[Pre-print version of: Rivista Concorrenza e Mercato, Vol. 29/2022: Numero Speciale Concorrenza e Regolazione nei Mercati Digitali, pp. 191-212. Please cite the full reference.]

THE CIRCULARITY OF CONSENT IN THE DMA: A CLOSE LOOK INTO THE PREJUDICED SUBSTANCE OF ARTICLES 5(2) AND 6(10)

ALBA RIBERA MARTÍNEZ*

ABSTRACT

The Digital Markets Act (DMA) captures gatekeeper power to address the lack of contestability and unfairness in digital markets. Its provisions imbricate into the regulatory landscape bearing in mind complementarity regarding other acts of Union law which also apply to certain aspects of the digital arena, namely the General Data Protection Regulation (GDPR) or the e-Privacy Directive.

The DMA does not override the provisions of these rules, although the practical implementation of its do's and don'ts will question the value of non-economic interests which have been at the forefront of EU policy at large in their interaction with digital business models. In the particular case of the intersection between privacy and antitrust, Articles 5(2) and 6(10) of the DMA stand out as the two key areas where the interpretation of the GDPR will play a major role, namely through the force of consent, legal basis, and user choice. Although both provisions impose negative and positive obligations on personal data, their role is tempered when the user is presented with a specific choice and grants consent to the gatekeeper to combine and use personal data.

The paper analyses the potential implications of both provisions in light of the existence of power and information asymmetries between gatekeepers and end users. The paper navigates the cases that have inspired the framework of the DMA in this regard, from an antitrust and data protection perspective. The paper identifies that the interaction between the concept of consent and the massive collection and processing of personal data is designed according to a circular concept. The DMA builds up its provisions on Articles 5 and 6 on the same premise. The paper identifies the circularity which the DMA's enforcers might incur when enforcing the regulatory instrument.

KEYWORDS: Consent; Opt-in Systems; Digital Markets Act; Data; Self-management

JEL CLASSIFICATION: K210 – Antitrust Law; K230 – Regulated Industries and Administrative Law

[Pre-print version of: Rivista Concorrenza e Mercato, Vol. 29/2022: Numero Speciale Concorrenza e Regolazione nei Mercati Digitali, pp. 191-212. Please cite the full reference.]

SUMMARY

[Pre-print version of: Rivista Concorrenza e Mercato, Vol. 29/2022: Numero Speciale Concorrenza e Regolazione nei Mercati Digitali, pp. 191-212. Please cite the full reference.]

1. Introduction

The DMA entered into force on the 1st of November 2022 and its provisions will come into full force starting from March 2024[1]. The purpose of the Regulation is to ensure contestability and fairness for the markets in the digital sector, in general, to contribute to the proper functioning of the internal market. In this regard, the DMA sets out a designation process for core platform service providers to categorise them as gatekeepers. Once they are designated in the terms of Article 3 of the DMA, those gatekeepers are legally bound by the DMA's provisions, especially concerning the prohibitions and obligations outlined in Articles 5, 6 and 7. Compliance with these obligations is due six months after the designation is completed, regardless of the delay in particular provisions contained in Articles 6 and 7 of the DMA.

Alongside contestability and fairness, the DMA is aimed to avoid fragmentation of the internal market in terms of rulemaking from the perspective of the Member States in the area of competition law as far as digital markets are concerned. According to Recitals 10 and 11 of the DMA and Article 1(6) of the DMA, the Regulation is inspired by the principle of complementarity. Thus, its force should not, in principle, hinder the application of Articles 101 and 102 TFEU[2] and the corresponding national competition rules concerning anticompetitive multilateral and unilateral conduct. In this regard, the DMA does not impugn the effective enforcement of competition as a whole, although several practical problems may arise as a consequence of the overlapping dispositions applying to the same digital players. In this same vein, other acts of Union law that regulate certain aspects of the provision of core platform services are equally inspired by this same idea. The DMA does not amend nor impinge any of the concepts contained in the rest of the rules of the Eu law framework, such as the GDPR[3], the e-Privacy directive[4], the P2B Regulation[5], or the Unfair Commercial Practices Directive[6]. The

* PhD Student at University Carlos III of Madrid and Lecturer in Competition Law at University Villanueva. Email: riberamartinezalba@gmail.com. According to the ASCOLA Declaration of Ethics, I have nothing to disclose.

