FACULTY OF LAW

LUND UNIVERSITY

Agata Szymanek

“Relationship status: It’s complicated” The interaction of competition law and data protection law in the light of the *German Facebook* case and the integrationist theory

JAEM01 Master Thesis

European Business Law, LL.M

15 higher education credits

Supervisor: Julian Nowag

Term: Spring 2023

Table of contents

ABSTRACT ... 1

ABBREVIATIONS ... 2

INTRODUCTION ... 3

RESEARCH QUESTIONS ... 4
METHODOLOGY ... 4

1. THE DIGITAL ERA ... 6

1.1. THE DIGITAL ECONOMY ... 7
1.2. THE POWER OF DATA ... 8
1.3. ECONOMIES OF SCOPE ... 9
1.4. NETWORK EFFECTS ... 10
1.5. MULTI-SIDEDNESS ... 10
1.6. CONCLUSIONS ... 11

2. LEGAL FRAMEWORK FOR THE INTERACTION OF COMPETITION LAW AND DATA PROTECTION LAW ... 12

2.1. COMPETITION LAW ... 12
2.2. DATA PROTECTION LAW ... 13
2.3. GENERAL OBJECTIVES OF EU LAW ... 14
2.4. CONCLUSIONS ... 16

3. THE APPROACH OF EU AND NATIONAL INSTITUTIONS TO THE PROBLEM OF APPLYING THE PROVISIONS ON THE PROTECTION OF PERSONAL DATA IN COMPETITION LAW ... 17

3.1. THE SEPARATIST APPROACH ... 17
3.2. THE INTEGRATIONIST APPROACH ... 18
3.2.1. The German Facebook case at the national level ... 19
3.2.2. The German Facebook case at the EU level ... 23
3.2.3. Comments on the German Facebook case ... 24
3.3. CONCLUSIONS ... 25

4. THE DUAL ROLE OF THE GDPR ... 27

4.1. POTENTIAL GAPS IN COMPETITION LAW THAT CAN BE FILLED WITH DATA PROTECTION LAW (AND VICE VERSA) ... 27
4.2. DISADVANTAGES OF USING THE GDPR AS THE LEGAL BASIS FOR FINDING A VIOLATION OF COMPETITION LAW ... 29
4.3. DIVISION OF COMPETENCES ... 31
4.4. CONCLUSIONS ... 32

5. POSSIBLE SOLUTIONS TO THE PROBLEM OF OVERLAPPING COMPETITION LAW AND DATA PROTECTION LAW ... 33

CONCLUSIONS ... 36

BIBLIOGRAPHY ... 38

Abstract

This thesis aims to present the relationship between competition law and data protection law in the digital market. The paper illustrates the economic background that creates certain conditions for the interplay between the bodies of law. The emergence of the digital economy with platform-based business models is a challenge that cannot be tackled within a single system. Therefore, the paper presents opposing theories, which address the problem of privacy violation in the internal market. The separatist and integrationist approaches will be introduced together with the relevant case law from which the views are derived. Subsequently, the paper analyses the strengths and weaknesses of the integrationist theory applied by the German competition authority in the *German Facebook* case. The purpose of the assessment is to examine the consequences of using the GDPR as a normative point of reference in competition law. Finally, the thesis presents *de lege ferenda* solutions to the problem of overlapping competition law and data protection law.

Abbreviations

AG	Advocate General
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
CJ	Court of Justice
CJEU	Court of Justice of the European Union
Commission	European Commission
DHRC	Düsseldorf Higher Regional Court (Oberlandesgericht Düsseldorf)
DMA	Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
ECN	European Competition Network
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
EUCFR	Charter of Fundamental Rights of the European Union
FCJ	German Federal Court of Justice (Bundesgerichtshof)
FCO	German Federal Cartel Office (Bundeskartellamt)
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
IMF	International Monetary Fund
NCA	National competition authority
NSA	National supervisory authority for personal data protection
OECD	Organisation for Economic Cooperation and Development
Regulation 1/2003	Council Regulation (EC) 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
SSNIP	Small but significant and non-transitory increase in price
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union

Introduction

The digital transformation has created new patterns of consumption, and thus of production, which required new business models that would allow undertakings to compete effectively in the digital market. In this digital environment, platforms are perceived as “the main actors of the digital economy”.[1] This conclusion will be seen in my paper, which will focus on the characteristics of platforms as a main point of reference for further discussion on competition in the digital era. Particular emphasis will be placed on understanding the phenomena that shaped the position of these contemporary economic “creatures” that are adapted to digital times.

New technologies and the knowledge associated with their development enabled market players to find modern solutions to serve customers better and faster. Data have proven to be a unique key to success in the digital world. However, as a result of these processes, the lines between factors of production and the products themselves have been blurred. Information can be a product itself or a raw material necessary for its creation. The possession and proper use of data became an indicator of market power, which can no longer be measured effortlessly with traditional economic tools.

The invention of the power of data brings with it new challenges relevant not only to competition law but also to personal data protection law. Nevertheless, with the intensity of the digital economy development, it became troublesome to consider regimes separately. The problems occurring in the digital market create risks to consumer privacy, which has traditionally been seen as something to be protected solely by data protection laws. However, the need to consider privacy aspects has also become a focus of competition law. Despite this, the division of “responsibilities” between systems has never been clearly defined. Therefore, the current relationship between competition law and data protection law can be considered complicated.

In the decisional practice of EU institutions, a separatist theory has been an approach to dealing with the problem of overlapping competition law and data protection law. According to the separatists, the systems ought to remain independent – privacy concerns should only be dealt with by data protection authorities. Nonetheless, this static theory is not the only way to address the problem of interaction between the spheres. The wind of change in the perception of the challenge came with the *German Facebook* case. The German NCA presented an integrationist theory that assumes that privacy can be seen as a concern of competition law. In this revolutionary approach, the GDPR serves as a normative point of reference in competition law proceedings. The provisions of the data protection law have been used as a tool in the hands of the competition authority, which entails multiple consequences for both systems.

[1] Selçukhan Ünekbaş, ‘Competition, Privacy, and Justifications: Invoking Privacy to Justify Abusive Conduct under Article 102 TFEU’ [2022] Journal of Law, Market & Innovation <http://dx.doi.org/10.2139/ssrn.4094990> accessed 25 April 2023

Research Questions

The thesis aims to analyse the relationship between competition law and data protection law, shaped by the digital economy and phenomena related to this new order. The ultimate purpose of the paper is to describe and evaluate a solution to the problem of overlapping two separate branches of EU law, which was presented in the *German Facebook* case. Interaction dynamics captured by the integrationist theory will be examined and compared with the separatist theory to illustrate the discourse on the incorporation of privacy into competition law. In order to conduct the research, the following questions will serve as guidelines.
The fundamental question:

1. Should the provisions on the protection of personal data play a dual role, i.e. be a separate regulation of privacy rules and a normative point of reference in the course of competition law assessments (according to the integrationist theory)?

Together with additional questions:

2. Why there is an intersection of competition law and data protection law?
3. Can the integrationist theory replace the separatist theory in the assessment of the CJEU and the Commission in competition law cases?

Methodology

In order to analyse and answer the research questions, the thesis will engage mostly a doctrinal approach. According to the method, the objective of the research is to systemise principles or ideas distinctive to a given field of law and examine the connections and dependencies between them. The result of the analysis is used to address areas of ambiguity and inadequacy within the legal framework. The main aim of the legal doctrine is to describe and understand the present law.[2] The method will be used to assess the strengths, weaknesses and effectiveness of competition law and data protection law. Moreover, the doctrinal approach will be applied to search for interdependencies between the bodies of law. The method mainly involves source research, including traditional sources of information such as legislation (primary and secondary), the jurisprudence of the CJEU and national courts, and the decisional practice of the Commission and NCAs. The study will be supplemented by relevant literature, such as scientific articles, journals, and books.

In addition, because competition law captures multiple dimensions of the internal market, the first chapter will be focused on the economic approach to provide an overview of the economic background of functioning the digital market. This method will be used to analyse the most important aspects of data-driven companies in the context of competition and the use of data. This part will focus in particular on the analysis of reports of various economic organisations, such as the OECD, the APEC or the IMF, and literature on phenomena where data are important resources.

[2] Jan M. Smits, 'What is legal doctrine? On the aims and methods of legal-dogmatic research', [2017] Rethinking Legal Scholarship: A Transatlantic Dialogue, New York [Cambridge University Press] 207

Outline

The thesis consists of five chapters. The first chapter provides an economic background of the research, in particular the circumstances in which competition law and data protection law may interact. The second chapter introduces the two branches of EU law separately, together with the general objectives of the EU. It aims to illustrate the characteristics of the systems and the fact that the goals they pursue may overlap to some extent. The third chapter presents and compares two cases, the *Asnef-Equifax* case and the *German Facebook* case, from which the separatist and integration approaches are derived. Particular emphasis is placed on the *German Facebook* case, which provides valuable insight into the integrationist theory. The fourth chapter, which is the central part of the thesis, contains an assessment of the integrationist approach. The chapter illustrates the advantages, weaknesses, opportunities, and threats related to the idea of including the GDPR as a normative point of reference in competition law proceedings. Finally, the fifth chapter provides a brief overview of solutions proposed in the literature regarding the interplay between competition law and data protection law.

1. The Digital Era

It is not a groundbreaking statement that the birth of the Internet has revolutionised every aspect of individuals' lives, creating new, seemingly endless possibilities. The rapid process of change is not only quickly earned benefits, but also challenges and hard to qualified phenomena that are an inevitable part of the "revolution", as some call the events taking place right before our eyes.

Although it is not the first technological revolution in the history of humanity (the other three embodied respectively steam engine, electrification, and automatization along with computerisation),[3] this one is special because it is based on patterns that have never occurred before. The "founding technologies", all rooted in the Third Revolution, such as the Internet, computers, and smartphones, laid the foundations for the development of the Fourth Revolution and enabled the emergence of digital innovation.[4] The difference between past revolutions and the present one can be characterised by the ethereal nature of the latter, as the Guardian journalist aptly pointed out: "It's easy to picture Thomas Edison inventing the lightbulb, because a lightbulb is easy to visualize. You can hold it in your hand and examine it from every angle. The internet is the opposite. It's everywhere, but we only see it in glimpses.".[5]

Despite its otherness from anything we have known so far, in January 2023 the Internet gathered around 5.1 billion users.[6] If the population of the Earth[7] were reduced to 100 persons, 62 of its inhabitants would have access to cyberspace and almost 60 of them would be present on social media.[8] These numbers are not just insignificant statistics, especially for companies that profit from online assets. The Internet and its resources became a medium for economic activities and an invaluable factor in the creation of many firms that have based their business model on the opportunities offered by the new system. The most prominent form that has appeared is a platform, built on the knowledge of how to use the Internet's by-product, i.e. data.

The Fourth Revolution has created an environment with new models of interactions between market players and different consumption and production styles, making the interplay between competition law and data protection law possible. Before addressing issues arising from the interaction of the two fields of EU law, an economic perspective can be a valuable complement

---

[3] Katarzyna Śledziewska and Renata Włoch, *The Economics of Digital Transformation. The Disruption of Markets, Production, Consumption, and Work* (Routledge 2021) 4

[4] Katarzyna Śledziewska and Renata Włoch, *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat* (Wydawnictwo Uniwersytetu Warszawskiego 2020)

[5] Ben Tarnoff, 'How the Internet was invented' *The Guardian* (London, 25 July 2016) <https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf> accessed 3 April 2023

[6] Ani Petrosyan, 'Number of internet and social media users worldwide as of January 2023' (*Statista*, 23 February 2023) <www.statista.com/statistics/617136/digital-population-worldwide/> accessed 3 April 2023

[7] The current total population of the Earth is around 8 billion according to Statista Research Department, 'Forecast about the development of the world population from 2022 to 2100' (*Statista*, 23 August 2022) <www.statista.com/statistics/262618/forecast-about-the-development-of-the-world-population/> accessed 1 April 2023

[8] Petrosyan (n 6)

to understanding interdependencies. The purpose of Chapter 1 is to provide an overview of the background in which data-driven undertakings operate and the patterns that they employ, which create multidisciplinary challenges that may fall within the scope of various branches of EU law. The chapter aims to present the economic characteristics of the e-market to explain why interactions between different areas of law have materialised. In addition, I intend to bring closer the conditions created by the Fourth Revolution for a common understanding of the functioning of big-tech companies and the relationship (or rather dependence) between passive and active market participants, as well as between competition law and data protection law.

