ARTICLES

FUTURE-PROOF REGULATION AND ENFORCEMENT FOR THE DIGITALISED AGE

Edited by Gavin Robinson, Sybe de Vries *and* Bram Duivenvoorde

MARKET POWER AND THE GDPR: CAN CONSENT GIVEN TO DOMINANT COMPANIES EVER BE *FREELY* GIVEN?

ALESSIA SOPHIA D'AMICO*

TABLE OF CONTENTS: I. Introduction. – II. The Facebook case. – II.1. Case overview. – II.2. The opinion of the AG. – III. Dominance for GDPR purposes. – III.1. Market power and the GDPR. – III.2. Dominance in AG Rantos' opinion. – III.3. The definition of "gatekeeper" under the DMA. – IV. Dominance and the validity of consent. – IV.1. Freely given consent under the GDPR. – IV.2. A two-tier approach. – IV.3. The legitimate interests legal basis. – IV.4. Obligations under the DMA. – V. Conclusion.

ABSTRACT: The GDPR is designed to render data protection rights more effective and to address the challenges created by the digital world. In line with the understanding of the right to data protection as data subjects' right to have control over their data, the GDPR empowers data subjects through individual choice. However, the market power of big tech casts doubts on individuals' ability to choose. In particular, reliance on consent is problematic when dealing with dominant platforms. If an individual does not have alternatives on the market, can the consent for the processing of personal data be considered as freely given? This issue is at the core of the case against Facebook brought by the German competition authority, now before the CJEU. This *Article* puts the case into context and discusses what it could mean for the regulation of big tech in the future. The focus is on the novel assertion of Advocate-General Rantos that dominance plays a role in the assessment of the freedom of consent under the GDPR. This statement raises two main issues surrounding the role of market power in the GDPR that this *Article* seeks to address. Firstly, how should data protection authorities assess dominance? Secondly, what role should dominance play in the assessment of the validity of consent? The *Article* aims to further the debate around how to ensure the continued future-proofness of the GDPR in the digital market, in light of the market power of tech companies. It proposes to introduce a two-tier approach which reduces the extent to which dominant firms can rely on consent for data processing.

KEYWORDS: GDPR – digital platforms – freely given consent – dominance – competition law – DMA.

* Assistant Professor, Utrecht University, a.s.damico@uu.nl.

ISSN 2499-8249
doi: 10.15166/2499-8249/678

I. Introduction

The General Data Protection Regulation (GDPR)[1] is the cornerstone of EU data protection law and is designed to render data protection rights more effective and to address the challenges created by the digital world. The aim of the Regulation is to "ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market".[2] Under the GDPR, data subjects are treated as active agents; they are granted a set of "micro-rights"[3] and empowered through individual choice regarding the way their data is used.[4] At the same time, the GDPR contains provisions designed to create a reliable and secure environment for data subjects, through technological measures (*e.g.* security measures and privacy by default settings) and organisational means (*e.g.* the accountability principle and the data protection impact assessment).[5]

The GDPR is designed in a technologically neutral way[6] and adopts a risk-based approach,[7] in order to prevent circumvention and be future-proof.[8] In the staff working document evaluating the GDPR two years after its adoption, the Commission wrote: "The GDPR's technologically-neutral and future-proof approach was put to the test during the COVID-19 pandemic and has proven to be successful".[9] Nonetheless, as argued by Colomo, "the success of future-proof regulation does not depend—at least, not primarily—on the *ex ante* design of a regime, but on the ability of authorities and legislatures to credibly commit, over time, to the same design. The challenge, in other words, is fundamentally exogenous, as opposed to endogenous".[10]

In the digital world, one of the risks to the rights of data subjects, which undermines the success of the GDPR's future-proofness, is that "in the face of recent technological developments and emergence of new social practices which seem to undermine the

[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).

[2] Recital 13 of the General Data Protection Regulation (hereinafter, GDPR).

[3] For instance, the right to access personal data, the right to rectification, erasure and data portability (GDPR, arts 15-20).

[4] Through the role of consent as a legal basis for processing (GDPR, arts 6 and 7). See also D Clifford, 'Data Protection and Consumer Protection: The Empowerment of the Citizen-Consumer' (2020) ANU College of Law Research Paper No 20.11 ssrn.com, pp. 2-3.

[5] GDPR, arts 5(1) and 5(2) and 25.

[6] GDPR, recital 15.

[7] See for instance GDPR, recital 76-77; GDPR, arts 24(1) and 25(1).

[8] Communication COM(2020) 264 final from the Commission to the European Parliament and the Council of 24 June 2020 on Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition - two years of application of the General Data Protection Regulation.

[9] *Ibid*.