[1] EUROPEAN COMMISSION, *Digital Markets Act (DMA)*, available at http://competition-policy.ec.europa.eu (accessed 10 November 2022).

[2] Consolidated version of the Treaty on the Functioning of the European Union in OJ C32/47.

[3] European Parliament and Council, 27 April 2016, 2016/679, Regulation 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) in OJ L119/1.

[4] European Parliament and Council, 12 July 2002, 2002/58/EC, Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) in OJ L201/37.

[5] European Parliament and Council, 20 June 2019, 2019/1150, Regulation on promoting fairness and

DMA applies «without prejudice» to these rules, as far as Recital 12 is concerned. However, that does not mean that the DMA is completely unaware of the impact of these same rules on the provision of core platform services.

For the particular case of privacy protection, the regulatory instrument considers the interaction in three different forms: i) by transposing the GDPR's concepts into the DMA; ii) by upholding consent and some (not all) of the GDPR's legal bases for collection[7], cross-using[8] and processing[9] of personal data as an exemption which overrides the application of Articles 5(2) and 6(10); and iii) by introducing an obligation of an audit on any of the techniques used for profiling of consumers, which can be used for overseeing compliance of both the DMA and the GDPR.

First, the DMA imports the GDPR's concepts on personal data, profiling, and consent directly into its provisions[10]. Compliance with data protection regulation of the DMA is ensured through Article 8, insofar as the gatekeeper will also have to demonstrate compliance with the DMA's provisions by design in line with the GDPR's requirements. The obligations compelling gatekeepers under Articles 5(2) and 6(10) demonstrate the interplay between privacy protection and the DMA by including the end user's consent[11] as a loophole for compliance with those provisions. In other words, the prohibitions and prescriptions imposed on the gatekeeper under these provisions are superseded when the

transparency for business users of online intermediation services in OJ L186/57.

[6] European Parliament and Council, 11 May 2005, 2005/29/EC, Directive concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') in OJ L149/22.

[7] When the DMA was first proposed, the prohibition of Article 5(2) was drafted only regarding the combination of personal data sourced from the core platform services across the rest of services catered by the gatekeeper, although the exemption around consent was already included under Article 5(a). Following European Parliament and Council, 15 December 2020, COM/2020/842 final, Proposal on contestable and fair markets in the digital sector (Digital Markets Act).

[8] At the stage of the Rapporteur's report, cross-using was also included in the prohibition, as per Amendment 104. Following Committee on the International Market and Consumer Protection, 30 November 2021, A9-0332/2021, REPORT on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) and European Parliament, 15 December 2021, P9_TA(2021)0499, Amendments adopted on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

[9] The prohibition on processing was included at the stage of the final negotiations before the European Parliament. See European Parliament, 5 July 2022, P9_TA(2022)0270, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

[10] *DMA*, Article 1(25), (26), (31) and (32).

[11] User and data subject are used interchangeably throughout the paper.

end user consents to the exercise of these same activities. When consent is not obtained by the gatekeeper from the end user, the gatekeeper is compelled to anonymise personal data, when appropriate, under Article 13 of the DMA.

Building up on the contextual reading of these provisions alongside the ongoing debate on the intersection between privacy and competition law, the DMA does not make neutral policy assumptions in terms of the GDPR's interpretation when considered in the background of the applicable rules to the gatekeepers[12]. Instead, Articles 5(2) and 6(10) are based on a narrow reading of the GDPR's provisions, based on the individual perspective of self-management in the field of data protection. Moreover, the end user's consent is also given a prevalent position in terms of policy. For instance, in terms of the prohibition set out in Article 5(2) on the combination, cross-using and processing of personal data across the gatekeeper's core platform services, the effective consent of the end user reverses the prohibition completely and pre-empts its lawfulness in the eyes of the DMA. This policy choice comes at a moment when the interaction and causality between dominance and effective consent has not been delineated yet (even if the European Court of Justice's ruling clarifies this interplay through its awaited ruling on C-252/21[13]).

Against this background, the paper navigates the concept of effective consent as understood from the perspective of the GDPR to understand the implications of the exceptions set out in Articles 5(2) and 6(10) of the DMA.

