Studia Iuridica 89
ISSN 0137-4346; e-ISSN 2544-3135

DOI: https://doi.org/10.31338/2544-3135.si.2022-89.10

Iga Małobęcka-Szwast
University of Warsaw, Poland
e-mail: i.malobecka@wpia.uw.edu.pl
ORCID: 0000-0002-4719-4899

FACEBOOK ENFORCEMENT "SAGA": HOW TO ENFORCE COMPETITION, CONSUMER, AND DATA PROTECTION LAWS IN THE DIGITAL ECONOMY

Abstract

The digital economy has brought new challenges to the enforcement of consumer, competition, and data protection laws as certain market practices (in particular, data practices) can simultaneously infringe all these three areas of law. However, the interdependence between consumer, competition, and data protection laws in the digital economy has so far been rarely reflected in their enforcement by national agencies. As evidenced by the Facebook enforcement "saga", uncoordinated enforcement efforts by competition, consumer, and data protection agencies, which act in silos and focus only on national perspective, pose a threat to the effective protection of consumer welfare and data subject (consumer) rights in the EU. Therefore, it is proposed to introduce cooperation mechanisms between different agencies, both at the EU and national level, in cases involving practices that may potentially infringe all three areas of law and present a risk to sustainable development of the digital economy. It is argued that only a coordinated, cross-institutional, and multi-disciplinary enforcement can provide an effective response to such practices applied by digital giants, such as Facebook, Google, Amazon or Apple, and ensure that consumer welfare and data subject (consumer) rights are not compromised.

KEYWORDS

digital economy, personal data, data protection, antitrust enforcement, consumer protection, GDPR

SŁOWA KLUCZOWE

gospodarka cyfrowa, dane osobowe, ochrona danych osobowych, egzekwowanie prawa konkurencji, ochrona konsumentów, RODO

1. INTRODUCTION

The collection and use of personal data have become a key feature of digital economy. There is no doubt that ensuring an adequate level of protection of personal data is subject to regulation by data protection law (within the European Economic Area, mainly the General Data Protection Regulation)[1], and counteracting possible violations in this respect is generally vested in national supervisory authorities (Art. 51 GDPR).

However, over the last few years it can be observed that the way in which companies process personal data has become the subject of interest not only to supervisory authorities, but also to competition and consumer protection authorities[2]. In several cases, national competition and consumer protection authorities and courts in the EU have reached a conclusion that the way in which companies process personal data may be a decisive criterion in assessing whether there has been a breach of competition or consumer protection law, respectively. It should not come as a surprise, as in the digital economy the line between competition, consumer, and data protection blurs[3] and the same practice may well violate all the three areas of law.

As a consequence, drawing clear demarcation lines between competition, consumer, and data protection laws has become increasingly difficult. The question

[1] 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), OJ L 119 of 4 May 2016, p. 1 ("GDPR").

[2] A. Reyna, *Breaking down silos in public enforcement: Lessons from consumer-facing markets*, 2021, https://ssrn.com/abstract=3838697 (accessed 1.11.2021).

[3] I. Graef, *Blurring boundaries of consumer welfare: How to create synergies between competition, consumer, and data protection law in digital markets*, (in:) M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė (eds.), *Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach?*, Berlin 2018, pp. 122–148.

is also whether drawing such strict lines is indeed necessary. This article argues that one should rather accept mutual overlaps and make use of enforcement tools and strengths of all agencies to better protect consumers in the digital economy.

The article discusses national cases involving Facebook data practices pursued by competition, consumer, and data protection authorities, which are referred to jointly as the Facebook "saga". These cases show that processing of consumer personal data that is inconsistent with data protection laws may be sanctioned not only by data protection regime, but also may be of key importance to establish that a firm has abused a dominant position, engaged in unfair market practices, or otherwise violated consumer protection law. It is worth noting that both the areas of competition law, consumer protection law, and personal data protection are characterised by far-reaching harmonisation within the EU. For this reason, decisions and judgments made on the basis of national regulations, both in the field of competition, consumer protection and data protection law, may constitute a valuable interpretative guideline for the application of similar provisions in other Member States.

However, the current uncoordinated enforcement efforts illustrated in this article by the Facebook "saga" lead to rather opaque and unsatisfactory results – the goals of competition, consumer, and data protection laws seem to be achieved only to a limited extent.

Therefore, it is proposed to introduce cooperation mechanisms between different agencies, both at the EU and national level, in cases involving practices that may potentially infringe all the three areas of law (in particular, data practices)[4] and pose a threat to sustainable development of the digital economy. It is argued that only a coordinated, cross-institutional, and multi-disciplinary enforcement can provide an effective response to such practices applied by digital giants, such as Facebook, Google, Amazon or Apple, and ensure that consumer welfare and data subject (consumer) rights are not compromised[5].

The article is structured into seven sections. Section 2 explains why processing of personal data may be an important issue for competition and consumer protection. Section 3 examines the complex relationship between competition, consumer, and data protection law in the digital economy. Section 4 discusses cases forming part of Facebook enforcement "saga" from the perspective of competition, consumer, and data protection regimes. These cases are used as an example to show that uncoordinated enforcement undertaken by national agencies separately and based solely on national laws may be insufficient and may put goals of all three regimes at risk, which is elaborated in Section 5. To counter

[4] Data practices are understood in this article as practices which are based on data processing (collection, use, sharing etc.) and usually involve infringement of data protection law.

[5] In a similar vein, see A. Ezrachi, A. Reyna, *The role of competition policy in protecting consumers' well-being in the digital era*, BEUC 2019, pp. 22–25, https://www.beuc.eu/publications/beuc-x-2019-054_competition_policy_in_digital_markets.pdf (accessed 1.11.2021).

these flaws Section 6 suggests that what we need in the digital economy is coordinated, cross-institutional, and multidisciplinary enforcement. Some general conclusions follow in section 7.

2. WHY PROCESSING OF PERSONAL DATA MAY BE AN ISSUE FOR COMPETITION AND CONSUMER PROTECTION

Personal data has acquired significant economic value over the last decade, in particular for firms operating on the Internet. Data has been heralded as the "new currency", "new oil", or "new gold" of the current economy[6]. Personal data is one of the most valuable resources for companies operating in the digital markets. On the user side of the market, they can use data to create new or improve existing products and services, provide users with a more personalised experience, and thus build customer loyalty. On the advertiser side of the market, they can use data to offer advertisers better targeted and thus more effective advertising services. As a consequence, the control over large amounts of data may allow them to strengthen their market position and gain competitive advantage over their competitors.

It should therefore come as no surprise that firms are interested in collecting as much data as possible and processing it unlimitedly for whichever purpose is more profitable. Data protection law (in particular, the GDPR), by establishing detailed rules for the processing of personal data, inhibits these attempts and restricts the use of personal data by these firms.

Nevertheless, a company whose business model is based on the processing of personal data may find it profitable to breach data protection rules and impose unfair contractual provisions that violate the GDPR on consumers to obtain as much personal data as possible and process them freely. By violating data protection rules, such firm may be able to collect more valuable data than its competitors who comply with data protection laws and use it to improve its services, expand its user and customer base, and consequently reinforce its market power. One can argue that the risk of breaching the GDPR and imposition of fines is rooted in their business models and decision making.

In these circumstances data protection law intersects with competition and consumer protection law, and the way in which personal data is processed by businesses may have an impact on competition in the digital market and its key actors – consumers. It is so also when competition and consumer protection authorities

[6] *The world's most valuable resource is no longer oil, but data*, "The Economist" 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 1.11.2021).

may come into play and use data protection law as a criterion (a yardstick)[7] for assessing whether a firm has abused a dominant position, committed an act of unfair competition, engaged in unfair commercial practice or otherwise violated consumer rights and interests.

This complex relationship between the fundamental right to data protection, consumer rights, and competitive effects of data processing, as well as its influence on market power, has sparked debate about which regulatory regime is better placed to address the concerns emerging from the use of personal data in the digital markets, in particular from data practices of online platforms.

