colangelo, 'Platform and Device Neutrality Regime: The Transatlantic New Competition Rulebook for App Stores?' (2022) Transatlantic Technology Law Forum Working Papers No. 83. In another paper, Colangelo and Cappai observe that the European approach to competition is further shifting from the "more economic approach" to a "more regulatory approach", in which effect-based analysis of a given conduct is replaced by a one-size-fit-for-all discipline. See Marco Cappai, Giuseppe Colangelo, 'Taming digital gatekeepers: the 'more regulatory' approach to antitrust law' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572629> accessed 3 February 2022.

[656] However, Komninos highlights that the private enforcement of the DMA (which is a regulation, and as a result potentially invokable by individual before national courts provided that its provisions are sufficiently clear and unambiguous) may in practice increase the risk of fragmentation. See Assimakis P. Komninos, 'The Digital Markets Act and Private Enforcement: Proposals for an Optimal System of Enforcement' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3914932> accessed 3 February 2022.

[657] Pierre Larouche, Alexandre de Streel, 'The European Digital Markets Act: A Revolution Grounded on Traditions' (2021) 12 Journal of European Competition Law & Practice, 558; Germany, France and the Netherlands published an amendment proposal in which they suggest to strengthen the role of national competition authorities in the enforcement of the DMA. See Federal Ministry for Economic Affairs and Energy, Ministère de l'écononomie, des Finances et de la Relance, Ministry of Economic Affairs and Climate Policy, 'Strengthening the Digital Markets Act and its Enforcement' (2021), available at https://www.permanentrepresentations.nl/permanent-representations/pr-eu-brussels/documents/publications/2021/09/9/strengthening-the-digital-markets-act-and-its-enforcement.

CONCLUSIONS

The rapid technological development of the last few years and the following so-called "datification" of our day to day life has made possible the development of super-profiles about almost every person using digital services and products, which can easily be exploited to manipulate people's behaviour, thus putting at risk not only the respect of fundamental rights, but also democracy.

The development of these super-profiles was possible because of the concentration of large amounts of data in the hands of a few companies, providers of the most widely used digital services, such as Facebook or Twitter for social networks, or Google for the search engine, but also for the Android operating system, together with Apple's iOS.

Access to people's data is a key element for the competitiveness of firms in digital markets, this is due also to the data-driven business model adopted by major firms operating in such markets, which are usually structured as two/multi-sided platforms: thanks to consumer's data, they can develop an accurate profile and use it, *inter alia*, to sell targeted advertising and to develop their product (and acquire more users and consequently more data). In fact, massive amounts of data allow the development of cutting-edge algorithms which are used to organise unstructured data and to extract knowledge. In this way, companies with access to larger quantities and high-quality data can identify new market trends at an early stage and adapt their services ahead of competitors who do not have such an advantage.

Because of this, most digital services and products are designed to keep the user connected for as long as possible, so to collect more data and make the profile they have on each user more accurate. In fact, these services are designed to create addiction by exploiting the mechanisms in our brains that lead to the production of dopamine. A number of studies have also shown how these design choices translate into negative consequences for the health of users, especially younger ones.

These digital platforms share a number of characteristics (such as, network effects – and related price dynamics – economies of scale and scope, ecosystems and acquisition zones), which favour market tipping and, at the same time, challenge the "traditional" application of competition law, leading to a situation of underenforcement which has caused the concentration of market power into the hands of only a few firms as well as the creation of a

market failure where individuals are not paid for the data they give up to firms, nor they can chose not to give up data to begin with.

In particular, the propensity to develop ecosystems means that these digital platforms are often vertically integrated, creating an unfavourable situation for both users and competitors in downstream markets. The development of these ecosystems favours user lock-in, making it difficult to switch to different, even if ideally more efficient, services. At the same time, with respect to competitors in downstream markets, platforms play the role of access point to users and to the market itself (e.g. the role of Amazon for retailers, or the role of Facebook and Google for advertisers).

The central role of data, the characteristics of digital platforms and the fact that their services are offered for free are all factors that make the instruments adopted in the application of competition law inadequate. The approach developed within the Chicago School, which aims to maximise consumer welfare and is based on the neoclassical price theory model, is predominant. Due to the focus on price and profit dynamics, this approach was not able to capture the typical dynamics of digital markets and the consequent negative effects, leading to a situation of under-enforcement and to the present situation where market power is concentrated in very few firms.

Against this backdrop, the approach followed by the Neo-Brandeis movement seems to be a more appropriate alternative to respond to the challenges posed by digital competition. In fact, according to the proponents of this movement, competition law should be applied in a way that preserves healthy competition both in terms of processes and market structure. In this perspective, in order to protect the freedom of the individual and ensure respect for the rule of law, it is necessary to prevent the formation of conglomerates such as those represented by large digital platforms.

Due to the crucial role of data on consumers' behaviour in the development of digital services and products, data protection law, and in particular the GDPR, acquired a crucial role in defining the competitive dynamics of digital markets as well. The GDPR regulates how and to what extent firms can lawfully collect and further process users' personal data. Being it a regulation, it directly applies throughout European Union's territory. However, due to the one-stop-shop mechanism, some firms, and in particular large digital platforms, benefitted from a less strict application of the GDPR, which resulted in a further competitive advantage to the detriment of competitors operating in Member States whose national data protection authorities apply the GDPR more diligently.

A number of other GDPR-related elements tend to favour market concentration as well. First of all, the most relied upon legal basis to collect personal data, i.e., the data subject's consent, makes it easier for companies offering a diversified range of services to collect more data than firms offering a limited number of services. Secondly, the accountability principle, and its extension even outside the boundaries of the dataset of the same data controller, discourages data transfers between firms belonging to different groups. At the same time, to avoid multiple transfers, firms with larger datasets are preferred over firms with smaller ones. Furthermore, to avoid the risks linked to the potential breach of GDPR provisions, firms are encourage to develop ecosystems, so to avoid data transfers in the first place. Moreover, some companies use the excuse of GDPR compliance to adopt practices that have the effect of excluding their competitors, as in the case of the exclusion of third-party cookies in the browser provided by Google, Chrome.