[10] P Ibáñez Colomo, 'Future-Proof Regulation against the Test of Time: The Evolution of European Telecommunications Regulation' (2022) OJLS 1194.

very capacity, if not the will, of individuals to 'self-manage' their informational privacy [the] apparently simple and familiar notion [of control] becomes very ambiguous".[11] Individuals' ability to control what happens with their data is particularly threatened by the market power of data-driven tech companies. These companies often benefit from economies of scale, network effects, and self-reinforcing positive feedback loops, which create entry barriers and are conducive to market tipping and monopolization.[12] Internet giants such as Google, Facebook, Amazon and Apple all have a significant degree of market power in one or more markets within the digital sphere. The problem, as described by Kerber, is that: "especially the examples of Google and Facebook with their often alleged dominant market positions have raised the question whether weak competition might lead to an excessive collection of private data and to an insufficient provision of privacy options for fulfilling the different privacy preferences of users".[13]

One specific shortcoming of the current application of the GDPR, in this respect, relates to the validity of consent obtained by dominant players. If an individual does not have alternatives on the market, can the consent for the processing of personal data be considered as freely given? In the words of the European Data Protection Supervisor (EDPS): "where there is a limited number of operators or when one operator is dominant, the concept of consent becomes more and more illusory".[14]

This issue is at the core of the case against Facebook brought by the German Competition Authority, the Bundeskartellamt (BKA),[15] now before the CJEU.[16] On 20 September 2022, Advocate-General (AG) Rantos gave his opinion in the case. This *Article* will put the case into context and discuss how it can contribute to a better protection of individuals' rights over data. It will start by presenting the issues raised by the BKA case against Facebook and the implications of the AG's opinion. The focus will be on the AG's assertion that dominance does play a role in the assessment of the freedom of consent under the GDPR. This statement raises two main issues surrounding the role of market power in the GDPR that the *Article* seeks to address. Firstly, how should dominance be

[11] C Lazaro and D Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) SCRIPTed 3, 4.

[12] R Pollock, 'Is Google the Next Microsoft? Competition, Welfare and Regulation in Online Search' (2009) ssrn.com. See also OECD, *Data-Driven Innovation for Growth and Well-being: Interim Synthesis Report* (October 2014) www.oecd.org.

[13] W Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection' (MAGKS Joint Discussion Paper Series in Economics 14-2016) MACIE Paper Series Nr. 2016/3, Philipps-Universität Marburg, p. 7.

[14] European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) edps.europa.eu 35.

[15] BKA Decision B6-22/16 of 6 February 2019.

[16] Case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* ECLI:EU:C:2023:537. This contribution was written before the Meta judgment was published by the CJEU on 4 July 2023.

established by data protection authorities (DPAs)? Secondly, what role should dominance play in the assessment of the lawfulness of data processing? The *Article* aims to further the debate around freely given consent for data processing in the digital market and anticipate what issues DPAs will grapple with if the CJEU follows the AG's opinion in the Facebook case. It will propose how DPAs can ensure that individuals' data protection rights are adequately safeguarded in a space dominated by the interests of big tech and thus ensure the future-proofness of the GDPR in this space. More generally, the *Article* seeks to show that to regulate digital platforms effectively, we cannot look at different regulatory regimes in isolation, but must ensure that we adopt a coherent approach and use relevant expertise across regimes.

II. The Facebook case

II.1. Case overview

In February 2019, the BKA imposed on Facebook restrictions on the processing of user data, upon finding that it was imposing exploitative business terms under Section 19(1) GWB (largely corresponding to art. 102 TFEU).[17] Facebook was found to be abusing its dominant position, because it essentially forced users to agree to its terms and conditions, under which it could collect user data also outside of the Facebook website[18] and combine this data with users' Facebook profiles. The BKA argued that "there is no effective consent to the users' information being collected if their consent is a prerequisite for using the Facebook.com service in the first place".[19] The finding of a lack of valid consent was also tied to Facebook's dominance and the lack of alternative social networks on the market. Furthermore, the BKA maintained that the merging of data deprived consumers of control over their personal data and, thereby, constituted a violation of the right to informational self-determination.[20] Under German competition law, Section 19(1) GWB must be applied in order to protect constitutional rights, including

[17] Bundeskartellamt, 'Facebook, Exploitative Business terms Pursuant to Section 19(1) GWB for Inadequate Data Processing' (6 February 2019) www.bundeskartellamt.de.

[18] The BKA talks about third party sources as services owned by Facebook, like WhatsApp and Instagram as well as third party websites that "embedded Facebook products such as the 'like' button or a 'Facebook login' option or analytical services such as 'Facebook Analytics', data"; Bundeskartellamt, 'Background Information on the Facebook Proceeding' (19 December 2017) www.bundeskartellamt.de.

[19] Bundeskartellamt, 'Facebook, Exploitative Business terms Pursuant to Section 19(1) GWB for Inadequate Data Processing' cit.

[20] In one of the first articulations of the right to informational self-determination, the German Federal Constitutional Court defined it as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others", BVerfGE 65, 1 – Volkszaehlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die muendliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren ueber die Verfassungsbeschwerden.

data protection rules, in particular "in cases where one contractual party is so powerful that it is practically able to dictate the terms of the contract and the contractual autonomy of the other party is abolished".[21] Accordingly, the BKA could rely on GDPR rules when assessing whether Facebook's conduct was abusive.