In this context, it is worth relating to goals of competition, consumer, and data protection law to determine mutual relationships between them.

3. THE RELATIONSHIP BETWEEN COMPETITION, CONSUMER, AND DATA PROTECTION LAW IN THE DIGITAL ECONOMY

In the EU competition, consumer, and data protection regimes are regulated in different legal acts, have different focus and objectives, and in principle are supervised by separate authorities that have distinct mandates[8] and can impose different remedies[9].

In terms of goals, EU competition law aims at safeguarding undistorted competition within the EU internal market, enhance (aggregate) consumer welfare, and ensure efficient allocation of resources. To this end, competition law intervenes against restrictive practices, abusive behaviour, and concentrations that significantly impede effective competition[10].

The objective of consumer law is to safeguard the informed free choice of consumers and protect them as the weaker party in market transactions. It aims to prevent or remedy market failures (in particular, information inefficiencies such as imperfect information, information asymmetries or bounded rationality)[11]. Rather than enhancing the aggregate consumers' welfare as competition law does, consumer law focuses on the welfare of individual consumers[12].

---

[7] F. Costa-Cabral, O. Lynskey, *Family ties: The intersection between data protection and competition in EU law*, "Common Market Law Review" 2017, Vol. 54, issue 1, pp. 29 *et seqq.*

[8] In the EU Member States some authorities are responsible for enforcing more than one set of rules, in particular competition and consumer protection, such as the Polish President of the Office of Competition and Consumer Protection or the Netherlands Authority for Consumers and Markets (ACM).

[9] A. Reyna, *op. cit.*

[10] F. Costa-Cabral, O. Lynskey, *op. cit.*, pp. 29 *et seqq.*

[11] I. Graef, *op. cit.*, p. 126.

[12] OECD Secretariat, The interaction and coordination of competition policy and consumer policy: Challenges and possibilities (background note), DAF/COMP/GF(2008)10, 2008, pp. 18–22,

EU data protection law aims to safeguard the fundamental right to data protection by giving data subjects control over their personal data and by setting the rules that restrict processing of personal data. Importantly, the right to data protection is protected in the EU as a fundamental right enshrined in Art. 8 (2) of the EU Charter of Fundamental Rights and Art. 16 TFEU. The scopes of the concepts of "consumer" and "data subject" are not identical. Every consumer is a data subject, but not every data subject is a consumer. In this respect, the concept of the data subject is broader.

However, EU competition, consumer, and data protection laws share some common goals and features[13], which are rightly referred to as "family ties"[14]. Looking from broader perspective, data protection law along with competition and consumer protection laws form part of the EU system of protection of consumer rights (including the fundamental right to protection of personal data) and consumer welfare[15]. All these three legal regimes aim to protect consumers (in data protection law – data subjects) and contribute to the development of the internal market[16].

Some authors argue that competition law is not a suitable legal instrument to tackle such practices and they should instead be addressed by consumer or data protection laws[17]. Nonetheless, one can argue that in the digital economy we cannot easily separate consumer, competition, and data protection issues from each other. These three areas of law are intertwined and complement each other on various levels, which is particularly visible in the digital economy[18]. To

---

https://www.oecd.org/regreform/sectors/40898016.pdf (accessed 1.11.2021); M. Botta, K. Wiedemann, *The interaction of EU competition*, *consumer*, *and data protection law in the digital economy: The regulatory dilemma in the Facebook odyssey*, "The Antitrust Bulletin" 2019, Vol. 64, pp. 428, 435.

[13] I. Graef, *op. cit*., p. 123.

[14] F. Costa-Cabral, O. Lynskey, *op. cit*., pp. 21–22.

[15] *Ibidem*, pp. 14–22.

[16] I. Graef, *op. cit*., p. 123.

[17] G. Colangelo, M. Maggiolino, *Data protection in attention markets: Protecting privacy through competition?*, "Journal of European Competition Law & Practice" 2017, Vol. 8, issue 6, p. 363; G.A. Manne, R.B. Sperry, *The problems and perils of bootstrapping privacy and data into an antitrust ramework*, "CPI Antitrust Chronicle" 2015, https://www.competitionpolicyinternational.com/assets/Uploads/ManneSperryMay-152.pdf (accessed 1.11.2021); M.K. Ohlhausen, A.P. Okuliar, *Competition*, *consumer protection*, *and the right [approach] to privacy*, "Antitrust Law Journal" 2015, Vol. 80, p. 121; A. Lamadrid, S. Villiers, *Big data*, *privacy and competition law: Do competition authorities know how to do it?*, "CPI Antitrust Chronicle" 2017, p. 4.

[18] European Data Protection Supervisor, Preliminary Opinion, 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, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (accessed 1.11.2021); N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, "Common Market Law Review" 2017, Vol. 54, issue 5, p. 1429.

ensure effective competition in the digital economy we need effective enforcement of data protection and consumer laws, and vice versa. Effective enforcement of competition rules is needed to better protect personal data and consumer rights. Therefore, instead of looking for the best suited regime to tackle certain practices one should focus on how to make use of all three areas of law to more efficiently fight potentially abusive and unfair data practices.

However, despite these common grounds, currently in the EU we can observe that rules on data protection, consumer protection, and competition are applied in silos separately by the respective national agencies[19]. As the example of the Facebook enforcement "saga" shows, such separation and lack of cooperation between authorities casts doubt over effectiveness of such approach.

4. FACEBOOK ENFORCEMENT "SAGA" FROM THE PERSPECTIVE OF COMPETITION, CONSUMER, AND DATA PROTECTION REGIMES

In this section I will look at Facebook data practices that have been pursued by the German competition authority (*Bundeskartellamt*), the Italian consumer and competition authority (*Autorita Garante della Concorrenza e del Mercato*, AGCM) and the Belgian data protection authority (*Gegevensbeschermingsautoriteit*). The above proceedings concerned similar (but not identical) data practices of the incumbent social network provider – Facebook and were based on national laws. Therefore, they constitute a good yardstick for comparing and assessing enforcement approaches of respective regimes.

4.1. COMPETITION LAW PERSPECTIVE: THE PROCEEDINGS OF THE *BUNDESKARTELLAMT*

On 6 February 2019, the *Bundeskartellamt* issued a long-awaited prohibition decision[20] in the Facebook case, which terminated the abuse investigation

[19] European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 2016, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (accessed 1.11.2021).

[20] *Facebook* (Case B6-22/16), *Bundeskartellamt* decision of 6 February 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=8 (accessed 1.11.2021).

initiated in March 2016[21]. In the view of the *Bundeskartellamt*, Facebook[22] abused its dominant position on the market for social networks by imposing on its users terms of service that are incompatible with data protection law[23]. The NCA based its assessment on German Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*, GWB), and not the Art. 102 TFEU, which is an important circumstance in this case. More precisely, the *Bundeskartellamt* found that Facebook, by implementing data policy which allowed it to collect user and device-related data from sources outside of Facebook and to merge it with data collected on Facebook, committed an abuse of its dominant position on the German market for social networks in the form of exploitative business terms pursuant to Section 19 (1) GWB[24].

The theory of harm applied by the *Bundeskartellamt* is based on the assumption that Facebook imposes unfair (exploitative) terms on users (in this case, terms of service and privacy policy contrary to the provisions of data protection law). Their exploitative character consists in making the use of the dominant social network conditional upon the users granting the undertaking unlimited permission to use their personal data. Taking into account that there is no alternative social network available on the market, users have to choose between agreeing to "the whole Facebook package" (i.e. Facebook's terms and conditions), including an extensive permission to process their personal data, or not to use social networks at all[25]. In the view of the *Bundeskartellamt*, the harm for the users lies in a loss of control, as they are no longer able to control how their personal data is used[26].

