INSIGHT

META V BUNDESKARTELLAMT: SOMETHING OLD, SOMETHING NEW

PETER J. VAN DE WAERDT*

ABSTRACT: *Meta v Bundeskartellamt* is the culmination of an issue years in the making: the relation between data protection and competition. In contention is the Bka's finding that Meta's practice of combining personal data across its many services, in addition to data collected through the integration of its services into third-party websites and apps, constitutes a violation of competition law. In this case, the ECJ holds that a competition authority is at liberty to consider GDPR violations as a "vital clue" to a finding of abuse of dominance, provided it first requested the cooperation of the competent data protection authorities. Furthermore, it finds that, apart from consent, no legal bases from the GDPR justify Facebook's data processing. Through the principle of sincere cooperation, the Court opens the door to further integration of data protection and competition, acknowledging that data collection is at the core of digital market companies' business models. Although the case is based on German national law, there is reason to believe that the same line of reasoning could also apply to the European Commission, thus expanding its options in digital market oversight. In contrast, the Court's analysis of the GDPR is not quite as innovative, but still helpfully lists and reaffirms existing law.

KEYWORDS: *Meta v Bundeskartellamt* – competition law – data protection law – digital markets – sincere cooperation – GDPR.

I. INTRODUCTION

Back in 2019, when Meta was still just "Facebook", a competition Decision from the federal competition authority in Germany, the Bundeskartellamt (Bka), sparked the imagination of competition lawyers and data protection lawyers alike. In its Decision against Facebook, made in cooperation with German data protection authorities, it found an abuse of a dominant position on the basis of a violation of the General Data Protection Regulation (GDPR). Since then, the relations between European Union (EU) competition law and data protection law have only become more prominent.

* PhD researcher, University of Groningen, p.j.van.de.waerdt@rug.nl.

EUROPEAN PAPERS www.europeanpapers.eu ISSN 2499-8249
VOL. 8, 2023, NO 3, PP. 1077-1103 doi: 10.15166/2499-8249/703
(EUROPEAN FORUM, 8 JANUARY 2024), PP. 1077-1103

Today, in 2023, the case is more relevant than ever. It has not only served as a direct inspiration for the Digital Markets Act (DMA),[1] it has also finally come to a head through a European Court of Justice (ECJ/the Court) ruling on preliminary questions. In the *Meta v Bundeskartellamt* case, the ECJ finally had the opportunity to rule on the legality of using data protection violations in a competition case. Furthermore, it clarified how the GDPR should be applied to digital markets, specifically the market of social media, in terms of data combination within an ecosystem company, data analysis, personalization, and targeted advertising.

This *Insight* will first summarize the original Bka Decision and its result before the ECJ. Afterwards, it will provide some reflections on the judgement. In a way, the case can be characterized as "something old, something new".

In terms of "the new", we see the ECJ adopt a new approach to competition law's relation to data protection, and how this impacts both national competition authorities and the European Commission. Furthermore, this *Insight* will discuss how the judgement also empowers the European Commission to find abuse under competition law based on serious GDPR violations, in a way that it has never done before. The Bka's new and innovative approach, as confirmed by the ECJ in this case, opens new avenues of enforcement; not only for national authorities, but also for the Commission.

In contrast, "the old" refers to the old approach in the ECJ's application of the GDPR. Or rather, an approach that is much older than it first appears. Although the ECJ goes over art. 6 and art. 9 GDPR at great length, the extent to which any new data protection law can be derived from this case is questionable indeed.

This *Insight* thus aims to provide a comprehensive analysis of *Meta v Bundeskartellamt* and conclude with some suggestions for further research.

II. From German Competition Decision to EU Judgement

II.1. Bundeskartellamt Decision B6-22/16 of 6 February 2019

As stated above, the case all started with a Decision from the Bundeskartellamt, the federal German competition authority.[2] Since this Decision was meticulously drafted in order to justify the Bka's new approach to competition and data protection, and that justification proved successful before the ECJ, it is worth discussing in detail.

[1] Specifically, art. 5(2) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act); Commission staff working document SWD/2020/363 final of 15 December 2020, Impact assessment report accompanying the document proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Table 2 on p. 53.

[2] Bundeskartellamt, 'Decision B6-22/16 of 6 February 2019'.

Before this Decision was issued, the Bka consulted with German consumer organisations, Hamburg's Commissioner for Data Protection, and the Federal Commissioner for Data Protection, who all supported these proceedings.[3] Their blessing was particularly important, as the Decision relies heavily on the application of the GDPR for its finding of abuse.

The Bka Decision was taken under art. 19(1) GWB,[4] which prohibits the abuse of a dominant market position similarly to art. 102 TFEU. As such, it followed a similar structure as the European Commission would use, going over respectively market definition, market power, and finally abusive conduct. Ultimately, the Bka found that Meta had abused its dominant position on the market for social media because it had collected personal data of its users in violation of the GDPR.

a) Market Definition and Dominance

The Bka first determined the market on which Facebook was active. It found that Facebook was active on the market for social media in Germany. Notably, the Bka excluded professional social media platforms, such as LinkedIn, from the market; focussing instead on social media for private and personal use.[5] Professional networks, in the eyes of the consumer, have distinctly different functions from private social networks.[6] For example, only very few users indicated that they had ever used Facebook to search for employment. Since social media is multi-sided market,[7] the Bka also found Facebook active on the advertising market.[8] On advertising, a distinction can be made between between online and offline advertising.[9] Online advertising allows for far more and far more accurate targeting, which is a major feature for many advertisers.

However, the Bka noted that Facebook also had many branches beyond the social media platform and advertising alone. These other branches include Instagram and WhatsApp, but also "Facebook Business Tools".[10] These Business Tools, of which the Facebook Like button and Share button are the most widely recognized, are plug-ins which connect directly to third-party websites and apps. Indeed, Facebook's offering of these other kinds of services would become the main thrust of the Bka's arguments as regards abusive conduct.

[3] *Ibid.* para. 162.

[4] *Gesetz gegen Wettbewerbsbeschränkungen* 26 June 2013. lit: Law against competition limitations.

[5] Bundeskartellamt Decision B6-22/16 cit. para. 264.

[6] *Ibid.* paras 277-278.

[7] Meaning it acts as an intermediary between two or more types of consumers. In Facebook's case, it connects social media users to advertisers. One side of the market subsidizes the free service for the other side of the market. *Ibid.* paras 212-213.

[8] *Ibid.* para. 352-353.

[9] *Ibid.* paras 354-355.

[10] *Ibid.* paras 50-54.

As for dominance, the Bka focused strongly on the amount of daily active users. On the market defined above, only very few relevant competitors to Facebook exist, and it was found to have a share of over 95 per cent of daily active users.[11]

Additional factors only reinforced the finding of dominance. For example; the high barriers to entry on the market for social media due to its high dependence on network effects;[12] the high switching costs due to lacking data portability;[13] and finally access to "competitively relevant data" since Facebook has many sources of personal data and reaches many users.[14]

With all of these factors, the Bka had little difficulty finding Facebook dominant on the market for private-use social media.

b) GDPR Violation as Abusive Conduct

That said, for the purposes of this *Insight* the Bka's findings on the abusive conduct by Facebook are the most relevant.

The Bka justifies its competition law enforcement by arguing that privacy policies are in effect an extension of the terms of service, which function as the contract between Facebook and its consumers.[15] Under German law, unfair contractual obligations can constitute an abuse of dominance.[16] Therefore, unfair privacy policies can as well. The unfairness, and indeed the core of the Bka's enforcement proceedings, hinges on a violation of the GDPR by Facebook.

Namely, it found that Facebook was collecting and combining personal data from its consumers without a valid legal basis as is required under art. 6 and art. 9 GDPR.[17] Of particular concern was the fact that consumers who subscribe to the Facebook social media platform would also, by virtue of Facebook's privacy policy, be subject to data collection on Facebook's other services as well. Personal data from Instagram, WhatsApp, Oculus, and Facebook Business Tools was all available for collection after agreeing *only* to the social media platform's privacy policy. In other words, the pooling of data between the different branches of the Facebook ecosystem was the primary cause for concern.