Following Facebook's appeal, the Higher Regional Court in Düsseldorf suspended the BKA's order in interim proceedings.[22] Among other reasons, the Düsseldorf Court argued that an infringement of data protection rules by a dominant firm cannot be seen as a violation of competition law, if there is no causal connection between the illegitimate data processing and the firm's market power. The Federal Court of Justice annulled the decision of the Düsseldorf Court,[23] reasoning that to prove an abuse of Facebook's dominant position, it sufficed to show that it had restricted users' freedom of choice. The main proceedings are still ongoing in the Düsseldorf Court, which filed a request for a preliminary ruling to the CJEU. The request comprises key questions of data protection law and the relationship between competition and DPAs. This *Article* discusses whether dominant firms should carry a higher responsibility than non-dominant firms in regard to compliance with data protection law. More specifically, the Düsseldorf court referred the following question to the CJEU: "Can consent within the meaning of Article 6(1)(a) and Article 9(2)(a) of the GDPR be given effectively and, in accordance with Article 4(11) of the GDPR in particular, freely, to a dominant undertaking such as Facebook Ireland?".[24]

What is noteworthy is how a competition law case raised crucial questions regarding the interpretation of the GDPR. The BKA stated that the GDPR includes elements of market power when assessing whether consent is freely given, *e.g.*, power imbalances and the availability of options. The BKA explored this issue by using data protection rules as a benchmark to establish an exploitative abuse in competition law, where market power and the notion of "special responsibility" are inherent parts of the analysis. However, according to the BKA, the Facebook case was not only a case of a dominant undertaking violating competition law through a GDPR breach, but also a case of an undertaking breaching GDPR, because of its dominance. In this way, the BKA extended the notion in competition law of 'special responsibility' to the GDPR.[25] In this respect, Graef and Van Berlo argue that "in formulating this two-way interaction between data protec-

[21] *Ibid*.

[22] Higher Regional Court of Düsseldorf VI-Kart 1/19 of 26.08.2019 Facebook / Bundeskartellamt available at www.olg-duesseldorf.nrw.de.

[23] Courtesy translation of Press Release No 080/2020 published by the Bundesgerichtshof (Federal Court of Justice) on 23 June 2020 www.bundesgerichtshof.de provided by the Bundeskartellamt, available at www.bundeskartellamt.de.

[24] *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* cit.

[25] I Graef and S Van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' (2020) European Journal of Risk Regulation.

tion law and competition law, the Bundeskartellamt has not only incorporated data protection principles into its competition analysis, but similarly transferred elements of competition law into data protection".[26]

II.2. The opinion of the AG

The judgment in this case has yet to be handed down, but the opinion of the AG sheds some light on how the court might answer the questions. As to the question concerning the role of dominance in freely given consent, the AG has responded as follows: "In the present case, 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 [...] Besides, that circumstance alone cannot, in principle, render the consent invalid".[27]

Thus, according to the AG, while dominance plays a role in the assessment of the freedom of consent, it is not determinative.[28] This seems like a rather neutral outcome, which will give both controllers and authorities flexibility in assessing the validity of consent. However, on a closer look, it does raise some fundamental questions. Firstly, although dominance is a concept commonly used by competition authorities, DPAs are not accustomed to it, and might not have the necessary expertise to assess whether a company is or is not dominant on the market. As will be discussed below, the AG claimed that a dominant position for GDPR purposes does not necessarily need to "be regarded as a dominant position within the meaning of Article 102 TFEU".[29] But then, how should dominance be established by DPAs? Secondly, if consumers[30] do not have a viable alternative on the market, increasing the requirements for valid consent could compensate for the fact that data subjects do not have the freedom to choose among different providers. Dominant firms can, thus, be held to have a higher burden to satisfy, in order to be able to use consent as a ba-

[26] *Ibid*.

[27] Case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* ECLI:EU:C:2022:704, opinion of AG Rantos, para. 75. In its judgment, published on 4 July 2023, the CJEU agreed with the AG on this point; case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* ECLI:EU:C:2023:537 paras 147-148.

[28] *Ibid*. para. 77.

[29] *Ibid*. para. 75. In its judgment, the CJEU does not mention anything about the concept of dominance. Case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* ECLI:EU:C:2023:5379.

[30] In this *Article* the terms "individuals", "consumers" and "data subjects" are used somewhat interchangeably. Although, the terms "consumers" and "data subjects" are distinct and, respectively, belong to the areas of competition (and consumer) law and data protection regulation, when it comes to the digital market, these regimes are interconnected, as this paper demonstrates. The conduct of market players, and their regulation, can affect individuals' interests as consumers and data subjects contemporaneously.

sis for processing. But how should DPAs integrate market power concerns in their assessments? These two issues will be discussed in turn in the remainder of the *Article*.

III. Dominance for GDPR purposes

III.1. Market power and the GDPR

In competition law, the presence of market power is determined by the fact that an undertaking does not face significant competitive pressure, allowing it to behave to an appreciable extent independently of its competitors, customers and, ultimately, its consumers.[31] This means that it can profitably raise prices above competitive levels or restrict output or quality below competitive levels and, in the present case, impose data protection terms that users would otherwise not accept. Digital markets are particularly prone to concentration, due to network effects, which occur when an increase in the number of participants improves the value of a good or service. Direct network effects typically characterise social media platforms, in which users directly benefit from other users being active on the same platform. Indirect network effects exist in two-sided markets, if, for example, the number of users on a platform benefit the advertisers. Facebook, for instance, benefits from both forms of network effects.[32]

Market power is evidently also relevant for the purposes of the GDPR, especially when data controllers rely on consent as a basis for processing. Currently, however, when determining data controllers' obligations under the GDPR, only limited weight is given to their market power, and DPAs do not assess whether a market is competitive enough for consumers to have a real choice. Depending on whether the CJEU follows the AG's opinion in the Facebook case, DPAs might need to start having a closer look at market dynamics. In order to take a more market-focused approach to data protection, DPAs would need to resort to economic concepts used in competition law.[33] This would allow DPAs to get a better idea of the market forces that can impact the level of data protection afforded by these firms and to have a benchmark for evaluating when obligations need to be enforced more strictly.