1.1. The digital economy

The changes taking place in the economic landscape under the influence of rapidly growing information and communication technologies required new conceptual proposals, which would allow us to capture them. As a result of the Fourth Revolution, the digital economy is gradually emerging. As the earliest recorded origin of the concept, Bukht and Heeks pointed out the 1996 publication by Don Tapscott "The Digital Economy: Promise and Peril in the Age of Networked Intelligence". Although the author did not provide a precise definition, he described the digital economy as a phenomenon of networking technologies and connecting people through technology.[9]

Lately, the notion of the digital economy has been widely recognised by international organisations and bodies. For instance, in 2015 the European Parliament released a working paper, which discussed the challenges that competition policy must face in this new economic order. As noted in the document "the digital economy is increasingly interwoven with the physical or offline economy", hence there is a need for in-depth reflection on this area in the context of functioning the internal market.[10] In the same year, the OECD published an overview of the digital economy, which observed that mass and low-cost adoption of technologies allowed for some distinctive features, such as the use and analysis of data or the growing popularity of platforms.[11] Within the framework of the different studies, the OECD expressed the need to develop various policies in areas exposed to the impact of the digital economy. The spheres indicated by the OECD in this context were competition and privacy, around which the problem of lack of transparency is growing.[12] In 2018, the IMF broadly characterised the process of digitalizing the economy as "incorporation of data and the Internet into production processes and products, new forms of household and government consumption, fixed-capital

[9] Rumana Bukht and Richard Heeks, *Defining, Conceptualising and Measuring the Digital Economy* (Centre for Development Informatic Global Development Institute SEED 2017) 6

[10] European Parliament, 'Challenges for Competition Policy in a Digitalised Economy' (European Parliament, 2015) 15 <www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU(2015)542235_EN.pdf> accessed 3 April 2023

[11] OECD, 'Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report' (OECD Publishing 2015) <http://dx.doi.org/10.1787/9789264241046-en> accessed 3 April 2023

[12] OECD, 'OECD Digital Economy Outlook 2015' (OECD Publishing 2015) <http://dx.doi.org/10.1787/9789264232440-en> accessed 3 April 2023

formation, cross-border flows, and finance".[13] However, perhaps because the concept of the digital economy has appeared relatively recently, a clear definition has not been formulated so far. Regarding the elusiveness of the digital economy, in 2019 the APEC expressed an opinion that the absence of consensus on the definition creates challenges in measuring and describing the concept, thus raising many important questions. The lack of agreed limitations prevents the creation of measurement frameworks, which is the essence of economic science.[14]

It might be difficult to fully grasp the concept of the digital economy. Although a uniform definition has not yet been developed, based on the aforementioned understating of the term, it is possible to distinguish features that may pose challenges to competition and privacy. Concepts such as networking, datafication, and autonomisation may serve as helpful indicators to describe the business operating conditions for companies present in the digital market.[15] The following subchapters will discuss the most important elements of the platform business model, resulting from the existence of the digital economy.

1.2. The power of data

As Zuboff pointed out, a new "breed of economic power" has emerged, where "every casual search, like and click was claimed as an asset to be tracked, parsed, and monetized".[16] In such circumstances, privacy has become a price to pay for unlimited access to digital goods and services.[17] To stay connected to the global network, individuals are encouraged (or forced, depending on the understanding of the nature of this trade) to share data. The power of big-tech giants was built on discovering the practical exploitation of data exhaust[18] and using it as a competitive advantage. Initially, this knowledge was used only to improve services, as algorithms needed information to learn and create more accurate and complex answers to customers' needs. This solution allowed them to attract users, but it was not yet an ideal business model. Later, digital companies managed to turn data into a source of steady income, starting to use them as a reflection of the minds of users, tailoring advertising to their needs. The pioneer of the use of the "Behavioural Surplus" (as Zuboff called the information that cannot be used directly, but if processed correctly can become a valuable resource), Google, in 2003 submitted a patent titled "Generating User Information for Use in Targeted Advertising", which enabled the company to create an individual data set called "User Profile Information

[13] IMF, 'Measuring the Digital Economy' (International Monetary Fund 2018) 6 <www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy> accessed 3 April 2023

[14] APEC, 'APEC Economic Policy Report 2019: Structural Reform and the Digital Economy' (APEC Secretariat 2019) 97 <www.apec.org/docs/default-source/Publications/2019/11/2019-APEC-Economic-Policy-Report/2019-AEPR---Full-Report.pdf> accessed 3 April 2023

[15] Śledziewska and Włoch (n 4) 93

[16] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 52

[17] ibid

[18] According to the Collins Dictionary, "data exhaust" means "*the byproducts of our online behaviour and interaction with digital devices as opposed to the information we specifically choose to leave behind*" (Collins Dictionary <www.collinsdictionary.com/submission/7418/DATA+EXHAUST> accessed 3 April 2023). Data exhaust usually come in a form of an unstructured, large collection of information, which can then be stored and analysed.

(UPI)", based on the individual queries. UPI turned out to be a breakthrough. Discovering the real behavioural patterns allowed companies to avoid uncertainty, poorly matched advertising, and thus losses in the marketing budget.[19] This technological invention enabled the creation of "business models depending on the acquisition and monetisation of personal data".[20]

The described events have led to the emergence of Big Data – large and unstructured volumes of data that cannot be processed by man, which for this reason requires the use of technologies to extract value from it.[21] One of the tools commonly used to manage this challenge is AI, which can not only support data processing but also improve itself during this activity. Amazon admitted that "AI becomes 'smarter' and learns faster with more data, and every day, businesses are generating this fuel for running machine learning and deep learning solutions".[22] The ability to process data more efficiently is therefore conditioned by the amount of data collected. A distinguishable feature of Big Data is also its time value, only up-to-date information can serve as a valuable resource,[23] which is why a constant and stable flow of data is necessary.

It comes as no surprise that "data is the new oil".[24] Data, as a unique raw material, have become the basis for all online economic activities. Data-driven companies can carefully identify business opportunities and directly reach the customer, while all their decisions are based on current information. Consequently, the ability to take advantage of data can determine competitive strength.

1.3.Economies of scope

Data make an important contribution to creating the economic strength of digital companies. However, there are also other patterns that drive growth, such as economies of scope. The concept explains how companies can reduce their production costs, grow, and serve better. In a nutshell, the economies of scope indicate the situation where the average total cost per unit will decrease if the variety of products increases. The economies of scope can be also referred to as "efficiencies wrought by variety, not volume", a system, where one type of equipment or resource may be used to manufacture different products.[25] For online businesses, where no physical production exists, data play the role of the main input that can be used to produce various outputs. Information collected from the end-user while using platform functionality can

---

[19] Zuboff (n 16) 77-79

[20] Inge Graef, *EU competition law, data protection and online platforms data as essential facility* (Kluwer Competition Law 2016) 127

[21] OECD, 'Big Data: Bringing Competition Policy to the Digital Era' (OECD Secretariat 2016) 5 <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> accessed 4 April 2023

[22] 'What is Artificial Intelligence? Machine Learning and Deep Learning' (*Amazon Web Services*) <https://aws.amazon.com/machine-learning/what-is-ai/> accessed 4 April 2023

[23] OECD (n. 20) 6

[24] See: Meglena Kuneva, 'European Consumer Commissioner Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling' (Roundtable on Online Data Collection, Targeting and Profiling, European Commission, 31 March 2009) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156> accessed 4 April 2023

[25] Joel D. Goldhar and Mariann Jelinek, 'Plan for Economies of Scope' [1993] Harvard Business Review <https://hbr.org/1983/11/plan-for-economies-of-scope> accessed 5 April 2023

then be applied to improve other services or develop new ones, quickly meeting the user's demand.[26] Regarding the cost structure, once the expensive AI infrastructure is fully functional, the Big Data operator reaches the plateau stage, where marginal costs are close to zero.[27] In addition, the unique feature of data that cannot be found in physical materials, which is the possibility of its multiplication and simultaneous processing by different algorithms, intensifies the effect of the economies of scope.

1.4.Network effects

Another economic concept, indirectly related to the economies of scope, which can positively influence its utilization, may be network effects. The term describes a structure where consumers of a digital product benefit from the influx of new users (direct network effects). Using the example of social networks, users can be attracted to the platform if more of their friends appear in this space.[28] In terms of indirect network effects, the growth of buyers (end-users) attracts sellers, and vice versa.[29] It then creates a challenge for digital companies to capture the attention of as many customers as possible. Accordingly, the expansion of networks accelerates datafication, being a process of converting "social behaviour into quantified data by applying sophisticated mathematical analysis",[30] which then enables better personalisation of products.[31] Consequently, because of the network effect implemented successfully together with the economies of scope, "winner-takes-it-all" tendencies might appear. Without network effects, it is difficult to compete on product quality or price alone, thus it poses a threat to weaker competitors who may face serious difficulties in entering the market or trying to expand without a strong database.[32]

1.5.Multi-sidedness

As network effects show, data collected from users can serve not only as a currency for a "free" digital product but can also be used as an incentive to attract customers located on the other side of the platform – sellers or advertisers. Active participants are motivated by the usefulness of the user data and are willing to pay to reach this audience.[33] However, to conduct normal business activities, the "online architecture" provider must strike a balance between the sides in this digital ecosystem. Therefore, platforms serve as intermediaries responsible for

[26] Body for European Regulators for Electronic Communication, 'BEREC Report on the Data Economy' (BEREC, 2019) 11, <www.berec.europa.eu/sites/default/files/files/document_register_store/2019/6/BoR_%2819%29_106_BEREC_Report_on_the_Data_Economy.pdf> accessed 5 April 2023
[27] OECD (n 20) 11
[28] OECD, 'Abuse of Dominance in Digital Markets' (OECD 2020) 8 <www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf> accessed 5 April 2023
[29] European Parliament (n 10) 22
[30] Raphael Santos, 'What is datafication and why it is the future of business' (*Airswift*, 15 September 2022) <www.airswift.com/blog/datafication> accessed 5 April 2023
[31] Śledziewska and Włoch (n 3) 27
[32] OECD, 'An Introduction to Online Platforms and Their Role in the Digital Transformation' (OECD Publishing 2019) 24 <https://doi.org/10.1787/53e5f593-en> accessed 5 April 2023
[33] Laurent Muzellec, Sébastien Ronteau and Mary Lambkin, 'Two-sided Internet platforms: A business model lifecycle perspective' (2015) 45 Industrial Marketing Management 139

facilitating unwavering, direct connection and interaction between two (or more) different groups of market participants.

1.6. Conclusions

It is important to note that the digital economy has been founded on data, which became an indispensable tool for successfully competing in digital markets. End-user data serve many roles – they can be a means of payment, an essential facility, or a commodity themselves. As discussed above, due to the short lifespan of Big Data, a constant flow of information needs to be maintained to ensure product development. The success of online companies is based on the broadly understood growth of service recipients – reaching the tipping point may safeguard the concentrated structure of the market, creating insurmountable barriers to entry. Consequently, the more users, the more intensive the flow of the "new oil". All the above-mentioned elements of the new economic order create a background with challenges that incorporate various legal issues. While the digital competitive process still leads to "choosing the winner", the patterns involved in its course went over the boundaries of traditionally perceived competition. In this way, the interaction between competition and privacy turns out to be necessary to safeguard the interest of all market participants. As indicated in this chapter, the vague characteristics of the digital economy are of interest to international organisations and bodies, which pay particular attention to the risks arising from the massive use of new technologies and data.

2. Legal framework for the interaction of competition law and data protection law

After discussing the economic aspects of the interaction between competition law and data protection law, the legal structure of both systems will be presented to fully assess the existing dependencies. The subchapters describe the main characteristics of these two branches of law to bring closer the objectives they serve and the methods they implement. For both competition law and data protection law following aspects will be discussed: (1) the structure and objectives of the law, (2) the subject matter of protection or control, and (3) the enforcement mechanism. Subsequently, the general goals of the EU will be introduced to illustrate the direction of the EU in the area of the digital economy.