The reason for such concern is two-fold:

Firstly, the Bka finds that for the type of data being collected about Facebook's users, art. 9 GDPR is in effect. Art. 9 effectively provides for a stricter regime of data protection where "Special categories of personal data" are involved. These include data relating to racial or ethnic origin, political opinions, religious beliefs, sexuality, health; sensitive data

[11] *Ibid.* para. 392-393.

[12] *Ibid.* paras 441-444.

[13] *Ibid.* para. 469.

[14] *Ibid.* para. 481.

[15] *Ibid.* paras 561, 564 – 566.

[16] *Gesetz gegen Wettbewerbsbeschränkungen* cit, art. 19. See also art. 102(a) TFEU, which considers "unfair trading conditions" abusive.

[17] Bundeskartellamt Decision B6-22/16 cit. paras 629 – 630.

which could cause a person to become subject to discrimination.[18] According to the Bka, there are a number of ways through which Facebook could amass this kind of data. For example, a social media user could simply post their dating preferences to their profile. However, some methods of collection were decidedly less obvious, and this is where the contention lies. In particular, because of the Facebook Business Tools, which collect data through third-party websites, Facebook was amassing highly sensitive data from any number of potential sources without the user's knowledge or consent. For example: Tinder, Queer.de,[19] official websites of political parties, and healthcare websites all feature integrated Facebook tools.[20]

Having access to these kinds of data sources can indirectly reveal sensitive personal data about an individual. A person who visits the Green Party's website once for a short amount of time does not as such reveal their political affiliations, but a person who visits the site often and also interacts with Facebook's integrated Like and Share buttons is likely to be left-leaning politically. According to the Bka, these kinds of indirect inferences, especially when they can be combined with Facebook's other data points about the individual, are enough to classify the data as sensitive under art. 9.[21] Since art. 9 GDPR is applicable, the relevant standards for data protection become more strict. This especially includes the standards of valid consent; *explicit* consent is needed.

Having established Facebook's data processing activities and the types of personal data involved, the Bka looks at the legal bases which can justify them. These are listed in art. 6 GDPR, as well as art. 9 GDPR in so far as sensitive data is concerned.

The Bka spent the most time examining the legal basis of consent; art. 6(1)(a) GDPR. Under the GDPR, consent must be "freely given, specific, informed and unambiguous".[22] 'Freely given' was especially problematic in Facebook's case. Recital 43 of the GDPR explicitly states that consent is not freely given if the provision of a service is conditional on that consent.[23] In other words, the ability to use the Facebook social media platform at all should not hinge on the user's consent.[24] In Facebook's case the problem was even greater, since the use of the social media platform was conditional on consent for data collection across the entire Facebook ecosystem. Moreover, the Bka held that freely given consent was not possible in this case, because of the "clear imbalance" between the user

[18] Hereinafter referred to as "sensitive data" for ease of use. For full list see: 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), art. 9.

[19] A website which is described by the Bka as a "homosexual partner exchange", but which also features news and articles about LGBTQ advocacy. Bundeskartellamt Decision B6-22/16 cit. para. 587.

[20] *Ibid.* para. 587.

[21] *Ibid.* para. 588.

[22] Art. 4(11) Regulation 2016/679 cit.

[23] Recital 43 Regulation 2016/679 cit.

[24] Bundeskartellamt Decision B6-22/16 cit. para. 645.

and Facebook.[25] Facebook's dominant position on the market for social media means that the average consumer does not have a realistic option to choose a different social media platform. An individual who wants to use social media to keep in touch with their friends is thus dependent on Facebook and must accept the privacy policy for its use. This does not comply with the spirit of consent as the GDPR envisions it. In cases where sensitive data under art. 9 is involved, the issue is further exacerbated, since the standard for consent is also stricter. Simply put: if Facebook does not have valid consent under art. 6 GDPR, then it *certainly* does not have the required explicit consent under art. 9. Considering that Facebook's extensive data combination, up to and including data obtained through third-party websites, often captures such data as well, the Bka effectively finds that data has been collected without legally valid consent on a large scale.[26]

That being said, consent is not the only possible legal basis under the GDPR. The Bka also discussed the other possibilities, and also found them inapplicable.

Under art. 6(1)(b) GDPR, data processing is lawful when "processing is necessary for the performance of a contract to which the data subject is party". Facebook claimed, at least for part of its processing activities, that this is the case. The Bka, however, held that Facebook's data processing might be useful for the functioning of its business model, but it was not "necessary".[27] After all, a social media platform could also be monetized in other ways, and data collection from off-Facebook sources could easily be restricted. There is no reason for the Like and Share buttons to send data to Facebook when they are not being interacted with by the user. In effect, the Bka applies a proportionality and subsidiarity test, and finds that Facebook's data collection is not necessary or proportional to the social media service contract it has with its consumers.

Art. 6(1)(c), (d), and (e) GDPR are all quite specific circumstances that rarely become relevant for a commercial actor. Nevertheless, Facebook relied on all of them, and the Bka in turn rejected all of them. Under these provisions, data processing can be legal if the undertaking is acting in compliance with a legal obligation to which it is subject, if it is in service to the vital interests of the consumer, or if it is carrying out a task in the public interest or in the exercise of official authority. According to the Bka, none of these would apply to Facebook:

- Although it might be asked to assist police investigations in the future, that does not impose on Facebook a legal obligation to collect all of its consumer data at this point in time;[28]

- Vital interests of the consumer only apply in life-or-death circumstances, which is not relevant to a social media platform;[29]

[25] *Ibid.* para. 646.
[26] *Ibid.* para. 650.
[27] *Ibid.* para. 690.
[28] *Ibid.* paras 716 – 719.
[29] *Ibid.* paras 720-722.; The traditional example for art. 6(1)(d) GDPR is an ambulance worker responding to an emergency. Processing the patient's medical records at that moment in time is in the patient's "vital interest".

- There was no evidence that Facebook was entrusted with a task in the public interest, nor did it exercise official authority.[30]

The last legal basis, art. 6(1)(f) GDPR, is a safety net. Data processing can be legal if it is necessary for the undertaking's own legitimate interest. However, it must then be balanced against the consumer's fundamental rights interests. Here, the Bka held that personal data analytics for commercial purposes is not in itself a sufficiently clear legitimate interest.[31] Although cybersecurity interests might be legitimate, Facebook was not able to explain why the collection and pooling of data throughout its entire ecosystem was legitimate. Personal profiling in itself cannot serve as a legitimate interest for Facebook entire data-driven business model.[32] Even if such a legitimate interest did exist, the data processing would not be necessary, and it would be overridden by the consumers' privacy interests. Consumers, even those with a Facebook social media account, should not have to expect that sensitive data about them is collected not only on the social media platform, but also on Instagram, WhatsApp, and anywhere that Facebook has its Business Tools integration.[33] Moreover, Facebook's dominance on the social media market made this hard for consumers to avoid, and Facebook had not implemented any protective measures to minimize the potential privacy impact of its data collection.[34]

Since none of the legal bases of art. 6 or art. 9 GDPR apply to Facebook's data processing activities, the Bka concluded that Facebook was illegally collecting personal data in violation of the GDPR.

However, while the above might justify a GDPR fine, it does not yet justify competition law intervention. Therefore, the final step in the Bka's reasoning is bridging the gap between the GDPR violation and a finding of abuse of dominance. To do so, it explained that not only was the GDPR violated, the violation also had anti-competitive effects on the social media market. Data is an important factor in the business models of digital market companies such as Facebook. Collecting and analysing personal data allows a service to personalize itself to the individual user, as well as target them more effectively with advertising. As a result, advertising space can be rented at a higher price, thereby also improving that undertaking's competitive position on the advertising market. In other words: personal data enjoys network effects.[35]

More importantly, according to the Bka, is that Facebook's data collection also increases the barriers to entry on the market for social media. Competitors who do not have the same expansive dataset as Facebook does will not be able to compete to the

[30] *Ibid.* paras 724-726.
[31] *Ibid.* para. 738.
[32] *Ibid.* paras 738–739.
[33] *Ibid.* para. 778.
[34] *Ibid.* paras 787–788.
[35] See generally: P van de Waerdt, '"Everything the Data Touches Is Our Kingdom": Reassessing the Market Power of "Data Ecosystems"' (2022) World Competition Law and Economics Review 65.

same level. This is not in itself anti-competitive, since this could also be seen as simply competing on product quality, but it becomes a problem when it is the result of illegal data collection. In effect, the Bka finds that Facebook is illegitimately improving its competitive position vis-à-vis its competitors who who do -or at least are assumed to- comply with the GDPR.[36] Finally, although it is hard to quantify, Facebook's conduct also leads to potential consumer harm. Users forced to give up more data than they would want can lead to behavioural changes and risks identity theft or fraud.[37] More generally, consumer welfare in a broad sense is reduced, in that consumers face non-material damage from privacy infringements.