[31] Case C-27/76 *United Brands v Commission* ECLI:EU:C:1978:22.

[32] ML Katz and C Shapiro, 'Network Effects, Competition, and Compatibility' (1985) American Economic Review 424.

[33] I Graef, D Clifford and P Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law' (2018) International Data Privacy Law 206.

III.2. Dominance in AG Rantos' opinion

In his opinion, AG Rantos argues that "the validity of consent should be examined on a case-by-case basis"[34] and that it is for the controller to demonstrate that consent was given freely, "taking into account, where appropriate, the existence of a clear imbalance of power between the data subject and the controller [...]".[35] This was already suggested by Clifford et al., who argued that: "in keeping with the accountability principle, the controller may be required to prove not only that informed, specific, and unambiguous consent has been provided in line with the requirements in the GDPR, but also that the clear imbalance in power did not affect the consumer-citizen's decision to consent, despite the fact that this consent was required to access the service in question".[36]

Even if the burden to prove that consent was freely given is on data controllers, DPAs, when enforcing the GDPR, will need to determine the extent to which market power or other barriers to competition reduce choice and, correspondingly, in which situations consent is valid. Furthermore, in order to increase legal certainty and compliance, there should be guidance for data controllers as to when they have a higher threshold to satisfy to obtain valid consent.

The AG has not specified how market power should be established, but has argued that, for the purposes of GDPR enforcement, it "need *not necessarily* be regarded as a dominant position within the meaning of Article 102 TFEU [emphasis added]".[37] This suggests that there might be more leeway when establishing dominance under the GDPR compared to competition law. Accordingly, DPAs might not necessarily have to carry out the extensive economic analysis of the market required in competition law. At the same time, however, the statement implies that competition law assessments may be used as a baseline for the purposes of GDPR enforcement. It would, indeed, be desirable for DPAs to use findings of dominance in competition law when enforcing the GDPR. Not only would this be efficient inasmuch as it would allow DPAs to make use of the existing expertise and analysis of competition authorities, it would also contribute to consistency in the definition of dominance across different legal frameworks. The latter is particularly important in digital markets, in which the regimes are increasingly interrelated.[38]

[34] Case C-252/21*Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, opinion of AG Rantos, cit. para. 76.

[35] 21*Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, opinion of AG Rantos, cit. para. 77.

[36] D Clifford, I Graef and P Valcke, 'Pre-formulated Declarations of Data Subject Consent: Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) German Law Journal 713.

[37] AG Opinion, para. 75, emphasis added.

[38] See A D'Amico, 'Conceptualising the Interrelation between Data Protection Regulation and Competition Law' in E Kosta and R Leenes (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar 2022).

Nonetheless, since dominance in competition law is established in relation to specific relevant markets, the existence of dominance in one market cannot usually be simply transferred to another market. To illustrate the point, Google can be dominant in the markets for general search services and the licensing of smart mobile OSs, but not in the market for mobile web browsers.[39] DPAs' greater flexibility in determining dominance means that they could adopt findings of dominance from competition law, without paying too much attention to the precise market definition. Clarifying how definitions of dominance can be transferred from one regime to the other should not be a major obstacle; the main limitation of DPAs relying on competition law classifications of dominance is that they are restricted to recent competition law cases or investigations that are underway. This could prove a major obstacle, in particular, if new dominant companies that do not raise competition law issues emerge.

III.3. The definition of "gatekeeper" under the DMA

To fill the gap, DPAs could use the classification of gatekeepers of the Digital Markets Act (DMA),[40] in addition to findings from competition law. The DMA is considered one of the centrepieces of the European digital strategy and aims to ensure that platforms that act as gatekeepers in digital markets behave fairly.[41] It is designed to complement competition law, recognising that "existing Union law does not address, or does not address effectively, the challenges to the effective functioning of the internal market posed by the conduct of gatekeepers that are not necessarily dominant in competition-law terms".[42]

The DMA formulates a set of criteria for determining gatekeeping status. It foresees that an undertaking is a gatekeeper if: [43]

it has a significant impact on the internal market;[44]

it provides a core platform service[45], which is an important gateway for business users to reach end users;[46] and

[39] Case T-604/18 *Google and Alphabet v Commission (Google Android)* ECLI:EU:T:2022:541.

[40] 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).

[41] Commission website, *The Digital Markets Act: ensuring fair and open digital markets* ec.europa.eu.

[42] Digital Markets Act, recital 5.

[43] *Ibid*. arts 3(1) and 3(2).