2.1. Competition law

The main objective of competition law is to ensure the proper functioning of the internal market.[34] The adoption of measures safeguarding this area is possible in particular on the basis of Article 101 and Article 102 TFEU. However, the articles do not provide a precise answer to the question of what is meant by the concept of "proper functioning". Stylianou and Iacovides observed that competition laws might be "the most concise, cryptic, and abstract legal provisions",[35] which makes it difficult to decide whether it is a suitable instrument to correct all defects occurring on the internal market. Nevertheless, after the analysis of 4000 different sources (e.g. decisions of the CJEU, Commission or AG) they formulated seven main goals: "efficiency, welfare, economic freedom and protection of competitors, competition structure, fairness, single market integration, and competition process".[36] Stylianou and Iacovides put forward the opinion that competition law has various priorities, the importance of which might fluctuate over the years, and new goals are emerging, such as environmental protection, labour rights and privacy.[37] According to the results of the comprehensive research of the authors, competition law can be seen as a flexible tool capable of adjusting to changing circumstances. Therefore, it has the potential to effectively protect and support all market participants, both active and passive, regardless of the nature of the area it concerns.

The subject of control in competition policy is an undertaking. The concept was described by the CJ in *Höfner and Elser v Macrotron GmbH* as "every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed".[38] This definition was the starting point for further considerations in the case law of the CJEU, but "undertaking" always remained "a relative concept in the sense that a given entity might be regarded as an

[34] Radostina Parenti, 'Competition policy' (*Fact Sheets on the European Union* 2022) <www.europarl.europa.eu/factsheets/en/sheet/82/competition-policy> accessed 5 April 2023
[35] Konstantinos Stylianou and Marios Iacovides, 'The goals of EU competition law: a comprehensive empirical investigation' [2022] Cambridge University Press 620
[36] ibid
[37] ibid
[38] Case C-41/90 *Klaus Höfner and Fritz Elser v Macrotron GmbH* [1991] EU:C:1991:161, para 21

undertaking for one part of its activities while the rest fall outside the competition rules".[39] Concerning the subject matter of protection, as expressed above, it is rather vague what competition law is intended to protect, hence the identification of a specific person or event is difficult. Intuitively, we can indicate that consumers are at the centre of interest of the competition policy,[40] as they are usually the main beneficiaries of its effects.[41] However, due to the multiplicity of objectives of competition law, we cannot unequivocally state that it focuses only on this group (which is also not clearly defined in EU law, as each legal act creates a separate notion of "consumer").

The *ex post* enforcement mechanism in competition law is based on Regulation 1/2003, which gave the executive power to the Commission. Moreover, Article 35 of Regulation 1/2003 requires the Member States to designate authorities, including administrative and judicial bodies, responsible for the parallel application of Articles 101 and 102 TFEU. Member States are required to ensure that NCAs are appointed through transparent, law-based procedures and perform their duties impartially and independently of political or other influence.[42] The cooperation of NCAs and the Commission is facilitated by the ECN, which is a space for information exchange and discussion. Within public enforcement, two stages can be extracted – detection and intervention. In the first step, authorities must find anti-competitive conduct, relying on the effect-based or object-based approach. After the successful detection of the infringement, the second stage can be performed. Intervention may consist of fines, behavioural remedies, or structural remedies.[43] All decisions of NCAs and the Commission are subject to judicial review, respectively under national or EU procedure.

2.2. Data protection law

The goals of the EU data protection law are more structured than those of competition law. The system ensuring uniform privacy rules is based on the GDPR, which objectives are presented in Article 1 as "protection of natural persons with regard to the processing of personal data" and ensuring "the free movement of personal data within the Union". These two goals may seem contradictory, as the stricter protection of the former may obstruct the latter.[44] Recital 4 states that "the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality", which can mitigate the risk of conflict. The

---

[39] Case C-475/99 *Firma Ambulanz Glöckner v Landkreis Südwestpfalz* [2001] EU:C:2001:577, Opinion of AG Jacobs, para 72

[40] See: Neelie Kroes, 'Consumers at the heart of EU Competition Policy' (Address at BEUC dinner, The European Consumers' Association, 22 April 2008) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_08_212> accessed 6 April 2023

[41] John Madill and Adrien Mexis, 'Consumers at the heart of EU competition policy' [2009] Competition Policy Newsletter 27

[42] See: Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market [2018] OJ L 11/3

[43] Kai Hüschelrath and Sebastian Peyer, 'Public and Private Enforcement of Competition Law: A Differentiated Approach' (2013) 36 World Competition 585

[44] Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall Law Review 995

preamble provides also that the GDPR aims to support both the development of economies within the internal market and the well-being of individuals. However, the declared balance is negated in the literature – Gal and Aviv drew attention to the numerous impediments in the digital market created by the GDPR, such as high costs of organising datasets or reduction of economic incentives.[45]

Concerning the subject of control, GDPR is "binding upon all entities which process personal data as part of their business or professional or statutory activities"[46] within the EU. The controller can be any entity, regardless of its legal status or size. Regarding the subject matter of protection, although the personal data were limited to "information relating to an identified or identifiable natural person", the dual division of personal data and non-personal data is disrupted by Big Data. In Big Data datasets, these two categories are intertwined – information processed in real-time can be aggregated in a split second, thus upholding the rigorous division may be difficult. Due to the ease of harvesting data by algorithms, Bart van der Sloot suggested that every piece of data has the potential to be classified as personal, which consequently degenerates the value of the concept of personal data. Since the nature of information is constantly changing, protection of only one category of data may be inadequate.[47] The delimitation of the scope of protection concerning the digital market is undoubtedly challenging.

The mechanism of enforcement is based on local authorities. According to Article 51 GDPR, each Member State is required to appoint at least one public body responsible for monitoring the application of the legal act, this way contributing to the general enactment of the GDPR. NSAs shall perform their task independently of any external influence. The NSAs have investigative, advisory, and corrective powers, which enable them to impose administrative fines or to order the suspension of data flows.

2.3. General objectives of EU Law

From the general scope of EU law, privacy and consumer protection can be distinguished as areas particularly related to the problem of linking competition law and data protection law. Both values play an important role in the EU legal system as a whole – they are enshrined in EU primary law as fundamental rights.[48] Improving consumers' rights has become one of the main objectives of the EU – aspects such as safety, self-awareness, or aligning rights are promoted to increase welfare and "enable consumers to take full advantage of the internal

[45] Michal S. Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16 Journal of Competition Law & Economics 349

[46] Mariusz Krzysztofek, *GDPR: Personal Data Protection in the European Union* (Wolters Kluwer Law International 2021) 37

[47] Bart van der Sloot, *Health Data Privacy under the GDPR* (Routledge 2020)

[48] The right to the protection of personal data is guaranteed by Article 16(1) TFEU and Article 8 EUCFR, and consumer protection by Article 169 TFEU and Article 38 EUCFR.

market".[49] Privacy can also be seen as an element of consumer protection, in *Meta Platforms Ireland* the CJ said that authorising consumer protection associations to bring civil actions against unlawful data processing "contributes to strengthening the rights of data subjects".[50]

Despite the focus on the consumer, EU law has no consistency in the perception of this term. In neoclassical economic theories, the consumer is perceived as *homo oeconomicus,* represented by three attributes: individuality, egoism, and rationalism. In this model, a person acts logically, carefully calculating every aspect to maximise profits.[51] However, years of development of economic sciences resulted in criticism of this static concept. Taking into account human nature allowed researchers to recognise consumer flaws, such as information asymmetry, the influence of emotions or cognitive biases, which expose the fact that a fully rational "economic man" does not exist.[52] In the digital economy, the imperfect consumer is further affected by the *privacy paradox* – while consumers declare that data privacy is important, they take actions that contradict their preferences.[53] The phenomenon completes the picture of the functioning of the consumer in the digital market. As pointed out by Chen et al. "the data *privacy paradox* thus provides an entry to understanding how consumers trade off their privacy concerns with data-sharing needs to satisfy their digital demands, the foundation of the data economy".[54] Consequently, some consumers recognise the value of personal data, but as imperfect individuals, do not see the risks resulting from this exchange. Adequate institutional protection is therefore required.

Regarding the overall objectives, it is worth noting that the EU is currently implementing the Digital Single Market strategy. According to the EU declaration, the initiative is based on three pillars: (1) providing consumers and entrepreneurs with access to digital goods and services, (2) creating an environment supporting the growth of digital networks and innovative solutions, (3) facilitating the development of the digital economy.[55] This strategy creates a framework for better consumer and competition protection in the context of digital challenges, which include privacy concerns.

---

[49] European Parliament, 'Briefing EU policies – Delivering for citizens. Protecting European consumers' (European Parliament 2019) <https://what-europe-does-for-me.eu/data/pdf/focus/focus22_en.pdf> accessed 7 April 2023

[50] Case C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV* [2022] ECLI:EU:C:2022:322, para 74

[51] Sophie Donnelly and Senior Sophister, 'Homo Oeconomicus: Useful Abstraction or Perversion of Reality?' (2018) 32 Student Economic Review 95

[52] Justyna Brzezicka and Radosław Wisniewski, 'Homo Oeconomicus and Behavioral Economics' (2014) 8 Contemporary Economics 353

[53] Susan Athey, Christian Catalini and Catherine Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' [2018] Stanford University Graduate School of Business 1

[54] Long Chen, Yadong Huang, Shumiao Ouyang and Wei Xiong, 'Data Privacy and Digital Demand' [2021] <http://wxiong.mycpanel.princeton.edu/papers/Privacy_Paradox.pdf> accessed 10 April 2023

[55] EU Digital Single Market <https://eufordigital.eu/discover-eu/eu-digital-single-market/> accessed 10 April 2023

2.4. Conclusions

Due to the blurred lines of competition law objectives, privacy can be perceived as an area where data protection and competition goals overlap. The intersection line can run where the data-driven undertakings operate – both competition law and data protection law recognise this form of economic activity.

It must be noted that activities in the digital market, such as the emergence of Big Data, create problems that cannot be fully solved within a single body of law. The literature shows that the classic concept of personal data is becoming obsolete, which may affect the quality of data protection within the EU. Moreover, consumer activity in the digital market, which goes against the classic economic perception of consumer behaviour, further complicates the division of laws forcing the interaction between two systems. Additionally, the EU strategy for the coming years assumes supporting the expansion and strengthening of the digital economy, which is not possible without uninterrupted data flow, as shown by the economic mechanisms of data-driven companies. This plan additionally stimulates interactions between competition and privacy.

Despite the complicated current economic structure, the main objectives remain common: "data protection, competition and consumer law in the EU all aim (…) to protect and to promote the welfare and to help create a single European market".[56] Therefore, it is reasonable to consider various models of interactions between antitrust law and data protection law.

[56] EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data (2016)

3. The approach of EU and national institutions to the problem of applying the provisions on the protection of personal data in competition law

Given the economic perspective and overall objectives of the EU competition and privacy policies, it is clear that the two areas overlap, creating many challenges for the application of EU law and the implementation of the Digital Single Market. Bearing in mind the need to ensure legal coherence, the problem of integrating competition law and data protection law was discussed in decisions of national and EU institutions. Based on the decisional practice, two views have been introduced into the academic literature – separatism and integrationism. In Chapter 3, both approaches will be discussed to illustrate a discourse consisting of opposing perspectives on the problem of applying the provisions on the protection of personal data in competition law cases involving infringements of privacy.