It is noteworthy that the Bka acknowledges both exploitative and exclusionary anti-competitive effects in its Decision, and seems to give both of them approximately equal weight. Although it aimed to strengthen its case against a likely appeal by including both elements, the Decision strongly implies that either element would have been sufficient to find a violation.[38]

With this, the Bka had made its case. The GDPR has been infringed, because there is no legal basis for broad data collection from off-Facebook sources. This conduct, performed by a dominant undertaking, has anti-competitive effects and harms consumer welfare. Therefore, it qualifies as an abuse of dominance under competition law. As a remedy, Facebook was to cease using its inadequate privacy policy, and cease combining data without first ensuring legally valid consent.[39]

Afterwards, the Decision was subject to legal challenges within the German court system. Facebook appealed to the Oberlandesgericht Düsseldorf,[40] which granted Facebook interim relief and strongly hinted that it would quash the Decision on the merits. Then the Bka filed for cassation, upon which the Düsseldorf judgement was overturned by the Bundesgerichtshof.[41] Both of these judgments are extremely interesting in their own right, as they show very different perspectives on competition law and the role of personal data therein. However, for the purposes of this contribution, the focus will be on what came next; on the merits the case returned to the Oberlandesgericht, which saw fit to refer preliminary questions to the European Court of Justice.

[36] Bundeskartellamt Decision B6-22/16 cit. para. 888.

[37] *Ibid.* paras 909–910.

[38] *Ibid.* Compare paras 905, and 909–910, 914. An interesting element of multi-sided digital markets is that the same conduct can give rise to both exploitative and exclusionary effects. Exploitation of consumers on one side raises the barriers to entry on the other, and the line between the two types of anti-competitive effects starts to blur. The Bka Decision does not relevantly examine this connection, however.

[39] *Ibid.* paras 917, 940, and 946.

[40] Oberlandesgericht Düsseldorf Judgement of 26 August 2019, WRP 2019 *Facebook v Bundeskartellamt*.

[41] Der Bundesgerichtshof, *Pressemitteilungen Aus Dem Jahr 2020 - Bundesgerichtshof Bestätigt Vorläufig Den Vorwurf Der Missbräuchlichen Ausnutzung Einer Marktbeherrschenden Stellung Durch Facebook* www.bundesgerichtshof.de; Bundesgerichtshof Judgment of 23 June 2020, Beschluss KVR 69/19 *Facebook v Bundeskartellamt*.

II.2. Judgment of the Court (Grand Chamber) of 4 July 2023

As one might imagine, the Bka's innovative approach in its Decision, using data protection arguments to find a competition law violation, raised a number of legal questions and challenges. Given that both competition law and data protection law are subject to EU law, it should not be surprising that preliminary questions were asked regarding the Bka's Decision. The most pressing of these questions is undoubtedly: does the Bka have the power, even with the data protection authorities' permission, to find an abuse of dominance based on a GDPR violation?

On the 4th of July 2023, over four years after the Bka's Decision, the ECJ gave its answer: Yes.[42]

The ECJ, closely following the Opinion of AG Rantos,[43] can be neatly subdivided into three sections: the principle of sincere cooperation, art. 9 GDPR, and art. 6 GDPR.

a) Sincere cooperation between data protection and competition

First and foremost, the Court was asked whether art. 51 GDPR, which establishes (national) data protection authorities, precludes others from ruling on GDPR violations.

According to the Court, there are no specific rules for this kind of cooperation between a national data protection authority and a national competition authority.[44] Moreover, neither are there rules which preclude a competition authority from taking stock of the GDPR, provided it does so in the context of its competition Decision.[45] The Court succinctly explains the role of data protection within a national competition authority's mandate as follows:

> "As the Advocate General observed [...] a competition authority must assess, on the basis of all the specific circumstances of the case, whether, by resorting to methods different from those governing normal competition in products or services, the conduct of the dominant undertaking has the effect of hindering the maintenance of the degree of competition existing in the market or the growth of that competition. [...] In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers".[46]

In short, competition authorities must assess whether an undertaking has acted outside the methods governing normal competition, and a GDPR violation can be a "vital clue" that this has occurred.[47] This is especially true since the collection and use of personal data is vital to digital markets, as evidenced by Meta's business model. As the Court observes:

[42] Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* ECLI:EU:C:2023:537 para. 63.

[43] Opinion C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* ECLI:EU:C:2022:704.

[44] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 43.

[45] *Ibid.*

[46] *Ibid.* para. 47.

[47] This wording was derived from AG Rantos: Opinion C-252/21 cit. para. 23; *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 47.

> "As pointed out by the Commission, inter alia, access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, excluding the rules on the protection of personal data from the legal framework to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union".[48]

Ultimately, because of the role of personal data as a "significant parameter of competition", it would not be realistic for a competition authority to carry out its investigations without taking personal data into account as a substantial factor.

That said, care must be taken to ensure that the competition authority does not encroach on the territory of the data protection authorities. Even if a competition authority has the power to issue a competitive Decision based on GDPR violations, it still cannot issue a GDPR fine.[49]

The Court resolves this issue by applying the EU law principle of sincere cooperation as enshrined in art. 4(3) TEU.[50] On the basis of this principle, a competition authority faced with questions regarding data protection has the responsibility to "consult and cooperate sincerely" with the relevant national data protection authority.[51] It must research whether the conduct under review has already been subject to a decision by the national data protection authority. If so, a competition authority may not deviate from that decision even within the context of its competition law investigations.[52] Where no prior data protection decisions exist, the competition authority must consult with its data protection colleague and seek its cooperation.[53] The data protection authority, in turn, may provide the information the competition authority needs, it may grant leave to continue the investigation if it has no objections, it can inform the competition authority of its plans to open its own investigation, or cooperate in other ways.[54] In the absence of a reply within a reasonable time, the competition authority may also continue its investigation.[55]

In the Bka's case it was clear that it had, at an early stage, sought the cooperation of both the Hamburg and the Federal data protection authorities. Since they had no objections, the ECJ finds that the Bka has fulfilled its obligation of sincere cooperation and had not exceeded its legal competence.[56]

[48] *Meta Platforms Inc and Others v Bundeskartellamt* cit. paras 50–51.
[49] *Ibid.* para. 49.
[50] *Ibid.* paras 52–53.
[51] *Ibid.* para. 54.
[52] *Ibid.* para. 56.
[53] *Ibid.* para. 57.
[54] *Ibid.* para. 58.
[55] *Ibid.* para. 59.
[56] *Ibid.* paras 61-63.

b) Art. 9 GDPR

Having established the Bka's competence, the Court reviews its interpretation of the GDPR. In particular, whether the Bka was correct to apply art. 9 GDPR to the pooling of data from the Like and Share buttons.

The Court not only agrees with the Bka's assessment, but goes even further than the Bka did in its Decision. The Court and AG both point out that art. 9 GDPR is applicable regardless of whether the obtained information is correct, and regardless of whether Facebook intended to collect sensitive data.[57] This is justified by the significant risks to their fundamental rights and freedoms that consumers inherently face if such sensitive data is processed.[58] When the processing of data, including the collection and pooling data from off-Facebook sources collected through cookies or integrated applications, reveals information covered by the categories of art. 9, then Facebook must comply with art. 9 GDPR.[59]

Facebook furthermore aimed to rely on art. 9(2)(e) GDPR, which provides for a derogation when sensitive data is "manifestly made public by the data subject". This provision, however, receives a strict interpretation by the Court. Namely, the fact that an individual visits a site does not mean that data from such a visit has been manifestly made public.[60] A user does not have to expect, even with a Facebook Like button active, that their website visit will become known to the social media platform. Even clicking the Like button is not a manifest publication per se, depending on the user's social media settings. Only when the individual settings, selected freely and in an informed manner, are such that the data will be made available to an unlimited number of people, will art. 9(2)(e) apply.[61] Put simply: for it to be considered manifestly made public, the data must be knowingly and willingly made available to anyone and everyone who wants to access it.