Also, in digital markets, an individual is often a data subject and a consumer at the same time. Due to the economic relevance of personal data, the same economic conduct undertaken by a firm may have relevant implications not only under data protection law, but also under competition, and consumer protection law. This has brought to a debate among scholars and authorities over the opportunity to adopt a more integrated enforcement of those legal frameworks in order to properly address the issues underlying the misallocation of resources in digital markets, namely, the lack of competition and the deep information asymmetry between users and firms.

Weak competition allows dominant firms to set the standard when it comes to the amount of data collected and inferred from their users, thus causing the so-called "race to the bottom" with respect to the level of privacy ensured by digital services and products. Weak competition also impedes the development of the supply of more privacy-preserving services: privacy-preserving services are usually provided in exchange for the payment of a price (as they cannot be financed through the monetisation of users' data), or generally speaking, they result less functional because they cannot rely on users' data to be improved. Users, who are generally not aware of the costs linked to the use of privacy-degrading services, have no incentive to use these services because they only perceive their disadvantages.

In fact, users are unable to comprehend the real value of their personal data, nor they can assess the costs they bear when giving them up. This is caused by a number of reasons. First of all, operators tend to adopt complex and misleading privacy policies, so that users are discouraged from reading them. Secondly, the negative consequences of giving up personal data, such as price discrimination or the possibility to make negative assumptions on their

creditworthiness (only to name a few), are generally unknown to users. At the same time, users are unable to properly value their data also because they are excluded from markets where personal data are exchanged and are thus prevent from acquiring the experience needed to understand when a service is requiring too much data (similarly to what happens in regular "price-based" markets).

In this context, many national authorities and scholars advocate for a more synergetic approach in the enforcement of competition law and data protection law in digital markets. Among the various proposed options, it was also suggested that it would be appropriate to qualify excessive data collection carried out by dominant firms as exploitative abuses, where data protection law could be used as a benchmark in this assessment.

On the other hand, some scholars are against this approach and argue that the application of these different sets of rules should remain separate. First of all, issues relating to information asymmetry and the protection of individuals' freedom of choice are usually dealt with by consumer or data protection law rather than competition law: increasing competition would only result in more firms adopting the same opaque privacy policies. Furthermore, taking into account data protection-related elements in the application of competition law would undermine the legitimacy of the latter and introduce a blurred concept such as privacy in the evaluation guiding its application (which would be contrary to the rigorous economic analysis that it is now at its basis).

Against this backdrop, the BKA and the AGCM adopted two decisions against Facebook in which they addressed issues which are generally linked back to the scope of application of data protection law, demonstrating how competition law and consumer law can and must address practices which have relevance under their provisions, even if they have to do with personal data.

In its decision the BKA adopted data protection law, and in particular the GDPR provisions regulating the legal bases upon which a data controller must rely to lawfully process data subjects' personal data, as a standard to assess whether Facebook's data-related practices were to be qualified as exploitative towards German users.

The BKA based its decision on Article 19 (1) GWB, as interpreted by the Federal Court of Justice, which (in a nutshell) allows to address unbalanced negotiations where the dominant position of a party unduly compresses the right to self-determination of the other. According to the case law of the FCJ, the provisions aimed at restoring the balance in unbalanced negotiations must be taken into account in the evaluation. As a result, the BKA assessed

whether Facebook's data policy violated the GDPR in order to establish a violation of Article 19 (1) GWB.

According to the BKA, Facebook's users were forced to give consent to the combination of their data across Facebook's services and products (such as Facebook.com, WhatsApp, Instagram, Oculus, Masquerade) and third parties' websites using Facebook's Business Tools. Indeed, users' consent to this combination of data was necessary in order to use the Facebook.com service. Given Facebook's dominant position and the absence of alternative services on the market for social networks in Germany, users were de facto deprived of a genuine choice. As a consequence, the consent thus given was not freely given, in violation of the GDPR requirements for a valid consent.

The violation of the GDPR was a manifestation of Facebook's market power, meaning that Facebook's dominant position made possible the restriction of private users' right to self-determination. This normative causality is deemed to be enough to substantiate a violation of competition law, without the need to prove that Facebook could undertake the at-issue data practice only because of its dominant position.

The BKA's approach has been the subject of both criticism and praise.

As for the criticism, it has been argued that the BKA should have applied Article 102 TFEU rather than national law, and that the BKA improperly used data protection law. According to some scholars, there was room to apply Article 102 TFEU because of the cross-border relevance of the practice and because it was both exploitative to end users and exclusionary with regard to Facebook's competitors on the advertising market.

As for the improper use of data protection law, it was argued that following the BKA approach, competition law risks becoming a gap-filler for the shortcomings of other fields of law, thus intervening to address any violation of any law that could have the effect of giving a competitive advantage to the company.

However, these criticism failed to consider that national competition authorities are allowed to apply national law rather than European law where the former provides a stricter legal discipline. As a consequence, the BKA properly applied the GWB because it was the most suited tool to address the at-issue conduct. Furthermore, from the legitimate application of national law also derives the legitimate use of data protection law. In fact, the case law of the FCJ establishes that in the assessment of abusive conduct the discipline aimed at restoring the balance in unbalanced negotiations may be used as a standard of reference. The BKA therefore used data protection law to assess whether the conduct amounted to an abuse of a

dominant position. Consequently, it is wrong to argue that competition law risks becoming a general gap-filler because only certain rules can be used as a standard.

The BKA decision was welcomed as an innovative way of exploring the limits of competition law in order to find a solution to dynamics that could damage the competitive process. Indeed, this decision is emblematic of both the pioneering role which Germany has always had in the competition law field, and of the detachment that Germany has always shown with regard to the process of modernisation of competition law at European Union level and to the transition to the "more economic" approach of its enforcement.

The BKA ordered Facebook to give users connecting from Germany the option of using the Facebook.com service without having to agree to their data being combined with data collected outside the social network. This solution is very useful as a first step to give users back the possibility of making a choice with respect to an aspect of digital services that until now has always been imposed, without the possibility of expressing any different preference.