3.1. The separatist approach

The dynamic between antitrust and data protection has been first captured in 2006 in the *Asnef-Equifax* case,[57] which gave rise to the separatist approach. The case arose around a dispute between Spanish entities – the credit information bureau Asnef-Equifax and Ausbanc, the Association of Users of Banking Services. In 1998 Asnef-Equifax applied for permission to open and run an electronic register, which aim was to "provide solvency and credit information through the computerised processing of data relating to the risks undertaken by participating organisations engaging in lending and credit activities". The Asnef-Equifax's register contained personal data, such as the identity and business activities of the debtors as well as specific pieces of information about bankruptcy or insolvency.[58] Contrary to the negative opinion of the NCA, the Spanish court allowed the opening of the register under certain conditions. The decision was undermined by Ausbanc, which argued that the register might restrict competition, as it enabled the exchange of information about customers between financial institutions in Spain. Ausbanc pointed out that data contained in the registry were normally considered business secrets – possessing this knowledge would enable financial institutions to cooperate by unifying their policies towards people applying for loans. These conditions could encourage or facilitate collusion and therefore a violation of EU law.[59] The Tribunal Supremo decided to request a preliminary ruling on whether, in the light of Article 101 TFEU, the exchange of information about customers could be considered compliant with EU law and, if not so, whether this system could benefit from the exemption provided for in Article 101 (3) TFEU.[60]

The CJ rejected Ausbanc's arguments and ruled that a system for the exchange of credit information between financial institutions did not restrict competition within the meaning of Article 101 TFEU. The interpretation of the provisions of competition law must take into

[57] Case C-235/08 *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios* [2006] ECLI:EU:C:2006:734
[58] ibid para 7
[59] ibid paras 10 and 27
[60] ibid para 11

account a specific economic and legal context. The national court must consider aspects such as the degree of market concentration, the availability (legal and factual) of the register, and the fact that the identity of lenders is not disclosed. As long as the relevant market is not concentrated, and other conditions are satisfied, the register can operate, because the risk of cooperation between undertakings is reduced. Furthermore, positive effects of the register can be observed, as financial instructions have a reliable tool to distinguish customers who are more likely to default and adapt their loan offers to a financial situation of a borrower.[61] Lastly, and most importantly, the CJ observed that "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection".[62] While this statement was not further discussed, the judgment shows unequivocally that there is no place for the analysis of data protection issues in competition law. The opinion represents the separatist point of view, which is in favour of the full independence of the systems. The line between the bodies of law should be clear and impassable to avoid confusion.

The maintenance of "separatist tendencies" can also be observed in further decisional practice. For example, in *Facebook/WhatsApp*, where a merger of two online service providers was examined, the Commission excluded privacy issues from proceedings. Although the Guardian of the Treaties noticed that privacy becomes a factor valued by consumers,[63] it stated that "any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".[64] The presented cases show that both the CJEU and the Commission share the view that privacy issues should be considered only in the light of the provisions of data protection law and that the answers to individual problems should be sought there.[65]

3.2. The integrationist approach

While the EU institutions take a firm stance, another approach to the interactions between competition and privacy can be distinguished. According to the integrationist theory, the incorporation of data protection into the competition law framework is possible. This postulate is particularly visible in the *German Facebook* case,[66] where the boundaries defined by the separatist approach were no longer observed. The decision of the FCO also draws attention to many problems that arise in connection with the activities of data-driven undertakings and the digital economy.

---

[61] ibid paras 55-62
[62] ibid para 63
[63] *Facebook/WhatsApp* (Case No COMP/M.7217) Commission Decision 32014M7217 [2014], para 87
[64] ibid para 164
[65] Iga Małobęcka-Szwast, 'Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi' (2018) 8 IKAR 139
[66] FCO, Decision of 6 February 2019, B6-22/16 (*German Facebook* Decision)

3.2.1. The *German Facebook* case at the national level

In 2019, after three years of investigation, the FCO issued a decision in which Facebook was found guilty of abusing its dominant position. The facts of the case are as follows. Facebook, a provider of social network services used by 23 million daily active users in Germany,[67] required its users to open an account to enjoy the functionalities of the platform. Before start using a profile, users had to agree to various terms and conditions for the service itself, data and cookies policy, and other Facebook products.[68] In accordance with the rules imposed unilaterally by the platform, it was allowed to process users' personal data, including information provided by users and device-related information, to a large extent. As Witt aptly summed up, Facebook was authorised (without additional consent) to "collect, combine, and analyze user-generated data from a number of different online sources, namely, data generated on (1) Facebook.com itself, (2) any other Facebook-owned service, and (3) any third-party websites that used 'Facebook Business Tools'".[69] All these sources of data were collectively referred to as "Products", used to provide a consistent "personalized experience".[70] The most relevant Facebook-owned services at that time were Instagram or WhatsApp, where an additional registration process (based on a separate agreement) was necessary to use them.[71] Free-of-charge Facebook Business Tools were used on independent, external websites – the most important were social plugins (eg. "Share", "Like" or "Comment" buttons), Facebook Login (allowing users to identify themselves with a Facebook account), Ads Reporting (measuring users' interactions with advertisements) or Facebook analytics (allowing websites operators to measure how users interact with services).[72] These tools were offered to businesses to integrate with Facebook and interact with customers. In practice, when a user visited a third-party website or app, all data were redirected to Facebook.[73] The acquired data were then assigned to the profiles of individual users on Facebook.[74] According to the FCO, "by integrating Facebook Business Tools, users are tracked across all services and devices", including e.g. dating apps or political parties' websites, where sensitive personal data were collected.[75] In the proceedings, the FCO focused in particular on the problem of obtaining user data from these external sources.

The legal assessment was based on national competition rules. According to Article 3 (1) Regulation 1/2003, the application of EU law is required if the conduct is prohibited by Article 102 TFEU, however, the FCO concluded that the concept of protection developed in German law had no equivalent in EU law.[76] As noted by Witt, the FCO could not find relevant case law or decisional practice regarding Article 102 (a) TFEU, because it looked for an infringement of

[67] ibid para 17
[68] ibid paras 88-90
[69] Anne C. Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021) 66(2) The Antitrust Bulletin 276
[70] *German Facebook* Decision (n 63) paras 92-93
[71] ibid para 680
[72] ibid paras 55-73
[73] ibid para 139
[74] ibid para 146
[75] ibid para 838
[76] ibid para 914

the GDPR as a basis for the theory of harm. Violation of individuals' constitutional rights has never been unequivocally recognized as a form of abuse within EU law.[77]

The legal analysis of the case began with the delineation of the relevant market. Following the EU practice, the FCO acknowledged that even though the service is seemingly[78] free of charge for private users, it can be considered a market activity.[79] Defining the market, the FCO took into account aspects typical of the digital market, such as network effects (both direct and indirect), and multi-sidedness, concluding that for "advertisers, publishers and developers, Facebook meets different requirements than for private users".[80] In order to decide which competing services were included in the market, some characteristic features and functions of social networks were distinguished: the need to register and set up a personal user profile, friend-finding functionalities, communication tools, a newsfeed, or the fact that it can be used on different devices.[81] Additionally, the FCO recognized the SSNIP test as inapplicable and assessed the demand-side substitutability. The FCO examined and compared 30 other online services.[82] The substitutability of these services was significantly limited because of the strong direct network effects on Facebook resulting in a so-called "lock-in effect" (difficulty to switch networks due to the presence of friends). The messaging services were additionally classified as only complementary to social media services, so they could not be perceived as substitutes at all.[83] These findings allowed the FCO to exclude most social services from the product market and conclude that "even a 'market for Facebook' (single-platform market) can be considered".[84] Regarding the geographical market, it was defined as Germany-wide. The FCO stated that due to the national specifics of digital services and the dependence of market entry on the network, it is difficult to expand the geographic scope in a short time.[85] Finally, the relevant market was defined as the social network for private users in Germany.[86]

Based on findings on the scope of the market, the FCO confirmed Facebook's dominance. The FCO followed the definition developed by the CJEU, according to which dominance "enables the company to prevent effective competition being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, customers and, ultimately, consumers".[87] In line with this concept, the FCO analysed aspects that enhance market power, such as the relationship between the amount of data collected and market power or the *privacy paradox,* which strengthens data flow. The FCO emphasized the importance of data for competition, where superior access to information provided Facebook with the ability to quickly adapt to market demand. All these factors created the entry barrier

---

[77] Witt (n 66)
[78] Cf. *German Facebook* Decision (n 63) para 244, where the FCO suggested that data sharing can be considered a form of compensation for a digital service
[79] ibid para 234
[80] ibid para 232
[81] ibid paras 258-263
[82] Cf. ibid paras 182-211
[83] ibid para 286
[84] ibid para 276
[85] ibid para 350
[86] ibid para 165
[87] ibid para 376

to the social network market, which was already highly concentrated, with Facebook's market share in daily active users estimated at over 90%.[88]

Bearing in mind that the mere possession of a dominant position is not prohibited, the FCO sought to determine whether an infringement of data protection principles could constitute abuse. To assess Facebook's conduct, the authority built its consumer and competition harm theory on the premise that the platform imposed exploitative business terms on users, namely the terms violating the data protection principles enshrined in the GDPR.[89] Facebook, using its market power causing the lack of alternative social networks, forced users to accept unfair contract terms, which allowed it to collect and aggregate data excessively. Although users did not pay for the service, they suffered from the loss of control over how their personal data is used, which limited their welfare. Consumer harm then entailed competition harm – the more data were unlawfully acquired, the more intense the network effects were. Consequently, the "lock-in" effect was created, which could significantly influence competition.[90]

In the central part of the decision in which the abuse was found, the FCO presented the assumptions of the integrationist approach. The authority outlined several arguments in favour of applying provisions on the protection of personal data in antitrust proceedings. First, the FCO referred to the rules on competence stipulated in GDPR. It noted that the use of privacy principles by NCAs or other authorities is not prohibited by national or EU data protection laws.[91] The FCO observed that data protection law enforcement had been entrusted inter alia to consumer protection associations.[92] Moreover, the FCO noted that "the substantive application of data protection law through competition law stipulations does not in any way threaten the consistent interpretation of data protection law, but rather promotes consistency", since in both systems the final interpretation of the law is supervised by the CJEU.[93] The FCO noted also that it used the tools provided for in the GDPR to monitor the scope of data processing in competition proceedings.[94] Additionally, the FCO cooperated with the German data protection authorities throughout the proceedings, so the risk of misinterpretation of the GDPR was minimised.[95]

The above findings allowed the FCO to consider itself authorised to review Facebook's privacy policy which was the source of the infringement. The examination was to be based merely on the premise of compliance with the "European data protection values", however, the authority went further than that. Instead, the FCO carried out an extensive scientific legal assessment under the provisions of the GDPR.[96] The in-depth analysis covered all the elements

---

[88] Cf. ibid paras 374-521
[89] Małobęcka-Szwast (n 62)
[90] FCO, 'Background information on the Facebook proceeding' (2017) <www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6> accessed 18 April 2023
[91] *German Facebook* Decision (n 63) para 535
[92] ibid para 540
[93] ibid para 541
[94] ibid para 551
[95] Witt (n 66)
[96] ibid

characteristic of proceedings concerning the infringement of personal data protection law. The FCO determined that Facebook is a data controller, processing and profiling personal data, including special categories of data collected through Facebook Business Tools. Subsequently, the authority decided that Facebook's behaviour was not justified either on the basis of Article 6 or 9 GDPR, even though Facebook had invoked all the justifications provided for in the legal act.[97] The FCO based its interpretation of the GDPR on the conclusions from the first part of the decision – because Facebook was in a quasi-monopolistic position, and users could not effectively consent to the processing, there was a violation of the GDPR. Due to the imbalance of power between the service provider and the recipient, unconditional acceptance of the service was the only way to participate in the social network, thus the consent could not be considered voluntary. Contrary to Facebook's view that users could control "add preferences" in the privacy settings, it was not enough to opt out of collecting data from third-parties' websites, and thus adjust the scope of consent. Similarly, the FCO rejected the necessity to process data to perform the contract if the content of the agreement was unilaterally imposed by the dominant undertaking. Furthermore, it was not clear what the role data acquired through Facebook Business Tools played in the provision of the social network service. Finally, Facebook's overriding interest argument failed because data collection through Facebook Business Tools was against the principle of balancing interests between the collector and the data subject.[98]

In the final part of the substantive assessment, the FCO addressed causality to demonstrate the link between the infringement and the dominant position. Referring to the judgements of the FCJ, the FCO explained that "normative causality" is sufficient to establish abuse.[99] The relationship manifested in the form of "restriction of private users' right to self-determination (…) clearly linked to Facebook's dominant position in the market".[100] This effect resulted from the lack of voluntary consent to unilaterally imposed, unfavourable contract terms, which would not have been possible without such a strong market position. Although Facebook argued that limiting data processing under the GDPR would result in less competitive and poorer-quality products, the authority remained adamant. The FCO admitted that the data protection standard formulated in the GDPR may seem "debatable" from an economic perspective, however, it must be accepted, as the EU legislator had decided to restrict economic benefits in this way to balance interests.[101] In addition, the FCO found a causal link between dominance and data processing conditions regarding "the actual and potential impediment effects to the detriment of competitors", not only on the social network market, but also in online advertising, and other markets where Facebook-owned companies operated.[102]

---

[97] According to Article 6 (1a-f) GDPR, the basis for lawful personal data processing is: (a) consent of the data subject, (b) performance of a contract, (c) fulfilment of the legal obligation imposed on the controller, (d) protection of the vital interests of the data subject, (e) performance of a task carried out in the public interest, (f) legitimate interests of the controller or a third party.
[98] Cf. *German Facebook* Decision (n 63) paras 573-870
[99] ibid para 873
[100] ibid para 876
[101] ibid para 882
[102] ibid paras 885-888

The FCO required Facebook to terminate the exploitative abuse (i.e. change the trading conditions violating the privacy principles). However, the case did not stop at this stage – it was reviewed by the DHRC, which referred a question to the CJEU for a preliminary ruling on selected aspects of the case. It is also worth noting that due to "serious doubts as to the legality" of the decision, the DHRC ordered the suspensive effect of the appeal,[103] which was subsequently overruled by the FCJ.[104] The next paragraph will discuss the further course of the *German Facebook* case at the EU level.