---

[21] Bundeskartellamt, *Bundeskartellamt prohibits Facebook from combining user data from different sources*, Press release, 7 February 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (accessed 1.11.2021); Bundeskartellamt, *Bundeskartellamt initiates proceeding against Facebook*, Press release, 2 March 2016, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2016/02_03_2016_Facebook.html (accessed 1.11.2021).

[22] Facebook Inc., Facebook Ireland Ltd., Facebook Deutschland GmbH.

[23] Bundeskartellamt, *Facebook*, *exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing – Case Summary*, 15 February 2019, p. 10, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108 (accessed 1.11.2021).

[24] It is important to note that the proceeding was based on the national law – Section 19(1) of the German Competition Act (GWB), which is a national equivalent of Art. 102 TFEU. See Bundeskartellamt, *Facebook*, *exploitative*…, p. 7.

[25] Bundeskartellamt, *Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive*, 19 December 2017, p. 2, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6 (accessed 1.11.2021).

[26] Bundeskartellamt, *Bundeskartellamt prohibits*…, p. 5. See also A. Mundt, *Implications of the German Facebook decision.* Presentation from GCLC – Lunch Talk, 17 April 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Reden/L1/Andreas%20Mundt%20-%20%20Global%20Competition%20Law%20Centre.pdf?__blob=publicationFile&v=2 (accessed 1.11.2021).

Specifically, they cannot reasonably foresee what data and from which sources is combined with data from Facebook accounts, and for what purposes such data is further used[27]. It is important to note that the *Bundeskartellamt* drew a line between user data that is generated through the use of Facebook ("on Facebook") and user data obtained from third party sources ("off Facebook"), and focused its proceedings only on the latter[28]. According to the *Bundeskartellamt*, Facebook's terms of service allow for collecting data from users when they call up one of the third party's websites with embedded Facebook APIs, even if they blocked web tracking in their browser or device settings or did not click "like" or "log in". The data collected in this way is then combined with data from the user's Facebook account, creating a detailed profile of each user. The use of personal data generated by users on Facebook ("on Facebook") is not the subject of the proceedings. As argued by the *Bundeskartellamt*, within the network users can influence the scope of their data collected by Facebook by paying attention to the way they use the network and the content they post[29]. Moreover, the *Bundeskartellamt* noted that user data is an indispensable factor for the functioning of the social network, and when users decide to use a free service, they can reasonably expect that their data will be processed[30].

The *Bundeskartellamt* also pointed to an exclusionary effect of the practice. In the view of the *Bundeskartellamt*, Facebook's conduct impedes competitors, since by the unlawful processing of data and their combination with Facebook accounts, Facebook gains access to a large number of further data sources[31]. Thereby, the practice also allowed Facebook to illicitly gain a competitive advantage over its competitors, which lacked access to comparable data resources, and increase barriers to entry. That, in turn, ultimately cements Facebook's market power towards end customers (users and advertisers)[32].

The *Bundeskartellamt* used data protection law (the GDPR) as a benchmark to establish the exploitative nature of Facebook's conduct. Such approach is not surprising given that back in May 2016, the NCA, in a joint paper with the French *Autorite de la Concurrence*, expressed the view that even though data protection and competition law serve different goals, the use of privacy policies and

[27] Bundeskartellamt, *Bundeskartellamt prohibits*…, p. 5.

[28] "Off Facebook" data includes data generated by the use of services owned by Facebook, such as WhatsApp or Instagram, or by the use of third-party websites and apps, which have embedded Facebook products such as the "like" or "log in" button or analytical services such as "Facebook Analytics". These data will be transmitted to Facebook via APIs the moment the user calls up that third party's website for the first time. See Bundeskartellamt, *Preliminary Assessment*..., p. 2.

[29] *Ibidem*, pp. 2–3.

[30] *Ibidem*, p. 2; Bundeskartellamt, *Facebook*, *exploitative*..., p. 1.

[31] *Ibidem*, p. 11.

[32] *Ibidem*.

the corresponding processing of personal data can be considered if they affect competition[33].

Since the case was examined under national competition law (Section 19 (1) GWB), the authority relied upon the relevant case law of the Federal Court of Justice (*Bundesgerichtshof*, BGH) to substantiate its approach (in particular, *VBL-Gegenwert* and *Pechstein* cases)[34]. According to the BGH's judgements, business terms, which violate, respectively, German Civil Code and constitutional rights, are considered abusive under Section 19 (1) GWB, in particular, if applied as a manifestation of market power or superior bargaining power of an undertaking concerned[35]. The BGH considers that Section 19 GWB must be asserted in cases where one contractual party is so powerful that it can dictate the terms of the contract, which may breach provisions of other branches of law and abolish the contractual autonomy of the other party[36].

In the view of the *Bundeskartellamt*, as far as the appropriateness of conditions agreed upon in an unbalanced negotiation is concerned, the BGH's case law applies to all other areas of law. In particular, it also applies to data protection law, which aims to "counterbalance asymmetries of power between undertakings and individuals and ensure an appropriate balancing of interests between data controllers and data subjects"[37]. Thus, the *Bundeskartellamt* concluded that to protect the constitutional right to informational self-determination, which was implemented by data protection law, Section 19 GWB must be applied in the case at issue, where Facebook was so powerful that it was able to impose on users the contractual terms that were in breach of data protection law[38]. Thus, according to the *Bundeskartellamt*, the EU data protection regulations, based on constitutional rights, should be considered when assessing whether data processing terms are appropriate under competition law[39].

The *Bundeskartellamt* appears to argue that Facebook's potential to unilaterally impose terms of service on users is rooted in Facebook's dominant position

---

[33] Autorite de la Concurrence and Bundeskartellamt, Competition law and data, 2016, p. 23, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob¼publicationFile&v¼2 (accessed 1.11.2021).

[34] *Ibidem*, pp. 7–9; Case B6-22/16 *Facebook*, *Bundeskartellamt* decision of 6 February 2019, paras 525–534; Case KZR 6/15 *Pechstein*, BGH judgement of 7 June 2016, and KZR 61/11 *VBL vs. Gegenwert*, BGH judgement of 6 November 2013.

[35] Bundeskartellamt, *Bundeskartellamt prohibits…*, p. 8; Case KZR 6/15 *Pechstein*, BGH judgement of 7 June 2016, and case KZR 61/11 *VBL vs. Gegenwert*, BGH judgement of 6 November 2013.

[36] Bundeskartellamt, *Facebook*, *exploitative*…, p. 8; G. Colangelo, M. Maggiolino, *Antitrust über alles. Whither competition law after Facebook?*, "World Competition Law and Economics Review" 2019, Vol. 42, p. 355.

[37] Bundeskartellamt, *Facebook*, *exploitative…*, p. 8.

[38] *Ibidem*; G. Colangelo, M. Maggiolino, *Antitrust über.*…, p. 355.

[39] Bundeskartellamt, *Facebook*, *exploitative…*, p. 8.

on the relevant market[40]. The abuse at issue constitutes a manifestation of Facebook's market power and superior bargaining power[41]. In line with the reasoning of the BGH, Facebook conduct (i.e. the imposition of unlawful terms of service) would not be possible if it were not for its dominance[42].

Against this background, the *Bundeskartellamt* examined Facebook's data processing policies and found that Facebook had no effective justification for collecting data from third-party's services and combining that data with Facebook user accounts[43]. In particular, the *Bundeskartellamt* established that such data processing was not required to fulfil contractual obligations (Art. 6 (1) (b) GDPR), nor did a balancing of interests result in the conclusion that Facebook's interests in data processing outweigh the users' interests (Art. 6 (1) (f) GDPR)[44]. Moreover, Facebook also did not obtain valid consent for processing the data affected in this case. In the view of the *Bundeskartellamt*, since users consent to Facebook's terms and conditions for the sole purpose of concluding the contract, their consent cannot be considered freely given[45], as required by Art. 7 (4) GDPR[46]. Thus, the *Bundeskartellamt* concluded that Facebook processed user data from third party's sources without legal ground, contrary to the lawfulness principle enshrined in Art. 5 (1) (a) GDPR. The *Bundeskartellamt* assured that it closely cooperated with data protection authorities in the case[47]. However, no national data protection authority (DPA) has formally issued a decision or statement that would determine that Facebook infringed data protection laws in a way specified by the *Bundeskartellamt* in its decision.