On the other hand, the AGCM chose to apply consumer law to address data-related conducts undertaken by Facebook. According to the AGCM Facebook misled consumers claiming that the Facebook.com service was free, failing to point out with the same transparency that the service used consumers' personal data for commercial purposes. As a consequence, consumers were denied the possibility to take an informed decision, as the costs and the real economic dynamics underlying the provision of the service were not clearly stated.

According to the AGCM, Facebook also adopted an aggressive commercial practice towards registered users as the wider sharing of users' personal data between Facebook and third parties' services was allowed by default. In particular, as a result of this setting, the user would have to uncheck the permissions on data sharing with third parties already provided by Facebook upon using the social network to access third-party services and applications. Furthermore, in the event the user managed to discover this default setting and wanted to change it, Facebook is said to have set out a number of excessively negative consequences, worded in such a way as to lead the consumer to believe that by deselecting the setting, he would run the risk of losing a large part of the data relating to the use of third-party services and that in any event the proper functioning of the social network would be compromised.

The AGCM argued that the economic exploitation of consumers' data has the effect of turning the provision of the data into the consideration demanded of consumers for the use of the service. It follows that the choices related to the registration and use of the social network can be qualified as economic choices liable to be protected under consumer protection law.

Therefore, consumer protection law imposes transparency obligations on top of those already provided for by data protection law.

The AGCM held that the fact that a conduct is relevant under data protection law does not preclude it from being relevant also under a different set of laws, such as, in this case, consumer protection law. Thus the AGCM affirmed its competence to address the at-issue conducts in order to preserve the freedom of consumer with respect to the economic choices linked to the social network.

As a result, the AGCM imposed a fine of five million euro for each unfair commercial conduct, for a total of ten million (however, in the following grades of appeal the second fine was annulled). Furthermore, the AGCM imposed the publication of a corrective statement on the Facebook.com service website and application explaining in very short terms the findings of the AGCM with regard to the abusive practices sanctioned.

To remedy the violation singled out by the AGCM, Facebook has now added right on top of the sign in button a statement warning that consumers' data collected through the use of the social will be used to display targeted advertisements.

This decision is part of a wider context, in which the AGCM usually addresses through consumer protection law data-related practices undertaken by firms, also if GDPR-compliant. This approach has been welcomed by the literature because, *inter alia*, avoids supporting the theory according to which data constitute a fundamental right which cannot be the object of economic negotiations by the data subject, thus being potentially suitable to rise consumers' awareness on the economic value of their data.

Both decisions proved that a more integrated enforcement of all three disciplines is necessary to address the shortcomings of digital markets. The AGCM was able to develop a consistent approach to unfair data practices, thus increasing the transparency requirements firms have to comply with and, as a consequence, increasing the possibilities for consumers to understand the economic dynamics underlying the provision of digital services. The BKA, using data protection law as a benchmark to assess whether a dominant firm imposed exploitative terms to its users, has addressed data-related abuses which are commonly put in place by dominant firms and which were never addressed before under competition law.

While both decisions are good examples of innovative responses to the shortcomings of digital markets, the BKA's decision provides a more forward-looking solution than the one issued by the AGCM. In fact, the AGCM's approach may raise the awareness of consumers about the economic relevance of their data, yet they will still be deprived of any meaningful choice given that the great majority of digital services and products will remain privacy-

degrading. On the other hand, the BKA has provided users with a concrete choice by imposing the divestiture of the service offered on the basis of the level of privacy guaranteed.

Both decisions are emblematic of a situation of over-enforcement and fragmentation which has replaced the initial paralysis of competition and consumer law enforcement in digital markets. In fact, at both European and extra-European level the number of decisions issued against large digital platforms is drastically increasing. Also at legislative level, many countries are adopting new rules to speed up the application of competition law to digital markets and to properly address digital platform specific characteristics.

This is representative of the general uncertainty about what are the best tools to regulate digital markets, which leads to a lack of coordination and awareness on how to deal with practices covered by more than one policy.

The German approach may be a good example to be followed also by other Member State, both at legislative and enforcement levels. However, this is unlikely to happen. In fact, we are heading toward a process of centralisation at both institutional and legislative levels. With the introduction of the DMA, the Commission will be the competent enforcement and regulatory authority with regard to major digital platforms, thus limiting a great deal of the competences of national competition authorities.

Even if a pan-European response is definitively the best approach to achieve a uniform answer to the issues highlighted throughout this thesis, national competition authorities should be recognised more enforcement powers, so to give each Member States the opportunity to participate in the shaping of the digital future of the European Union.

BIBLIOGRAPHY

Acquisti A, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature

Akman P, 'Searching for the Long-Lost Soul of Article 82EC' (2009) 29 Oxford Journal of Legal Studies

Alagna I, Centofanti N, 'La consumerizzazione della privacy tra California Consumer Privacy Act e GDPR' in *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven* (Giuffrè Francis Lefebvre 2021)

Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203 2 April 2013)

—— 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217 9 April 2014)

—— 'Opinion 05/2014 on Anonymisation Techniques' (WP 216 10 April 2014)

—— 'Guidelines on the right to data portability' (WP 242 rev.01 5 April 2017)

—— 'Guidelines for identifying a controller or processor's lead supervisory authority' (WP 244 rev.01 5 April 2017)

—— 'Opinion 4/2007 on the concept of personal data' (WP 136 20 June 2017)

Autorità Garante della Concorrenza e del Mercato, 'Proposte di riforma concorrenziale, ai fini della Legg Annuale per il Mercato e la Concorrenza' (2021)

Autorità Garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la Protezione dei Dati Personali, 'Indagine Conoscitiva sui Big Data' (2020)

Autorità Garante per la Protezione dei Dati Personali, 'Relazione Annuale 2020' (2020)

Autorità per le Garanzie nelle Comunicazioni, 'News vs. Fake Nel Sistema dell'Informazione' (2018)

Autorité de la Concurrence, Bundeskartellamt, 'Competition Law and Data' (2016)

Autorité de protection des données, ‘Décision quant au fond n° 02/2021 du 12 janvier 2021’ (2021)