3.2.2. The *German Facebook* case at the EU level

The DHRC asked several questions regarding the interpretation of the GDPR, part of them related the specific aspects such as the scope of sensitive data, the use of justifications under Articles 6 and 9 GDPR or the nature of the consent given to a dominant undertaking. From the perspective of the interaction between competition and privacy, the first and seventh questions were the most relevant. First – whether an NCA, which is not an NSA within the meaning of the GDPR, can establish a breach of the GDPR and issue an order to end it. Seventh – whether an NCA, in a course of investigation of abuse that does not constitute a violation of the GDPR, can determine whether data processing terms and their implementation comply with the GDPR when assessing the case (even if the case is handled by an NSA at the same time).[105]

At the present stage of the case, AG Rantos has issued an opinion. The first question AG considered irrelevant because the FCO had not penalized the breach. Regarding the seventh question, AG emphasized that an NCA is not competent to determine a breach of the GDPR, however, it may assess the compatibility of actions with the legal act. The NCA must be able to determine whether conduct deviates from the measures commonly used in non-price competition. If the interpretation of the provisions of the GDPR may be a vital indication of abuse within the meaning of Article 102 TFEU, the NCA should be entitled to carry out such an incidental examination. This assessment is without prejudice to the application of the GDPR by an NSA. Although EU law does not provide for a mechanism of cooperation between antitrust and data protection authorities, in the light of Article 4 (3) TEU requiring sincere cooperation they should inform and consult each other. The NCA shall endeavour to comply with decisions of the NSA adopted in respect of the same conduct.[106]

AG Rantos appears to have opted for the integrationist approach by allowing the NCA to include a privacy assessment based on the GDPR in antitrust proceedings. Even though AG's opinion is non-binding, it may significantly influence the CJ's position. The case provides the CJ with the opportunity to reconsider its approach to the integration of data protection and competition law.

---

[103] DHRC, Decision of 26 August 2019, VI-Kart 1/19 (V) (*Facebook v Bundeskartellamt)*

[104] FCJ, Decision of 23 June 2020, KVR 69/19 (*Facebook v Bundeskartellamt)*

[105] Case C-252/21 *Facebook Deutschland GmbH v Bundeskartellamt* [2021] OJ C320/16, Request for a preliminary ruling from the DHCR

[106] Case C-252/21 *Facebook Deutschland GmbH v Bundeskartellamt* [2022] ECLI:EU:C:2022:704, Opinion of AG Rantos, paras 17-33

3.2.3. Comments on the *German Facebook* case

While the CJ has not yet issued a ruling on this matter and the case is pending, it is already said that "the German case opens up a new Pandora's box of regulatory issues".[107] After the announcement of the FCO verdict, the literature buzzed with comments. Starting from the delimitation of the market, Małobęcka-Szwast argued that by focusing solely on users, the FCO ignored the fact that Facebook operates in a two-sided market, which cannot exist without the presence of advertisers (who "sponsor" the free use of the website). Moreover, following the Commission's view from *Facebook/WhatsApp*, she indicated that social networks are usually available worldwide. Limiting the market to private users in Germany seems questionable,[108] but the narrow definition, therefore, made it easier to determine market dominance.[109]

Regarding the theory of harm, Witt was hesitant to measure consumer welfare through the privacy parameter, outside the economic context. She suggested that FCO should have translated welfare into the economic language to show that privacy was a factor in service quality (according to the separatist theory). This doubt recalls the general question of what the objectives of competition law are and whether it should protect all forms of consumer harm, including those that appear not as an economic loss but as a violation of a fundamental right.[110] Furthermore, it is argued that the decision lacked a deeper analysis of the anti-competitive effects, as raising barriers to entry is an element of strengthening dominance rather than abusing it.[111]

The causal link between dominance and abuse was discussed. The FCO applied "normative causality", which was further explained by the FCJ as the view that "the conduct in question (…) only have a negative impact on competition if applied by a dominant undertaking".[112] However, the fact that Facebook may impose unfair contract terms resulted not only from its position but also from the characteristics of the market and the user's attitude towards privacy along with information asymmetries.[113] While non-dominant companies may also introduce harmful privacy policies that violate the GDPR, the FCO ignored these aspects[114] and provided no substantive evidence to demonstrate that the competitive structure of the market would prevent Facebook from operating in violation of privacy principles.[115] Nevertheless, from the perspective of EU law, the causal link would be irrelevant, as it is not required to establish an abuse of a dominant position.[116]

---

[107] Aoife White, Stephanie Bodoni and Stefan Nicola, 'Facebook's Data-Sharing Plans Threatened by New Rules in Germany' *Bloomberg* (2 July 2019)
[108] Małobęcka-Szwast (n 62)
[109] Christoph Becher, 'A Closer Look at the FCO's Facebook Decision' (2019) 3 Eur Competition & Reg L Rev 116
[110] Witt (n 65)
[111] Pranvera Këllezi, 'Data protection and competition law: non-compliance as abuse of dominant position' [2019] sui-generis 343
[112] *Facebook v Bundeskartellamt* (n 101) para 71
[113] Małobęcka-Szwast (n 62)
[114] Małobęcka-Szwast (n 62)
[115] Witt (n 66)
[116] Dzhuliia Lypalo, 'Can Competition Protect Privacy? An Analysis Based on the German Facebook Case' (2021) 2 World Competition 169

The FCO approach can also be seen as establishing dominance "by object" without assessing *in concreto* the anti-competitive effects of the alleged violation. The default assumption of the interconnectedness of data protection breaches and anti-competitive behaviour is too far-reaching.[117] This conclusion can be confirmed by the *AstraZeneca* case, where the CJ stated that "the illegality of abusive conduct under Article 82 EC is unrelated to its compliance or non-compliance with other legal rules".[118] Therefore, Lypalo argued that violation of other rules can serve as a significant indicator but cannot be the sole ground for antitrust assessment.[119] Nonetheless, Körber rhetorically asked whether competition law should allow the doctrine of "competitive advantage through violation of the law".[120]

In terms of procedural economy, it was argued that the NCA should not investigate cases that fall within the competence of other authorities. Given the workload and limited resources, the NCA should only deal with matters strictly related to competition law to minimise the risk of inefficiency. Moreover, the FCO claimed to have cooperated with the German NSA, but so far, the NSA has not found a violation of the GDPR in Facebook case. This may raise doubts as to whether the cooperation was fruitful, and whether the NSA had anything to add to the proceedings.[121]

3.3. Conclusions

While the separatist approach rejects the possibility of evaluating data protection rules in antitrust proceedings, it does not imply an absolute rejection of privacy considerations. It rather indicates that "antitrust rules should be applied in pursuit of antitrust goals", with reflection on privacy matters. In parallel, the competent authorities should separately enforce data protection law.[122] The values enshrined in the privacy regime may provide interpretive guidance for NCAs when applying competition rules. Most proponents of separatism recognise privacy as a useful competitive factor in terms of product or service quality, but not as a goal of competition law *per se.*[123]

The separatist view, which advocates the "purity" of systems, is significantly disturbed by the integrationist theory, which proposes the direct application of the provisions on the protection of personal data. Such an approach is possible due to the broad definition of consumer welfare, which allows the concept to include various parameters.[124] The supporters of this doctrine argue

[117] ibid
[118] Case C-457/10P *AstraZeneca AB and AstraZeneca plc v European Commission* ECLI:EU:C:2012:770, para 132
[119] Lypalo (n 113)
[120] Torsten Körber, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law' [2018] NZKart <https://ssrn.com/abstract=3112232> accessed 25 April 2023
[121] Małobęcka-Szwast (n 62)
[122] Cadwalader, Wickersham & Taft LLP, 'European Union: No Such Thing As A Free Search: Antitrust And The Pursuit Of Privacy Goals' (*Mondaq,* 8 June 2015) <www.mondaq.com/unitedstates/antitrust-eu-competition-/403262/no-such-thing-as-a-free-search-antitrust-and-the-pursuit-of-privacy-goals> accessed 25 April 2023
[123] Ünekbaş (n 1)
[124] ibid

that competition law and data protection law safeguard the same values (such as market integration, protection of individuals or combating power asymmetries) by affecting economic activity, operating "at different ends of the same spectrum".[125] When circumstances characteristic for both systems occur (i.e. competition is based on data), these two realms must meet. Based on objectives and the subject matter of protection, perceived as common to both, the representatives of the integrationist approach conclude that data protection should be included in competition law. They seem to emphasize the centrality of the consumer in the system to facilitate the theory. According to the integrationists, if data subjects are natural persons, they can be also consumers, and subsequently, if data protection is relevant for consumer protection, it means that competition can enhance privacy to better protect the consumer.[126] These findings were also noticeable in the FCO decision.

Although the pioneer *German Facebook* decision is not free from legal flaws, as the comments show, it brings important issues to the table regarding the digital economy. In order to determine an abuse of dominance, the FCO used not only values enshrined by the GDPR but incorporated the legal act along with mechanisms provided for therein in the antitrust proceedings. In this way, the GDPR has become merely a means to achieve the objectives of competition law, namely privacy. This bold manoeuvre, which was for the benefit of consumers' welfare, calls into question the nature of the GDPR. The consequences of the application of the integrationist approach will be discussed in the next chapter.

[125] Francisco Costa-Cabral and Orla Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' [2017] Common Market Law Review 11

[126] ibid

4. The dual role of the GDPR

The integrationist approach tries to respond to the needs and challenges of the digital economy, answering the question of what should be the role of privacy in the application of competition law. The direct use of the GDPR as a tool for finding infringements of antitrust law creates a situation in which the legal act plays a dual role. It is no longer only a separate form of legislation but also a mechanism incorporated into other proceedings. The advantages and weaknesses of the theory will be analysed in this chapter.

4.1. Potential gaps in competition law that can be filled with data protection law (and vice versa)

Due to the "family ties", as Costa-Cabral and Lynskey called common objectives of data protection and competition law,[127] they can positively influence each other, and when applied together in a case, they provide a comprehensive assessment basis. According to Kerber "a separate application of competition law and data protection law will lead to suboptimal results".[128] In the literature, there is an emphasis on several reasons why the direct application of the GDPR may improve competition law enforcement and vice versa.

