6. Conceptualising the interrelation between data protection regulation and competition law

Alessia Sophia D'Amico

1. INTRODUCTION

Big data has revolutionised the landscape of information technology, carrying profound implications for the digital economy. For digital consumers,[1] the increased value of data signifies the possibility to trade their personal information against digital services and content, transforming it into a commodity.[2] However, the peculiarity of big data and the way it obtains its value make it difficult for consumers to make informed decisions in relation to the terms under which they disclose their personal information.[3] Multiple facets of the big data market contribute to consumers' lack of control, including information asymmetries, consumers' cognitive biases and market concentration.[4] As a result of these, the market is tilted in favour of internet companies, which are in a position to process more personal data than would be the case, had data subjects more control over it.[5]

In light of the fact that the developments of the digital market do not give us reason to believe that this market failure will correct itself,[6] the dynamics of data collection and utilisation call for a renewed analysis of the legal tools designed to guarantee the sound functioning of this market. These tools should ensure that consumers can make informed choices about

[1] In this chapter, the terms '(digital) consumers' and 'data subjects' are used interchangeably because the chapter focuses on a market failure that affects individuals as consumers and data subjects simultaneously. As explained in the first part of the chapter, in the digital market, personal data acquires a commercial value, meaning that individuals have an interest in it, not only from a fundamental rights perspective, as data subjects, but also from an economic perspective, as consumers. Although, the terms 'consumers' and 'data subjects' are distinct and, respectively, belong to the areas of competition law and data protection regulation, when it comes to the digital market these regimes are partially interconnected and can affect individuals' interests as consumers and data subjects at the same time.

[2] David S. Evans, 'The Antitrust Economics of Free' (2011) 555 Univ. of Chicago John M. Olin Law & Econ., Working Paper.

[3] See Katherine J. Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) University of Chicago Legal Forum 95; Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behaviour in the Age of Information' (2015) 247(6221) *Science*.

[4] See Andrea Carignania and Vanessa Gemmo 'New Media and Privacy the Privacy Paradox in the Digital World: I Will Not Disclose My Data. Actually, I Will ... It Depends' (2017) 27(1) *International Journal of Computer* 201; Christophe Lazaro and Daniel Le Metayer, 'Control over Personal Data: True Remedy or Fairy Tale' SCRIPT-ed, Vol. 12, No. 1, June 2015; Dan Ariely, 'Predictably Irrational' (Harper 2010); Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer law and Data Protection' (2016) 11(11) *Journal of Intellectual Property Law & Practice* 860.

[5] Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) 40(2) *William Mitchell Law Review*, Article 12.

[6] Stucke and Grunes, *Big Data and Competition Policy* (OUP 2016); Joseph Farrell, 'Can Privacy Be Just Another Good?' (2012) 10 *Journal on Telecomm. & High Tech. L* 251.

data protection terms and that the market offers options for them to choose from. There is no specific regulatory framework covering all aspects of this market failure; the issue is approached from different angles by distinct regulatory regimes. Since the General Data Protection Regulation (GDPR)[7] is specifically designed to deal with the problem of lack of individuals' control over personal data, it is generally treated as the first avenue of recourse. The role of data protection regulation is, among other things, to safeguard individuals' control over data, by correcting power and information asymmetries between digital companies and individuals.[8] However, the GDPR does not consider to what extent market power can affect individuals' interests, which falls under the scope of competition law instead. Competition law is devised to safeguard the competitive process and protect consumers' economic interests, by preventing the illegitimate exercise of market power.[9] Accordingly, while data protection regulation promotes individuals' ability to choose how much data they are willing to disclose and under what conditions, competition law protects the availability of options in the market and ensures that consumers can in fact exercise their choices.

Having been prompted by the developments in the digital market that gave data its key role, the interrelation between the two regimes in the regulatory landscape has not been defined by the lawmakers and has only been briefly touched upon by the courts. In *Asnef-Equifax* for example, the European Court of Justice (CJEU) stated that any issues relating to the sensitivity of personal data are not, as such, a matter for competition law, but may be resolved on the basis of the relevant provisions governing data protection.[10] In the literature, different dimensions of the interrelation have been discussed, but a comprehensive assessment of the interrelation is missing.[11]

---

[7] 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) [2016] OJ L119/1. In the EU, the GDPR represents the core of the EU data protection regulatory regime.

[8] It shall be noted that the GDPR's approach is one that seeks to empower individuals to take decision regarding their data. As explained by Clifford:

> Data protection aims to rebalance the inherent asymmetries through the application of notions such as informed data subject consent and data subject rights in order to provide protections, empower individuals and enhance decision-making capacity. In the information society services (ISS) context, through the application of such data subject orientated protections or 'micro-rights', individuals are positioned as the key actors and are empowered to make decisions regarding their personal data.

Damian Clifford, 'Data Protection and Consumer Protection – The Empowerment of the Citizen-Consumer', ANU College of Law Research Paper No 20.11, electronic copy available at: https://ssrn.com/abstract=3611436, pp. 2–3. A different issue is whether data protection regulation represents a suitable tool for ensuring individual control, since 'in the face of recent technological developments and emergence of new social practices which seem to undermine the very capacity, if not the will, of individuals to 'self-manage' their informational privacy this apparently simple and familiar notion becomes very ambiguous..Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12:1 SCRIPTed 3 https://script-ed.org/?p=1927, p. 4.

[9] OECD Global Forum on Competition, 'The Objectives of Competition Law and Policy' (2003) CCNM/GF/COMP(2003)3.

[10] Judgment of 23 November 2006, *Asnef-Equifax*, C-238/05, ECLI:EU:C:2006:734, para. 63.

[11] See, for instance, Inge Graef, 'Beyond Compliance: How Privacy and Competition can be Mutually Reinforcing', Computers, Privacy & Data Protection Conference (2017); Francisco Costa-Cabral and Orla Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' (2017)

Characterising the interrelation between the GDPR and the EU competition law is all but straightforward, but vital if one wants to increase the coherence and effectiveness of regulatory responses. This is particularly important in view of the fundamentally different and partially opposed roles of the two regimes. The starting point for the development of a more comprehensive approach that can be used by the Commission and the competent national authorities is to define a framework which brings structure to the different dimensions of the interrelation.[12] Freeman and Rossi carried out a comprehensive assessment of what they termed 'shared regulatory space'.[13] The authors split multi-agency regulation into different categories and discuss the respective implications for coordination. The four types of interrelation they identify are:[14]

(1) overlapping *agency functions*, where lawmakers assign essentially the same function to more than one agency;
(2) *related jurisdictional assignments*, where Congress assigns closely related but distinct roles to numerous agencies in a larger regulatory or administrative regime;
(3) *interacting jurisdictional assignments*, where Congress assigns agencies different primary missions but requires them to cooperate on certain tasks; and
(4) *delegations requiring concurrence*, where all agencies must agree in order for an activity to occur.