Although the *Bundeskartellamt* stated that an abuse control proceeding against Facebook "would generally also be possible" under Art. 102 TFEU, at the same time it recognised that so far, only the above case law of the highest

---

[40] I. Małobęcka-Szwast, *Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi*, "Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, No. 8, p. 150; Case B6-22/16 *Facebook*, *Bundeskartellamt* decision of 6 February 2019, para 871.

[41] I. Małobęcka-Szwast, *Naruszenie prawa*..., p. 150.

[42] G. Schneider, *Testing Art. 102 TFEU in the digital marketplace: Insights from the Bundeskartellamt's investigation against Facebook*, "Journal of European Competition Law & Practice" 2018, Vol. 9, issue 4, pp. 223–224.

[43] Bundeskartellamt, *Bundeskartellamt prohibits*…, p. 6; Bundeskartellamt, *Facebook*, *exploitative*..., pp. 10–11.

[44] Bundeskartellamt, *Bundeskartellamt prohibits*…, p. 6; Bundeskartellamt, *Facebook*, *exploitative*..., p. 10.

[45] *Ibidem*.

[46] According to this provision, 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 the consent to the processing of personal data that is not necessary for the performance of that contract. For *Bundeskartellamts's* assessment under the GDPR, see Case B6-22/16 *Facebook*, *Bundeskartellamt* decision of 6 February 2019, paras 573–870.

[47] Bundeskartellamt, *Bundeskartellamt prohibits*…, p. 7.

German court explicitly allowed for taking into account constitutional or other legal principles (in this case, data protection) when assessing abusive practices of a dominant undertaking[48].

The *Bundeskartellamt* has not imposed any fine on Facebook. Instead, the authority issued a prohibition decision, in which it prohibited Facebook from: (1) stipulating in its terms of service that the use of its social network is subject to the company being able to collect and use data generated by the use of Facebook-owned services and assign them to the user accounts of the social network without the users' consent; (2) using terms and conditions allowing the company to collect user data generated by calling up third party's websites or using mobile apps via interfaces (Facebook Business Tools), and to use and assign them to Facebook user accounts; and (3) implementing the contested terms and conditions in actual data processing activities carried out by Facebook based on these terms[49]. With the aim of terminating the anticompetitive conduct, Facebook has been required to implement the necessary changes and to adapt its data and cookie policies accordingly within twelve months[50].

Facebook appealed against the decision of the *Bundeskartellamt* to the Higher Regional Court in Düsseldorf (*Oberlandesgericht Düsseldorf*, OLG Düsseldorf). Although the court has not yet decided on the merits of the complaint, at Facebook's request, pursuant to § 65 par 3 GWB, it assigned the complaint a suspensive effect due to serious doubts as to the legality of *Bundeskartellamt* decision[51]. As a result, the *Bundeskartellamt* decision would not have to be implemented until the appeal is decided on the merits.

However, the BGH did not share the stance of the OLG Düsseldorf expressed in its decision of 26 August 2019 (case number KVR 69/19). On 23 June 2020, in the long-awaited decision in the proceedings against Facebook for abuse of a dominant position, the BGH temporarily confirmed the decision of the *Bundeskartellamt* of 6 February 2019, repealed the decision of the OLG Düsseldorf and rejected Facebook's request to assign the complaint a suspensive effect. According to the BGH, there are no serious doubts that Facebook has abused its dominant position by applying the terms of service regarding the processing of users' personal data

[48] *Ibidem*, p. 6.

[49] *Ibidem*, p. 2, 7; Bundeskartellamt, *Facebook*, *exploitative*..., p. 12.

[50] *Ibidem*, p. 12.

[51] OLG Düsseldorf, *Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug*, Press release, 26 August 2019, https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/index.php_(accessed 1.11.2021); Case VI – Kart 1/19 (V), OLG Düsseldorf decision of 26 August 2019, https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf (accessed 1.11.2021).

prohibited by the *Bundeskartellamt*[52]. This means that Facebook must implement the *Bundeskartellamt* decision – at least until the final judgment in the main proceedings before the OLG Düsseldorf is delivered. It means that in Germany Facebook is not allowed to collect personal data of users from external sources (i.e. from third party websites as well as from other Facebook-owned services) and to assign this data to user accounts on Facebook without the consent of the users, and then continue to use them.

The BGH explained that the decisive factor in this case is not the question which the *Bundeskartellamt* brought to the fore in the contested decision, as to whether the processing and use of personal data of Facebook users is in accordance with the provisions of the GDPR. In the view of the BGH, the crucial issue is that the terms of use are abusive and leave private Facebook users no choice as to: (1) whether they want to use the network with a more intensive personalisation of the user experience, which may result in potentially unrestricted access to their online activities outside of Facebook, or (2) whether they only agree to personalisation based on the data they disclose themselves on Facebook. Thus, the BGH sees the abuse of a dominant position not in violating the GDPR (as the *Bundeskartellamt* did), but in limiting the freedom of choice of Facebook users by imposing specific terms and conditions by Facebook[53].

On 30 November 2020, Facebook again submitted a request to the OLG Düsseldorf for the suspensive effect of the appeal. With a so-called "hanging order" (*Hängebeschluss*) issued on the same day, the OLG Düsseldorf ordered the appeal against the abuse decision of the *Bundeskartellamt* provisionally to be suspensive[54]. It has thus temporarily suspended Facebook's obligation to implement the decision of the *Bundeskartellamt*. The OLG Düsseldorf did not allow the appeal of the *Bundeskartellamt* on points of law against this decision. In response to the Bundeskartellamt's non-admission complaint, the BGH approved the appeal against the decision of the appellate court. The fundamental question that has to be clarified by the BGH are the conditions under which "hanging orders" can be issued in the cartel administrative proceedings[55].

On 24 March 2021, the OLG Düsseldorf heard the case of *Bundeskartellamt* v. Facebook (case number VI Kart 2/19 [V]) but decided that the case would

[52] Case KVR 69/19, BGH decision of 23 June 2020, https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=fa3bf79f899e0a03ef9d918b672def4a&nr=109506&pos=0&anz=1 (accessed 1.11.2021).

[53] BGH, *Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook*, Press release, 23 June 2020, https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html (accessed 1.11.2021).

[54] Case VI-Kart 13/20 (V), OLG Düsseldorf decision of 30 November 2020.

[55] BGH, *Bundesgerichtshof überprüft "Hängebeschluss" des OLG Düsseldorf in Sachen Facebook*, *KVZ 90/20*, Press release, 16 December 2020, https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020162.html (accessed 1.11.2021).

be referred to the CJEU[56]. Seven questions referred by the OLG Düsseldorf are extensive and concern mainly the interpretation of the GDPR. The crucial question aims to determine whether the Bundeskartellamt is competent – for the purposes of monitoring abuses of competition law – to establish that the company's contractual terms relating to data processing and their implementation breach the GDPR and issue an order to end that breach, or whether there is a conflict with the system of jurisdiction set out in Art. 51 *et seq*. of the GDPR. If no, the question is whether Bundeskartellamt is allowed to determine, when assessing the balance of interests, whether those data processing terms and their implementation comply with the GDPR. The referral of several questions to the CJEU for a preliminary ruling may clarify the scope of competence of national competition authorities and dispel doubts which have arisen in the legal scholarship in this regard. However, it will certainly not shorten the already lengthy proceedings.