The first section of the paper addresses the force of effective user consent in terms of its interpretation in the field of the protection of personal data in the GDPR, in light of the misunderstanding that user consent as a legal basis for the processing of personal data empowers individuals over the control of their personal data. Stemming from this idea of self-management as a means to counteract power imbalances of data controllers and processors, the paper reflects on the circularity of the interpretation of consent from the data protection perspective. The section sets out that the criterion to establish whether

[12] W. KERBER, *Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law*, in *The Antitrust Bulletin*, 67, no. 2, 2022, pp. 280-301; A.C. WITT, *Data, Privacy and Competition Law*, in *Graz Law Working Paper*, no. 24-2021, 2021, pp. 1-14; J. BRILL, The Intersection of Consumer Protection and Competition in the New World of Privacy, in *Competition Policy International*, 7, n.1, 2011, pp. 7-23; K. Bania, *Fitting the Digital Markets Act in the existing legal framework: the myth of the "without prejudice" clause*, in *European Competition Journal*, 2022.

[13] CURIA, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social) Case C-252/21*, available at http://www.curia.europa.eu (accessed 13 November 2022).

effective consent has been granted by the user is based on a premise (imbalances in power) which is defined in relation to vulnerability that, in turn, refers back to the concept of imbalances in power between the data controller and the data subject. By this token, the conclusion on the side of the authority interpreting whether effective consent has been provided by the data subject is related to the realisation of an argument based on factual elements rather than on strict legal requirements.

The second section addresses the translation of the concept of effective consent into competition law, namely through the analysis of the seminal *FCO v. Facebook* case[14], alongside other cases which have been rendered at the national level. This section builds on the circularity of self-management in the context of dominance and the interplay between the interpretation of the GDPR and its inclusion in the antitrust analysis.

The final section of the paper deals with the interplay between the circular line of reasoning around the interpretation of the concept of consent and its introduction into the DMA, considering the consequences of the latest of the European Court of Justice's rulings on *DB Station & Service*[15]. Throughout the different sections, the paper questions the transposition of the concept of consent understood from the perspective of self-management rendered by the end user of the designated gatekeepers into the provisions of the DMA, namely Articles 5(2) and 6(10), and its interplay with the capacity to exempt those provisions in light of the circular concept of effective consent rendered to the data controller.

2. Consent from the Perspective of the Processing of Personal Data

The GDPR frames consent as a legal basis to process personal data in Article 6(1)(a) and sets out the conditions for its exercise in Article 7. However, not all expressions of consent are admitted in the eyes of the GDPR[16]. Instead, consent shall 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». Therefore, consent in the form of silence or inactivity is not admitted as valid consent.

[14] Bundeskartellamt, 15 February 2019, B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*.
[15] Court of Justice, 27 October 2022, C-721/20, *DB Station & Service*.
[16] Advocate General Szpunar, 21 March 2019, Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*.

Consent as a legal basis for processing personal data must meet three requirements, which result in a clear indication of the user's wishes. First, it shall be freely given, in the sense that the user shall have a free choice when granting consent. In this sense, Recital 42 of the GDPR establishes that there is no genuine free choice when the data subject is unable to refuse or withdraw consent without detriment to her, namely by being excluded from being provided a service due to not granting consent to the processing of her personal data. In short, the end user must be uncoerced when granting consent[17]. In addition, Recital 43 presumes that free consent is not granted in two specific cases. On one hand, in situations where there is a clear imbalance between the data subject and the controller. On the other hand, when the provision of a service is dependent on consent, despite such consent not being necessary for such performance. Second, consent shall be specific. In other words, the data subject should be aware of the fact that and the extent to which consent is given. Third, consent shall be informed in the sense that the data subject should be aware of the identity of the controller and the purposes of the processing of personal data. For special categories of personal data relating to racial or ethnic origin, and religious or philosophical beliefs, the processing of personal data is banned in principle based on the nature of the data, under Article 9, although the consent of the data subject may override the prohibition. Moreover, the force of explicit consent from the perspective of the end user also overrides other limitations of the GDPR concerning processing recognised as rights in favour of the data subject, namely the right not to be subject to a decision based on profiling.

2.1 The Incorporation of the Notion of Consent into the GDPR

Similar to US regulation, the GDPR follows the fallacy that shifting the regulatory burden on the end user must confer the data subject greater control and protection over her personal data[18]. At least, the Article 29 Working Party and a number of scholars have interpreted the notion of consent in the sense that it must overtly reflect control on the

[17] Article 29 Data Protection Working Party, 28 November 2017, 17/EN, Guidelines on Consent under Regulation 2016/679, WP259 rev.01.