The case at hand does not easily fit into any of these categories, since it is difficult to point to one regulatory task or goal that the regimes share, or type of conduct that they are both concerned with. Furthermore, the concept of 'shared regulatory space' seems to be better suited for the characterisation of more linear relationships, while in this case the two regimes interact in a multitude of indirect ways. The realisation that the interrelation between the GDPR and EU competition law cannot easily be classified under known categories calls for the development of a new way of looking at the regimes' interrelation in the digital market.

The interrelation between the GDPR and EU competition law can be conceptualised by clearly delimitating the mandates of the two regimes but treating their boundary as a permeable membrane that allows elements of one regime to spill over into the other. This spilling over can occur to different degrees and manifest itself in different ways; three categories that raise distinct issues and have different policy implications are discussed in this chapter.[15] The first section discusses how independent actions of the regimes can lead to mutual reinforcement of their policy goals. The following section analyses how opposing policies can raise compatibility issues and hinder successful regulatory outcomes. Finally, it is examined how the regimes can find themselves tackling the same conduct from two different angles, which calls for a closer look at the boundary between the regimes. The identification of the diverse ways in which the regimes relate to one another, when it comes to issues around data and market

---

54(1) *Common Market Law Review* 11; Michal S. Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) *Journal of Competition Law and Economics* 349.

[12] This can lay the foundation for future research on how to optimise the interrelation from a substantive and enforcement point of view.

[13] Jody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) *Harvard Law Review* 1131.

[14] Jody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) *Harvard Law Review* 1145.

[15] These are not mutually exclusive, but the issues they raise require independent analysis.

power, is designed to shed light on how to enhance the effectiveness of the regulatory framework as a whole and lay the foundation for future research on how to optimise this interrelation from a substantive and enforcement point of view.

2. TWO SIDES OF THE SAME COIN

The key role of the GDPR is to safeguard individuals' right to the protection of personal data,[16] while competition law regulates market power and safeguards consumers' economic interests on the market.[17] Although the market failures that the two regimes tackle and the forms of harm that they are designed to solve generally differ (see Figure 6.1 below), in the digital market the lines between these forms of harm and market failures blur. Both market concentration and information and power asymmetries contribute to a market in which, despite the existing legislation, consumers do not have enough control over their data and firms can collect and monetise excessive amounts of such data. Furthermore, it is almost impossible to separate individuals' economic interests and fundamental rights over data. Individuals' data has both an economic and an intrinsic value; its excessive collection can, thus, simultaneously harm individuals' economic interests (if they are inadequately compensated for the data or if it results in an economic loss) and their right to protection of personal data. Therefore, preventing one form of harm will contribute to averting the other one. What this means is that the two regimes are mutually reinforcing; they can, each through their own means, prevent both forms of harm by improving the functioning of the market and contributing to better conditions for individuals. In fact, it can be argued that both regimes are necessary for sound competition on data protection to take place and consumer control over data to be secured.[18]

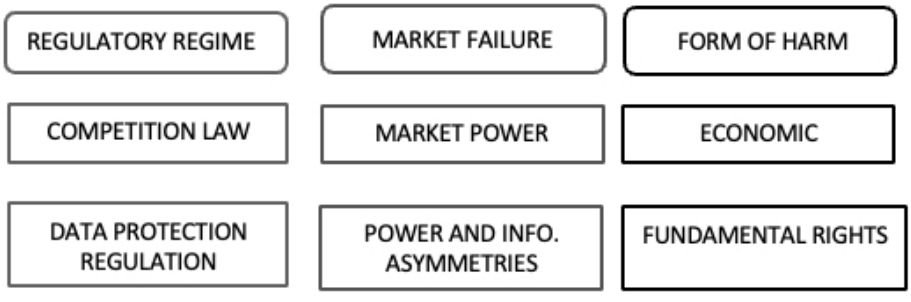

Figure 6.1 Market failures and forms of harm

[16] Article 1(2) GDPR.

[17] Commission, Guidelines on the application of Article 81(3) of the Treaty [2004] OJ C101/08; Commission, Guidelines on Vertical Restraints [2010] OJ C131/01; Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2011] OJ C11/1; and Commission, Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004] OJ C31/03.

[18] Inge Graef, 'Beyond Compliance: How Privacy And Competition Can Be Mutually Reinforcing', Computers, Privacy and Data Protection Conference (2017); Inge Graef, 'Blurring Boundaries of

Firms must be able to communicate to consumers that they are offering better terms, and enough consumers must respond to these terms, so that it pays off for the firms to offer them. Data protection regulation's role here is to shape consumers' demand by increasing their awareness of and control over the terms they are getting. Data protection creates the conditions for competition on data protection to take place, insofar as it sets a benchmark for legitimate terms and enhances transparency, meaning that consumers are in a better position to respond to changes in the level of protection. For instance, data protection certifications 'enhance transparency and compliance… allowing data subjects to quickly assess the level of data protection of relevant products and services'.[19] This, in turn, creates incentives for firms to offer better data protection terms, in order to gain a competitive advantage.[20]

Competition law, on the other hand, controls anticompetitive conduct and ensures that the structure of the market remains competitive, so that, if consumers formulate demand for more data protection, the market will deliver better data protection terms, including better information and control over data. It achieves this mainly by controlling that firms do not illegitimately restrain competition, in particular by stopping harmful mergers and regulating the behaviour of dominant players. Accordingly, competition increases the effectiveness of data protection regulation and vice versa.[21] Both regimes can contribute to a better functioning digital market and, thereby, increase consumers' choices, preventing the two forms of harm, i.e., economic harm and the interference with fundamental rights.[22]

When talking about competition leading to better data protection terms, it is, however, important to bear in mind that competition can take place on the goods or services offered by a company that collects users' data and/or the level of data protection offered.[23] Lynskey argues that currently competition is primarily driven by the main goods and services offered by a company, while competition on data protection is only secondary. This difference is relevant, because more competition might not necessarily lead to an increase of competition on data

---

Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets', in *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds) (Springer 2018).

[19] Recital 100 GDPR.

[20] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer law and Data Protection' (2016) 11(11) *Journal of Intellectual Property Law & Practice* 860; Monopolkommission, 'Competition Policy: The Challenges of Digital Markets' Special Report No 68 (2015) 75.