Finally and most importantly, the Court points out that when data is combined which includes both sensitive and non-sensitive data, and when that data is collected in such a way that it is impossible to separate the two categories, the entire dataset must be considered under the strict art. 9 regime.[62] Even one sensitive data point in the pool, as long as it cannot be separated, effectively renders the whole pool sensitive.[63]

c) Art. 6 GDPR

Thirdly and finally, the Court examined the legality of Facebook's data processing under art. 6 GDPR. That said, given the broad nature of art. 9 granted to it by the Court above, it is worth emphasizing that a significant portion, if not the vast majority, of Facebook's data will be covered not by art. 6 but by the strict art. 9 regime.

[57] *Ibid.* para. 69.
[58] *Ibid.* para. 70.
[59] *Ibid.* para. 73.
[60] *Ibid.* para. 78.
[61] *Ibid.* paras 82-83.
[62] *Ibid.* para. 89.
[63] *Ibid.*

In so far as art. 6 GDPR applies, the Court largely agrees with the assessment of the Bka described above in Section II.1. If anything, as was the case for art. 9, the Court goes a step further.

As for consent, the Court notes that for consent to be valid, it must be freely given, separate consent must be allowed for separate data processing activities, and the performance of a contract may not be conditional on consent.[64] The Court does note, however, that Facebook's dominant position on the social media market does not in itself prevent valid consent from being given.[65] Consent *can* still be "freely given" even to a dominant undertaking. Nevertheless, a company's dominance could result in a "clear imbalance" between the consumer and such a company, which could, per Recital 43, render consent invalid.[66] The undertaking thus has the responsibility to ensure that its consumers are free to refuse consent, without then being barred from using the service in its entirety.[67] At the very least, consent between Facebook social media data and off-Facebook data must be separated.[68]

As for the performance of a contract as a legal basis, the Court notes that the data collection in question must be "objectively indispensable for a purpose that is integral to the contractual obligation".[69] Only when the main thrust of the contract cannot be achieved through any other means may data collection occur. Where several services are subject to the same contract, this determination must be made for each service separately.[70] The individual personalization of a service, although useful, does not meet this necessity standard, as an equivalent alternative non-personalized version of the service could be offered without the requirement of data collection.[71]

As for art. 6(1)(c), (d), and (e) GDPR, the Court finds that they are not applicable. Although the Court has little information to determine whether Facebook has a legal obligation for its data collection, or a task in the public interest, it does note that "given the type of activity and the essentially economic and commercial nature thereof, it seems unlikely that that private operator was entrusted with such a task".[72] As for the vital interests of its consumers, the Court is even clearer: Facebook, as a commercial actor, cannot in an abstract and preventative manner rely on this legal basis.[73]

Finally, the legitimate interests of Facebook also cannot serve as a legal basis. The principle of data minimization provides that no more data may be collected than is

[64] *Ibid.* paras 144-145.
[65] *Ibid.* paras 147.
[66] *Ibid.* para. 149.
[67] *Ibid.* para. 150.
[68] *Ibid.* para. 151.
[69] *Ibid.* para. 98.
[70] *Ibid.* para. 100.
[71] *Ibid.* para. 102.
[72] *Ibid.* para. 133.
[73] *Ibid.* para. 137.

necessary for a specific purpose, which also means that Facebook may only collect so much data as is strictly required to meet its legitimate interests.[74] In addition, these interests can be overridden by the interests and fundamental rights of the user. In Facebook's case, while advertising may be within its legitimate interest,[75] the Court held that users of a social network cannot reasonably expect that their data will be processed for targeted advertising.[76] Furthermore, Facebook's data collection was extensive, as it relates to a potentially unlimited amount of data collected from almost all of the users' online activity.[77]

As such, Facebook could not rely on the legitimate interest, nor indeed any other legal basis for data processing. The ECJ agreed with the Bka's assessment that the GDPR had been violated, and as discussed above, it also agreed that such a violation can be a legitimate reason for the Bka to find abuse of dominance under competition law.

III. Comment

III.1. Something new: relations between competition law and data protection

The *Meta v Bundeskartellamt* case has been long awaited, for good reason. In particular, this case shows a new approach towards the integration of personal data protection in competition law.

On an EU level, the European Commission has generally been of the opinion that data protection only has a limited role to play in its competition law oversight. In the *Facebook/WhatsApp* merger, for example, it indicated that it would investigate personal data only as a resource that might lend itself to exclusionary abuses.[78] This is consistent with its broader policy of prioritizing exclusionary abuses in its competition oversight. More recently, the Commission has subjected data's role in digital market companies' business models to closer scrutiny, such as in the *Google/Fitbit* merger.[79] Nevertheless, it still focused on the potential for exclusionary abuse; the potential for large-scale data collection to raise barriers to entry. The Commission has never investigated the potential for dominant undertakings to violate their consumers' privacy interests as a possible exploitative abuse. Ultimately, the legal fields of data protection and competition are still

[74] *Ibid.* para. 109.

[75] *Ibid.* para. 115

[76] *Ibid.* para. 117.

[77] *Ibid.* para. 118.

[78] In the Facebook/WhatsApp merger Decision, the Commission would only review the collection and combination of personal data "if the concentration of data within Facebook's control were to allow it to strengthen its position in advertising". Decision C(2014) 7239 final from the European Commission of 3 October 2014 on case M7217 – Facebook/WhatsApp, para. 187.

[79] Decision C(2020) 9105 final from the European Commission of 17 December 2020 on case M.9660 Google/Fitbit, paras 427–429.

largely separate. Although personal data is seen as a "non-price parameter of competition" and the necessity of a large dataset can be one of many barriers to entry, the Commission has yet to find excessive data collection as abusive conduct under art. 102 TFEU.

Meta v Bundeskartellamt unambiguously shows that it is within the wheelhouse of a competition authority to consider personal data not only as a competitively relevant resource, but also to consider infringements on consumers' data protection as abusive conduct. In doing so, it also confirms the Bka's Decision which explicitly included exploitative abuse as well and exemplifies that excessive data collection often has simultaneous exploitative and exclusionary effects. Although the preliminary questions presented do not explicitly cover the distinction between exploitation and exclusion, there is no indication in the case that such a distinction would be relevant to the Court's finding. The Court, for example, notes that a competition authority may examine GDPR compliance in order to "assess the consequences of a certain practice (..) for consumers",[80] of which exploitation would be a prime candidate. Moreover, in its answer to the Oberlandesgericht the Court simply refers to "the examination of an abuse", with no further indication that the type of abuse found by the national competition authority is a relevant factor.

This is a positive development which emphasizes the close connections between data protection and competition law with regards to digital markets. Indeed, the Court itself notes that keeping a strict separation between data protection and competition "would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union".[81]

The Court explains quite clearly and logically why competition law oversight has room for data protection. As the Court shows, from the perspective of competition law, the question of whether privacy violations may constitute an abuse of dominance is much easier than it first appears. After all, whether an abuse of dominance has been committed ultimately comes down to a (deceptively) simple question, namely: was this conduct outside of "competition on the merits?"[82] Whether certain conduct qualifies as competition on the merits or not is often matter for debate, but in the present case it is rather straightforward. After all, a serious violation of EU law has been committed, which in the words of AG Rantos is already "a vital clue".[83] Put simply: is it outside competition on the merits for a dominant undertaking to violate EU law in order to gather significantly more of an essential resource than is allowed? Of course it is. If that is the starting point, then the rest of the Bka's reasoning naturally follows.

[80] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 47.

[81] *Ibid.* para. 51.

[82] Or "methods different from those governing normal competition", as the Court phrases it: *Ibid.* para. 47.