[18] D. J. SOLOVE, W. HARTZOG, *The FTC and The New Common Law of Privacy*, in *Columbia Law Review*, 114, 2014, pp. 583-676; T. B. NORTON, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, in *Fordham Intellectual Property, Media & Entertainment Law Journal*, 27, n. 1, 2016, pp. 181-210; P. M. SCHWARTZ, K.N. PEIFER, *Transatlantic Data Privacy Law*, 106, n. 1, 2017, pp. 115-178; J. KRÖGER, O. LUTZ, S. ULLRICH, *The Myth of Individual Control: Mapping the Limitations of Privacy Self-Management*, 2021, https//www.papers.ssrn.com (accessed 28 November 2022).

side of the end user[19]. This overreliance on individual consent throughout the GDPR follows the privacy self-management approach, where the data subject is conferred the superpower to override the existing interference with two fundamental rights recognised in the Charter[20] (Articles 7 and 8) when massive harvesting activities with their personal data is performed[21].

Consent in the GDPR is formulated as a binary choice -either the data subject grants it, or she does not-, and the extent to which she is protected will be overridden (or not) by choice, even though she has a right to withdraw consent at any time[22]. When consent is rendered, the gate for the access and processing of personal data is opened to the data controller. By virtue of consent, the end user may authorise particular activities regarding data processing which would have been prohibited otherwise under the same provisions of the GDPR[23].

Following this line of reasoning, the expression of consent embodies the perception of the data subject towards a particular normative situation and her capacity to alter its terms before the data controller/processor[24]. For instance, if an end user grants her consent to profiling on an app, the app developer should understand that the particular data subject perceives profiling as admissible and should act accordingly. In the context of data protection, consent is an expression of individual autonomy with legal repercussions on the user's informational self-determination[25].

---

[19] Article 29 Data Protection Working Party, 13 July 2011, 01197/11/EN, Opinion 15/2011 on the definition of consent, WP187; A. F. WESTIN, *Privacy and Freedom*, in *Administrative Law Review*, 22, no. 1, 1969, pp. 101-106; J. KANG, *Information Privacy in Cyberspace Transactions*, in *Stanford Law Review*, 50, n. 4, 2004, pp. 1193-1294.

[20] Charter of Fundamental Rights of the European Union, in OJ C326/391.

[21] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, in *Harvard Law Review*, 126, 2013, pp. 1880-1903; S. BAROCAS, H. NISSENBAUM, *Computing Ethics: Big Data's End Run Around Procedural Privacy Protection*, in *Communications of the ACM*, 57, n. 11, 2014, pp. 31-33; E. BIETTI, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, in *Pace Law Review*, 40, n. 1, 2020, pp. 314-396; S. SPIEKERMANN, J. GROSSKLAGS, B. BERENDT, *E-privacy in 2nd generation E-commerce: Privacy Preferences versus Actual Behaviour*, in *EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce*, 2001, pp. 38-47.

[22] E. EDENBERG, M. L. JONES, *Analyzing the legal roots and moral core of digital content*, in *New Media & Society*, 21, n. 8, 2019, pp. 1804-1823.

[23] E. BIETTI, Consent as a Free Pass, cit. p. 317; R. BROWNSWORD, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in S. GUTWIRTH, Y. POULLET, P. HERT, C. TERWANGNE, S. NOUWT (edited by), *Reinventing Data Protection?* New York, Springer, 2009, pp. 83-110.

[24] J. RAZ, *The Morality of Freedom*, Oxford, Oxford University Press, 1988, p. 81; J. KLEINIG, *The Nature of Consent*, in F. MILLER, A. WERTHEIMER (edited by), *The Ethics of Consent: Theory and Practice*, Oxford, Oxford University Press, 2009, pp. 3-24; B. KOOPS, M. GALIČ, *Unity in Privacy Diversity: A Kaleidoscopic View of Privacy Definitions*, in *South Carolina Law Review*, 73, no. 2, pp. 1-36.