[21] This is particularly important in the digital market in which consumers do not pay directly, because this limits their incentives to switch. This means that new entrants or existing competitors must attract users through demonstrably better quality rather than being able to undercut prices. CMA, 'Online platforms and digital advertising market study', interim report, 18 December 2019, p. 39, available at https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study accessed 12 November 2021.

[22] Kesler and others studied the data collection strategies of 65,000 developers of mobile apps and monitored 300,000 apps over four years; they concluded that 'the market share is strongly correlated with using intrusive permissions. Stronger apps seem to use their market power for acquiring more data'. Reinhold Kesler, Michael Kummer and Patrick Schulte, 'Mobile Applications and Access to Private Data: The Supply Side of the Android Ecosystem' (2017) Centre for European Economic Research Discussion Paper 17-075, p. 26.

[23] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54(1) *Common Market Law Review* 11; Samson Esayas, 'Competition in (data) Privacy', (2018) 8(3) *International Data Privacy Law*.

protection, if the preconditions for it are not present. For competition on data protection to become an 'independent factor for the acquisition of personal data',[24] consumers must respond to changes in data protection terms and not only to changes in the products or services themselves. While data protection regulation can help achieve this, competition authorities can and arguably should intervene specifically to safeguard this form of competition.

As the European Data Protection Supervisor (EDPS) noted in its preliminary opinion on privacy and competitiveness in the age of big data,[25] EU rules in the areas of competition law and data protection both aim to promote growth and innovation and to promote the welfare of individual consumers. It argued that synergies in the enforcement of these rules should be explored in order to increase their effectiveness and stimulate the market for privacy-enhancing services. This can be taken to entail two things: (1) the regimes have an interest in supporting each other and not to undermine each other's regulatory goals and (2) when it comes to circumstances at the interface between the two regimes, the authorities might need to take into account factors falling under the competency of the other regime.

3. INCOMPATIBILITY BETWEEN THE REGIMES

Having regard to each other when their goals are compatible should be relatively straightforward for the two regimes, since collaboration can lead to better outcomes for both. However, there are also instances in which the regimes' approaches collide. To the extent that the regimes are incompatible, it is unlikely that they will forgo achieving their own aims for the other's sake. At the end of the day, they are two separate regulatory regimes, accountable independently for enforcing their regulatory frameworks. Nonetheless, the interdependence of the two regimes and the indispensability of both in order to successfully tackle the market failure means that it is of utmost importance to address these conflicts and develop a compatible approach.

3.1 Two Different Approaches

Although data protection and competition law can complement each other when acting to empower consumers and create a well-functioning market, their aims are only partially overlapping, and they operate in two very distinct ways. Incompatibilities between the regimes arise due to the fact that while competition law promotes the natural functioning of the market and adopts an economic view of personal data, data protection regulation perceives data as a fundamental right and works by directing the behaviour of market players in relation to it. Generally speaking, while competition law encourages the sharing of data to facilitate compe-

[24] Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54(1) *Common Market Law Review* 11, p. 13.

[25] Preliminary Opinion of the European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', March 2014.

tition,[26] data protection regulation is wary of the duplication of personal information and can restrict competition by imposing requirements around data processing.[27]

A concrete manifestation of the intrinsic divergence between data protection and competition law can be found when data is used as a form of payment (or counter-performance) for an online service. From a competition policy perspective, whether consumers pay with money or data is irrelevant; as long as the competitive process is not distorted by anticompetitive practices, the market forces are well placed to offer consumers what they want. If consumers are content with exchanging their data for online services, the market will provide them with this option. Unduly limiting what firms are able to offer restricts competition and reduces economic efficiency. Data protection authorities, on the other hand, protect data as a fundamental right and do not take into account that data can exist within a market context and that individuals (want to) exchange their data for online services. The EDPS claimed that 'One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction.'[28]

The refusal to look at data from a market perspective prevents data protection regulators from assessing both sides of the transaction taking place in relation to data in the online market, i.e., the data that individuals disclose and the content or services they get in return. The problem that this creates in practice can be exemplified by a case in which consumers were given the choice between a free/cheaper service, which used personal data, and a more expensive, privacy friendly, version. In the case, the UK Information Commissioner's Office (ICO) issued a warning to the US-based Washington Post over the way it obtained consent for cookies and tracking.[29] The *Post* offered EU users three subscription options: a free one with limited access to articles, conditional upon the use of cookies and tracking, one with unlimited access for $6, also conditional upon the use of cookies and tracking, and one for $9 without the use of cookies and tracking. The ICO found that the option costing $9 was not a free alternative and, thus, the consent for processing (under the free or $6 option) was not freely given, because the service was 'conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.[30] In response to this approach, it has been argued that 'the ICO's rigid interpretation, requiring free alternative, is based on a misconception that the user's information is not part of the price in the free or discounted

---

[26] For instance, competition authorities can impose data sharing as a remedy in Article 102 TFEU cases, if data is found to constitute an 'essential facility' and the refusal to grant access to it gives rise to an exclusionary abuse, see Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' (2019) 53(1) Revue juridique Thémis de l'Université de Montréal. In merger cases the parties can offer data sharing commitments to address competition concerns raised by the competition authority, see Nils-Peter Schepp and Achim Wambach, 'On Big Data and Its Relevance for Market Power Assessment' (2016) 7 *Journal of European Competition Law and Practice* 120.

[27] For example, through the principles of 'purpose limitation' and 'data minimisation' (Article 5(1)(b) GDPR and (c)) and 'data protection by design and by default' (Article 25 GDPR).

[28] EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017, available at https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf accessed 12 November 2021.

[29] The Register, 'Washington Post offers invalid cookie consent under EU rules – ICO: UK watchdog waves fist in paper's general direction, asks it to stop forcing people to accept tracking' 19 November 2018, available at https://www.theregister.co.uk/2018/11/19/ico_washington_post/ accessed 12 November 2021.

[30] Article 7(4) GDPR.

deal in exchange for content that is not supposed to be free'.[31] The current approach taken by data protection authorities ignores the way businesses in the online market currently operate. The ICO issued a written warning to the Washington Post advising it to give access to all three subscription levels without users having to consent to the use of cookies. It is apparent why, from an economic perspective, such a request cannot be accommodated by a company that needs to make a profit in order to survive in the market.