[44] Defined as €7,5 billion annual Union turnover or €75 billion market valuation and it provides the same core platform service in at least three MSs.

[45] "'Core platform service' means any of the following: (a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communications services; (f) operating systems; (g) web browsers; (h) virtual assistants; (i) cloud computing services; (j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i)" (Digital Markets Act, art. 2(2)).

it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.[47]

With the DMA, DPAs will soon have an updated list of gatekeepers in the digital market, monitored by the Commission.[48] Given that the DMA is designed, among other things, to regulate the behaviour of digital companies that can unilaterally impose unfair terms on end-users,[49] the definition of a "gatekeeper" is useful for GDPR purposes as well. The high threshold to reach a gatekeeping status means that these companies can be considered dominant for the purposes of GDPR enforcement, as suggested by AG Rantos[50] (even though not necessarily under art. 102 TFEU). Again, relying on existing definitions of market power and gatekeepers is efficient and contributes to consistency and legal certainty in the way digital platforms are regulated. This is particularly important in light of the EU's digital strategy and recent legal acts intersecting with the GDPR in the digital arena. To guarantee the GDPR's future-proofness and meet the challenges posed by the digital market, efforts need to be made to ensure that the GDPR is compatible and synergistic with the regulatory landscape that surrounds it.

The largest digital platforms will fall under the definitions of competition law and the DMA and, by using these definitions, DPAs have a solid ground on which to impose special obligations on these platforms. In cases in which DPAs believe that specific companies should have higher responsibilities under the GDPR and these have not (yet) been labelled as dominant under competition law or do not fall under the definition of a gatekeeper under the DMA, DPAs can carry out their own case-by-case assessments and determine whether market power impedes consent from being given freely. When doing so, DPAs can follow guidance used by competition authorities when assessing

[46] Defined as 45 million monthly active end users in the Union and 10 000 yearly active business users.

[47] The thresholds must be met in the previous three financial years.

[48] Digital Markets Act, arts 3 and 17.

[49] In particular, in recital 13 of the Digital Markets Act the following rationale behind the need to regulate specific gatekeepers is put forward: "Weak contestability and unfair practices in the digital sector are more frequent and pronounced for certain digital services than for others. This is the case in particular for widespread and commonly used digital services that mostly directly intermediate between business users and end users and where features such as extreme scale economies, very strong network effects, an ability to connect many business users with many end users through the multisidedness of these services, lock-in effects, a lack of multi-homing or vertical integration are the most prevalent. Often, there is only one or very few large undertakings providing those digital services. Those undertakings have emerged most frequently as gatekeepers for business users and end users, with far-reaching impacts. In particular, they have gained the ability to easily set commercial conditions and terms in a unilateral and detrimental manner for their business users and end users".

[50] *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, opinion of AG Rantos, cit. para. 75.

dominance[51] and make use of the increased collaborations taking place with competition authorities.[52]

In this part it was proposed how to determine which companies should have higher responsibilities under the GDPR. The next part builds upon this and discusses what the higher responsibilities of these companies should entail. More specifically, what role market power should play in the assessment of the validity of consent.

IV. Dominance and the validity of consent

IV.1. Freely given consent under the GDPR

Under the GDPR, consent is one of the six legal bases for processing.[53] In order to be valid, it "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her [...]".[54] This *Article* focuses on the "freely given" component of consent, and, specifically, how this requirement should be interpreted when data controllers are dominant companies.

Consent is the only legal basis which requires data subjects to be actively involved in the decision regarding the processing of their data.[55] When data processing is not "necessary" under one of the other legal bases,[56] firms can still obtain permission for the data processing directly from the data subjects. This is in line with the core value underlying data protection to give individuals control over their data. The nature of the digital market, with its monopolistic tendencies, however, has apparent repercussions on the validity of consent. Dominant firms can obtain consent through users' lack of alternatives or user lock-ins, thereby potentially fulfilling the safeguards imposed by the GDPR in a purely formalistic fashion. A problem that is linked to the controllers' market power is that, upon seeing privacy terms, users are often only given a take-it-or-leave-it option. They are

[51] For an overview, see for instance Communication from the Commission of 24 February 2009 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', p. 7-20.

[52] For instance, at EU level, the EDPS launched the Digital Clearinghouse "as a voluntary network of regulators involved in the enforcement of legal regimes in digital markets, with a focus on data protection, consumer and competition law" (www.digitalclearinghouse.org), which has been endorsed by the European Parliament. Furthermore, a number of member states, including the Netherlands, Spain, and France have formal collaboration agreements. In the Netherlands, the Authority for Consumers and Markets and the Data Protection Authority collaborate as part of a wider cooperation platform, the Digital Regulation Cooperation Platform ("SDT"), which was launched in October 2021 (autoriteitpersoonsgegevens.nl).

[53] GDPR, art. 6.

[54] GDPR, recital 32.

[55] The other legal bases are: contract performance, legal obligation, vital interest, public interest and legitimate interests (GDPR, art. 6).