[83] *Ibid.* paras 47-48; Opinion C-252/21 cit. para. 23.

The Court's ruling in *Meta v Bundeskartellamt* can also be seen as an extension of *Case C-457/10P AstraZeneca*.[84] In this case, the Court confirmed that misleading representations of fact, which granted AstraZeneca longer patent protections than it would otherwise have had, can be classified as abusive conduct.[85] According to the Court, "Such an approach is manifestly not consistent with competition on the merits".[86] In this case too competition law was paired with another field of law, patent law, and here too competition law enforcement was allowed to proceed. AG Rantos in his Opinion also draws on *AstraZeneca* to argue that a dominant undertaking's conduct relating to data processing could be in breach of competition rules even if it does not violate the GDPR, since *AstraZeneca* establishes that "the compliance of conduct with specific legislation does not preclude the applicability, to that conduct, of arts 101 and 102 TFEU".[87] Nevertheless, *Meta v Bundeskartellamt* is novel on a few fronts. Firstly, the type of abuse differs between these cases. In *AstraZeneca*, the abuse seems to have been in "abuse of administrative procedures". In his annotation, Podszun posits there was proof of bad faith on AstraZeneca's part and that a "strategy to misrepresent or to fiddle with facts" explains the enforcement more so than the objective conduct.[88] There is no indication that the Bka similarly relied on bad faith in its Decision against Meta. Rather, it found objective GDPR violations and the anti-competitive effects of those violations to be sufficient for further action. Secondly, there is a notable difference in the substance of patent law versus data protection law. AstraZeneca's violation lay in its misrepresentation of facts towards the patent office. In contrast, the GDPR is consumer-facing, in that it provides privacy protections and rights directly towards (Meta's) consumers. *Meta v Bundeskartellamt* therefore takes the *AstraZeneca* ruling a step further. Misleading an official authority is not required; the violation of EU citizens' rights under art. 8 of the Charter of Fundamental Rights, at least in so far as they are actualized by the General Data Protection Regulation, can have exploitative and exclusionary effects, and can therefore itself be abusive under competition law.

The bigger problem is thus not one of competition law, but one of data protection law; namely whether establishing a supervisory authority under art. 51 GDPR takes data considerations outside the purview of the competition authority. The Court solves the issue rather elegantly: if a competition authority runs the risk of infringing the principle of sincere cooperation by issuing a data protection-based Decision, then such risks can be mitigated simply by actually cooperating with the relevant data protection authorities. The need for cooperation makes good sense; otherwise a competition authority finding a GDPR violation might face problems if that same conduct is later found not to violate

[84] Case C-457/10 P *AstraZeneca AB and AstraZeneca plc v European Commission* ECLI:EU:C:2012:770.

[85] *AstraZeneca AB* cit. para. 98.; R Podszun, 'Can Competition Law Repair Patent Law and Administrative Procedures? *AstraZeneca*' (2014) 51 CMLRev 281, 285.

[86] *AstraZeneca AB* cit. para. 98.

[87] Opinion C-252/21 cit. para 23 and footnote 18.

[88] R Podszun 'Can Competition Law Repair Patent Law and Administrative Procedures? *AstraZeneca*' cit. 285, 289.

the GDPR by the actual art. 51 supervisory authority. Care must be taken to ensure the consistency of GDPR application, so simply asking those responsible is an eminently logical first step.

The Court is clear that the extent of this cooperation is for the authorities to decide together, although the competition authority ultimately has to defer to its colleague. In contrast, the Court does not explicitly say what the consequence should be if the data protection authority does not grant permission for a data-based competition Decision. Nevertheless, from the foregoing considerations on sincere cooperation it can be inferred that in such a case the competition authority is not at liberty to conduct the investigation in that way, since doing so could endanger the coherent interpretation of the GDPR. It is, of course, still at liberty to find abuse of dominance through other avenues, just not one that is at its core based on a GDPR violation.

Through this ruling, the Court neatly conforms to a growing field of research which highlights this connection between data protection and competition on digital markets.[89] The role personal data plays on the competitive field is not to be underestimated. In particular, the network effects of personal data are key to the business models of many (dominant) data-driven undertakings. More data, about more individuals, results in more accurate analysis, a more personalized product, and more precise targeting of advertisements. While some diminishing returns might be expected, the Bka and the French competition authority in a joint report argued that strongly diminishing returns might not

[89] As an overview, by no means exhaustive, see for example: P van de Waerdt, 'From Monocle to Spectacles: Competition for Data and "Data Ecosystem Building"' (2023) 19 European Competition Journal 191; S Lucchini, J Moscianese, I de Angelis, and F Di Benedetto, 'Online Digital Services And Competition Law: Why Competition Authorities Should Be More Concerned About Portability Rather than About Privacy' (2018) 9 Journal of European Competition Law & Practice 563; I Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 World Competition Law and Economics Review 473; 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 Mackenrodt, and G Surblytė-Namavičienė (eds), *Personal data in competition, consumer protection and intellectual property law* (Springer Verlag 2018); M Bourreau and A de Streel, 'Digital Conglomerates and EU Competition Policy' (2019) www.ssrn.com; S Aravantinos, 'Competition Law and the Digital Economy: The Framework of Remedies in the Digital Era in the EU' (2021) 17 European Competition Journal 134; W Sauter, 'A Duty of Care to Prevent Online Exploitation of Consumers? Digital Dominance and Special Responsibility in EU Competition Law' (2020) 8 Journal of Antitrust Enforcement 649; N Economides and I Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective' (2019) papers.ssrn.com; M Buiten, 'Regulating Data Giants: Between Competition Law and Data Protection Law' in K Mathis and A Tor (eds), *New Developments in Competition Law and Economics* (Springer International Publishing 2019); Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, 'Investigation of Competition in Digital Markets' govinfo.gov; J Hoffmann and G Johannsen, 'EU-Merger Control & Big Data On Data-Specific Theories of Harm and Remedies' (2019) Max Planck Institute for Innovation & Competition Research Paper 74; M Botta and K Wiedemann, 'EU Competition Law Enforcement Vis-à-Vis Exploitative Conducts in the Data Economy: Exploring the Terra Incognita' (2018) No. 18-8 Max Planck Institute for Innovation & Competition Research Paper.

actually be the case for data collection and targeted advertising.[90] Regardless, being able to collect such data from a wide variety of sources, as was the point of contention in the Bka's case against Facebook, further supports this business model based on the consumer's particular interests. Each source can be used to collect a precise niche of personal data, which is pooled with all the other sources in order to form a business model best described as a "data ecosystem".[91] As emphasized by the Bka, such an ecosystem model can raise barriers to entry, as smaller competitors without such an ecosystem of personal data collection cannot realistically compete with the data analysis and targeted advertising of incumbents such as Meta. Meanwhile, as the Bka also emphasizes, consumers face difficulties in exercising their data protection rights which would block such large-scale data collection. In particular, they are often restricted in their choice to deny consent, and they face serious information asymmetries due to the complexity of data processing activities and the privacy policies that are supposed to explain them.[92] Ultimately, therefore, excessive data collection by such undertakings can have exploitative and exclusionary anti-competitive effects, and often those effects occur in tandem.[93]

Consequently, the *Meta v Bundeskartellamt* case is an important development, as it confirms that such a perspective, taken by a competition authority, is a valid and legally permissible one. This means, effectively, that a new avenue for enforcement of data protection norms has opened up, provided of course a dominant undertaking is involved. After all, based on the Bka's findings, Facebook could have faced a GDPR fine as well. However, the notorious lack of funding and capacity for data protection authorities can make a large-scale investigation of complex material quite problematic. Furthermore, GDPR enforcement for serious violations is restricted to maximum fines of €20 million or 4 per cent annual worldwide turnover, whichever is higher.[94] Competition law enforcement does not carry such a legally mandated maximum, although the Commission's Guidelines cap it at 10 per cent of annual worldwide turnover.[95] The deterrence offered by competition law enforcement therefore has the potential to be significantly more effective than the same violation found under the GDPR.