Unless the fundamental incompatibility between the perception of data as a fundamental right and its commodification[32] is solved, data protection misses the opportunity to improve the digital market's functioning in relation to the use of data. Under the current approach, there seem to be two possible outcomes:

(1) Data protection authorities strictly enforce the prohibition of making services dependent on consent to data collection, meaning that some firms will no longer be able monetise their services through data. As a consequence, some will probably start to charge monetary prices. In the *Washington Post* case, in order to comply with the ICO's request, the only reasonable solution for the newspaper would be to restrict its subscription models to the $9 option without the use of cookies and tracking. Such an outcome would deprive consumers of the choice to monetise their data instead of paying in monetary terms. This is not necessarily in line with the GDPR's goal to empower consumers over their data. It could also eliminate competition between different business models (i.e., services which are paid for and others that collect data) and lead to a worsening of conditions for consumers. Furthermore, preventing firms from monetising data as their business model could also be harmful for competition if, for instance, it means that smaller players that rely on data monetisation will no longer be able to compete against incumbents, if they need to charge monetary prices.
(2) Data protection authorities recognise that enforcing the rules too strictly will have far-reaching, possibly negative, consequences for the market and thus decide to be more permissive when it comes to data used as a counter-performance. However, the refusal of data protection authorities to formally accept data as a counter-performance leaves the authorities paralysed by not having the right means to regulate digital firms' utilisation of data in the digital market. Basically, authorities are unable to effectively control big data companies' behaviour, because they are reluctant to address the conditions under which the exchange of data against services takes place, since in theory they do not recognise this exchange as legitimate. This leaves individuals exposed to unfair and harmful data practices.

The current approach of data protection authorities leans towards the latter outcome; efforts are made to somehow regulate the behaviour of these companies, but without taking a strong enough stance in regard to the way they monetise data.[33] Instead, data protection authorities

---

[31] Mingli Shi, 'Ad-Tracking Consent & The Dilemma: Some Thoughts on the Washington Post Case', 6 December 2018, available at https://mingli.me/2018/12/06/ad-tracking-consent-the-dilemma/ accessed 12 November 2021.

[32] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on 9 April 2019, para. 51.

[33] For example, the French Data Protection Commission fined Google €50m for two GDPR violations. Firstly, it held that Google violated the obligation of transparency and information, because the

should try to find a balance between reducing power and information asymmetries, thereby empowering consumers, and enabling the market to function and naturally respond to consumer demand. A more flexible approach is needed, which allows data protection authorities to include in their assessment whether data is an intrinsic part of a business model and whether data subjects get something in return for their data. It is not argued that data protection regulation should align its goals with the ones pursued by competition law, but that it should adopt an approach that is consistent with the way the market functions.[34]

3.2 What Justifies a Reconciliation?

This chapter has argued that data protection regulation should allow for more flexibility when assessing what data practices are lawful; in particular, authorities should allow for the possibility to make services conditional on data disclosure. This does not mean permitting an unrestricted monetisation of data but accepting that, under certain conditions and with guarantees in place, internet companies should be allowed to offer their services in exchange for data. The following two approaches can be relied upon to apply data protection's regulatory framework in such a manner.

A. Balancing data protection and the freedom to conduct business

The current understanding of the right to data protection risks undermining online firms' freedom to conduct a business, recognised under Article 16 of the Charter of Fundamental Rights of the European Union (CFR), because it undermines a business model that is widely used in the digital market. In *Sky Österreich*[35] the Court stated that:

---

information provided to its users was neither clear nor comprehensive, too general, and spread over too many documents. Secondly, it was found to have violated the obligation to have a legal basis for processing in relation to ads personalisation, because consent, on which it relied, was not valid, since it was not sufficiently informed and neither specific, nor unambiguous. None of the two infringements tackle the problem of data being used as commodity; Google could comply with the obligations addressed in by French Commission and still monetise data in exchange for its service. Commission Nationale de l'Informatique et des Libertés, 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC', 21 January 2019, available at https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc accessed 12 November 2021.

[34] This chapter concentrates on the extent to which, when enforcing the GDPR, data protection authorities should adapt to the market functioning, because, as explained above, it is a major obstacle to a successful regulatory framework around the use of data in the digital market. Nonetheless, competition authorities also have to take data protection elements into account, for instance, when their actions may impact individuals' fundamental right to protection of personal data. See Article 51(1) Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (CFR):

> The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

[35] Judgment of 22 January 2013, *Sky Österreich GmbH v Österreichischer Rundfunk,* Case C-283/11, ECLI:EU:C:2013:28.

> The protection afforded by Article 16 of the Charter covers the freedom to exercise an economic or commercial activity, the freedom of contract and free competition…
>
> In addition, the freedom of contract includes, in particular, the freedom to choose with whom to do business… and the freedom to determine the price of a service…[36]

Andrea Usai speaks of a 'right to economic initiative' and argues that although it 'is an individual right that must be read according to its social function, it also serves a "socially useful" purpose, as it helps to preserve the system of competition'.[37] The freedom is not absolute and must be viewed in relation to its social function;[38] Article 52(1) CFR (which also applies to the right to data protection) states that:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[39]

The Court in *Sky Österreich* held that:

> where several rights and fundamental freedoms protected by the European Union legal order are at issue, the assessment of the possible disproportionate nature of a provision of European Union law must be carried out with a view to reconciling the requirements of the protection of those different rights and freedoms and a fair balance between them.[40]

The GDPR does foresee the potential conflict between data protection and other rights; recital 4 reads: 'the right to 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'[41] and 'this Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the … freedom to conduct a business…'.[42] In relation to the role of recitals, the Commission communicated that:

> the insertion of recitals is not a mere formality, it reflects the in-depth monitoring of the proposal's compliance with the Charter. The recitals which set out the proposal's conformity with the Charter will be chosen to indicate exactly which fundamental rights the proposal in question will affect.[43]

---

[36] Judgment of 22 January 2013, *Sky Österreich GmbH v Österreichischer Rundfunk,* Case C-283/11, ECLI:EU:C:2013:28, paras 42–43.

[37] Andrea Usai, 'The Freedom to Conduct a Business in the EU, its Limitations and its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration' (2013) 14(9) *German Law Journal* 1867.

[38] Judgment of 22 January 2013, *Sky Österreich GmbH v Österreichischer Rundfunk,* Case C-283/11, ECLI:EU:C:2013:28, para 45.

[39] Article 52(1) CFR.

[40] Judgment of 22 January 2013, *Sky Österreich GmbH v Österreichischer Rundfunk,* Case C-283/11, ECLI:EU:C:2013:28, para 60.

[41] Recital 4 GDPR.

[42] Recital 4 GDPR.

[43] Commission, 'Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union' (Communication) COM(2010) 573/4, p. 7.