[56] GDPR, art. 6.

thereby deprived of the freedom to exercise a meaningful choice, since they do not have the possibility to select their data protection preferences in the market and to tailor these to different contexts.[57] It has been argued that the "binary choice is not what the privacy architects envisioned four decades ago when they imagined empowered individuals making informed decisions about the processing of their personal data".[58]

The GDPR contains requirements for consent to qualify as "freely given".[59] The central element for the purposes of this *Article* is the following recital: "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller".[60] The Regulation specifically refers to public authorities as type of controllers that would have difficulties to rely on consent because it would be "unlikely that consent was freely given in all the circumstances of that specific situation".[61] The European Data Protection Board (EDPB) also mentions an employment context as one in which an imbalance of power could undermine the validity of consent.[62] It then states that:

> "Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by the WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will".[63]

The element of imbalance of power appears to be relevant in monopolised markets as well as in markets in which consumer choice is undermined, for instance, through strong network effects or lock-ins.[64] Nonetheless, so far market power has not played a role in the assessment of the validity of consent.[65]

[57] See O Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015); and F Costa-Cabral and O Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) CMLRev 11.

[58] F Cate and V Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (2013) International Data Privacy Law 67.

[59] GDPR, art. 4(11).

[60] *Ibid.* recital 43.

[61] *Ibid*.

[62] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, version 1.0, adopted on 4 May 2020, para. 21.

[63] *Ibid*. para. 24.

[64] See F Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) MaineLRev 15 digitalcommons.mainelaw.maine.edu.

[65] See, for instance, the GDPR case brought by the French Data Protection Commission (CNIL) against Google in 2019. The CNIL held that Google had violated the obligation to have a legal basis for processing in relation to ads personalisation, because consent, on which it relied, was not informed, specific and un-

A second key element of freely given consent is contained in art. 7(4),[66] which states that "when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".[67] It seems difficult to reconcile this requirement with a take-it-or-leave-it approach that forces data subjects to consent to the processing of their data in exchange for using a service. However, the term "utmost account" leaves room for interpretation and this provision has indeed been interpreted in a flexible manner. In *Planet49*[68] an online gaming company held an online promotional lottery that required users to give personal information in order to participate. The case was mainly about explicit consent, with the CJEU ruling that consent is not valid if given by way of pre-checked checkboxes. However, this was also a case in which users were obliged to disclose data in order to participate in the lottery. The Advocate General saw no problems with the "selling" of personal data and the Court did not raise the question around art. 7(4) GDPR.[69]

IV.2. A TWO-TIER APPROACH

So far it has been argued that the way consent is currently collected by dominant digital platforms sits uneasily with the notion of freely given consent. The GDPR does contain provisions which could render consent invalid when *i)* the data controller is dominant and users do not have alternatives on the market and *ii)* the data controller does not give users a choice but to accept its terms, if they want to use its service. However, they have not played a significant role in the assessment of the validity of consent in the digital market. The Facebook case could mark a turning point in this respect. In that case, the president of the BKA claimed that: "voluntary consent means that the use of Facebook's services must not be subject to the users' consent to their data being collected and combined in this way. If users do not consent, Facebook may not exclude them from its services and must refrain from collecting and merging data from different sources".[70]

ambiguous. The CNIL ordered Google to correct these shortcomings, but failed to address Google's market power and the fact that many users considered Google indispensable. Commission Nationale de l'Informatique et des Libertés, 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against Google LLC' (21 January 2019) www.cnil.fr.

[66] See also GDPR, recital 42: "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

[67] GDPR, art. 7(4); see also GDPR, recital 43.

[68] Case C-673/17 *Planet49* ECLI:EU:C:2019:801.

[69] Case C-673/17 *Planet49* ECLI:EU:C:2019:46, opinion of AG Szpunar.

[70] Bundeskartellamt prohibits Facebook from combining user data from different sources, Bundeskartellamt (7 February 2019) www.bundeskartellamt.de.

Andreas Mundt thereby suggests that, *since it is dominant*, Facebook cannot make the data processing a prerequisite for using its service, but must give users the option to opt out of the data processing in question. This approach seems to be compatible with the relevant provisions of the GDPR described in this section. In accordance with this, the AG's opinion points to the fact that dominant companies should be treated as having a special responsibility also under the GDPR.

This would lead to a form of asymmetric regulation, as is typically found in cases in which a formerly monopolistic sector is deregulated. In those cases, it is believed that regulating dominant incumbents and new entrants asymmetrically can reduce impediments to market contestability.[71] Asymmetric regulation also characterises the DMA; gatekeepers in the digital space have to adhere to stricter rules than other companies. In the case of the GDPR, a somewhat inverse rationale applies: asymmetric regulation is not meant to improve competition,[72] but to compensate for the lack thereof and secure the protection of individuals' rights. Although this approach is consistent with the goals of the GDPR, it is not immediately clear how the relevant GDPR provisions should be interpreted, to put this approach into practice. In other words, what role should dominance play when establishing whether consent is freely given? A possible answer is proposed in the rest of this section.

It was mentioned that DPAs allow for consent to be used as a legal basis when firms offer services in exchange for data, despite sitting uneasily with art. 7(4) GDPR.[73] This reflects the fact that in the digital market there are situations in which individuals can effectively choose whether to use a service that comes with data collection or not, in the same way in which they can choose whether to use a service that requires monetary payment. When consumers have multiple options and lock-in and network effects are not particularly strong, it is arguably legitimate to leave the discretion to firms as to what kind of data to request in return for their services, as long as they obtain informed, specific, and unambiguous consent. In these cases, it can be assumed that consumers would only agree to the terms, if they considered them fair in relation to what they are getting in return.[74] Essentially, this will allow firms in competitive markets to compete on data protection terms.