The "competition on privacy" has become a form of business in which undertakings willingly engage. As the assessment of the FCO showed, a quasi-monopoly position of a platform allows exercising power to harvest above-average amounts of data, which constitutes anti-competitive conduct. Since data are an integral part of this model, the GDPR can be a "normative benchmark" for antitrust law, which lacks precise tools to assess this aspect of data-driven companies.[129] In particular, the data protection assessment may alleviate uncertainties about "free" services, which are characteristic elements of data-oriented businesses and have so far caused interpretative doubts.[130] The traditional measurement methods proposed by the separatist proponents, who view privacy as only a qualitative aspect of service, are unsuitable for data-driven market. The *German Facebook* case indicated that the factual and legal situation created by the platform environment is complex – data are collected not only to improve the service or reduce its cost but also to attract advertisers and secure the market position of the undertaking. Moreover, Kerber and Zolna argued that „the direct analogy of excessive data-collection with excessive prices is difficult to make because due to the non-rivalrous character of data, consumers do not have less personal data after data-collection (and retain the right to share these data with others)".[131] Consumers do not "lose" in a classic monetary sense. Privacy is difficult to quantify, users may experience the same data practices differently, therefore

[127] ibid
[128] Wolfgang Kerber, 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law' (2022) 67(2) Antitrust Bulletin 280
[129] Costa-Cabral and Lynskey (n 122)
[130] ibid
[131] Wolfgang Kerber and Karsten Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (2022) 54 European Journal of Law and Economics 217

alternative analysis is required to assess consumer freedom on the digital market.[132] The GDPR can help to measure "the real cost of non-monetary pricing".[133]

Most importantly, in terms of consent, the GDPR provides better tools for examining user decisions (in particular, it offers extensive literature on voluntary consent or its withdrawal) than traditional competition law.[134] Using the GDPR as a normative point of reference can be significant for a consumer theory of harm. Since the data can serve as a means of payment, the consumer decision-making process became more complicated as the service recipients must evaluate the value of the data.[135] The difficulty can be reinforced by the *privacy paradox* or the simple imperfection of *homo oeconomicus.* If we look at the numbers, it turns out that 68% of Europeans are not aware of the value of their personal data and see certain categories of data (eg. behavioural) as less valuable or less deserving of protection.[136] Additionally, platforms collecting huge amounts of data can use them to manipulate consumers' preferences.[137] The situation is complicated because personal data, although commonly treated as a currency, is still the subject of fundamental protection. Thus, some authors argue that "the fundamental right of data protection should prevail over economic interests" in antitrust proceedings,[138] and that the former could serve as an external restrain which, for example, could prevent commitments in merger proceedings that impede the right.[139]

On the other hand, underenforcement, in particular vis-à-vis big tech companies, is a potential gap in the data protection system that can be remedied by competition law. Some authors considered the fact that the German NSA was not the first to find a violation of the GDPR as its ineffectiveness.[140] Insufficient enforcement may be related to increasing difficulties in distinguishing between data and personal data, which creates uncertainty as to whether the GDPR should be applied. In addition, the GDPR cannot address privacy concerns related to market structure that undermines consumer welfare,[141] as it "does not recognise the long-term harms to the platforms' users".[142] This grey area could be covered by competition law. Kerber and Zolna argued that if personal data protection is sufficiently enforced, undertakings will

[132] Beatriz Kira, Vikram Sinha and Sharmadha Srinivasan, 'Regulating digital ecosystems: bridging the gap between competition policy and data protection' (2021) 30 Industrial and Corporate Change 1337

[133] Giovanni Buttarelli, 'This is not an article on data protection and competition law' [2019] CPI Antitrust Chronicle

[134] Chun Sang Wong and Sze Lam Chan, 'At the Junction of Consumer Protection: Dual Role of Data Protection in EU Law' (2021) 6(2) London School of Economics Law Review 109

[135] Wolfgang Kerber and Louisa Specht-Riemenschneider, 'Synergies Between Data Protection Law and Competition Law. Report for the German consumer association Verbraucherzentrale Bundesverband' (2022) 30 <www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf> accessed 9 May 2023

[136] EOS, 'What's the value of data?' (2020) <https://pl.eos-solutions.com/pl/dam/jcr:055985a9-dda5-4718-90fd-73159a71c1dc/EOS%20survey%20What&%23039;s%20the%20value%20of%20data.pdf?nameFrom=8eb82626-073f-434c-8389-c006f1432d0b> accessed 9 May 2023

[137] Wong and Chan (n 131)

[138] ibid

[139] Costa-Cabral and Lynskey (n 122)

[140] Kerber and Specht-Riemenschneider (n 132) 26

[141] Wong and Chan (n 131)

[142] Arletta Gorecka, 'Competition law and privacy: extensive data acquisition as the "eye" of the problem' [2023] Network Law Review <www.networklawreview.org/phd-privacy/> accessed 4 May 2023

restrict data processing to avoid risks, and thus "in well-functioning markets, a higher level of privacy protection can be expected than what the minimum standards of the GDPR require".[143] In practice, the stricter sanctions offered by competition law may significantly support GDPR enforcement. While the GDPR limits sanctions to 4% of the total worldwide annual turnover of the preceding financial year,[144] competition law sanctions are up to 10% of the total turnover of the corporate group in the preceding business year.[145] In addition, competition law offers behavioural remedies. This can be a strategic advantage, enhancing the deterrent effect.[146] Increased limits could be significant in cases involving big-tech giants, operating with huge resources, and for which the sums calculated in accordance with the GDPR may be only "petty cash".[147] While fines imposed under competition law are counted in billions, those applied for violations of personal data protection regulation amount to merely millions – the highest penalty imposed based on the GDPR was "only" €746 million in the Amazon case.[148]

In the broader context of the EU objectives, the common application of the GDPR and competition law can further facilitate market integration. Both systems were introduced to provide substantive and procedural harmonisation, which should improve consumer welfare.[149] The synergy between these two fields of law can be of particular importance for the emergence and development of the Digital Single Market, which inevitably requires effective enforcement of both systems. In fact, the EDPS has already called for the creation of a "Digital Clearing House", the activities of which would include identifying synergies between competition and privacy and discussing "theories of harm" using data protection standards. The network would be a space of cooperation between authorities responsible for the digital sector to provide "coherent enforcement of digital rights".[150]

4.2. Disadvantages of using the GDPR as the legal basis for finding a violation of competition law

Although some aspects indicate that the direct application of the GDPR in antitrust proceedings is a "win-win situation", the approach is associated with certain problems. First, it has been noted that enforcement of competition law and data protection law provide different outcomes. The former aims to prevent economic harm, which negatively influences consumer welfare or efficiency (by taking into account aspects such as price, quality or innovation), whereas the latter intends to cover also additional objectives. Data protection rules are designed to prevent violation of fundamental rights, including the right to privacy, non-discrimination or freedom of expression and information. Therefore, in some cases, it is possible that the objectives of

[143] Kerber and Zolna (n 128)
[144] Article 83 GDPR
[145] Article 23 Regulation 1/2003
[146] Wong and Chan (n 131)
[147] Körber (n 117)
[148] Niall McCarthy, 'The Biggest GDPR Fines of 2022' (EQS Group, 31 January 2023) <https://www.eqs.com/compliance-blog/biggest-gdpr-fines/> accessed 5 May 2023
[149] Costa-Cabral and Lynskey (n 122)
[150] EDPS (n 53)

competition law will not fully overlap with the principles of data protection.[151] It creates the risk that certain values of the GDPR could be omitted. Evaluation of privacy through the prism of competition could "flatten" the objectives of the data protection law, and consequently significantly affect the sense of the regulation.

Second, the GDPR controls the characteristics of a product or service – it affects its design, which should provide the data subject with a real and free choice as to whether to give or withdraw consent. It influences a "technical" side of a business, which policies should be adjusted to the requirements of the GDPR. On the other hand, competition law does not aim to determine the specifications of a good or to increase its quantity on the market. In traditional competition law, the assessment of the consumer's choice appears only in the context of the delimitation of the relevant market, in particular as a criterion of substitutability of different products.[152]

Third, the GDPR and Regulation 1/2003 introduce different sanctions that were created to serve different purposes. Various types of non-compliance were assigned to separate penalties to provide a logical and credible structure for the systems. Sanctions cannot be treated interchangeably as it undermines legal certainty and increases the risk of instrumental treatment of the law. This practice could extend the responsibility of undertakings. Moreover, it is not clear if the imposition of fines would be limited to a one-off competition procedure, or whether further fines could be imposed by the NSA, which retains competence in all matters relating to the GDPR. This ambiguity is liable to jeopardise the principle of *ne bis in idem,* according to which no one shall be subject to various procedures or be punished multiple times for the same act.

Fourth, when an infringement of the GDPR becomes a *per se* violation of competition law assessed on the basis of another system, the regulation loses its character. Including dominance in the assessment of the GDPR disturbs the mechanisms provided for therein. Evaluation of the consent or other justifications, within the meaning of privacy rules, should not include aspects such as the availability of other products or the structure of the market, thus dominance is an irrelevant factor. Moreover, by the "imbalance", referred to by the FCO, the GDPR means rather contractual dependencies between parties, for instance, relationships such as employment or subordination to public authority. The imbalance between the collector and the data subject cannot be removed by eliminating the dominant position. If it were the other way around and dominance affected consent, dominant undertakings could never use it as a justification for data processing.[153] Therefore, applying the competition law criteria, there is a risk of misinterpretation of the mechanisms provided for in the GDPR.

Fifth, as indicated in Chapter 2.2, in theory, the GDPR safeguards both rights of the data subject and the free movement of data within the internal market, however, in practice, these objectives remain unbalanced. The emergence of Big Data creates difficulties in distinguishing personal

[151] Costa-Cabral and Lynskey (n 122)
[152] Këllezi (n 108)
[153] Këllezi (n 108)

data from data, distorting the scope of the GDPR. It may significantly limit data flows and the development of Big Data, which is a crucial factor for the development of data-driven companies and innovation. Therefore, data protection law might prove to be an obstacle to competition.[154] The question then arises as to why competition law should enforce the rules, which promote objectives contrary to those pursued by competition law. Innovation, efficiency and improvement of products and services should be reinforced by antitrust law, not obstructed.

Finally, all the above aspects contribute to the lack of legal certainty. According to the CJ, the law ought to be "clear, precise and predictable as regards their effects, in particular where they may have unfavourable consequences for individuals and undertakings".[155] The uncertainty is also further deepened by a distortion of the division of powers between authorities.

4.3.Division of competences

It is indisputable that authorities should operate within the limits and on the basis of the law, which should provide a clear division of power. Some authors argue that by issuing the *German Facebook* decision, the FCO went "far beyond the limits of its legal competence".[156] In Këllezi's opinion, the integrationist approach "significantly expands the powers of competition authorities" through the application of fundamental rights.[157] The same can happen with other imperative standards that could be used as a basis for intervention. Consequently, the "special responsibility" of an undertaking in a dominant position would extend to non-competition issues indefinitely.[158] In the context of extending boundaries, Körber also drew attention to the risk of political instrumentalization of competition law, which has so far been minimised by focusing solely on competition protection.[159]

Furthermore, enforcement of the GDPR was designed as a "one-stop-shop", which indicates that all violations should be dealt with by only one NSA, according to the main establishment of a controller or processor.[160] As stated by the EDPB, the "mechanism is designed to reduce the administrative burden for organisations and make it simpler for individuals to exercise their rights from their home base".[161] If some of the GDPR enforcement powers were transferred to the NCAs, this convenience would lose its importance, which could undermine the protection of data subjects.

---

[154] Körber (n 117)

[155] Case C-72/10 *Criminal proceedings against Marcello Costa and Ugo Cifone* [2012] ECLI:EU:C:2012:80, para 74

[156] Giuseppe Colangelo and Mariateresa Maggiolino 'Antitrust über alles. Whither competition law after Facebook?' [2019] World Competition Law and Economics Review

[157] Këllezi (n 108)

[158] ibid

[159] Körber (n 117)

[160] Kerber and Specht-Riemenschneider (n 132) 108

[161] EDPB, 'One-Stop-Shop Leaflet' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_en> accessed 4 May 2023

AG Rantos seems to support the “self-proclaimed” authorities, allowing them to examine privacy matters if necessary. However, it is not clear when the need is so urgent that the NCAs can overstep the bounds of the law. This approach creates the risk that the NCAs would consider themselves competent to “incidentally” assess any matter. When the matter was within the scope of competence of both authorities, this “tacit permission” to act may cause a dispute about which body should exercise its power in the first place.[162] Without a legal framework allowing competition authorities to take a step further, the direct application of norms falling outside the scope of competition law will always be vague and threaten the rule of law.