The EDPB has expressly acknowledged the relevance of the freedom to conduct business when it comes to obligations under the GDPR; it stated that:

> Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. This supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter, and reflects the fact that sometimes the contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data.[44]

It is apparent why the freedom to conduct a business can be affected by the GDPR; what is controversial is assessing how to balance the two rights when it comes to the way businesses operate in the digital market. The Centre for Information Policy Leadership (CIPL) commented on EDPB's guidelines,[45] welcoming 'the acknowledgment that Article 6(1)(b) is intended to support the freedom to conduct a business'.[46] It then remarked that, when establishing what data is necessary for the performance of a contract, the distinction between the contract and the associated personal data is difficult to draw in the digital economy and requires a case-by-case assessment. Furthermore, it contended that the guidelines should 'remain flexible enough to allow for the future development of new technological, economic and contractual models involving the use of personal data. The Final Guidelines should account for the complexity of modern data uses and the changing nature of digital services'.[47]

These comments signal that it is difficult to determine in advance how the balance should be struck, and that data protection's assessments should consider the characteristics of each case and the role that data plays in the digital market. As pointed out by the CIPL, this is not only important for existing businesses, but also to ensure that new business models can be developed. Even if data protection authorities are reluctant to see data as a commodity, they must recognise that the right to data protection needs to be balanced against other interests and allow the market to take its course. This balance needs to be drawn even when data is used as a counter-performance; it should not be the case that, as in the ICO scenario described above,

---

[44] EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019, version 2.0, p. 4, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed 12 November 2021.

[45] EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 9 April 2019, version for public consultation, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf accessed 12 November 2021.

[46] 'Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Draft Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects Adopted on 9 April 2019', 23 May 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_guidelines_on_the_processing_of_personal_data_under_article_6_1__b__gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects.pdf accessed 12 November 2021.

[47] Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Draft Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects Adopted on 9 April 2019', 23 May 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_edpbs_guidelines_on_the_processing_of_personal_data_under_article_6_1__b__gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects.pdf accessed 12 November 2021.

the balance is automatically struck in favour of data protection rights and against the freedom to conduct a business. This reasoning applies to all legal bases for data processing, including consent and legitimate interests.[48]

B. Data as counter-performance can be compatible with the right to data protection

The second of the two approaches that can be used to allow internet companies to offer their services in exchange for data is to accept that, under certain circumstances, data used as counter-performance is compatible with the right to data protection. Under this approach, data protection authorities would adapt their view of the right to data protection to the realities of the digital market, in which individuals (want to) exchange data for services. Data protection can be understood as a transparency tool, promoting individuals' proactive right to control what happens with their data and rejecting the notion that there is something inherently wrong with collecting and using personal information.[49] If data protection is centred on the right of data subjects to have control over their data, it is not fundamentally incompatible with exchanging this data against services. Using data as a counter-performance, if it occurs under the guarantees established by the GDPR,[50] is in line with data subjects' freedom to determine what to do with their data. Data protection regulation is exactly what creates a framework that will guarantee that individuals' right over data is protected in these transactions and that places individuals in the position to exchange data in a fair manner.

Furthermore, earlier it has been argued that individuals' fundamental rights and economic interests in relation to data are closely interlinked in the digital world. When disclosing data to internet companies, data subjects are also consumers, and they have both an intangible and economic interest in the data concerning them. The separation of these two interests is artificial and disconnects the regulation from the real world, thereby threatening to undermine individuals' interests and needs.[51] In this regard it has been argued that 'trading (in a larger sense) with personal data has become a well-established phenomenon and lawyers should not refuse to deal with this phenomenon only by referring to the personality right of the respective consumers and other data subjects'[52] and that:

> the human-rights aspect of personal data and the capacity of personal data to serve as counter-performance are not mutually exclusive. In other legal disciplines it is well established that personality-related rights (such as authors' rights or publicity rights) can simultaneously have a monetary dimension, which their holders are free to realise. Such duality can equally apply to the

---

[48] Article 6(1)(a) and (f) GDPR.

[49] Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al. (eds.), *Privacy and Identity Management for Life* (Springer 2010); Henry Pearce, 'Could the Doctrine of Moral Rights be used as a Basis for Understanding the Notion of Control Within Data Protection Law?' (2018) 27(2) *Information & Communications Technology Law* 133.

[50] Crucially, the 'Principles relating to processing of personal data' under Article 5 GDPR and the 'Conditions for consent' under Article 7 GDPR.

[51] Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 4(6) *Journal of European Consumer and Market Law* 218.

[52] Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 4(6) *Journal of European Consumer and Market Law*, p. 219.

interface between data as reflecting a personal right (e.g., under the GDPR) and data as a commodity (e.g, under the [Digital Content Directive]).[53]

3.3 What Could a Reconciliation Look Like?

The aim of both the data protection and competition law regime is that individuals have sufficient control over their data and that the exchanges happening in the online market are in line with their interests.[54] So far, this chapter has argued that for this to happen data protection authorities should acknowledge data's market significance. This does not mean labelling data as a commodity but realising that it is used by data subjects to gain benefits in a market context and adapting the rules to this reality. Data's special nature will still lead to a stronger protection than if there was no fundamental right at play and 'than what can be derived from an economic efficiency standard'.[55] This means that in case of doubt, more rather than less protection should be provided to data subjects. The key is for data protection authorities to find a balance between the different dimensions of data in the market.

The way this could be achieved is through the legitimate interests[56] legal basis rather than basing the processing on consent. This legal basis contains an express balancing requirement between the controllers' interests and data subjects' fundamental rights, which gives data protection authorities the flexibility to assess transactions in which data is exchanged for services.[57] The benefit of relying on this legal basis is that data protection authorities can, during their monitoring and enforcement activities,[58] verify whether the data collected and processed is proportionate, taking into account all the circumstances of the transaction. What qualifies as a legitimate interest when it comes to personal data used as a counter-performance can be determined on a general level and/or on a case-by-case basis.

If the balancing under the legitimate interest legal basis results in data subject's interests overriding the data controller's, meaning the latter cannot rely on it for processing, it might still be possible to rely on consent as a legal basis, provided that the conditions for 'freely given' consent are adhered to. According to the GDPR 'when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.[59] If one wanted to allow consent to be used as a legal basis when exchanging services for data, this provision

---

[53] Axel Metzger et al., 'Data-Related Aspects of the Digital Content Directive' 9 (2018) *JIPITEC* 90, p. 94.

[54] An important discussion here is whether it is justified to rely on data subjects' control over their personal data, given that the whole ecosystem is built in a way that makes it impossible for individuals to have complete control, and the fact that individuals' data disclosure can affect third parties. See Elettra Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn' (2020) 40(1) *Pace Law Review* 307.