If one looks at the timeline of the proceedings, it does not encourage optimism, in particular given the dynamic character of the digital markets. After almost 5 years since the beginning of the proceedings and 2 years since the issuance of the Bundeskartellamt decision, Facebook has still not been effectively forced to change its abusive data practices. Apart from these procedural aspects, it is worth noting that the case still has to be decided on merits by the OLG Düsseldorf, and the latter can decide only after the CJEU issues a preliminary ruling.

4.2. CONSUMER PROTECTION LAW PERSPECTIVE: THE PROCEEDINGS OF THE AGCM

On 7 December 2018, the Italian Competition and Consumer Authority (AGCM) imposed two fines amounting to EUR 10 million on Facebook[57] for implementing two unfair commercial practices in breach of the Italian Consumer Code[58].

---

[56] Case C-252/21 *Facebook Inc. and Others v Bundeskartellamt*, Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021, OJ C 320 of 9 August 2021, p. 16. For the decision of the OLG Düsseldorf see Case Kart 2/19 (V), OLG Düsseldorf decision of 24 March 2021.

[57] Facebook Ireland Ltd. and its parent company Facebook Inc.

[58] Autorità Garante della Concorrenza e del Mercato, *Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes*, Press release, 7 December 2018, https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes (accessed 1.11.2021); *Italian regulator fines Facebook £8.9m for misleading users*, "The Guardian" 7 December 2018, https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users (accessed 1.11.2021). The Code implements the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC,

First, the Italian agency found that Facebook violated national provisions of consumer law by misleading users who register in the Facebook platform as to the extent to which their personal data will be used for commercial purposes. In the view of the AGCM, consumers are not adequately and immediately informed during the creation of the account that the data they provide will be used for commercial purposes. The authority noted that Facebook emphasizes only the free nature of the service but not the commercial objectives that underlie the provision of the social network service. Thereby, Facebook induces users into making a transactional decision (i.e. to register in the social network and to continue using it) that they would not have taken if they were in possession of complete information[59].

The second commercial practice that the AGCM has found unfair was transferring the registered users' data, without their prior express consent, from the social platform to third party websites or applications and vice versa, to use this data for profiling and other commercial purposes. In the view of the authority, this practice should be considered aggressive, because Facebook exerts undue influence on users by using a default setting consisting of the broadest consent to data sharing (in this case, users could in fact only deselect the pre-setting operated by Facebook, without being able to make a free, informed choice). When users chose to limit their consent, they faced significant restrictions on the use of the social network and third party websites or applications, which induced users to keep the pre-selected choice (i.e. unlimited consent to data processing). The AGCM stated that this mechanism may, through undue influence, significantly limit the freedom of choice of the average consumer, thus forcing him to make a transaction decision that he would not otherwise have taken – in this case, to consent to the processing of his personal data by third parties basically for unlimited purposes[60].

Although the AGCM did not mention the GDPR provisions in its decision, its findings could be equally considered as the infringement of, *inter alia*, the principle of transparency and the information obligation referred to in Art. 12 and Art. 13 GDPR (commercial practice) and the principle of lawfulness (Art. 5 (1) (a) of the GDPR in conjunction with Art. 6 (1) (a) of the GDPR) by processing of personal data without a legal basis. The consent given by users at the registration stage could be deemed not voluntary and informed – Art. 4 (11) of the GDPR in conjunction with Art. 6 (1) (a) and Art. 7 (4) of the GDPR) (second practice).

98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No. 2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices Directive"), OJ L 149 of 11 June 2005, p. 22.

[59] *Facebook Inc. and Facebook Ireland Ltd*, AGCM Decision of 29 November 2018, paras 4, 18–22, 55–56. Text of the decision (only in Italian) is available at: https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf ("Decision of the AGCM").

[60] Decision of the AGCM, paras 5, 23–32, 57–67.

While admitting that the proceedings were conducted efficiently and the decision of the AGCM was delivered rather fast, one may question the actual deterrent effect of the fine imposed[61]. According to Italian consumer law, the AGCM can impose a maximum fine of EUR 5 million per each unfair commercial practice (in this case the fine totalled EUR 10 million because it involved two practices)[62]. Comparing to fines that can be imposed for breaching competition law (i.e. generally 10% of the undertaking's annual turnover)[63], the amount of the fine imposed seems rather limited, even despite the fact it was a maximum possible fine under Italian consumer law and was doubled due to finding two practices. It seems that the national limits of the amounts of fines are not suitable when a consumer protection agency is confronted with practices of global corporations like Facebook, which generate enormous revenue. The relatively low amount of fine and the fact that the AGCM did not impose any behavioural commitments on Facebook may undermine the effectiveness of such enforcement – it is rather unlikely that Facebook confronted with such a decision will change its data practices[64]. In fact, in February 2021 the AGCM had to sanction Facebook Ireland Ltd. and its parent company Facebook Inc. again, this time for a total of EUR 7 million because the companies had failed to comply with the order issued against them in November 2018[65]. The AGCM's investigation showed that the two companies had not published the amending declaration and had not ceased the misleading practice. In the AGCM's view, although the companies removed the reference to the free nature of the service, they still do not provide an immediate and clear information on the collection and use of user data for commercial purposes[66].

4.3. DATA PROTECTION LAW PERSPECTIVE: THE PROCEEDINGS OF BELGIAN DPA

The Belgian DPA pursued a similar data practice by Facebook but based on national data protection legislation and the GDPR. Belgian proceedings, which date back to 2015, concerned alleged infringements of data protection laws by Facebook Inc., Facebook Ireland Ltd., and Facebook Belgium BVBA (collectively referred to as "Facebook"), consisting, *inter alia*, of the unlawful collection and

[61] M. Botta, K. Wiedemann, *op. cit.*, p. 444.

[62] Decision of the AGCM, paras 72 *et seqq*.

[63] The maximum fine that the European Commission and national NCAs can impose for breaching Art. 101 and 102 TFUE amounts to 10% of the undertaking's annual turnover.

[64] M. Botta, K. Wiedemann, *op. cit.*, p. 444.

[65] Autorità Garante della Concorrenza e del Mercato, *IP330 – ICA: Facebook sanctioned for 7 Million*, Press release, 17 February 2021, https://en.agcm.it/en/media/press-releases/2021/2/IP330 (accessed 1.11.2021); *Facebook Inc. and Facebook Ireland Ltd*, AGCM Decision of 9 February 2021, https://www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf (accessed 1.11.2021).

[66] Autorità Garante della Concorrenza e del Mercato, *IP330 – ICA…*

use of information on the private browsing behaviour of Internet users in Belgium by means of technologies such as cookies, social plugins, and pixels. The DPA found that Facebook uses various technologies to monitor and track individuals when they browse from one website to another, and then uses the information collected to profile their browsing behaviour and on that basis shows them targeted advertising, without properly informing the persons concerned or obtaining their valid consent. Facebook carries out these practices regardless of whether or not the person concerned is a Facebook registered user, i.e. has signed up or not to Facebook's social network[67]. The DPA requested that Facebook be ordered to cease, with respect to any Internet user established on the Belgian territory, to place, without their consent, cookies that remain active for two years on the devices used by those individuals when browsing a web page in the Facebook.com domain or the website of a third party, as well as to cease collecting data, in an excessive manner, by means of social plugins and pixels on third-party websites. The DPA also requested the destruction of all personal data obtained by means of cookies and social plugins relating to each Internet user established on the Belgian territory (the case at issue concerned processing only on the Belgian territory). The President of the Court of First Instance in Brussels issued an interim order of 9 November 2015, in which it confirmed that it had jurisdiction to hear the case and that the action was admissible with regard to all three defendants. The court also provisionally ordered the defendants to cease certain activities with regard to the Internet users situated on the Belgian territory[68].