Bagnoli V, ‘The Big Data Relevant Market As a Tool for a Case by Case Analysis at the Digital Economy: Could the EU Decision at Facebook/WhatsApp Merger Have Been Different?’ (12th ASCOLA Conference 2017)

—— ‘Questions that Have Arisen since the EU Decision on the Whatsapp Acquisition by Facebook’ (2019) 1 Market and Competition Law Review

Barczentewicz M, ‘The Digital Services Act: Assessment and Recommendations’ (2021)

Bastiat F, That Which is Seen, and That Which is Not Seen: Bastiat and the Broken Window (1853)

Becher C, ‘Germany: A Closer Look at the BKA's Facebook Decision’ (2019) 3 European Competition and Regulatory Law Review

Blair R, Sokol D, ‘Welfare Standards in U.S. and E.U. Antitrust Enforcement’ (2013) 81 Fordham Law Review

Borgogno O, Colangelo G, ‘Platform and Device Neutrality Regime: The Transatlantic New Competition Rulebook for App Stores?’ (2022) Transatlantic Technology Law Forum Working Papers No. 83.

Bork R, ‘Legislative Intent and the Policy of the Sherman Act’ (1966) 6 The Journal of Law & Economics

Bork R, Bowman W, ‘The Goals of Antitrust: A Dialogue On Policy’ (1965) 65 Columbia Law Review

Botta M, Solidoro S, ‘Fourth Annual Conference: Hipster Antitrust, the European Way?’ (2020) Florence competition programme

Botta M, Wiedemann K, ‘The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey’ (2019) 64 The Antitrust Bulletin

—— ‘Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision’ (2019) 10 Journal of European Competition Law & Practice

Bourreau M, ‘Some Economics of Digital Ecosystems’ (Hearing on Competition Economics of Digital Ecosystems 3 December 2020)

Braghieri L, Levy R, Makarin A, ‘Social Media and Mental Health’ (2021)

Brandeis L, Competition and Smallness: a Dilemma Re-examined’ (1956) 66 The Yale Law Journal

Budzinski O, Grusevaja M, Noskova V, ‘The Economics of the German Investigation of Facebook’s Data Collection’ (2020)

Buiten M, ‘Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law’ (2020) Journal of Antitrust Enforcement

—— ‘The Digital Services Act: From Intermediary Liability to Platform Regulation’ (2021)

Bundeskartellamt, ‘Market Power of Platforms and Networks’ (2016)

Bureau Européen Des Unions De Consommateurs, ‘Data Governance Act: BEUC Position Paper’ (2021)

Cabral L and Others, *The EU Digital Markets Act* (Publications Office of the European Union 2021)

Campbell J, Goldfarb A, Tucker C, ‘Privacy Regulation and Market Structure’ (2015) 24 Journal of Economics & Management Strategy

Cappai M, Colangelo G, ‘Taming digital gatekeepers: the ‘more regulatory’ approach to antitrust law’ (2020)

Carugati C, ‘The 2017 Facebook Saga: A Competition, Consumer and Data Protection Story’ (2018) 2 European Competition and Regulatory Law Review

Cervone A, ‘Unfair Contract Terms and Sharing of Data with Facebook, Towards a Better Protection of Social Media Users: The WhatsApp Cases’ (2017) 2 Rivista Italiana di Antitrust

Chirico F, ‘Digital Markets Act: A Regulatory Perspective’ (2021) Journal of European Competition Law & Practice

Coase R, ‘The Problem of Social Cost’ (1960) 3 The Journal of Law and Economics

Colangelo G, ‘Facebook and the Bundeskartellamt’s Winter of Discontent’ (2019) Competition Policy International

Colangelo G, Maggiolino M, ‘Data Protection in Attention Markets: Protecting Privacy through Competition?’ (2017) 8 Journal of European Competition Law & Practice

—— ‘Antitrust über alles. Whither competition law after Facebook?’ (2019) 3 World Competition Law and Economics Review

Commission Nationale de l'Informatique et des Libertés, ‘Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium’ (6 May 2017)

Competition & Markets Authority, ‘The Commercial Use of Consumer Data’ (2015)

Competition & Market Authority, Information Commissioner’s Office, ‘Competition and Data Protection in Digital Markets: a Joint Statement Between the CMA and the ICO’ (2021)

Cooter R, Ulen T, *Law and Economics* (6th edn, Addison-Wesley 2012)

Costa-Cabral F, Lynskey O, ‘Family Ties: The Intersection Between Data Protection and Competition in EU Law’ (2017) 54 Common Market Law Review

Crane D, ‘How Much Brandeis Do the Neo-Brandeisians Want?’ (2019) 64 The Antitrust Bulletin

—— ‘Ecosystem Competition’ (Hearing on Competition Economics of Digital Ecosystems, 28 October 2020)

Crémer J, De Montjoye Y, Schweitzer H, *Competition Policy for the digital era* (Publications Office of the European Union 2019)

D’Ippolito G, ‘Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust’ (2018) 6 Diritto dell’informazione e dell’informatica

De Filippi P, ‘The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies’ [2016] Journal of Peer Production

De Streel A, Larouche P, ‘The European Digital Markets Act Proposal: How to Improve a Regulatory Revolution’ (2021) 2 Concurrences

—— ‘The European Digital Markets Act: A Revolution Grounded on Traditions’ (2021) 12 Journal of European Competition Law & Practice

Delmastro M, Nicita A, Big Data: Come Stanno Cambiando il Nostro Mondo (il Mulino 2019)

Digital Competition Expert Panel, *Unlocking digital competition* (March 2019)

Duivenvoorde B, The Consumer Benchmarks in the Unfair Commercial Practices Directive (Springer 2015)

Economides N, Lianos I, ‘Data, networks, and platforms: What effects on economic development? Antitrust and restrictions on privacy in the digital economy’ (2020) 2 Concurrences Review

European Commission, Guidelines on the application of Article 81(3) of the Treaty [2004] OJ C 101/98

—— Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/03

—— ‘Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices’ (2016)

—— ‘Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in
the internal market’ (2021)

European Data Protection Board, ‘Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content’ (2017)