[55] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 15.

[56] Article 6(1)(f) GDPR.

[57] See Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', 9 April 2014, 844/14/EN, WP 217; Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?' (2014) 51(3) *Common Market Law Review*.

[58] Articles 57 and 58 GDPR.

[59] Article 7(4) GDPR.

can be interpreted as meaning that consumers must be given an option that does not involve data collection, but that, for instance, requires monetary payment. In this case, the provision of a service would not be conditional on consent, because individuals would have another way to get access to the service. Alternatively, since the term 'utmost account' leaves space for interpretation, it can also be accepted that consent can be deemed to be freely given in cases in which the data subject uses a service in which data is collected in lieu of monetary payment, because individuals freely accept the exchange in the same way in which they would accept to pay for a service.[60]

The second relevant limitation on valid consent is contained in recital 42, which states that 'consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'.[61] On a strict reading, this recital appears to be irreconcilable with data used as a counter-performance, since a refusal to consent would implicate a denial of the service, or the obligation to pay in monetary terms, both of which can be seen as detrimental for the individual. Nevertheless, the ICO claimed that:

> it may still be possible to incentivise consent to some extent. There will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal. However, you must be careful not to cross the line and unfairly penalise those who refuse consent.[62]

It is apparent that these are not clear-cut obligations, meaning that the EDPB or national data protection authorities have the opportunity to decide on an interpretation that is consistent with the way the market functions, if this would allow them to achieve better regulatory outcomes.

4. THE REGIMES' BOUNDARIES

Given the different mandates of EU data protection and competition authorities, there are only few instances in which the question of the boundary between the regimes arises. The main situation in which this happens is when a problematic data practice of a dominant firm is in some way related to its market power.[63] Data protection authorities have the mandate to intervene, if the data processing breaches data protection rules; competition authorities, on the other hand, have the power to start proceedings, if they have reason to believe that the conduct constitutes an exploitative or exclusionary abuse of a dominant position under Article 102 TFEU. While the regimes should work together towards their common goal, it is desirable to have a closer look at where the line between the regimes should be drawn and which authority is best placed to intervene. This part argues that the regimes should not cover the same conduct; while competition authorities should intervene when the behaviour of dominant companies threatens

---

[60] Data protection authorities are still there to ensure that the data collection and processing complies with the other GDPR principles.

[61] Recital 42 GDPR.

[62] ICO website, 'What is valid consent?', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ accessed 12 November 2021.

[63] See the German Facebook case discussed below.

to foreclose competition, they should not bring exploitative abuse cases for data practices of dominant players that are covered by the GDPR.

4.1 Competition vs Sector-specific Regulation

The basic rule laid down by the CJEU is that when both national or EU regulatory frameworks and competition law apply to the same conduct, competition law remains applicable *ex post* to undertakings' conduct, where 'the sector-specific legislation does not preclude the undertakings it governs from engaging in autonomous conduct that prevents, restricts or distorts competition'.[64] Thus, competition authorities can enforce EU competition rules even when sector-specific regulation covers the same conduct and independently of the fact whether regulatory obligations are complied with or not. There are a number of advantages deriving from competition law remaining applicable in regulated markets; Colomo argues that:

> EU competition law is a valuable instrument to ensure that the objectives of sector-specific regimes are achieved… Provisions such as Articles 101 and 102 TFEU are more flexible — both in the formal and in the substantive sense of the expression — and thus allow for intervention in a wider range of contexts.[65]

However, the fact that competition authorities can intervene does not mean that they should always do so. A relevant factor in this regard is that competition authorities are reluctant to bring exploitative abuse cases and have done so only on a few occasions.[66] The fact that Article 102 has been applied mostly to exclusionary abuses can partially be explained by the fact that if a dominant company can exploit consumers over a considerable amount of time, it is likely that there is a problem with the way the market functions, because in a well-functioning market the conduct would attract new competitors. For this reason, competition authorities tend to look at the causes of a market failure rather than its consequences in terms of higher prices, lower quality etc.[67]

The Commission enforcement priorities guidelines state that in relation to behaviour that directly exploits consumers, competition authorities may intervene, 'in particular where the protection of consumers and the proper functioning of the internal market cannot otherwise be adequately ensured'.[68] Accordingly, it has been suggested that when the protection of consumers is guaranteed by a specific regulator that has jurisdiction over the matter, competition authorities should not bring exploitative abuse cases covering the same issue, unless 'the

---

[64] *Deutsche Telekom AG* [2003] OJ L263/9, para. 54. The decision was confirmed by the Court of Justice in Judgment of 14 October 2010, *Deutsche Telekom v Commission,* C-280/08P, ECLI:EU:C:2010:603.

[65] Pablo Ibáñez Colomo, 'EU Competition Law in the Regulated Network Industries', LSE Working Papers 08/2016, p. 3.

[66] OECD, 'Excessive Prices' (2012) DAF/COMP(2011)18.

[67] Damien Geradin, 'The Necessary Limits to the Control of 'Excessive' Prices by Competition Authorities - A View from Europe' Tilburg University Legal Studies Working Paper 2007, available at https://ssrn.com/abstract=1022678.

[68] European Commission, 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (2009) OJC 45/2, para. 7.

decision of the sectoral regulator was manifestly wrong'.[69] The Court has repeatedly stated that the Commission has a broad discretion to select the cases that it deals with under competition rules.[70] A similar discretion to set enforcement priorities is given to national competition authorities under the ECN+ Directive.[71] As emphasised by Wils, in setting enforcement priorities, the fact that another authority is also capable of dealing with the issue, and may indeed be better placed to do so, is a highly relevant consideration.[72]

4.2 Exploitative Abuses vs GDPR Infringements

While EU law permits a parallel application of competition law and sector-specific regulation, the existence of a regulatory framework should be taken into account when setting competition law enforcement priorities. This section looks at policy arguments that can provide more specific guidance on how to apply the law in these overlap cases.

The fact that the regimes perform different functions could be taken to signify that they could very well act independently of each other. When competition authorities bring exploitative abuse cases, they do so to protect consumers' economic interests from the abuse of market power by dominant firms, while data protection authorities intervene to protect individuals' fundamental rights. Why should competition authorities be prevented from intervening based on whether data protection authorities could intervene? As explained at the beginning of the chapter, although distinct, in the digital market the harms that the authorities are designed to prevent, as well as the conduct causing them, are interlinked. Consequently, interventions to correct firms' behaviour in one area will also affect the other one. If the authorities recognise this correlation, it is in their interest to think about dividing their work in a suitable manner.