On 2 March 2016, Facebook filed a notice of appeal against that order with the Brussels Court of Appeal. In a judgment of 29 June 2016, the court amended the first-instance order and ruled that it had no jurisdiction with regard to the actions against Facebook Inc. and Facebook Ireland Ltd., whereas it does have jurisdiction in respect of the action brought against Facebook Belgium BVBA. As a result, the main proceedings became restricted to the actions against Facebook Belgium BVBA. That appeal was overturned and on 16 February 2018, the Court of First Instance ruled on the merits and backed the findings of the DPA[69]. Facebook appealed against this decision and argued that when the GDPR became applicable in 2018, the Belgian DPA lost its competence to continue the legal proceedings in this case. In the view of Facebook, since Facebook's lead supervisory authority under the GDPR is the Irish Data Protection Commission, the case

[67] Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:5, Opinion of AG Bobek, paras 19–23.

[68] Gegevensbeschermingsautoriteit, *The judgment in the Facebook case*, Press release, 10 November 2015, https://www.dataprotectionauthority.be/citizen/the-judgment-in-the-facebook-case (accessed 1.11.2021).

[69] Gegevensbeschermingsautoriteit, *Victory for the Privacy Commission in Facebook proceeding*, Press release, 16 February 2018, https://www.dataprotectionauthority.be/citizen/victory-for-the-privacy-commission-in-facebook-proceeding (accessed 1.11.2021).

could only be enforced by the Irish DPA. The Brussels Court of Appeal referred several questions to the CJEU, including whether the "one-stop-shop" mechanism introduced by the GDPR[70] prevents national DPA from initiating proceedings in the national courts and enforcing data protection rules despite the fact it is not a lead supervisory authority in the case at issue[71].

The question that was finally decided by the CJEU on 15 June 2021[72] is of crucial importance for enforcing data protection rules in case of cross-border processing, i.e. almost all processing activities by incumbent platform providers. Advocate General M. Bobek in his opinion expressed the view, which was later endorsed by the CJEU, that the lead DPA has a general competence over cross-border data processing, including the commencement of judicial proceedings for the breach of the GDPR, and, by implication, the other data protection authorities concerned enjoy a more limited power to act in that regard. However, both the AG and the CJEU emphasize that the lead DPA cannot be deemed as the sole enforcer of the GDPR in cross-border situations and must, in compliance with the relevant rules and time limits provided for by the GDPR, closely cooperate with the other DPA concerned, the input of which is crucial in this area[73]. The CJEU observes that the GDPR establishes certain exceptions to the general rule that it is the lead supervisory authority which is competent to adopt decisions in the context of the "one-stop-shop" mechanism, in particular urgency mechanism from Art. 66 GDPR[74]. On the top of that the CJEU notes that where a competent supervisory authority does not comply with the obligations for mutual assistance imposed on it by the GDPR (as is the case with the Irish DPA – lead supervisory

[70] "One-stop-shop" mechanism was introduced in Art. 56 GDPR. Art. 56(1) GDPR states that the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Art. 60 GDPR. According to Article 56(6) GDPR, the lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

[71] See Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483. The CJEU has to decide i.a. whether (1) the GDPR permits a supervisory authority of a Member State to bring proceedings before a court of that State for an alleged infringement of that regulation with respect to cross-border data processing, where that authority is not the lead supervisory authority with regard to that processing, (2) or the new "one-stop-shop" mechanism prevents such a situation from happening.

[72] Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483.

[73] CJEU, *Advocate General's Opinion in Case C-645/19 Facebook Ireland Limited*, *Facebook INC*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, Press release, 13 January 2021, https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-01/cp210001en.pdf (accessed 1.11.2021); Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483, para 53.

[74] Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021], ECLI:EU:C:2021:483, paras 57–63.

authority for most tech giants), the supervisory authority concerned can bring actions against any alleged infringement of the GDPR before a court of that Member State even though it is not the lead supervisory authority. The judgement was welcomed by the consumer organizations as it bolsters GDPR enforcement and helps better protect consumer data[75]. Now the Brussels Court of Appeal has to decide on the merits based on the CJEU's guidance.

If we look at the length of these proceedings, the enforcement by data protection authorities also raises concerns over its effectiveness. Given that this case has been initiated in 2015 and considering the rapid technological changes that take place in the context of tracking technologies, one may question whether it is still reasonable to continue this case in the current scope and form. It is also a good example of lack of cooperation between DPAs, despite the cooperation mechanisms implemented by the GDPR (in particular, Art. 60–62 GDPR), and the consequences it may lead to.

As I have tried to evidence above, all the above proceedings have certain flaws and awareness of their existence may help to avoid enforcement mistakes and contribute to their effectiveness. One could argue that if the actions of all engaged agencies were coordinated both at national and EU level, Facebook would be effectively pressured to change its data practices, which share some common features. Acting on their own, the agencies can impose remedies or fines, but their impact is postponed or diminished due to lengthy appeal procedures or due to national legislation which sets the insufficient limits to the fines imposed. All these proceedings have lasted for several years and either stuck in the appeal procedure or their actual severeness for Facebook is rather limited. The enforcement actions undertaken in these cases by different agencies have so far not managed to force Facebook to change its doubtful data practices, neither at the EU nor national level.

5. UNCOORDINATED ENFORCEMENT: TOOTHLESS ENFORCEMENT?

Uncoordinated enforcement undertaken by national agencies and pursuing certain practices by platforms operating at least on an EU-wide basis separately and based solely on national laws (in other words, acting in enforcement silos)[76] may be insufficient or simply put – toothless. Lack of cooperation between

[75] BEUC, *EU court ruling to bolster GDPR enforcement and help protect consumer data*, Press release, 15 June 2021, https://www.beuc.eu/publications/eu-court-ruling-bolster-gdpr-enforcement-and-help-protect-consumer-data/html (accessed 1.11.2021).

[76] A. Ezrachi, A. Reyna, *op. cit.*, p. 22.

different agencies, both at the national and EU level, casts doubt on the effectiveness and soundness of such enforcement and may compromise consumer welfare and data subject (consumer) rights. Such approach may even distort the functioning of the internal market if different national agencies manage to impose distinct remedies on a firm operating and offering services to consumers across the EU.

Moreover, it should also be noted that uncoordinated enforcement actions may also lead to contradictory decisions of different authorities and incompatible remedies. That, in turn, may create legal uncertainty, both on the part of consumers and companies. If competition and consumer protection authorities, on the one hand, and supervisory authorities, on the other, simultaneously adjudicate on a violation of the data protection laws, it may lead to a double-track enforcement and interpretation of the provisions of the GDPR, as well as a double punishment for *de facto* same infringement. Such a double-track application of the GDPR may, in turn, lead to divergent decisions made on the basis of the same provisions and under the same circumstances.

It is not difficult to imagine a situation where based on the same facts a consumer protection authority finds that a certain practice infringes the interests of consumers to the extent it violates data protection rules, and the supervisory authority reaches a different conclusion and finds that no such violation has occurred. Since the violation of the GDPR in such a scenario would be a criterion for assessing the legality (fairness) of a given practice by a competition and consumer protection authority, such divergences in the interpretation of the data protection provisions may have far-reaching consequences, both for proceedings in the field of competition, consumer, and data protection laws.

One should also be mindful that competition, consumer, and data protection authorities must act on the basis and within the limits of the law, in accordance with the principle of legality, which is a common concept to all EU Member States' constitutions. Thus, if competition and consumer protection authorities claim competence to find a breach of data protection law, without having a proper legal basis in national law and without due procedures, they risk being accused of acting outside the law in a manner contrary to the principle of legality[77].

This question is particularly important in the case of enforcing of data protection law, as the competence of supervisory authority to control compliance with data protection rules follows directly from the EU primary law. The obligation for Member States to establish supervisory authorities and exercise institutional supervision over the processing of personal data is one of the foundations of the EU data protection system, which is mentioned in the Treaty on the Functioning of the European Union (Art. 16 (2) TFEU) and the Charter of Fundamental Rights (Art. 8 (2) of the CPP), as well as in a secondary law – the GDPR. The GDPR sets out detailed requirements and tasks of the supervisory authority. Art. 51 GDPR

[77] I. Małobęcka-Szwast, *Naruszenie prawa…*, p. 151.

stipulates that each member state is obliged to ensure that at least one independent public authority is responsible for monitoring the application of the GDPR. National laws should therefore determine the public authority which is to act as supervisory authority. This provision explicitly allows a member state to entrust the task of monitoring compliance with the GDPR to more than one supervisory authority, but their competence should be explicitly expressed in national laws[78].