—— ‘Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects’ (2019)

—— ‘Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR’ (9 November 2020)

—— ‘Guidelines 05/2020 on Consent under Regulation 2016/679’ (2020)

—— ‘Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR’ (28 July 2021)

—— ‘Statement 05/2021 on the Data Governance Act in light of the legislative developments’ (2021)

European Data Protection Board, European Data Protection Supervisor, ‘Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)’ (June 2021)

European Data Protection Supervisor, ‘Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy’ (2014)

—— ‘Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data’ (2016)

—— ‘Opinion 8/2016 on Coherent Enforcement of Fundamental Rights in the Age of Big Data’ (2016)

European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European data protection law* (Publications Office of the European Union 2018)

Ezrachi A, ‘EU Competition Law Goals and the Digital Economy’ (2018) Oxford Legal Studies Research Paper No. 17/2018

Ezrachi A, Robertson V, ‘Competition, Market Power and Third-Party Tracking’ (2019) 42 World Competition: Law and Economics ReviewEzrachi A, Stucke M, ‘The Fight Over

Antitrust's Soul' (2018) 9 Journal of European Competition Law & PracticeFederal Ministry for Economic Affairs and Energy, Ministère de l'écononomie, des Finances et de la Relance, Ministry of Economic Affairs and Climate Policy, 'Strengthening the Digital Markets Act and its Enforcement' (2021)

Ferrari G, Maggiolino M, 'GAFAM's Power Accross Markets: How Should We Deal with It?' (2021) Orizzonti del Diritto Commerciale

First H, 'Woodstock Antitrust' (2018) Law & Economics Research Paper Series Working Paper No. 18-24

Fletcher A, 'Digital competition policy: Are ecosystems different?' (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020)

Forbrukerrådet, 'Out of control: How Consumers are exploited by the Online Advertising Industry' (2020)

Fountoukakos K, Nuys M, Penz J, Rowland P, 'The German FCO's decision against Facebook: A First Step toward the Creation of Digital House Rules?' (2019) 18 Competition Law Journal

Friedman M, 'The Social Responsibility of Business is to Increase its Profits' (September 13, 1970) The New York Times Magazine

Gal M, Rubinfeld D, 'Data Standardization' (2019) 94 New York University Law Review

Gal M, Aviv O, 'The Competitive Effects of the GDPR' (2020) 16 Journal of Competition Law & Economics

Geradin D, Karanikioti T, Katsifis D, 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech' (2020) TILEC Discussion Paper

Giannone Codiglione G, 'I Dati Personali come Corrispettivo della Fruizione di un Servizio di Comunicazione Elettronica e la "consumerizzazione" della Privacy' (2017) 2 Il Diritto dell'Informazione e dell'Informatica

Gobbato S, 'Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo' (2019) 3 Rivista di diritto dei media

Gormsen L, ‘The Conflict Between Economic Freedom and Consumer Welfare in the Modernisation of Article 82 EC’ (2007) 3 European Competition Journal

Grandy C, ‘Original Intent and the Sherman Antitrust Act: A Re-examination of the Consumer Welfare Hypothesis’ (1993) 53 The Journal of Economic History

Grunes A, ‘Another Look At Privacy’ (2013) 20 George Mason Law Review

Hacker P, ‘Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law’ (2021) European Law Journal (Forthcoming)

Haucap J, ‘Data Protection and Antitrust: New Types of Abuse Cases? An Economist’s View in Light of the German Facebook Decision’ (2019) CPI Antitrust Chronicle

Hirschman A, Exit, Voice and Loyalty. Responses to Decline in Firms, Organisations, and States (Harvard University Press 1970)

Höppner T, Westerhof P, ‘Abrupt End to “Hipster Antitrust”? Tackling Facebook’s Expansion Following the First Court Ruling in Germany’ (2019) Hausfeld Competition Bulletin

Hovenkamp H, ‘Antitrust Policy After Chicago’ (1985) 84 Faculty Scholarship at Penn Law

—— ‘The First Great Law and Economics movement’ (1990) 42 Standford Law Review

—— ‘Is Antitrust’s Consumer Welfare Principle Imperiled?’ (2019) 45 Journal of Corporation Law

Ibáñez Colomo P, ‘The Draft Digital Markets Act: A Legal and Institutional Analysis’ (2021)

Information Commissioner’s Office, ‘Investigation into the use of data analytics in political campaigns’ (2018)

—— ‘Democracy Disrupted? Personal information and political influence’ (2018)

Irish Council for Civil Liberties, ‘Europe’s enforcement paralysis: ICCL’s 2021 report on the enforcement capacity of data protection authorities’ (2021)

Johnson G, Shriver S, Goldberg S, ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’ (2021)

Kamepalli S, Rajan R, Zingales L, ‘Kill Zone’ (2021) University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2020-19

Khan L, ‘Amazon’s Antitrust Paradox’ (2017) 3 The Yale Law Journal

—— ‘The New Brandeis Movement: America’s Antimonopoly Debate’ (2018) 9 Journal of European Competition Law & Practice

Khan L, Pozen D, ‘A Skeptical View of Information Fiduciduciaries’ (2019) 133 Harvard Law Review

Kemp K, ‘Concealed Data Practices and Competition Law: Why Privacy Matters’ (2020) 16 European Competition Journal 628

Kerber W, ‘Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection’ (2016) 11 Journal of Intellectual Property Law & Practice

Kerber W, Zolna K, ‘The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law’ (2021)

Kimmelman E, Harold Feld, Agustìn Rossi, ‘The limits of antitrust in privacy protection’ (2018) 8 International Data Privacy Law

Koenig C, ‘Exploit to Exclude: Federal Court of Justice Considers Facebook's Data Policy to Violate Competition Law’ (2020) 4 European Competition & Regulatory Law Review

Komninos A, ‘The Digital Markets Act and Private Enforcement: Proposals for an Optimal System of Enforcement’ (2021)

Lao M, ‘Strengthening Antitrust Enforcement Within the Consumer Welfare Rubric’ (2019) CPI Antitrust Chronicle