When it comes to data practices that are harmful for competition, i.e., exclusionary abuses, the open-ended texture of competition law has the advantage of permitting authorities to focus on the specific circumstances of each case. As proclaimed by the G7 competition authorities:

> with respect to data, the aggregation of data, in some circumstances, may create barriers to entry or enhance market power, but it does not necessarily have such a tendency, and in some instances can be procompetitive. Competition enforcers can evaluate data concerns based on the individual facts of a case to assess whether a firm's use of data benefits consumers or harms competition.[73]

---

[69] Massimo Motta and Alexandre de Streel, 'Excessive Pricing in Competition Law: Never say Never?' (2007) Konkurrensverket – Swedish Competition Authority (ed), *The Pros and Cons of High Prices*, p. 14. See also Lars-Hendrik Röller, 'Exploitative Abuses', in Claus-Dieter Ehlermann and Mel Marquis (eds), *European Competition Law Annual 2007: A Reformed Approach to Article 82 EC* (Hart Publishing 2008).

[70] See Judgment of 14 December 2000, *Masterfoods and HB*, C-344/98, EU:C:2000:689, para 46 and Judgment of 4 March 1999, *Ufex and Others v Commission,* C-119/97, EU:C:1999:116, paras 88 and 89.

[71] 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 [2019] OJ L11/3, Article 4(5).

[72] Wouter P. J. Wils, 'The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the *Facebook* Decision of the Bundeskartellamt' (2019) 3 *Concurrences* 58, Art. N° 91034.

[73] Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy", Paris, 5th June 2019, available at https://www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports-common-understanding-g7-competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf accessed 12 November 2021, p. 6.

Competition authorities are in a unique position to tackle conduct that harms competition, indicating that it is crucial that they concentrate their resources on this type of abusive behaviour. Behaviour that is exploitative, on the other hand, can be covered by data protection authorities, and competition authorities' intervention does not have much to add. It has been argued that:

> with regard to the digital debate, we should not forget that competition law cannot and should not tackle all conduct with negative consequences on the market. Certain other tools, including vigorous enforcement in other fields such as data protection, or legislation where there is a clearly defined and recurring issue that leads to systemic market failure, may be appropriate.[74]

If competition authorities wanted to bring exploitative abuse cases, it would not be enough to argue that the conduct harms consumers; they would have to show that the harm results from anticompetitive conduct, i.e., prove causation.[75] However, proving that under competitive circumstances privacy terms would be better is difficult to do, since consumers behave inconsistently towards privacy policies. Moreover, since the protection guaranteed by the GDPR is far reaching in terms of the level of control over data given to data subjects, it is unlikely that competition authorities will be able to argue that in a competitive market the way data is collected and processed by internet companies would be better than what it needs to be to comply with the GDPR. This indicates that when it comes to unfair data protection terms, it is not reasonable for competition authorities to intervene by bringing exploitative abuse cases, since they would try to protect the same interests protected by data protection regulation, but would do it under a legal framework under which it is less straightforward to demonstrate harm.

The GDPR, on the other hand, is specifically designed to deal with issues pertaining to personal data, giving the regulators the necessary instruments to assess what exactly is wrong with the data processing and design remedies accordingly. BEUC (the European Consumer Organisation) claimed that:

> Regulation may offer a valuable instrument to design the competitive landscape and clarify the boundaries of legality. Its strength lies in its ability to tackle, ex-ante, a wide range of concerns, and in doing so help prevent behaviour that the competition laws may be able to address ex-post. Regulation may form a superior instrument dealing with systemic market failures, sector specific problems, across the board standard setting and groups of customers in need of special protection…[76]

This line of reasoning is rooted in the belief that if under one framework it is more effective and efficient to address a specific aspect of the market failure, it should be treated as the preferred option. While being a relevant consideration, it must be borne in mind that it is not the only one. For instance, it does not account for the fact that regulators do not always perform their function perfectly; in these cases, having two regulators which can cover the same conduct can be desirable in order to prevent under-enforcement.

---

[74] Cecilio Madero Villarejo, 'Antitrust in times of upheaval' 2019 CRA Conference, Brussels, 10 December 2019, available at https://ec.europa.eu/competition/speeches/text/sp2019_13_en.pdf. accessed 12 November 2021.

[75] Pinar Akman, 'Exploitative Abuse in Article 82EC: Back to Basics?' (2009) ESRC Centre for Competition Policy and Norwich Law School, University of East Anglia Working Paper 09-1.

[76] BEUC, 'The Role of Competition Policy in Protecting Consumers' Well-being in the Digital Era' (2019), p. 23, available at https://www.beuc.eu/publications/beuc-x-2019-054_competition_policy_in_digital_markets.pdf accessed 12 November 2021.

A different argument is that since data protection is designed to assess what unfair terms are from a fundamental rights perspective, competition authorities making their own assessment about whether data protection terms are unfair could give rise to uncertainties and inconsistencies. GDPR rules have already been criticised for being complex and uncertain[77] and intervention by competition authorities would mean that dominant firms would also need to assess whether their terms are unfair in ways beyond the GDPR. If competition authorities end up simply using data protection principles to prove that terms are unfair, like in the German case discussed below, there does not seem to be a valid reason for competition authorities to intervene. Not only are data protection authorities better at making these kinds of assessments, but competition authorities are only capable of enforcing data protection rules when it comes to dominant firms, giving rise to uneven and potentially unfair outcomes. Letting competition authorities intervene in cases that involve a breach of data protection regulation 'would necessarily remain incomplete, because it would exclude the customers of non-dominant companies, who are no less worthy of the protection of privacy law'.[78]

In the case against Facebook brought by the German competition authority, the Bundeskartellamt (BKA), the BKA tried to bring an infringement of data protection principles under its competency, formulating it as both an exploitative and exclusionary abuse. It found that Facebook was abusing its dominant position, by forcing users to agree to its terms and conditions, under which it could collect user data also outside of the Facebook website[79] and combine this data with users' Facebook profiles. The BKA maintained that the merging of data exploited users by depriving them of control over their personal data and violating their right to informational self-determination.[80] Under its exclusionary theory of harm, it argued that Facebook's excessive data processing gave it a competitive advantage that prevented market entry by competitors.