In fact, there is even reason to believe that the same violation could give rise to both GDPR and competition law enforcement. Although the general principle of *ne bis in idem* must be respected, it is unlikely that it would bar dual data protection and competition

[90] Bundeskartellamt and Autorité de la Concurrence, 'Competition Law and Data',10 May 2016, bundeskartellamt.de 50.

[91] P van de Waerdt '"Everything the Data Touches Is Our Kingdom": Reassessing the Market Power of "Data Ecosystems"' cit.

[92] P van de Waerdt, 'Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market' (2020) Computer Law & Security Review 105436.

[93] P van de Waerdt 'From Monocle to Spectacles: Competition for Data and "Data Ecosystem Building"' cit.

[94] Art. 83(5) Regulation 2016/679 cit.

[95] Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, 2006/C 210/02, para. 32.

enforcement. ECJ jurisprudence identifies that *ne bis in idem* is activated by "identity of the facts, unity of offender and unity of the legal interest protected".[96] In the current case, competition law and data protection law aim to protect different legal interests. The GDPR is intended to protect against infringements of fundamental rights by data controllers *vis-à-vis* natural persons.[97] Competition is most commonly understood to protect consumer welfare and the effectiveness of competition in the internal market.[98] Considering that the Court has even allowed consecutive national and EU competition enforcement,[99] there is no indication that consecutive data protection and competition enforcement would be impermissible. This is also the view of AG Rantos,[100] and the Court confirms this approach in para. 56 of *Meta v Bundeskartellamt*. As discussed above, a competition authority must verify whether prior Decisions by the data protection authority exist. When it finds one, the Court does not say that the matter is then settled and *ne bis in idem* prevents further action. Instead, it says that the competition authority may not *depart* from those findings. It may not find a GDPR violation in its competition Decision if the data protection authority has examined the same conduct and officially found no violation. However, where the data protection authority has found a violation, the competition authority could then continue to use the "vital clue" on offer to find an abuse of dominance.

Finally, it also follows from the Court's reasoning that the scope of *Meta v Bundeskartellamt* is not necessarily limited to data protection law. After all, there is no reason to believe that the principle of sincere cooperation would not extent across various other fields of law. The ECJ says as much: "it may be necessary for the competition authority (...) also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, *such as* the rules on the protection of personal data".[101] As a result, it is possible for abuse of dominance to follow from the violation of other (EU) laws. For example, it is conceivable that non-compliance with environmental law could distort competition in markets where environmental obligations are an important factor to the business model, or where "being green" is valued by the consumer to such an extent that

[96] Joined cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P, and C-219/00 P *Aalborg Portland A/S (C-204/00 P), Irish Cement Ltd (C-205/00 P), Ciments français SA (C-211/00 P), Italcementi - Fabbriche Riunite Cemento SpA (C-213/00 P), Buzzi Unicem SpA (C-217/00 P) and Cementir - Cementerie del Tirreno SpA (C-219/00 P) v Commission of the European Communities* ECLI:EU:C:2004:6, para. 338.

[97] Recital 1 Regulation 2016/679 cit.; joined cases C-465/00, C-138/01, and C-139/01, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk* ECLI:EU:C:2003:294, paras 39-47; and see generally G González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

[98] D Zimmer, *The Goals of Competition Law* (Edward Elgar Publishing 2012).; V Vanberg, 'Consumer Welfare, Total Welfare and Economic Freedom - on the Normative Foundations of Competition Policy', *Competition Policy and the Economic Approach: Foundations and Limitations* (Edward Elgar Publishing 2011).

[99] Case C-17/10 *Toshiba Corporation and Others v Úřad pro ochranu hospodářské soutěže* ECLI:EU:C:2012:72, paras 98–102.

[100] Opinion C-252/21 cit. para 24 and footnote 21.

[101] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 48 [emphasis added].

it becomes a parameter of competition. In such situations, it is certainly possible that violating environmental law bestows such an advantage on a dominant undertaking that the conduct can be considered abusive. It must thus be carefully considered which fields of law fulfill this role for which markets, in a manner equivalent to data protection law's role in regulating social media, targeted advertising, and digital markets more broadly.

III.2. Something borrowed: *Meta v Bundeskartellamt* and the European Commission

Perhaps the most exciting aspect of this judgement is that it not only empowers national competition authorities, it also has the potential to empower the European Commission if it borrows the Bka's line of reasoning. Although the German law in question was not a one-to-one match to art. 102 TFEU, there is no reason to believe that the same line of reasoning could not be brought by the European Commission. The GDPR is an EU-wide instrument, and the role of personal data on EU digital markets is much the same as it is on the national German market. If anything, the network effects of personal data can be expected to be even greater on an EU level, since data from many more users from many more nationalities is collected. Provided the market definition allows for it, the Commission could surely examine the effects of personal data collection on the competitive effects on the EU social media market. In fact, such an EU-wide market was already found by the Commission in *Facebook/WhatsApp*.[102]

The biggest difficulty in applying the Bka's reasoning on a European level is that the GDPR system is strictly nationally enforced; there is no EU data protection authority with the power to find violations and issue fines. By the Court's reasoning, the Commission finding a data protection violation without input from the GDPR-mandated data protection authority thus risks interfering with the coherent interpretation of the GDPR.[103] However, this interpretation would be short-sighted, for several reasons. Firstly, although there is no EU body with supervisory authority over the GDPR, there is the European Data Protection Board, established by art. 68 GDPR. It may not have supervisory powers, but it does have the power to issue Guidelines, to advise the Commission on "any issue related to the protection of personal data in the Union", and examine "any question covering the application" of the GDPR.[104] The latter it may do on its own initiative, but also on request of the European Commission. As such, the Commission does have an avenue to ensure the consistency of GDPR interpretation as authorised by the GDPR.

Secondly, this avenue might not even be needed, as the Commission itself already has a number of powers under the GDPR. For one, the Commission actually has its own seat

[102] *Case M.7217 – Facebook/ WhatsApp* cit. para 36.
[103] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 45.
[104] Art. 70(1)(e) Regulation 2016/679 cit.

on the European Data Protection Board.[105] Its seat is non-voting, but it has the right to participate in Board activities nonetheless. More importantly, the Commission has specific supervisory powers granted to it by the GDPR. For example, it has the power to adopt delegated Guidelines for standardized icons to increase transparency, and to draft standard contractual clauses.[106] Most importantly, the Commission has the power to draft an Adequacy Decision, by which it verifies that a third country's law ensures an "adequate level of [data] protection".[107] In essence, the Commission can investigate the laws of a non-EU country and test them against the standards of the GDPR. The Commission may then decide that a third country's privacy laws are (not) equivalent to the GDPR. In other words: it may decide that an EU company following the third country's laws would (not) be GDPR-compliant. From there, the step to the Commission ruling on GDPR violations in other contexts would be quite small. If the Commission may find fault with data protection in another country's laws, then surely it may also find fault in data protection compliance with dominant undertakings within its competition Decisions. Especially if personal data collection is an integral part of economic activities of the undertaking under review, and *especially* if it asked for the European Data Protection Board's opinion beforehand.

In doing so, the Commission would be taking valuable steps in the regulation and enforcement of digital markets. For one, it would provide a pre-tested new form of abuse of dominance. In *Google Shopping*, the Commission (successfully) argued for a new form of abuse which consists of promoting one's own services in controlled search results while demoting the services of competitors.[108] The Commission was able to draft a complicated theory of harm based on leveraging market power, which was ultimately confirmed by the Court and included in the DMA. With the *Meta v Bundeskartellamt* case, the German national competition authority has already done the hard work for it. With the Court now confirming the Bka's approach, the Commission would have a much easier time incorporating a data protection based theory of harm in its own lexicon, from an exclusionary or an exploitative point of view.

Furthermore, doing so not only aids the Commission in its competition oversight, it also aids national data protection authorities in their privacy oversight. National data protection authorities might not have the funds or the capacity to conduct a large-scale investigation of such large companies. The Commission could offset some of this burden, effectively extending the reach of data protection norms through competition oversight.

The above does mean that the Court has effectively introduced a new obligation for national data protection authorities. They are expected to respond to requests for information or cooperation within a reasonable time.[109] Failure to reply to such a request

[105] Art. 68(5) Regulation 2016/679 cit.