Lasserre B, Mundt A, ‘Competition Law and Big Data: The Enforcers’ View’ (2017) 1 Italian Antitrust Review

Leistner M, ‘The Commission’s vision for Europe’s digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer’ (2021) Journal of Intellectual Property Law & Practice

Lorenzo-Rego I, ‘The Perspective of the Bundeskartellamt in the Evaluation of Facebook's Behaviour: Prior Considerations and Possible Impact’ (2019) 3 European Competition and Regulatory Law Review

Mackaay E, ‘History of Law and Economics’ in *Encyclopedia of law and economics* (Edward Elgar Publishers 2000)

Manne G, Sperry B, ‘The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework’ (2015) 2 CPI Antitrust Chronicle

Marco Colino S, ‘The Antitrust F Word: Fairness Considerations in Competition Law’ (2018) The Chinese University of Hong Kong Faculty of Law Research Paper No. 2018-09

Markham J W Jr, ‘Lessons for Competition Law from the Economic Crisis: The Prospect for Antitrust Responses to the “Too-big-to-fail” Phenomenon’ (2011) 16 Fordham Journal of Corporate & Financial Law

Marsden P, Podszun R, Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement (Konrad-Adenauer-Stiftung e. V. 2020)

Mashi D, Tamir D, Heekeren H, ‘The Emerging Neuroscience of Social Media’ 19 Trends in Cognitive Sciences (2015)

Massolo A, ‘Bundeskartellamt vs Facebook: Time to Refresh ‘GDPR’s Wall’?’ (2018) 1 Italian Antitrust Review

Melamed D, Petit N, ‘The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets’ (2019) 54 Review of Industrial Organization

Midiri F, ‘Proteggere i dati personali con le tutele del consumatore’ (2021) 5 Giornale di diritto amministrativo

Midiri M, ‘Privacy e antitrust: una risposta ordinamentale ai Tech Giants’ (2020)

—— ‘Le Piattaforme e il Potere dei Dati (Facebook non passa il Reno)” (2021) 2 Il Diritto dell’Informazione e dell’Informatica

Monti G, ‘The Digital Markets Act: Improving Its Institutional Design’ (2021) 5 European Competition and Regulatory Law Review

Nazzini R, ‘Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision’ (2019) Competition Policy International

Newman J, ‘Reactionary Antitrust’ (2019)

Nisevic M, ‘A study on the personal data processing and the UCPD focused on Italy, Germany and the UK’ (2021) 28 Maastricht Journal of European and Comparative Law

Norberg P, Horne D, Horne D, ‘The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors’ (2007) 41 The Journal of Consumer Affairs

OECD, ‘Big data: bringing competition policy to the digital era’ (2016).

Ohlhausen M, Okuliar A, ‘Competition, Consumer Protection, and the Right (Approach) to Privacy’ (2015)

Olivieri G, ‘Sulle “relazioni pericolose” fra antitrust e privacy nei mercati digitali’ (2021) Orizzonti del Diritto Commerciale

Orbach B, ‘The Antitrust Consumer Welfare Paradox’ (2010) 7 Journal of Competition Law & Economics

Palmieri A, Pardolesi R, ‘Clausole Unfair e Abuso da Sfruttamento’ (2018) 1 Mercato Concorrenza Regole

Parker G, Petropoulos G, Van Alstyne M, ‘Platform Mergers and Antitrust’ (2021) Boston University Questrom School of Business Research Paper No. 376351

Pasquale F, ‘Privacy, Antitrust, and Power’ (2013) 20 George Mason Law Review

Petit N, ‘Technology Giants, the Moligopoly Hypothesis and Holistic Competition: A Primer’ (2016)

—— ‘The Proposed Digital Markets Act (DMA): A Legal and Policy Review’ (2021) Journal of European Competition Law & Practice

Petit N, Teece D, ‘Taking Ecosystems Competition Seriously in the Digital Economy: A (Preliminary) Dynamic Competition/Capabilities Perspective’ (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020)

Petropoulos G, ‘Competition Economics of Digital Ecosystems’ (Hearing on Competition Economics of Digital Ecosystems, 3 December 2020)

Pitruzzella G, ‘Big Data, Competition And Privacy: A Look From The Antitrust Perspective’ (2016) 3 Concorrenza e Mercato

Podszun R, ‘After Facebook: What to Expect from Germany’ (2019) 10 Journal of European Competition Law & Practice

Posner R, ‘The Chicago School of Antitrust Analysis’ (1979) 127 University Of Pennsylvania Law Review

—— ‘Law and Economics is Moral’ (1990) 24 Valparaiso University Law Review

Pozzato V, ‘2014 Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law’ (2014) 5 Journal of European Competition Law & Practice

Reyna A, ‘The Shaping of a European Consumer Welfare Standard for the Digital Age’ (2019) 10 Journal of European Competition Law & Practice

Robertson V, ‘Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data’ (2019)

Rosenquist J, Scott Morton F, Weinstein S, ‘Addictive Technology and Its Implication for Antitrust Enforcement’ (2021) 100 North Carolina Law Review (forthcoming)

Santos C, Bielova N, Matte C, ‘Are cookie banners indeed compliant with the law?’ (2020) Technology and Regulation

Savin A, ‘The EU Digital Services Act: Towards a More Responsible Internet’ (2021) Law Research Paper Series No. 21-04

Scheele R, ‘Facebook: From Data Privacy to a Concept of Abuse by Restriction of Choice’ (2021) 12 Journal of European Competition Law & Practice

Schneider G, ‘Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt’s investigation against Facebook’ (2018) 9 Journal of European Competition Law & Practice

Sokol D, Comerford R, ‘Does Antitrust Have A Role to Play in Regulating Big Data?’ in Roger D. Blair and D. Daniel Sokol (eds), *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech* (Oxford University Press 2017)

Solinas C, ‘Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette’ (2021) 2 Giurisprudenza Italiana

Srinivasan D, ‘The Antitrust Case Against Facebook: a Monopolist’s Journey towards Pervasive Surveillance in spite of Consumers’ Preference for Privacy’ (2019) 16 Berkeley Business Law Journal