On the contrary, when it comes to players like Facebook or Google, which have significant market power and create consumer lock-ins, there is not a sufficient degree of com-

[71] EE Bailey and WJ Baumol, 'Deregulation and the Theory of Contestable Markets' (1984) Yale Journal on Regulation 111; A Pera, 'Deregulation and Privatisation in an Economy-wide Context' (1989) OECD economic studies 159.

[72] It could, however, result in more competition.

[73] Art. 7(4) GDPR states that "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

[74] This refers only to the freely given element of consent; there are other issues around consent, for instance whether it can ever be truly informed.

petition in the market that would guarantee consumer choice. In order to protect individuals' control over data it is, thus, justifiable to prohibit that these firms make the provision of their services conditional on consent to terms that go beyond what is necessary for the provision of their services. Instead, they should be ordered to give users a real choice (in terms of opting in or out) for consent to be valid.[75] Essentially, the "freely given" requirement of consent should play a more important role in digital markets, but should be interpreted as meaning that there needs to be *some* freedom as opposed to *complete* freedom: either the freedom to renounce a specific service or the freedom to choose whether or not to disclose data in connection to that service (when renouncing is not a possibility).

In the Proposal for the ePrivacy Regulation, the Council of the European Union reasons along the same line:

> "In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services [...] Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice... such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position".[76]

This also appears to be consistent with the DMA, a recital of which reads: "to ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent".[77]

In its guidelines on consent, endorsed by the EDPB, the art. 29 Working Party, however, seemed to reject such an approach, *i.e*. distinguishing between competitive and

[75] This differentiation applies to the determination of the lawfulness of processing (GDPR, art. 6), more specifically, whether undertakings can use consent as a legal basis for processing. The other data protection principles (*e.g*. purpose limitation and data minimisation, GDPR, art. 5) remain unaltered.

[76] Proposal COM(2017) 10 final for a Regulation of the European Parliament and of the Council of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), recital 20.

[77] Digital Markets Act, recital 36.

non-competitive markets for the purposes of establishing the validity of consent.[78] It maintained that, while controllers can rely on consent for use of data that is not necessary for the provision of the service, provided that they offer data subjects a genuinely equivalent service that does not require consenting to the data use, they cannot argue that data subjects have a choice between their own service and an equivalent service offered by another provider. Essentially, this implies that data subjects should always be able to opt out, regardless of the competitive situation in the market. The Working Party argues that otherwise: "the freedom of choice would be made dependant [sic] on what other market players do and whether an individual data subject would find the other controller's services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities".[79]

Nonetheless, as argued by Clifford et al., it appears unlikely that the Working Parties' "strict interpretation of consent [...] will be sustainable in light of the various moves to recognize the economic value of personal data and the broader internal market considerations of the EU legislator".[80] First of all, if the CJEU follows the AG's opinion, data controllers and DPAs will have no choice but to take market conditions into account in these circumstances. Besides, the problem identified by the Working Party only emerges if the threshold of market concentration is placed too low; when dealing with a tech giant and gatekeeper like Google, it is safe to say that users do not have a real choice among different providers. If DPAs adopt transparent and consistent methods of determining dominance, for instance, by relying on the classification of the DMA, identifying when individuals do and do not have sufficient alternatives will be straightforward. Implementing a two-tier approach is a way in which the GDPR can respond to the challenges represented by the market power of big tech and ensure its future-proofness when it comes to safeguarding data subjects in the digital market.

If such a two-tier approach is put into place, firms that cannot rely on consent, *i.e*. dominant firms, would have to offer consumers the choice to opt out of the data processing that is tied to consent. While this a beneficial outcome from the point of view of individuals' control over their data, firms will be reluctant to do, if they rely on the data to monetise their services. Allowing users to utilise a service without processing their data in exchange would involve offering the service truly for free. To compensate for the lack of data monetisation, firms might need to charge users a fee. This outcome would safeguard data protection rights, but deprive individuals of the choice to pay with

[78] Art. 29 Working Party, 'Guidelines on consent under Regulation 2016/679', adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018.

[79] Art. 29 Working Party, 'Guidelines on consent under Regulation 2016/679', adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, p. 9-10.

[80] D Clifford, I Graef and P Valcke, 'Pre-formulated Declarations of Data Subject Consent: Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' cit.

data instead of money. From a more holistic perspective, switching to monetary payment would empower consumers to the extent that they are better at comparing prices than the cost of a service in terms of the disclosure of their data. This could incentivise entry into the market, since new entrants could attract users by undercutting the dominant undertaking's prices.