[106] Arts 12(8) and art. 28(7) Regulation 2016/679 cit., respectively.

[107] Art. 45 Regulation 2016/679 cit.

[108] Case T-612/17 *Google LLC, formerly Google Inc and Alphabet, Inc v European Commission* ECLI:EU:T:2021:763, paras 615-616.

[109] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 58.

means that the competition authority may continue its investigation. This clearly implies that a reply of some kind, be it in detail or simply a reply of "objection"/"no objection", is expected and required. That said, it could easily be argued that this relatively minor new obligation is more than offset by the fact that more data protection violations can now be caught. As already discussed above, the Court in *Meta v Bundeskartellamt* effectively offers a new avenue of enforcement with regards to digital market companies. The conduct prohibited by the Bka could by definition have been subject to a GDPR fine, but the burden was taken up by the Bka instead. Given that national data protection authorities often indicate they are underfunded,[110] it is a positive development that GDPR enforcement can now be given new reach through competition law.

Be that as it may, it is worth emphasizing that the final decision must always be based on the competition authority's mandate. Even with a violation of adjacent EU law, the competition authority must always be able to argue and prove that the conduct amounts to a *competition* law violation such as abuse of dominance. As the Bka shows, this does not have to be an exclusionary abuse such as the Commission has traditionally prioritized; restricting consumer choice and infringing their data protection rights can also be sufficient as exploitative abuses. The exact standards for this will depend on the (national) law in question, but factors such as market power and the actual or potential anti-competitive effects of the conduct will invariably be part of the investigation. As a result, it should not be expected that any GDPR violation will always be an abuse of dominance, thereby subverting the fines and procedures of data protection law. Nevertheless, the types of scenario for which the Bka's line of reasoning is relevant have considerable implications on both of the data protection rights of many affected EU citizens as well as the functioning of digital markets dominated by a few large ecosystem companies.

To illustrate: in Meta's case, the GDPR violation lay in the collection of personal data without a proper legal basis. Every available legal basis was claimed (albeit some with more sincerity than others) yet all of them turned out invalid. Within the system of the GDPR, this is quite possibly the most fundamental violation imaginable. Indeed, the very first general principle of the GDPR reads: "Personal data shall be processed lawfully", where "lawful" means having a valid legal basis.[111] Violating this provision naturally results in the processing of data far beyond what would be available to a competitor which does comply with the lawfulness principle. A competition authority will not find it difficult to make the case that this goes beyond competition on the merits and has anti-competitive effects. Furthermore, in Meta's case the abusive conduct was only possible and profit-maximizing because of its dominance on the social media market. Despite its privacy

[110] European Data Protection Board, 'Lack of Resources Puts Enforcement of Individuals' Data Protection Rights at Risk' edpb.europa.eu; F Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) Maine Law Review 16, 52.

[111] Art. 5(1)(a) and art. 6(1) Regulation 2016/679 cit. It is also subject to the higher of the two maximum fines as per art. 83(5)(a) Regulation 2016/679 cit.

infringements, consumers found it impossible to leave the company as the main provider of social media services.[112] In such a situation competition law enforcement is well within the realm of possibility.

In contrast, the GDPR contains many rules and obligations of a much more specific nature. For example, rules about the information to be provided to data subjects, rules about the relation between data controller and data processor, and rules about proper cybersecurity measures.[113] Although these rules are equally binding on a company, they are less core to the data protection system. It is thus also far less likely that a violation of these provisions would have anti-competitive effects, or that consumers feel locked-in despite what they perceive as serious privacy violations. Consequently, it is far less likely for such conduct to constitute an abuse of dominance. This will of course always depend on the circumstances of the case as well as the competition authority's investigation, but the hard requirement to stick to established competition law norms prevents the competition authority from becoming a *de facto* data protection authority. And of course the national and EU courts remain the final arbiter of whether competition law and data protection law have been applied correctly.

Ultimately, the *Meta v Bundeskartellamt* approach is worth emulating not only by other national competition authorities, but also by the European Commission. The Court in this judgement provides ample justification for this approach to also be effective on an EU level, and doing so would go a long way to improving the efficacy of both data protection law and competition law. By virtue of the Bundeskartellamt and the European Court of Justice, the Commission has been offered new tools to add to its art. 102 TFEU repertoire. This is especially true if the Commission chooses, as the Bka has done, to base its art. 102 enforcement not only on exclusionary conduct but on exploitative conduct as well, or indeed the combination thereof. Choosing to actively employ this strategy would show an increasingly comprehensive understanding of "the reality of [the] economic development" of digital markets. In short; time for the Commission to borrow the Bundeskartellamt's "something new".

III.3. Something old: arts 6 and 9 GDPR

Compared to the Court's ground-breaking findings on the relations between competition law and data protection law, the rest of the judgement might seem easy to overlook. Nevertheless, a number of observations about the Court's views on art. 6 and 9 GDPR can be made here as well.

In particular, it is notable that the Court adopts a strict approach to almost every element and legal basis of these GDPR provisions. This can be observed most clearly in the Court's findings on the legal basis of contractual necessity. The Court takes the

[112] Bundesgerichtshof KVR 69/19 cit. paras 85–86, 102.

[113] Respectively arts. 13, 14, 26, and 32 Regulation 2016/679 cit.

"necessity" element very literally and very strictly. A subsidiarity and proportionality test must be conducted, and only when no other ways exist for a key ingredient of the contract to be performed may data collection occur under a contractual legal basis. Additionally, every separate service in the contract must be considered separately, so that data collection is strictly limited to the bare minimum required.

Meta v Bundeskartellamt is rife with such strong language. That being said, it is debatable whether such a strict approach is truly new. On the contrary, it is submitted that much of the Court's reasoning regarding the GDPR has long been settled law. The added value of this ECJ judgement is therefore less in its development of new rules, and more in its unambiguous listing of the strict rules the GDPR has always had.

For example, the strict interpretation of "contractual necessity" has been in force for some time. It was a point of contention in the Irish Data Protection Commission inquiries into Meta, in which it held that the Facebook social media platform was not entitled to rely on contractual necessity.[114] It did so after referring the matter to the European Data Protection Board for binding dispute resolution. The Board was clear: Meta can rely on contractual necessity only if behavioural analysis is objectively necessary to provide the service.[115] The contract's "fundamental objective" must be established, and the data processing must be "integral to the delivery" of that contractual service.[116] If realistic alternatives exist that do not rely on data processing, then it follows that the processing is not necessary.[117] In its ruling, the Board refers back to its own Guidelines, dating from 2019, in which this was already recorded.[118] Indeed, behavioural profiling is specifically called out as an example of illegitimate processing.[119] Moreover, the 2019 Guidelines themselves harken even further back, to a 2014 Opinion of the Article 29 Working Party, which *also* already called out behavioural profiling as illegitimate.[120] To emphasize: the Working Party is the predecessor to the Board, established under the predecessor of the GDPR. In other words, the strict interpretation of contractual necessity is older than the GDPR itself.

[114] Data Protection Commission, 'Data Protection Commission announces conclusion of two inquiries into Meta Ireland', 4 January 2023 www.dataprotection.ie; Decision of the Data Protection Commission made pursuant to Section 113 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation in the matter of LB, a complainant, concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service, DPC Inquiry Reference: IN-18-5-5, para. 4.56.

[115] Binding Decision 3/2022 of the European Data Protection Board of 5 December 2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR), para. 111.

[116] *Ibid*. para. 112.

[117] *Ibid*. para. 120.

[118] Guidelines 2/2019 of the European Data Protection Board of 8 October 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, para 25.

[119] *Ibid*. paras 35–36.

[120] Opinion 06/2014 of the Article 29 Working Party of 9 April 2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP217, p. 16–17.