Stigler Committee on Digital Platforms, ‘Final Report’ (2019)

Stucke M, ‘Should We Be Concerned About Data-Opolies?’ (2018) 2 Georgetown Law Technology Review

Stucke M, Grunes A, ‘No Mistake About it: The Important Role of Antitrust in the Era of Big Data’ (2015) The Antitrust Source

Syrmoudis E and Others, ‘Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20’ (2021) 3 Proceedings on Privacy Enhancing Technologies

Tarasco A, Giaccaglia M, ‘Facebook è gratis? “Mercato” dei dati personali e giudice amministrativo’ (2020) 2 Il diritto dell’economia

Thobani S, ‘Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente’ (2019) 3 Rivista di diritto dei media

Vezzoso S, ‘The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU’ (2021)

Weitbrecht A, ‘From Freiburg to Chicago and Beyond – the First 50 Years of European Competition Law’ (2008) 29 European Competition Law Review

Wiedemann K, ‘A Matter of Choice: The German Federal Supreme Court’s Interim Decision in the Abuse-of-Dominance Proceedings *Bundeskartellamt v. Facebook* (Case KVR 69/19)’ (2020) 51 International Review of Intellectual Property and Competition Law

Wils W, ‘The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the Facebook Decision of the Bundeskartellamt’ (2019) King's College London Law School Research Paper Forthcoming

Witt A, ‘The European Court of Justice and the More Economic Approach to EU Competition Law—Is the Tide Turning?’ (2019) 64 The Antitrust Bulletin

—— ‘Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case’ (2021) 66 The Antitrust Bulletin

Wu T, ‘After Consumer Welfare, Now What? The "Protection of Competition" Standard in Practice’ (2018) Columbia Public Law Research Paper No. 14-608

—— The Curse of Bigness: Antitrust in the New Gilded Age (Columbia Global Reports, 2018)

—— ‘The “Protection of the Competitive Process” Standard’ (2018) Columbia Public Law Research Paper No. 14-612

Zingales N, ‘Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law’ (2017) 33 Computer Law & Security Review

Zuboff S, The Age of Surveillance Capitalism (Profile Books 2019)

TABLE OF CASES

European Court of Justice

Aalborg Portland and Others v Commission (C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P) [2004] ECLI:EU:C:2004:6

Asnef-Equifax (C-238/05) [2006] ECLI:EU:C:2006:734

Asociaţia de Proprietari bloc M5A-ScaraA (C-708/18) [2019] ECLI:EU:C:2019:1064

Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH (C-673/17) [2019] ECLI:EU:C:2019:801

Commission of the European Communities v Federal Republic of Germany (C-51/94) [1995] ECLI:EU:C:1995:352

Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH (C-220/98) [2000] ECLI:EU:C:2000:8.

Gut Springenheide GmbH and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung (C-210/96) [1998] ECLI:EU:C:1998:369

Intel Corporation Inc. v Commission (C-413/14 P) [2017] ECLI:EU:C:2017:632

Konkurrensverket v TeliaSonera Sverige AB (C-52/09) [2011] ECLI:EU:C:2011:83Patrick Breyer v. Bundesrepublik Deutschland (C-582/14) [2016] ECLI:EU:C:2016:779

Peter Nowak v Data Protection Commissioner (C-434/16) [2017] EU:C:2017:994

Post Danmark A/S v. Konkurrencerådet (C-209/10) [2012] ECLI:EU:C:2012:172

Rīgas satiksme (C-13/16) [2017] EU:C:2017:336

Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein (C-120/78) [1979] ECLI:EU:C:1979:42

T-Mobile Netherlands BV, KPN Mobile NV, Orange Nederland NV, Vodafone Libertel NV v Raad van bestuur van de Nederlandse Mededingingsautoriteit (C-8/08) [2009] ECLI:EU:C:2009:343

Toshiba Corporation and Others v Úřad pro ochranu hospodářské soutěže (C-17/10) [2012] ECLI:EU:C:2012:72

United Brands Company and United Brands Continentaal BV v Commission of the European Communities (C-27/76) [1976] ECLI:EU:C:1978:22

Verbraucherschutzverein eV v Sektkellerei G.C. Kessler GmbH und Co. (C-303/97) [1999] ECLI:EU:C:1999:35

European Commission

Facebook/ WhatsApp (COMP/M.7217) (2014)

Autorità Garante della Concorrenza e del Mercato

Decision no. 26387 of January 25, 2017

Decision No. 26597 of May 11, 2017

Decision No. 27432 of November 29, 2018

Decision No. 28562 of February 9, 2021

Decision No. 28601of March 9, 2021

Decision No. 29645 of April 27, 2021

Decision No. 29888 of November 9, 2021

Decision No. 29889 of November 16, 2021

Decision No. 29890 of November 16, 2021

Decision No. 29925 of November 30, 2021

Tribunale Amministrativo Regionale Lazio

T.A.R. Lazio, Sez. I, 8 September 2009, No. 8399

T.A.R. Lazio, Sez. I, 19 May 2010, No. 12364

T.A.R. Lazio, Sez. I, 29 March 2010, No. 4931

T.A.R. Lazio, Sez. I, 9 September 2015, No. 11122

T.A.R. Lazio, Sez. I, 10 January 2020, No. 260

T.A.R. Lazio, Sez. I, 10 January 2020, No. 261

T.A.R. Lazio, Sez. I, 24 September 2021, No. 9903

T.A.R. Lazio, Sez. I, 08 November 2021, No. 11419

Consiglio di Stato

Consiglio di Stato, judgment of 22 June 2011, No. 3763

Consiglio di Stato, judgment of 17 February 2012, No. 853

Consiglio di Stato, judgment of 19 September 2017, No. 4378

Consiglio di Stato, judgment of March 29, 2021, No. 2630

Consiglio di Stato, judgment of March 29, 2021, No. 2631

Bundeskartellamt

Bundeskartellamt, 6 February 2019, B6–22/16—Facebook

Düsseldorf Higher Regional Court

Düsseldorf Higher Regional Court, 26 August 2019, VI-Kart 1/19(V)—Facebook I

Federal Court of Justice

Federal Court of Justice, judgment of 7 December 2010 – KZR 5/10 – *Entega II*

Federal Constitutional Court, judgment of 7 September 2010 – BvR 2160/09 – *Gasag*