4.4. Conclusions

The strict separation of the systems seems to be inadequate for the actual economic situation. Given the specificity of the digital economy and the rapidly growing importance of data, the idea of incorporating the provisions of personal data protection in competition law is not an unfounded proposal. The GDPR can provide a normative point of reference to supplement assessment in antitrust proceedings, which lacks certain tools to examine the conduct of data-driven undertakings. Kira et al. aptly commented that “creating a new framework for competition assessment of digital platforms would be ‘reinventing the wheel’”, thus data protection framework could be directly applied to provide “off-the-shelf” methods.[163] The integrationist approach might enhance the protection of consumers’ welfare and facilitate the development of the Digital Single Market. It may become a solution to efficiently address newly emerging issues in the digital market, strengthening the role of competition law and data protection law. The benefits of synergy are noticeable for both systems.

Nonetheless, the integrationist theory is fraught with many risks. As Körber brutally stated “competition law is not a universal tool for solving of all society’s ills”,[164] which is a reasonable statement, given the doubts associated with the integrationist theory. The discussed approach may cause damage to both systems, negatively affecting their structures, methods, and the competent authorities' power limits. A great number of questions, which the new approach brings, point to its flaws. At the same time, the integration of systems has potential, which could be used on a large scale. The next chapter will present intermediate *de lege ferenda* solutions concerning the methods of implementing the integrationist theory into the practice of EU law.

[162] Miriam Caroline Buiten, ‘Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law’ (2021) 9 Journal of Antitrust Enforcement 270
[163] Kira, Sinha and Srinivasan (n 129)
[164] Körber (n 117)

5. Possible solutions to the problem of overlapping competition law and data protection law

It seems that in the EU a strictly separatist approach is gradually relaxed. However, the Commission does not consider data protection issues to be a competition law concern, it notes the importance of privacy for consumers. This may signal the opportunity for the integrationist theory to be introduced into the EU decisional practice, which some accused of promoting "antitrust orthodoxy".[165] As the right to data protection is the fundamental right, Graef noted that, according to Article 51 (1) EUCFR, the EU institutions and the Member States have "a negative duty to respect the right to data protection and a positive duty to promote the application of the right to data protection".[166] Therefore, some authors present intermediate solutions for integrating the two systems within the EU structures to address privacy issues in the framework of competition policy.

Since cooperation between the NCAs and the NSAs has so far been rare and, as the *German Facebook* case showed, full of doubts, there are discussions about its strengthening. Kerber suggested the creation of space where "interdisciplinary cooperation between legal, economic, and tech experts" would be possible. The author argues that only a multidisciplinary approach created by a joint body can provide a common and comprehensive understanding of how to tackle problems created by the digital economy. The forum would be a space to coordinate in-depth research about the role of fundamental rights, and the potential effect of combining competition law and data protection law. The author believes that analysis and full understanding of the dependencies and challenges may facilitate the "appropriate division of labour".[167] This viewpoint seems particularly justified given the need to reduce the workload in the Commission and the NCAs[168], thereby enforcing the principle of procedural economy, which requires judicious use of available resources.

As mentioned in Chapter 4.1, the proposed holistic vision was also advocated by the EDPS, and in 2017 approved by the European Parliament, which established the Digital Clearinghouse as "a *voluntary* network of enforcement bodies".[169] The beginnings of the Digital Clearinghouse were promising – according to available sources, meetings of regulatory authorities were held regularly until 2020, but there is no information about cooperation in subsequent years.[170] This may suggest a weakness in the network, which is an ineffective tool to provide a firm

---

[165] Gregory Crawford, Johnny Ryan and Cristina Caffarra, 'The antitrust orthodoxy is blind to real data harms' (*VoxEU Centre for Economic Policy Research*, 22 April 2021) <https://cepr.org/voxeu/blogs-and-reviews/antitrust-orthodoxy-blind-real-data-harms> accessed 7 May 2023

[166] Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (vol. 68, Kluwer Law International 2016) 340

[167] Kerber (n 125)

[168] See: European Court of Auditors, 'The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight' (2020) <https://op.europa.eu/webpub/eca/special-reports/eu-competition-24-2020/en/> accessed 7 May 2023

[169] European Parliament, 'Report A8-0044/2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement' (2017)

[170] EDPS, 'Big Data & Digital Clearinghouse' <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en> accessed 7 May 2023

framework for systems integration. Perhaps more *mandatory* cooperation should be introduced. Subsequently, the lesson learned from enhanced cooperation could be applied in the legislative and policy-making processes. According to Kerber, sector-specific legislation could be introduced, combining consumer, data protection and competition law rules and remedies to cover all identified issues.[171]

Taking into account the interdisciplinarity of cases emerging within the digital market, it might be beneficial to introduce some more radical changes in the systems. The example of Digital Clearinghouse shows that the creation of the forum is an inefficient solution, as the cooperation has no framework. Moreover, cases concerning digital challenges continue to be dealt with by separate authorities, whose activities are not coordinated. It might still lead to situations similar to that presented in the *German Facebook* case, which are not desirable from the point of view of legal certainty.

Perhaps the time has come to create a new body combining the features of an NCA and an NSA, which would be entitled to use the tools provided for in competition law and data protection law. The competence of the authority would be assigned to selected sectors of the internal market, where big-tech giants, in particular platforms, operate. It should be ensured that the authority is represented by experts from various fields, not only economists and data protection officers but also IT specialists dealing with AI, algorithms, and Big Data. Considering the changes in consumer behaviour, the involvement of sociologists or psychologists should not be ruled out. These specialists could bring valuable insight into the theory of harm, which is gradually evolving in a less economically oriented direction. With appropriate expert support, the authority would be able to comprehensively assess privacy issues.

A structure similar to the one described above can be found in Article 40 DMA, which could serve as a benchmark for the creation of the new body dealing with digital challenges. According to the DMA, the Commission shall create the High-Level Group composed of various experts from five different bodies and networks whose activities are related to the digital market. The group includes professionals from the Body of the European Regulators for Electronic Communications, the EDPS, the EDPB, the ECN, the Consumer Protection Cooperation Network, and the European Regulatory Group of Audiovisual Media Regulators. The High-Level Group will ensure that "the DMA and other sectoral regulations applicable to gatekeepers are implemented in a coherent and complementary manner". However, at this point, the group's activities are scheduled for only two years, and the group is closely linked to the Commission, which is the only body that can consult it.[172]

As a side note, it is worth mentioning that DMA directly refers to the concepts introduced by the GDPR, such as "profiling" or "consent".[173] These terms are used to define gatekeepers'

---

[171] Kerber (n 125)

[172] Commission, 'Press Release: Digital Markets Act: Commission creates High-Level Group to provide advice and expertise in implementation' (2023) <https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-creates-high-level-group-provide-advice-and-expertise-implementation> accessed 20 May 2023

[173] Article 2 (32) and (33) DMA

obligations, inter alia, vis-à-vis end-users. This may suggest that the DMA incorporates the GDPR tools to assess several aspects of the functioning of the gatekeepers, such as the use of personal data collected on third-party websites to provide online advertising services[174] or combining personal data acquired from different sources.[175] These activities are prohibited unless consent is given. The obligations seem to resemble those of the *German Facebook* case, which may further enhance the impression that the DMA is strengthening the integration of data protection law and competition law.

Nevertheless, a direct application of the GDPR should be reconsidered, as the mere creation of the new body will not solve all the challenges presented before. It may be necessary to introduce a separate legal act adapted to the realities of dominant undertakings. As research shows, aspects such as dominance, market structure or the theory of harm are currently not compatible with the mechanisms provided for in the GDPR. A new form of assessment could be established to allow for an analysis more adapted to the conditions of the digital market, which would be suitable to evaluate conditions under which consent was given. Moreover, a uniform system of sanctions should be reviewed. It is apparent that penalties introduced by the GDPR are ineffective, thus the application of competition law sanctions should take the lead in order to achieve a deterrent effect. The creation of the body could help eliminate uncertainties about the division of power between existing authorities, facilitate the enforcement of fundamental rights and support the sustainable development of the Digital Single Market.

[174] Article 5 (2) (a) DMA
[175] Article 5 (2) (b) DMA

Conclusions

This paper has illustrated the new economic environment that facilitated the emergence of data-driven companies. The phenomena such as network effects, economies of scale, multi sidedness are characteristic elements of the functioning of platforms in the digital economy. Datafication, automatization and networking are one of the effects of the development of the digital market, where data are important materials. The novelty has created new competition law challenges that cannot be solved solely by a single body of law. The economic background of the digital market explains the reasons for the interaction between antitrust law and data protection law.

Further, the competition and data protection law structures have been presented to show the objectives, scopes of protection, and enforcement mechanisms. The goals of competition law demonstrate to be adaptable so that privacy can be perceived as an area where the scopes of the systems intersect. In addition, the changing perception of concepts such as personal data and the consumer affects the frameworks of competition law and data protection law. Finally, these findings were then compared to the overall objectives pursued by the EU policies, in particular with regard to the Digital Single Market, which requires interdisciplinary cooperation. It may suggest that the legal framework created by the EU enhances interactions between competition law and data protection law.

At the centre of the paper, two opposing approaches towards the relationship between competition law and data protection law have been presented. The separatist theory, derived from the *Asnef-Equifax* case, requires data protection issues to be analysed solely by NSAs. This point of view is noticeable in the jurisprudence of the CJEU and the decisional practice of the Commission. On the other hand, the *German Facebook* case gave rise to the integrationist approach. In a decision that found Facebook to be abusing its dominant position in Germany, the FCO applied the GDPR as a normative point of reference in the course of competition assessment. The direct application of the GDPR was an innovative solution, which seems to be a remedy for the digital challenges created by the digital economy. The theory can potentially strengthen the enforcement of both antitrust and data protection laws. However, it is not perfect and the dangers of such an approach were discussed. In addition, the last chapter of the paper contained a brief look at the solutions to the problem of overlapping systems.

It is indisputable that both competition law and data protection law face challenges due to the development of the digital economy. Platforms, as "children of the Fourth Revolution", create atypical, multidisciplinary problems that have never occurred before. It is natural, however, that changes bring with them novelties, the full understanding of which takes time. Perfect solutions cannot be expected to be introduced immediately, however, innovations should be studied and gradually implemented. The analysis shows that competition law and data protection law do not operate in a vacuum, they react with each other due to the new digital environment, and careful separation is no longer adequate. Therefore, new opportunities must be considered. The integrationist approach can provide answers to privacy concerns under competition law. The

decision of the FCO is particularly beneficial from the point of view of consumers who do not pay but somehow lose. It is therefore important to find a solution to these unfair conditions.

However, the theory poses various risks to the consistency of both systems. The analysis of advantages and disadvantages shows clearly that the use of the GDPR as a normative benchmark has great potential, but some limitations need to be developed. Care must be taken to ensure that antitrust authorities will not become universal bodies to resolve all legal issues that are loosely related to the functioning of the internal market. Potential negative consequences of degrading the importance of the GDPR and its tools should also be considered. The CJ will face a great challenge in answering the DHRC questions. It must scrutinize gains and losses to find a balance between the separation and integration of the systems. Nevertheless, it would be favourable for both competition and consumers to increase the importance of privacy within competition law and provide the NCAs with the necessary tools to investigate this aspect.