IV.3. The legitimate interests legal basis

This two-tier system, in which dominant companies are forced to either offer their service for free or charge monetary prices, while non-dominant companies can offer the same service in exchange for data (*i.e*. for "free" from the point of view of many consumers), will undoubtedly be disruptive for the business models of the companies affected. However, consent is not the only basis for data processing; an alternative is the "legitimate interests" legal basis. This legal basis contains an express balancing requirement between the controllers' interests and data subjects' fundamental rights.[81] Under this legal basis, dominant companies have the chance to monetise services through data (and offer them for "free"), but only when they have legitimate interests in doing so.

The EDPB provides guidance to data controllers and authorities as to what qualifies as a legitimate interest.[82] With the legitimate interests legal basis, DPAs can carry out their own substantive assessment to verify that the legitimate interests justification relied upon by a data processor constitutes a valid legal basis, and thereby protect data subjects' rights. When it comes to consent, on the other hand, if the framework conditions for its validity are met, the substantive assessment is in the hands of data subjects alone. It seems sensible that in a concentrated market, in which data subjects do not have the freedom to choose, data protection regulators are the ones ensuring that data is processed in a legitimate manner, by taking into account and balancing the interests of data controllers and subjects.

DPAs should take a more active role in regulating how digital platforms can legitimately process and monetise individuals' data. The first step would be to lay down more explicit rules regarding the exchange of data against services in the digital mar-

[81] GDPR, art. 6(1)(f); GDPR, recital 47: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller... At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place".

[82] See art. 29 Working Party 2014, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC' (WP 217) (9 April 2014).

ket.[83] The Board already indicated that it will issue new guidelines on the application of legitimate interest as a legal basis for processing, after stakeholders have pointed out a lack of guidance and a lack of consistency between national DPAs.[84] These new guidelines would represent a great opportunity to better regulate how dominant companies can process data, especially if their ability to rely on consent will decrease in the future.

IV.4. Obligations under the DMA

In parallel to the GDPR, the DMA introduces specific obligations for gatekeepers concerning their data practices. According to art. 5(2),

> "The gatekeeper shall not do any of the following:
> (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper;
> (b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services;
> (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and
> (d) sign in end users to other services of the gatekeeper in order to combine personal data".[85]

Since the DMA's aim is to increase the contestability of digital markets rather than protect individuals' rights over data, the obligations above concern only specific data practices that are seen as restricting competition and consolidating gatekeepers' market power. Nonetheless, it is good for DPAs to be aware of these obligations, in order to ensure consistency among the regimes. Art. 5(2) specifies that the forms of processing above are allowed if the end user has been presented with the specific choice and has given consent within the meaning of the GDPR. This is compatible with the approach suggested in this

[83] The EDPB and before that the art. 29 Working Party have published guidelines on when the legal bases can be relied upon, however, there is not one comprehensive guideline that sets out the views taken when it comes to the extent to which data can be used in exchange for digital content and services. For relevant guidelines, see art. 29 Working Party 2014, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC' (WP 217) (9 April 2014); EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679', version 1.0, adopted on 4 May 2020; and EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects', 8 October 2019, version 2.0.

[84] Commission Staff Working Document accompanying the document Communication COM(2020) 264 final from the Commission to the European Parliament and the Council of 24 June 2020 on Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation.

[85] Digital Markets Act, art. 5(2).

Article, meaning that the processing can be based on consent, if consent is truly freely given. A discrepancy however is potentially created by the last sentence of art. 5(2), which foresees that the obligations mentioned above, are "without prejudice to the possibility for the gatekeeper to rely on Article 6(1), points (c), (d) and (e)" of the GDPR.[86] The three legal bases mentioned in the Article do not include the "legitimate interests" legal basis. Thus, to prevent inconsistencies, when providing guidance on when the legitimate interest legal basis can be relied on by digital platforms, the EDPB and DPAs should take into account the obligations that apply to gatekeepers under the DMA.

V. Conclusion

In an age in which data is ubiquitous and an integral part of digital companies' business models, it is pivotal to ensure that individuals' rights and interests around data are adequately protected. This *Article* has focused on the issue surrounding the validity of consent given to dominant tech companies. Currently, when establishing whether consent is freely given, the market position of the data controller is not taken into account, although it can evidently foreclose individuals' choice. In the Facebook case, AG Rantos stated that dominance is a factor in the assessment of the freedom of consent under the GDPR. The *Article* addressed two main issues surrounding the role of market power in the GDPR, which the AG's opinion raises. Firstly, how should dominance be established by DPAs? It was argued that DPAs should rely on the findings of dominance in competition law and the designation of gatekeepers under the DMA, when available. Secondly, what role should dominance play in the assessment of the validity of consent? Here it was proposed that dominant companies should only be allowed to rely on consent if they give individuals the possibility to opt out of the processing. Alternatively, they can rely on the legitimate interests legal ground, if applicable.

By contextualising the issues raised by the Facebook case, the *Article* explored in what ways market power needs to be taken into account when determining the validity of consent in the digital market, in order to ensure the protection of individuals' rights under the GDPR. It has been indicated that this also requires DPAs to take a more active role in determining the ways in which dominant digital platforms are allowed to legitimately process data. Enforcing the GDPR in manner that takes into account the market realities and is consistent with neighbouring regulatory regimes is crucial for it to be future-proof and have a meaningful impact on individuals' rights in the digital world.

[86] These are the following legal bases: "(c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", GDPR, art. 6(1).