Much the same applies for the other legal bases as well. Mandatory obligations prescribed by law were always required, and the mere possibility that a company will be called upon to assist investigations was already found insufficient in the same 2014 Opinion;[121] the GDPR's recitals explicitly point out "vital interests" as being "essential for the life of the data subject";[122] and a public task already "pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing".[123]

Finally, the applicability of "legitimate interests" to targeted advertising was also already clear. Once again, it is explicitly used as an example by the Article 29 Working Party in 2014. According to the Working Party, behavioural analysis and personalization can be legitimate interests. However, this does not mean that data combination across many branches and through third-party integration is also allowed. Building complex personal profiles without the users' knowledge or consent "is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject".[124]

As such, although many of the Court's reflections on the legal bases of the GDPR sound impressive, they are simply the application of standard data protection law. To say the least, it is concerning that these fundamental principles of the GDPR still had to be spelled out by the Court, given that they had been settled by official authorities since the entering into force of the GDPR (and oftentimes before).

As for art. 9 GDPR, the finding that sensitive data need not be intentionally gathered nor even correct for it to receive enhanced protection is not new either. After all, art. 9 is explicitly introduced in order to protect data subjects against risks posed by such sensitive information falling into the wrong hands. It does not list any conditions except the processing of (specifically defined) sensitive data for it to take effect. For such data to be manifestly made public, the British data protection authority has a helpful guidance.[125] It says that a deliberate act by the data subject must be taken, and it must be realistically accessible to anyone, just as the Court emphasized in the underlying case.

What is still interesting, however, is how the Court delineates between art. 6 and art. 9 data. Namely that any piece of sensitive data, in so far as it is inseparable from the other data points in the pool, renders the entire pool subject to art. 9. This has potentially serious implications for digital market companies. After all, with their widespread data collection, it is very likely that they will also, accidentally or not, process sensitive data about its users. This is especially true if, as in Facebook's case, they use third-party integration for data analysis and targeted advertising purposes. In practice, most targeted

[121] *Ibid*. p. 19.

[122] Recital 46 Regulation 2016/679 cit.

[123] Article 29 Working Party Opinion 06/2014 cit. p. 22.

[124] *Ibid*. p 26.

[125] Information Commissioner's Office, 'What Are the Conditions for Processing?', 26 October 2023 ico.org.uk.

advertising schemes must therefore comply with the art. 9 regime over the standard of art. 6. It could certainly be argued that this already follows from the system of the GDPR. After all, any other reading leaves the distinct possibility that sensitive data, once lost in the pool, will be processed in the same way as non-sensitive data. This is exactly what art. 9 aims to prevent, so any interpretation that leads to such an outcome is suspect at best. Nevertheless, it is useful that the Court has now unambiguously confirmed this reading. Apart from its ruling on competition law and data protection discussed above, this is easily the biggest legal contribution in the case.

Finally, there is an important area in which the *Meta v Bundeskartellamt* case could have contributed to the application of EU data protection law, but unfortunately it seems that it failed to do so. Namely, where this ruling could have made waves, but failed to, is in the application of consent to dominant undertakings. Much is still unclear in the area of consent, especially when the relation is business-to-consumer. For example, it is well established in data protection law that an employer generally cannot rely on the legal basis of consent *vis-à-vis* their employees.[126] The power dynamics at play are simply too unbalanced for the employee to freely give consent to their employer. Whether this applies similarly to a strong market player *vis-à-vis* its customers is much more controversial. It notably does not appear in the section of the Board's Guidelines on consent which deals with imbalance of power.[127] Unfortunately the Court also does not provide a clear answer here, and in fact its answer is quite ambiguous. On the one hand, the Court notes that market dominance does not in itself prevent users from giving their consent freely.[128] On the other hand, such market dominance must still be taken into consideration, since it may create a clear power imbalance that could affect user consent.[129] The Court does emphasize that users must be able to consent freely to every distinct processing activity separately, and refusing consent may not be a reason to exclude them from the service completely. However, this is already an obligation under the GDPR for any company that relies on consent; it is not specific to dominant ones.

AG Rantos is only marginally more explicit in his Opinion. He states: "I am of the opinion that any dominant position on the market held by a personal data controller operating a social network is a factor when assessing whether users of that network have given their consent freely. Indeed, the market power of the controller could lead to a clear imbalance [...]". He goes a step further, arguing that dominance, by its competition law definition, is not required and other forms of power imbalance are also possible. Regardless, he too argues that dominance in itself is not sufficient, and that the validity of consent should be examined on a case-by-case basis.[130]

[126] Guidelines 05/2020 of the European Data Protection Board of 4 May 2020 on consent under Regulation 2016/679, para. 21.

[127] *Ibid.* Section 3.1.1.

[128] *Meta Platforms Inc and Others v Bundeskartellamt* cit. para. 147.

[129] *Ibid.* para. 149.

[130] Opinion C-252/21 cit. para 76.

Taking the picture as a whole, the Court seems to imply that market dominance makes obtaining valid consent very difficult indeed, but it does not quite explain what the consequences of that should be. It implies a responsibility for a dominant company to ensure that the consent granted by the consumer is truly freely given. Of course, that responsibility already exists regardless. Perhaps here the GDPR could take some inspiration from competition law in turn, where dominant undertakings carry a "special responsibility" above and beyond non-dominant undertakings.[131] The Court for its part is not clear on this point, which could certainly be viewed as a missed opportunity.

Ultimately, on the topic of art. 6 and art. 9 GDPR, the Court has not offered something new, but instead highlights something old we were already supposed to know.

IV. Concluding remarks

In summary, the *Meta v Bundeskartellamt* case can be characterized as a blend of the new and the old.

With regards to competition law and data protection, the European Court of Justice has confirmed a new and innovative approach by the Bka. As long as they make sure that the principle of sincere cooperation is complied with, competition authorities can work together with data protection authorities to investigate violations of the GDPR as grounds for finding abuse of dominance. After all, given the importance of personal data as a resource on digital markets, a GDPR violation offers a vital clue that a dominant digital market company has acted outside of competition on the merits. Contrary to the Commission's standard enforcement priorities, the Bka and ECJ show that such an approach is valid even if the abuse is exploitative rather than exclusionary, or where it is a combination of both. Furthermore, although the case reached the ECJ through national German law, the *Meta v Bundeskartellamt* case strongly suggests that the same approach could be taken on an EU level as well. In doing so, does *Meta v Bundeskartellamt* truly offer the Commission something new? Perhaps. Given the fierce debate on the Bka's approach in the German case, confirmation by the Court may well have been a necessary step. But perhaps not. Perhaps it merely shows the Commission something old that has always been available, if only it had made the attempt. Regardless, in terms of digital market oversight the connections between data protection and competition are now closer than ever.

With regards to the GDPR's application to digital markets, the Court lists and reaffirms old principles of data protection law in an unambiguous way. A cursory reading of the judgement could lead one to believe that the Court is establishing strict new interpretations of art. 6 and art. 9 GDPR. Upon closer inspection, however, it is clear that most if not all of those interpretations had already been established by the European Data Protection Board many years ago. In some cases the strict interpretations on display predate

[131] Case 322/81 *NV Nederlandsche Banden Industrie Michelin v Commission of the European Communities* ECLI:EU:C:1983:313, para. 57.

even the GDPR itself. Furthermore, on one of the remaining unresolved issues of the GDPR where the Court could have issued new guidance, it unfortunately did not do so. Namely, whether a consumer can "freely consent" to have their data collected by a dominant digital market company remains ambiguous despite receiving some attention in the underlying case. Regardless, if nothing else the Court has now rendered the strict old interpretations of art. 6 and 9 GDPR inescapable. The fact that a national court felt it prudent to include these issues in its preliminary questions indicates that the Court's thorough breakdown of these core GDPR provisions is still worthwhile.

Finally, it is interesting to note that this case is not the only recent addition to the field of digital market oversight, nor to the relations between competition and data protection. The recently entered into force Digital Markets Act aims to do the same. In particular, art. 5(2) DMA prohibits data combination and was inspired by the Bundeskartellamt Decision. The *Meta v Bundeskartellamt* case is thus not only of interest to data protection lawyers and competition lawyers, it also has serious implications for the interpretation and efficacy of the Digital Markets Act. As an invitation for further research, it would therefore also be worth investigating how the DMA can be made to supplement *Meta v Bundeskartellamt*.

Ultimately, *Meta v Bundeskartellamt* is an exciting development regarding the relations between data protection and competition, as well a clear reaffirmation of strict GDPR norms. It is an approach worth following as a new step in an evolving approach to digital markets oversight.