The Higher Regional Court in Düsseldorf suspended the BKA's order,[81] arguing that an infringement of data protection rules by a dominant firm cannot be seen as a violation of competition law, if there is not a causal connection between the illegitimate data processing and Facebook's market power. Furthermore, it held that it was not manifest how the data process-

---

[77] See for instance, G Teixeira, M Mira da Silva and R Pereira, 'The Critical Success Factors of GDPR Implementation - A Systematic Literature Review' (2019) 21(4) *Digital Policy, Regulation and Governance*, 402; S Agarwal, 'Towards Dealing With GDPR Uncertainty' (2016) 11th IFIP Summer School on Privacy and Identity Management, Sweden.

[78] Torsten Körber, 'Data, Platforms and Competition Law', (2018) p. 8, available at https://ec.europa.eu/competition/information/digitisation_2018/contributions/torsten_koerber.pdf accessed 12 November 2021.

[79] The BKA talks about third-party sources as services owned by Facebook, like WhatsApp and Instagram as well as third-party websites that 'embedded Facebook products such as the "like" button or a "Facebook login" option or analytical services such as "Facebook Analytics", data'; Bundeskartellamt, 19 December 2017 'Background information on the Facebook proceeding'; available at http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.html?nn=3591568 accessed 12 November 2021.

[80] Bundeskartellamt, 'Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing', B6-22/16, 6 February 2019.

[81] Oberlandesgericht Düsseldorf, Beschluss VI-Kart 1/19 (V), In der Kartellverwaltungssache Facebook gegen Bundeskartellamt, available at https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf accessed 12 November 2021.

ing foreclosed market entry. It 'did not rule out that Facebook's processing of additional data may secure its market position'[82] but stated that whether 'a market entry barrier actually exists or is reinforced requires "closer review and more detailed demonstration"'.[83] The Federal Court of Justice subsequently annulled the interim decision of the Düsseldorf Court;[84] the main proceedings are still ongoing.

Although the BKA can be applauded for bringing such an innovative case, it is a clear example of a competition authority trying to close a data protection enforcement gap. In relation to the alleged exploitative abuse, while it would have been straightforward to apply data protection rules to Facebook's illegitimate data practices, the BKA tried to twist competition law in a way that would allow it to cover the conduct. This is not conducive to a consistent and strong regulatory framework; it introduces uncertainty and can lead to unfair outcomes, because data protection obligations are enforced arbitrarily by competition authorities; furthermore, there is the risk that the time and resources spent in long investigations end up being wasted. The alleged exclusionary abuse, on the other hand, is the type of theory of harm that competition authorities should be concerned with. In fact, the court conceded that Facebook's data processing may entrench its market position but claimed that the BKA had failed to provide enough evidence for this. Possibly, the BKA would have been more successful, had it focused only on the latter theory of harm and invested its resources into examining how Facebook's data practices could strengthen its market power. If it had been unable to find evidence of a connection between the data practices and market power, it should probably have concluded that it was not a case for a competition authority to bring. As argued by Wils:

> Beyond the legal question of the applicability of Article 102 TFEU to the conduct at issue in the Facebook Decision of the Bundeskartellamt, a different question is whether, as a matter of policy, it is desirable or appropriate that the European Commission and/or the competition authorities of the EU Member States take up cases such as the Facebook case taken up by the Bundeskartellamt.[85]

Following the BKA's Facebook decision, a member of the European Parliament asked the European Commission: 'Does the Commission consider it desirable to convert the decision of the German Federal Cartel Office into a European standard in order to further strengthen

---

[82] Giuseppe Colangelo, 'Facebook and the Bundeskartellamt's Winter of Discontent' (23 September 2019) Competition Policy International, available at https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/?utm_source=CPI+Subscribers&utm_campaign=f83149b31e-EMAIL_CAMPAIGN_2019_09_23_10_15&utm_medium=email&utm_term=0_0ea61134a5-f83149b31e-236855437 accessed 12 November 2021.

[83] Giuseppe Colangelo, 'Facebook and the Bundeskartellamt's Winter of Discontent' (23 September 2019) Competition Policy International, available at https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/?utm_source=CPI+Subscribers&utm_campaign=f83149b31e-EMAIL_CAMPAIGN_2019_09_23_10_15&utm_medium=email&utm_term=0_0ea61134a5-f83149b31e-236855437 accessed 12 November 2021.

[84] Courtesy translation of Press Release No 080/2020 published by the Bundesgerichtshof (Federal Court of Justice) on 23/06/2020 (https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html) provided by the Bundeskartellamt, available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2 accessed 12 November 2021.

[85] Wouter P. J. Wils, 'The Obligation for the Competition Authorities of the EU Member States to Apply EU Antitrust Law and the *Facebook* Decision of the Bundeskartellamt' (2019) 3 *Concurrences* 58, Art. N° 91034, p.64.

the position of consumers?'[86] Commissioner Vestager responded that the BKA's 'concerns are based on German competition law. The European legislator has made sure that the type of conduct in question is addressed by the General Data Protection Regulation'.[87] This seems to indicate that the policy adopted by the Commission is to leave concerns surrounding this type of conduct to data protection regulators, when these can be tackled with the GDPR.

5. CONCLUSION

This chapter has explored the different dimensions of the relationship between data protection regulation and competition law when it comes to the role of data in the digital market. The aim was to understand the ways in which the two regimes affect one another and what circumstances call for greater coordination between them. To the extent that the regimes reinforce one another, it is important that these synergies are identified and strengthened. Furthermore, by collaborating, authorities can gain a better understanding of the elements that influence the market functioning, which can be used to inform their policies. Conflicts between the regimes necessitate attention since inconsistent policies risk to undermine the effectiveness of the regulatory framework as a whole. In this regard, it is desirable to find ways to harmonise the regimes' policies. The main problem that has been identified in this respect is data protection authorities' refusal to perceive data within a market context, which prevents them from designing their policies in a way that supports the market functioning. The last dimension that has been analysed is the overlap between the regimes; the discussion focused on drawing a line between the regimes and identifying the best regime to intervene in a given case. Aligning the two regimes in these three dimensions has several advantages for the effectiveness of the regulatory framework. More coherence in the first and last dimensions allows to exploit synergies, increase legal certainty, and avoid the wasteful duplication of functions. It is also conducive to better expertise in decision-making. Solving issues pertaining to the second dimension, on the other hand, avoids a loss of effectiveness resulting from the regimes working at cross-purposes.[88]

---

[86] Parliamentary questions, 5 March 2019, P-001183-19, Question for written answer to the Commission Rule 130, Pirkko Ruohonen-Lerner (ECR).

[87] Answer given by Commissioner Vestager on behalf of the European Commission to Question P-001183/2019 (8 May 2019).

[88] See Jody Freeman and Jim Rossi, 'Agency Coordination in Shared Regulatory Space' (2012) 125(5) *Harvard Law Review* 1131.