[25] T. L. BEAUCHAMP, *Autonomy and Consent*, in F. MILLER, A. WERTHEIMER (edited by), *The Ethics of Consent: Theory and Practice*, Oxford, Oxford University Press, 2009, pp. 55-78.

However, in line with the European court of justice's (ECJ) recent ruling on the dimension of privacy, the data subject's choice is not unambiguously reduced to the individual perspective, insofar as consent may also produce consequences on third parties[26]. In terms of digital platforms, the collective notion of consent can go as far as comprising those individuals with the same tastes and traits when they are targeted and profiled as well as on the user's close acquaintances, family, and friends through online and offline tracking[27].

Bearing in mind the consequences of consent both from an individual and collective perspective, the interpretation of the requirements set out by the GDPR regarding its validity is not near to being uncontested in the realm of data protection[28]. In this sense, the functioning of digital markets regarding the collection and processing of personal data has posed major concerns in terms of the underlying reasons and contexts in which end users render their consent for allowing data controllers/processors to process their personal data.

2.2 The Circularity of Consent Before Power Imbalances

The requirements set out by the GDPR to consider consent as a legal basis to justify the processing of personal data could seem quite straightforward. If they are met, consent will play a role in the context of the data controller's business model when retrieving personal data from data subjects. However, the same mechanics and interpretation should not be applicable when there is an imbalance in power between the end user and the data controller[29]. For instance, in the setting where the data subject must register with a service online to access it and, by doing so, she must also agree to the terms and conditions as well as to the privacy policy of the digital platform.

Against this background, the Article 29 Working Party has agreed throughout its Opinions and Guidelines that data subjects are particularly vulnerable in these scenarios[30].

[26] Court of Justice, 1 August 2022, C-184/20, *Vyriausioji tarnybinės etikos komisija*.

[27] E. BIETTI, *Consent as a Free Pass*, cit. p. 323; D. CVRCEK, M. KUMPOST, V. MATYAS, G. DANEZIS, *A study on the value of location privacy*, in *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, 2006, pp. 109-118.

[28] S. KOKOLAKIS, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon,* in *Computers & Security*, 64, C, 2017, pp. 122-134.

[29] S. LUKES, *Power: A Radical View*, London, Palgrave Macmillan, 2004.

[30] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014)*, https/www.ec.europa.eu/justice (accessed 15

End users are not at will to easily consent or oppose the processing of their personal data entirely[31]. As opposed to the narrow view of consent, vulnerability is considered contextual in nature. As such, the imbalance between the position of the data subject with regard to the data controller must be assessed in light of the effect of the actual processing on particular individuals[32]. In a similar sense, the GDPR is also especially focused on the impact of processing before the exercise of fundamental rights and freedoms[33]. Therefore, the power imbalance justifies the data subject's classification as a vulnerable person, whereas vulnerability is addressed through the capacity of exploiting that same imbalance.

This analysis of the imbalance between the two parties can be performed both during the processing of data as well as regarding the results produced through processing. In this sense, the power imbalance can have an early repercussion on the end user because she may be vulnerable to granting consent to particular processing activities she may not understand or perceive as entirely harmful due to information asymmetries caused by a lack of transparency and opacity[34]. Data protection authorities have tried to perfect consent in this same sense, by sanctioning those scenarios where digital platforms fail to comply with their transparency obligations as well as when interpreting the requirements of information, specificity, and unambiguous consent under the GDPR[35]. In addition, the end user may also be vulnerable when an outcome is produced through processing of her personal data, i.e., through price discrimination[36].

Theoretically, the GDPR and privacy protection should act in contrast to the existing power imbalance between the data subject and the data controller. At least, this idea has been proposed along the lines of the scholarly debate on power imbalances in the data

November 2022); Article 29 Data Protection Working Party, 4 April 2017, 17/EN, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, WP 248 rev.01.

[31] G. MALGIERI, A. DAVOLA, *Data-Powerful*, https/www.papers.ssrn.com (accessed 13 November 2022).

[32] Article 29 Data Protection Working Party, 2 April 2013, 00569/13/EN, Opinion 03/2013 on purpose limitation, WP 203; Article 29 Data Protection Working Party, 29 November 2017, 17/EN, Guidelines on transparency under Regulation 2016/679, WP260 rev.01.

[33] *GDPR*, Article 1(2) and Recitals 2-4.