6. COORDINATED AND CROSS-INSTITUTIONAL ENFORCEMENT: A WAY FORWARD?

Data practices that violate data protection law can breach also other areas of law, in particular competition and consumer protection laws. For this reason, to ensure consistent application of competition, consumer, and data protection laws it is proposed to introduce a systematic cooperation mechanism between supervisory authorities and competition and consumer protection authorities, both at the national and EU level. Calls for coordinated and cross-institutional enforcement have been present for several years now. The EDPS[79], the BEUC[80], and some authors[81] have endorsed the idea of introducing cooperation mechanisms between respective authorities and integrated approach to enforcement in the digital economy.

I would like to contribute to this debate by adopting the data protection perspective.

At the national level, where the assessment of the compliance of a given practice with competition and consumer protection laws depends on the finding of a breach of the GDPR by a firm, two solutions are possible. The first solution could be used in a situation where, in a given case, the supervisory authority has

[78] The Polish legislator decided that the role of the supervisory body in Poland should be played by only one public body – the President of the Personal Data Protection Office, as evidenced by Art. 34 sec. 2 of the Act on personal data protection. Therefore, currently in Poland, there is only one supervisory authority entrusted with the monitoring of compliance with the GDPR.

[79] European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (accessed 1.11.2021).

[80] BEUC, *BEUC calls for a cross-institutional scrutiny of Facebook's data practices*, 18 April 2019, https://www.beuc.eu/publications/beuc-x-2019-024_beuc_calls_for_a_cross-institutional_scrutiny_of_facebooks_data_practices_.pdf (accessed 1.11.2021); A. Ezrachi, A. Reyna, *op. cit*., pp. 22–25.

[81] See e.g. W. Kerber, *Digital markets*, *data and privacy: Competition law*, *Consumer law*, *and data protection*, "Journal of Intellectual Property Law & Practice" 2016, Vol. 11, issue 11, p. 856 *et seqq*; M. Botta, K. Wiedemann, *op. cit*., pp. 444–445; A. Reyna, *op. cit.*

already issued a legally binding decision stating that the firm (data controller) violated the provisions of the GDPR. In this case, if it is relevant to the case at issue, the competition and consumer protection authority may rely on the findings made by the supervisory authority in such a decision. This solution would allow to avoid possible discrepancies between the positions of the supervisory authority and the competition and consumer protection authorities.

The second solution could apply in cases which have not yet been investigated by the supervisory authority. In such cases, competition and consumer protection authorities could be obliged to consult the supervisory authority, and such obligation should be stipulated by law. To counter any allegations against such a procedure as regards the potential interference with the independence of competition and consumer protection authorities, the opinion expressed by the supervisory authority would not be binding. A competition and consumer protection authority could therefore disagree with the supervisory authority's position. However, it seems that in practice the competition and consumer protection authorities would be willing to take into account the opinion expressed by an authority specialised in a given field (supervisory authority). At least in Poland, such a mechanism would not be a completely innovative solution, as the Polish administrative procedure provides for a general cooperation mechanism between public administration bodies in cases set out in specific provisions. According to Art. 106 § 1 of the Polish Code of Administrative Procedure, if a legal provision makes issuance of a decision conditional on the taking of a position by another authority (expressing an opinion or consent or expressing a position in a different form), the public administration body dealing with the matter may issue a decision only after that authority has taken a position[82].

Moreover, due to the fact that data practices and processing activities may be of a cross-border nature, it is proposed to introduce a cooperation mechanism between supervisory authorities and competition and consumer protection authorities at the EU level. Such cooperation could be coordinated, for example, by the European Data Protection Board or the European Commission and would be aimed at developing a uniform approach to the assessment of data practices by a given controller within the EU. It could take the form of institutionalised cooperation or *ad hoc* cooperation on a specific case.

A model for organising such cooperation may be the mechanism of cooperation between supervisory authorities provided for in Art. 60–62 GDPR and within the European Data Protection Board (EDPB), cooperation between competition authorities and the European Commission within the European Competition Network (ECN) or cooperation between consumer protection authorities within the Consumer Protection Cooperation Network (CPCN).

[82] I. Małobęcka-Szwast, *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów*, "Monitor Prawniczy – Dodatek" 2020, No. 23, p. 100.

Already in 2017, the EDPS launched the Digital Clearinghouse, a voluntary network of regulators involved in the enforcement of legal regimes in digital markets, which aims to "bring together agencies from the areas of competition, consumer, and data protection willing to share information and discuss how best to enforce rules in the interests of the individual"[83]. Although one should praise such initiative, due to its informal character and insufficient commitment of the authorities involved, it seems that it has not released its full potential yet[84]. Therefore, to ensure effective enforcement of competition, consumer, and data protection laws in the EU it is proposed to institutionalise the cooperation mechanisms in a similar vein as the ECN, the CPCN or the EDPB. While creating cooperation mechanism "fit for the Digital Age" one could benefit from experiences of these EU networks of authorities.

Such solution would allow for the consistent application of the GDPR, competition, and consumer protection laws and, consequently, would enable the effective achievement of the objectives of the GDPR, competition and consumer protection laws within the EU. At the same time, by introducing institutionalised cooperation between the authorities, competition, and consumer protection authorities would dismiss the allegations that they are not competent to base the assessment of practices under competition and consumer protection laws on the violations of the GDPR provisions.

The joint enforcement bargaining power of all agencies speaking with one voice would be undoubtedly stronger and more effective when they would cooperate with each other rather than acting separately on their own, protecting only their nationals. One could expect that if the Facebook "saga" was coordinated at the EU level, for example, by the Digital Clearinghouse, the outcome of the proceedings would be different and could lead to EU-wide change of Facebook's practices for the benefit of the EU consumers.

7. CONCLUSION

In the digital economy it is not possible to easily separate consumer, competition, and data protection issues from each other. These three areas of law are intertwined and complement each other on various levels, which should also be reflected in their enforcement. It is argued that to ensure effective competition in the digital economy we need effective enforcement of data protection and consumer laws, and vice versa. Effective enforcement of competition rules is needed to better protect fundamental right to data protection and consumer rights.

[83] European Data Protection Supervisor, Opinion 8/2016…

[84] A. Ezrachi, A. Reyna, *op. cit.*, p. 22; M. Botta, K. Wiedemann, *op. cit*., p. 445.

As evidenced by the Facebook enforcement "saga", uncoordinated enforcement efforts by competition, consumer, and data protection agencies, which act "in silos" and focus only on national perspective, poses a threat to effective protection of consumer welfare and data subject (consumer) rights in the EU. Such approach may even distort the functioning of the internal market if different national agencies manage to impose distinct remedies on firm operating and offering services to the consumers across the EU.

Therefore, it is proposed to introduce cooperation mechanisms between different agencies, both at the EU and national level, in cases involving data practices that may potentially infringe all the three areas of law. It is argued that only a coordinated, cross-institutional, and multi-disciplinary enforcement can provide an effective response to practices applied by digital giants, such as Facebook, Google, Amazon or Apple, and ensure that consumer welfare and data subject (consumer) rights are not compromised.