Federal Court of Justice, judgment of 6 November 2013 – KZR 58/11 – *VBL Gegenwert I*

Federal Court of Justice, judgment of 7 June 2016 – KZR 6/15 – *Pechstein*

Federal Court of Justice, judgment of 24 January 2017 – KZR 47/14 – *VBL Gegenwert II*

Federal Court of Justice, judgment of 23 June 2020 – KVR 69/19 – *Facebook*

INTERNET SOURCES

Autorité de la concurrence, 'Fines handed down to Apple, Tech Data and Ingram Micro' (16 March 2020) <https://www.autoritedelaconcurrence.fr/en/article/fines-handed-down-apple-tech-data-and-ingram-micro>

—— 'The Autorité de la concurrence hands out a €220 millions fine to Google for favouring its own services in the online advertising sector' (7 June 2021) <https://www.autoritedelaconcurrence.fr/en/article/autorite-de-la-concurrence-hands-out-eu220-millions-fine-google-favouring-its-own-services>

Competition and Markets Authority, 'A new pro-competition regime for digital markets. Advice of the Digital Markets Taskforce' (2020) < Digital Markets Taskforce – GOV.UK (www.gov.uk)>

—— 'Investigation into Google's 'Privacy Sandbox' browser changes' (8 January 2021) <https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes?utm_medium=email&utm_campaign=govuk-notifications&utm_source=4e17cb10-a818-46ca-a4c9-e959ec65e945&utm_content=immediate>

—— 'CMA investigates Apple over suspected anti-competitive behaviour' (4 March 2021) <https://www.gov.uk/government/news/cma-investigates-apple-over-suspected-anti-competitive-behaviour>

—— 'Investigation into Facebook's use of data' (4 June 2021) <https://www.gov.uk/cma-cases/investigation-into-facebooks-use-of-data>

'What are the Meta Products?' (*Facebook Help Centre*) https://www.facebook.com/help/1561485474074139

European Commission, 'The Digital Markets Act: ensuring fair and open digital markets' <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en#new-rules-in-a-nutshell

Fowler G, 'Think you're anonymous online? A third of popular websites are 'fingerprinting' you.' (*The Washington Post* 31 October 2019) https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/

Garante per la Protezione dei Dati Personali, 'Lettera del Presidente del Garante al Presidente dell'EDPB - Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità' (1 August 2019) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126725#ENGLISH

—— 'Whatsapp: Garante privacy, informativa agli utenti poco chiara. L'Autorità intenzionata ad intervenire anche in via d'urgenza' (14 January 2021) https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9519943

Haynes T, 'Dopamine, Smartphones & You: A battle for your time' (*Harvard University Blog*, 1 May 2018) https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/

Information Commissioner's Office, 'Accountability and Governance' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Kayali L, Larger T, Leali G, 'Apple's new privacy feature backed by French competition watchdog' (*Politico*, 17 March 2021) https://www.politico.eu/article/french-competition-watchdog-backs-apple-privacy-push/

Lomas N, 'Twitter fined ~$550K over a data breach in Ireland's first major GDPR decision' (*TechCrunch*, 15 December 2020) https://techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/

—— 'Google's plan to replace tracking cookies goes under UK antitrust probe' (*Techcrunch* 8 January 2021) https://techcrunch.com/2021/01/08/googles-plan-to-replace-tracking-cookies-goes-under-uk-antitrust-probe/

—— 'WhatsApp faces $267M fine for breaching Europe's GDPR' (*TechCrunch*, 2 September 2021) https://techcrunch.com/2021/09/02/whatsapp-faces-267m-fine-for-breaching-europes-gdpr/

Lum K, Chowdhury R, 'What is an "algorithm"? It depends whom you ask' (*MIT Technology Review*, 26 February 2021) https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/

Lützow-Holm Myrstad F, 'How tech companies deceive you into giving up your data and privacy' (*TED*, September 2018) https://www.ted.com/talks/finn_lutzow_holm_myrstad_how_tech_companies_deceive_you_into_giving_up_your_data_and_privacy

Manne G, 'Doing double damage: The German competition authority's Facebook decision manages to undermine both antitrust and data protection law' (*Truth on the Market*, 8 February 2019) https://truthonthemarket.com/2019/02/08/doing-double-damage-bundeskartellamt-facebook/

Matsakis L, 'The Security Risks of Logging in With Facebook' (*Wired*, 20 April 2018) https://www.wired.com/story/security-risks-of-logging-in-with-facebook/

PayPal's Privacy Statement (version of September 9, 2021) https://www.paypal.com/va/webapps/mpp/ua/privacy-full#7

Podszun R, Bongartz P, Langenstein S, 'Proposals On How To Improve The Digital Markets Act' (*Competition Policy International*, 11 March 2021) https://www.competitionpolicyinternational.com/proposals-on-how-to-improve-the-digital-markets-act/

Singh M, 'India antitrust body orders investigation into WhatsApp's privacy policy changes' (*TechCrunch*, 24 March 2021) https://techcrunch.com/2021/03/24/india-antitrust-body-orders-investigation-into-whatsapp-privacy-policy-changes/

—— 'India tells WhatsApp to withdraw its new policy terms' (*TechCrunch*, 19 May 2021) https://techcrunch.com/2021/05/19/india-tells-whatsapp-to-withdraw-its-new-policy-terms/?guccounter=1

Staber G, Stütz A, 'Communication platforms face new obligations and high fines in Austria' (*Lexology* 22 March 2021) <https://www.lexology.com/library/detail.aspx?g=fcf46df4-4694-4f10-b11b-67564a824470>

Steel E, Locke C, Cadman E, Freese B, 'How much is your personal data worth?' (*Financial Times*, 12 June 2013) https://ig.ft.com/how-much-is-your-personal-data-worth/

Wells G, Horwitz J, Seetharaman D, ‘Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show’ (*The Wall Street Journal*, 14 September 2021) https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739