[34] P. BLUME, *The Data Subject*, in *European Data Protection Law Review*, 1, n. 4, 2015, pp. 258-264; P. DE HERT, S. GUTWIRTH, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in E. CLAES, A. DUFF, S. GUTWIRTH (edited by), *Privacy and the Criminal Law*, Brussels, Intersentia, 2006.

[35] Commission Nationale Informatique & Libertés, 21 January 2019, SAN-2019-001, *Délibération de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.*

[36] N. NEWMAN, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, in *William Mitchell Law Review*, 40, no. 2, 2013, pp. 1-54.

protection context[37].

Nonetheless, the presence of power imbalances in the relationship between the data controller and the data subject and the vulnerability of the end user is framed according to a circular argument: vulnerability is defined in terms of the presence of power imbalance, whereas the power imbalance is defined as the data controller's capacity to exploit the data subject's vulnerability[38]. In terms of valid consent, the circularity of this interplay between vulnerability and power imbalances also does impact the interpretation of its requirements, insofar as it adds to the precondition of the exercise of control. Although Recital 43 of the GDPR establishes some of the key aspects where the granting of consent is not valid because it has not been freely given, data protection authorities have had to overcome the complexity of defining power imbalances in the field of data protection[39].

3. Effective Consent in the Field of Competition Law

The circularity of consent when end users are in the context of digital dominant platforms triggers a complex discussion on vulnerability, control, and power imbalances, which cannot only be addressed through the instruments and interpretation of the GDPR. Due to this reason, some NCAs have enforced competition law to accommodate the notion of market power into the balancing of legitimate interests which will result in a finding that there is an imbalance between the data subject and the data controller[40]. However, the result of a sanctioning proceeding in the area of antitrust will not (or should not) produce a result in terms of understanding whether the GDPR was infringed or not. Instead, it will produce the outcome that Eu and/or national competition law was infringed, to the detriment of the structure of competition and the detriment of consumers at large.

Moreover, NCAs must overcome another distinct but relevant hurdle when considering

[37] D. J. SOLOVE, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, in *Stanford Law Review*, 53, n. 6, 2001, pp. 1393-1462; J. COHEN, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, New Haven, Yale University Press, 2012; L. AUSTIN, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, in A. SAURAT (edited by), *A World without Privacy: What Law Can and Should do?*, Cambridge, Cambridge University Press, 2014; R. CALO, *Privacy, Vulnerability and Affordance*, in *DePaul Law Review*, 66, 2017, pp. 591-604.
[38] G. MALGIERI, A. DAVOLA, *Data-Powerful*, cit. p. 7.
[39] E. BIETTI, *Consent as a Free Pass*, cit. p. 339.
[40] G. MALGIERI, A. DAVOLA, *Data-Powerful*, cit. p. 9; B.J. KOOPS, *The Trouble with European Data Protection Law*, in *International Data Privacy Law*, 4, n. 4, 2014, pp. 250-261; M. WASASTJERNA, *Competition, Data and Privacy in the Digital Economy*, Alphen aan den Rijn, Kluwer Law International, 2020.

consent in the antitrust analysis: not every non-economic interest can and should be captured under competition law, namely data protection concerns[41]. Even if they do, the most plausible approach is to analyse privacy in economic terms, to the extent that this is possible. Economists have voiced their concern about assigning a value to privacy, insofar as it is subjective and idiosyncratic as well as an elusive concept in terms of behavioural dynamics from the perspective of the individual[42].

On top of that, the regulation of privacy in the GDPR does not confer a property right upon the individual over her personal data, but rather the control over that same data. The granting of the end user's consent entails an expression of the passing on of control to the controller/processor based on a legitimate basis under Article 6(1)(a) GDPR, rather than a legitimate interference with a property right as provided by law. Therefore, the economic and legal exercise to draw a line between the abuse of a dominant digital platform with the end user's lack of control over her personal data is a difficult one to delineate[43].