Bibliography

Books

1. Bukht R and Heeks R, *Defining, Conceptualising and Measuring the Digital Economy* (Centre for Development Informatic Global Development Institute SEED 2017)
2. Graef I, *EU competition law, data protection and online platforms data as essential facility* (Kluwer Competition Law 2016)
3. Krzysztofek M, *GDPR: Personal Data Protection in the European Union* (Wolters Kluwer Law International 2021)
4. Śledziewska K and Włoch R, *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat* (Wydawnictwo Uniwersytetu Warszawskiego 2020)
5. Śledziewska K and Włoch R, *The Economics of Digital Transformation. The Disruption of Markets, Production, Consumption, and Work* (Routledge 2021)
6. van der Sloot B, *Health Data Privacy under the GDPR* (Routledge 2020)
7. Zuboff S, *The Age of Surveillance Capitalism* (Profile Books 2019)

Articles

8. Athey S, Catalini C and Tucker C, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' [2018] Stanford University Graduate School of Business 1
9. Becher C, 'A Closer Look at the FCO's Facebook Decision' (2019) 3 Eur Competition & Reg L Rev 116
10. Brzezicka J and Wisniewski R, 'Homo Oeconomicus and Behavioral Economics' (2014) 8 Contemporary Economics 353
11. Buiten M.C, 'Exploitative Abuses in Digital Markets: Between Competition Law and Data Protection Law' (2021) 9 Journal of Antitrust Enforcement 270
12. Buttarelli G, 'This is not an article on data protection and competition law' [2019] CPI Antitrust Chronicle
13. Chen L, Huang Y, Ouyang S and Xiong W, 'Data Privacy and Digital Demand' [2021] <http://wxiong.mycpanel.princeton.edu/papers/Privacy_Paradox.pdf> accessed 10 April 2023
14. Colangelo G and Maggiolino M, 'Antitrust über alles. Whither competition law after Facebook?' [2019] World Competition Law and Economics Review
15. Costa-Cabral R and Lynskey O, 'Family ties: the intersection between data protection and competition in EU Law' [2017] Common Market Law Review 11
16. Donnelly S and Sophister S, 'Homo Oeconomicus: Useful Abstraction or Perversion of Reality?' (2018) 32 Student Economic Review 95
17. Goldhar J.D and Jelinek M, 'Plan for Economies of Scope' [1993] Harvard Business Review <https://hbr.org/1983/11/plan-for-economies-of-scope> accessed 5 April 2023
18. Gorecka A, 'Competition law and privacy: extensive data acquisition as the "eye" of the problem' [2023] Network Law Review <www.networklawreview.org/phd-privacy/> accessed 4 May 2023
19. Hüschelrath K and Peyer S, 'Public and Private Enforcement of Competition Law: A Differentiated Approach' (2013) 36 World Competition 585

20. Këllezi P, ‘Data protection and competition law: non-compliance as abuse of dominant position’ [2019] sui-generis 343
21. Kerber W and Zolna K, ‘The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law’ (2022) 54 European Journal of Law and Economics 217
22. Kerber W, ‘Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law’ (2022) 67(2) Antitrust Bulletin 280
23. Kira B, Sinha V and Srinivasan S, ‘Regulating digital ecosystems: bridging the gap between competition policy and data protection’ (2021) 30 Industrial and Corporate Change 1337
24. Körber T, ‘Is Knowledge (Market) Power? On the Relationship between Data Protection, “Data Power” and Competition Law’ [2018] NZKart <https://ssrn.com/abstract=3112232> accessed 25 April 2023
25. Lypalo D, ‘Can Competition Protect Privacy? An Analysis Based on the German Facebook Case’ (2021) 2 World Competition 169
26. Madill J and Mexis A, ‘Consumers at the heart of EU competition policy’ [2009] Competition Policy Newsletter 27
27. Małobęcka-Szwast I, ‘Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi’ (2018) 8 IKAR 139
28. Muzellec L, Ronteau S and Lambkin M, ‘Two-sided Internet platforms: A business model lifecycle perspective’ (2015) 45 Industrial Marketing Management 139
29. Smits J.M, ‘What is legal doctrine? On the aims and methods of legal-dogmatic research’, [2017] Rethinking Legal Scholarship: A Transatlantic Dialogue, New York [Cambridge University Press]
30. Stylianou K and Iacovides M, ‘The goals of EU competition law: a comprehensive empirical investigation’ [2022] Cambridge University Press 620
31. Ünekbaş S, ‘Competition, Privacy, and Justifications: Invoking Privacy to Justify Abusive Conduct under Article 102 TFEU’ [2022] Journal of Law, Market & Innovation <http://dx.doi.org/10.2139/ssrn.4094990> accessed 25 April 2023
32. Witt A.C, ‘Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case’ (2021) 66(2) The Antitrust Bulletin 276
33. Wong C.S and Chan S.L, ‘At the Junction of Consumer Protection: Dual Role of Data Protection in EU Law’ (2021) 6(2) London School of Economics Law Review 109
34. Zarsky T.Z, ‘Incompatible: The GDPR in the Age of Big Data’ (2017) 47 Seton Hall Law Review 995

Legislation

35. Council Regulation (EC) 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
36. Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market [2018] OJ L 11/3
37. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

38. Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
39. Treaty on the European Union
40. Treaty on the Functioning of the European Union

Decisions by the CJEU

41. Case C-235/08 *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios* [2006] ECLI:EU:C:2006:734
42. Case C-41/90 *Klaus Höfner and Fritz Elser v Macrotron GmbH* [1991] EU:C:1991:161
43. Case C-457/10P *AstraZeneca AB and AstraZeneca plc v European Commission* ECLI:EU:C:2012:770
44. Case C-72/10 *Criminal proceedings against Marcello Costa and Ugo Cifone* [2012] ECLI:EU:C:2012:80
45. Case C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV* [2022] ECLI:EU:C:2022:322

Other decisions

46. *Facebook/WhatsApp* (Case No COMP/M.7217) Commission Decision 32014M7217 [2014]
47. FCO, Decision of 6 February 2019, B6-22/16 (*German Facebook* Decision)
48. DHRC, Decision of 26 August 2019, VI-Kart 1/19 (V) (*Facebook v Bundeskartellamt)*
49. FCJ, Decision of 23 June 2020, KVR 69/19 (*Facebook v Bundeskartellamt)*
50. Case C-252/21 *Facebook Deutschland GmbH v Bundeskartellamt* [2021] OJ C320/16, Request for a preliminary ruling from the DHCR

AG Opinions

51. Case C-252/21 *Facebook Deutschland GmbH v Bundeskartellamt* [2022] ECLI:EU:C:2022:704, Opinion of AG Rantos
52. Case C-475/99, *Firma Ambulanz Glöckner v Landkreis Südwestpfalz* [2001] EU:C:2001:577, Opinion of AG Jacobs

Other sources

53. 'What is Artificial Intelligence? Machine Learning and Deep Learning' (*Amazon Web Services*) <https://aws.amazon.com/machine-learning/what-is-ai/> accessed 4 April 2023
54. APEC, 'APEC Economic Policy Report 2019: Structural Reform and the Digital Economy' (APEC Secretariat 2019) <www.apec.org/docs/default-source/Publications/2019 /11/2019-APEC-Economic-Policy-Report/2019-AEPR---Full-Report.pdf> accessed 3 April 2023
55. Body for European Regulators for Electronic Communication, 'BEREC Report on the Data Economy' (BEREC, 2019) <www.berec.europa.eu/sites/default/files/files/document_

register_store/2019/6/BoR_%2819%29_106_BEREC_Report_on_the_Data_Economy.pdf > accessed 5 April 2023

56. Cadwalader, Wickersham & Taft LLP, 'European Union: No Such Thing As A Free Search: Antitrust And The Pursuit Of Privacy Goals' (*Mondaq*, 8 June 2015) <www.mondaq.com/unitedstates/antitrust-eu-competition-/403262/no-such-thing-as-a-free-search-antitrust-and-the-pursuit-of-privacy-goals> accessed 25 April 2023
57. Collins Dictionary <www.collinsdictionary.com/submission/7418/DATA+EXHAUST> accessed 3 April 2023
58. Commission, 'Press Release: Digital Markets Act: Commission creates High-Level Group to provide advice and expertise in implementation' (2023) < https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-creates-high-level-group-provide-advice-and-expertise-implementation> accessed 20 May 2023
59. Crawford G, Ryan J and Caffarra C, 'The antitrust orthodoxy is blind to real data harms' (*VoxEU Centre for Economic Policy Research*, 22 April 2021) <https://cepr.org/voxeu/blogs-and-reviews/antitrust-orthodoxy-blind-real-data-harms> accessed 7 May 2023
60. EDPB, 'One-Stop-Shop Leaflet' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_en> accessed 4 May 2023
61. EDPS, 'Big Data & Digital Clearinghouse' <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en> accessed 7 May 2023
62. EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data [2016]
63. EOS, 'What's the value of data?' [2020] <https://pl.eos-solutions.com/pl/dam/jcr:055985a9-dda5-4718-90fd-73159a71c1dc/EOS%20survey%20What&%23039;s%20the%20value%20of%20data.pdf?nameFrom=8eb82626-073f-434c-8389-c006f1432d0b> accessed 9 May 2023
64. EU Digital Single Market <https://eufordigital.eu/discover-eu/eu-digital-single-market/> accessed 10 April 2023
65. European Court of Auditors, 'The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight' (2020) <https://op.europa.eu/webpub/eca/special-reports/eu-competition-24-2020/en/> accessed 7 May 2023
66. European Parliament, 'BRIEFING EU policies – Delivering for citizens. Protecting European consumers' (European Parliament, 2019) <https://what-europe-does-for-me.eu/data/pdf/focus/focus22_en.pdf> accessed 7 April 2023
67. European Parliament, 'Challenges for Competition Policy in a Digitalised Economy' (European Parliament, 2015) <www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU(2015)542235_EN.pdf> accessed 3 April 2023
68. European Parliament, 'Report A8-0044/2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement' (2017)
69. FCO, 'Background information on the Facebook proceeding' (2017) <www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6> accessed 18 April 2023

70. IMF, ‘Measuring the Digital Economy’ (International Monetary Fund 2018) <www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy> accessed 3 April 2023
71. Kerber W and Specht-Riemenschneider L, ‘Synergies Between Data Protection Law and Competition Law. Report for the German consumer association Verbraucherzentrale Bundesverband’ (2022) <www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_SpechtRiemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf> accessed 9 May 2023
72. Kroes N, ‘Consumers at the heart of EU Competition Policy’ (Address at BEUC dinner, The European Consumers' Association, 22 April 2008) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_08_212> accessed 6 April 2023
73. Kuneva M, ‘European Consumer Commissioner Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling’ (Roundtable on Online Data Collection, Targeting and Profiling, European Commission, 31 March 2009) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156> accessed 4 April 2023
74. McCarthy N, ‘The Biggest GDPR Fines of 2022’ (EQS Group, 31 January 2023) <https://www.eqs.com/compliance-blog/biggest-gdpr-fines/> accessed 5 May 2023
75. OECD, ‘Abuse of Dominance in Digital Markets’ (OECD, 2020) <www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf> accessed 5 April 2023
76. OECD, ‘Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report’ (OECD Publishing 2015) <http://dx.doi.org/10.1787/9789264241046-en> accessed 3 April 2023
77. OECD, ‘An Introduction to Online Platforms and Their Role in the Digital Transformation’ (OECD Publishing, 2019) <https://doi.org/10.1787/53e5f593-en> accessed 5 April 2023
78. OECD, ‘Big Data: Bringing Competition Policy to the Digital Era’ (OECD Secretariat 2016) <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> accessed 4 April 2023
79. OECD, ‘OECD Digital Economy Outlook 2015’ (OECD Publishing 2015) <http://dx.doi.org/10.1787/9789264232440-en> accessed 3 April 2023
80. Parenti R, ‘Competition policy’ (Fact Sheets on the European Union 2022) <www.europarl.europa.eu/factsheets/en/sheet/82/competition-policy> accessed 5 April 2023
81. Petrosyan A, ‘Number of internet and social media users worldwide as of January 2023’ (*Statista*, 23 February 2023) <www.statista.com/statistics/617136/digital-population-worldwide/> accessed 3 April 2023
82. Santos R, ‘What is datafication and why it is the future of business’ (Airswift, 15 September 2022) <www.airswift.com/blog/datafication> accessed 5 April 2023
83. Statista Research Department, ‘Forecast about the development of the world population from 2022 to 2100’ (Statista, 23 August 2022) <www.statista.com/statistics/262618/forecast-about-the-development-of-the-world-population/> accessed 1 April 2023

84. Tarnoff B, ‘How the Internet was invented’ *The Guardian* (London, 25 July 2016) <https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf> accessed 3 April 2023
85. White A, Bodoni S and Nicola S, ‘Facebook's Data-Sharing Plans Threatened by New Rules in Germany’ *Bloomberg* (2 July 2019)