REFERENCES

Articles, opinions and reports

Autorite de la Concurrence and Bundeskartellamt, Competition law and data, 2016, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob¼publicationFile&v¼2 (accessed 1.11.2021)

Botta M., Wiedemann K., *The interaction of EU competition*, *consumer*, *and data protection law in the digital economy: The regulatory dilemma in the Facebook odyssey*, "The Antitrust Bulletin" 2019, Vol. 64

Colangelo G., Maggiolino M., *Antitrust über alles. Whither competition law after Facebook?*, "World Competition Law and Economics Review" 2019, Vol. 42

Colangelo G., Maggiolino M., *Data protection in attention markets: Protecting privacy through competition?*, "Journal of European Competition Law & Practice" 2017, Vol. 8, issue 6

Costa-Cabral F., Lynskey O., *Family ties: The intersection between data protection and competition in EU Law*, "Common Market Law Review" 2017, Vol. 54, issue 1

European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 2016, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (accessed 1.11.2021)

European Data Protection Supervisor, Preliminary Opinion, 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, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (accessed 1.11.2021)

Ezrachi A., Reyna A., *The role of competition policy in protecting consumers' well-being in the digital era*, BEUC 2019, https://www.beuc.eu/publications/beuc-x-2019-054_competition_policy_in_digital_markets.pdf (accessed 1.11.2021)

Graef I., *Blurring boundaries of consumer welfare: How to create synegies between competition*, *consumer*, *and data protection law in digital markets*, (in:) M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė (eds.), *Personal data in competition*, *consumer protection*, *and intellectual property law: Towards a holistic approach?*, Berlin 2018

Helberger N., Zuiderveen Borgesius F., Reyna A., *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, "Common Market Law Review" 2017, Vol. 54, issue 5

Kerber W., *Digital markets*, *data and privacy: Competition law*, *consumer law*, *and data protection*, "Journal of Intellectual Property Law & Practice" 2016, Vol. 11, issue 11

Lamadrid A., Villiers S., *Big data*, *privacy and competition law: Do competition authorities know how to do it?*, "CPI Antitrust Chronicle" 2017

Małobęcka-Szwast I., *Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi*, "Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, No. 8, https://ikar.wz.uw.edu.pl/images/numery/55/139.pdf (accessed 14.01.2022)

Małobęcka-Szwast I., *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów*, "Monitor Prawniczy – Dodatek" 2020, No. 23

Manne G.A., Sperry R.B., *The problems and perils of bootstrapping privacy and data into an antitrust framework*, "CPI Antitrust Chronicle" 2015, https://www.competitionpolicyinternational.com/assets/Uploads/ManneSperryMay-152.pdf (accessed 1.11.2021)

Mundt A., *Implications of the German Facebook decision.* Presentation from GCLC – Lunch Talk, 17 April 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Reden/L1/Andreas%20Mundt%20-%20%20Global%20Competition%20Law%20Centre.pdf?__blob=publicationFile&v=2 (accessed 1.11.2021)

OECD Secretariat, The interaction and coordination of competition policy and consumer policy: Challenges and possibilities (background note), DAF/COMP/GF(2008)10, 2008, https://www.oecd.org/regreform/sectors/40898016.pdf (accessed 1.11.2021)

Ohlhausen M.K., Okuliar A.P., *Competition*, *consumer protection*, *and the right [approach] to privacy*, "Antitrust Law Journal" 2015, Vol. 80

Reyna A., *Breaking down silos in public enforcement: Lessons from consumer-facing markets*, 2021, https://ssrn.com/abstract=3838697 (accessed 1.11.2021)

Schneider G., *Testing Art. 102 TFEU in the digital marketplace: Insights from the Bundeskartellamt's investigation against Facebook*, "Journal of European Competition Law & Practice" 2018, Vol. 9, issue 4

Case law

Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021], ECLI:EU:C:2021:483

Case C-645/19 *Facebook Ireland Limited*, *Facebook Inc.*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021], ECLI:EU:C:2021:5, Opinion of AG Bobek

Case C-252/21 *Facebook Inc. and Others v Bundeskartellamt*, Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021, OJ C 320 of 9 August 2021

Case VI – Kart 1/19 (V), OLG Düsseldorf decision of 26 August 2019, https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf (accessed 1.11.2021)
Case VI – Kart 13/20 (V), OLG Düsseldorf decision of 30 November 2020
Case KVR 69/19, BGH decision of 23 June 2020, https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=fa3bf79f899e0a03ef9d918b672def4a&nr=109506&pos=0&anz=1 (accessed 1.11.2021)
Case Kart 2/19 (V), OLG Düsseldorf decision of 24 March 2021
Facebook Inc. and Facebook Ireland Ltd, AGCM Decision of 29 November 2018, https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf (accessed 1.11.2021)
Facebook Inc. and Facebook Ireland Ltd, AGCM Decision of 9 February 2021, https://www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf (accessed 1.11.2021)
Case B6-22/16 *Facebook*, Bundeskartellamt decision of 6 February 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=8 (accessed 1.11.2021)
Case KZR 61/11 *VBL vs. Gegenwert*, BGH judgement of 6 November 2013
Case KZR 6/15 *Pechstein*, BGH judgement of 7 June 2016

Internet sources

Autorità Garante della Concorrenza e del Mercato, *Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes*, Press release, 7 December 2018, https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes (accessed 1.11.2021)
Autorità Garante della Concorrenza e del Mercato, *IP330 - ICA: Facebook sanctioned for 7 Million*, Press release, 17 February 2021, https://en.agcm.it/en/media/press-releases/2021/2/IP330 (accessed 1.11.2021)
BEUC, *BEUC calls for a cross-institutional scrutiny of Facebook's data practices*, 18 April 2019, https://www.beuc.eu/publications/beuc-x-2019-024_beuc_calls_for_a_cross-institutional_scrutiny_of_facebooks_data_practices_.pdf (accessed 1.11.2021)
BEUC, *EU court ruling to bolster GDPR enforcement and help protect consumer data*, Press release, 15 June 2021, https://www.beuc.eu/publications/eu-court-ruling-bolster-gdpr-enforcement-and-help-protect-consumer-data/html (accessed 1.11.2021)
BGH, *Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook*, Press release, 23 June 2020, https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html (accessed 1.11.2021)
BGH, *Bundesgerichtshof überprüft „Hängebeschluss" des OLG Düsseldorf in Sachen Facebook*, *KVZ 90/20*, Press release, 16 December 2020, https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020162.html (accessed 1.11.2021)
Bundeskartellamt, *Bundeskartellamt initiates proceeding against Facebook*, Press release, 2 March 2016, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/

Meldungen%20News%20Karussell/2016/02_03_2016_Facebook.html (accessed 1.11.2021)

Bundeskartellamt, *Bundeskartellamt prohibits Facebook from combining user data from different sources*, Press release, 7 February 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (accessed 1.11.2021)

Bundeskartellamt, *Facebook*, *exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing – Case Summary*, 15 February 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108 (accessed 1.11.2021)

Bundeskartellamt, *Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive*, 19 December 2017, p. 2, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=6 (accessed 1.11.2021)

CJEU, *Advocate General's Opinion in Case C-645/19 Facebook Ireland Limited*, *Facebook INC*, *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, Press release, 13 January 2021, https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-01/cp210001en.pdf (accessed 1.11.2021)

Gegevensbeschermingsautoriteit, *The judgment in the Facebook case*, Press release, 10 November 2015, https://www.dataprotectionauthority.be/citizen/the-judgment-in-the-facebook-case (accessed 1.11.2021)

Gegevensbeschermingsautoriteit, *Victory for the Privacy Commission in Facebook proceeding*, Press release, 16 February 2018, https://www.dataprotectionauthority.be/citizen/victory-for-the-privacy-commission-in-facebook-proceeding (accessed 1.11.2021)

Italian regulator fines Facebook £8.9m for misleading users, "The Guardian" 7 December 2018, https://www.theguardian.com/technology/2018/dec/07/italian-regulator-fines-facebook-89m-for-misleading-users (accessed 1.11.2021)

OLG Düsseldorf, *Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug*, Press release, 26 August 2019, https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2019/20190826_PM_Facebook/index.php (accessed 1.11.2021)

The world's most valuable resource is no longer oil, *but data*, "The Economist" 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 1.11.2021)