Notwithstanding the challenges, some NCAs have tried to infer an abuse of a dominant position under their national competition law regimes from an infringement of the GDPR, namely due to the existing power imbalances between the end user and the data processor/controller when the former consents to the processing of her personal data

[41] R.A. POSNER, *The Economics of Privacy*, in *Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association*, 71, n. 2, 1981, pp. 405-409; O. BROOK, *Non-Competition Interests in EU Antitrust Law*, Cambridge, Cambridge University Press, pp. 1-33; E. BIETTI, *Consent as a Free Pass*, cit. pp. 351-353; G.A. MANNE, R.B. SPERRY, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, in *Competition Policy International Antitrust Chronicle*, 2, 2015, pp. 5-6; D.D. SOKOL, R.E. COMERFORD, *Antitrust and Regulating Big Data*, in *George Mason Law Review*, 23, no. 5, 2016, pp. 1156-1161. In terms of Eu case law and decision-making, Court of Justice, 23 November 2006, C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios BaNCAsrios (Ausbanc)*, in *ECR*, 2006, I-11125, para 63; European Commission, 3 October 2014, Case No COMP/M.7217, *FACEBOOK/WHATSAP*, in *C(2014)7239 final*.

[42] A. ACQUISITI, C. R. TAYLOR, L. WAGMAN, *The Economics of Privacy*, in *Journal of Economic Literature*, 54, n. 2, 2016, pp. 442-492; J. WHITTINGTON, C.J. HOOFNAGLE, *Unpacking Privacy's Price*, in *North Carolina Law Review*, 90, 2012, pp. 1327-1368; B. A. HUBERMAN, E. ADAR, L.R. FINE, *Valuating Privacy*, in *IEEE Security and Privacy*, 3, no. 5, 2005, pp. 22-25; K.J. STRANDBURG, *Free Fall: The Online Market's Consumer Preference Disconnect*, in *The University of Chicago Legal Forum*, 2013, pp. 95-172; J. HAUCAP, *Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in light of the German Facebook Decision*, in CPI Team (edited by), *The Digital Economy – 2019*, Competition Policy International, 2019, pp. 57-61; T. KÖRBER, *Is Knowledge (Market) Power? – On the Relationship Between Data Protection, 'Data Power' and Competition Law*, https//www.papers.ssrn.com (accessed 27 November 2022); J. FARRELL, *Can Privacy Be Just Another Good?*, in *Journal on Telecommunications and High Technology Law*, 10, 2012, pp. 251-265.

[43] B. HERMALIN, M. KATZ, *Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy*, in *Quantitative Marketing and Economics*, 4, no. 3, 2006, pp. 209-239; L.H. SCHOLZ, *Privacy as Quasi-Property*, in *Iowa Law Review*, 101, 2016, pp. 1113-1141; J. DREXL, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in *Max Planck Institute for Innovation and Competition Research Paper*, no. 18-23, https/www.papers.ssrn.com (accessed 28 November 2022).

online.

3.1 The German Approach: An Invalid Consent Equals Abuse (and vice versa?)

The Federal Cartel Office[44] (FCO) was the first instigator in promoting the idea that an informed reading of the GDPR and its principles was necessary to establish whether a dominant digital platform had abused its position with detriment to users in the form of an exploitative abuse as far as the processing of personal data is concerned[45]. Without prejudice to the quasi-constitutional balancing which the Bundeskartellamt performed when assessing the GDPR principles to find an abuse under Section 19(1) GWB[46] and the reasonableness of Facebook's terms and conditions and privacy policy under Section 307 of the German Civil Code[47], the FCO aligns the legal interests of the GDPR in connection with the capacity of the end users of the digital platform (Facebook) to consent.

3.1.1 The Causality Between Effective Consent and Market Power

In the decision's terms, the infringement of data protection rules is linked with Facebook's dominant position. First, the FCO thoroughly reviews Facebook's terms and conditions, namely the conditions applicable to the processing of the personal data of end users. By doing that, the German competition authority interprets Articles 6(1)(a) and 9(2)(a) of the GDPR and finds: i) that voluntary consent was not granted; ii) that no explicit consent was given regarding special data categories covered by Article 9(1) of

[44] The Federal Cartel Office and Bundeskartellamt are used throughout the text interchangeably to designate the German competition authority.
[45] M. BOTTA, K. WIEDEMANN, *Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision*, in *Journal of European Competition Law & Practice*, 10, no. 8, 2019, pp. 465-478; A. C. WITT, *Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case*, in *The Antitrust Bulletin*, 66, no. 2, 2021, pp. 276-307; V.H.S.E. ROBERTSON, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data*, in *Common Market Law Review, 57*, no. 1, 2020, pp. 161-189; F. STUTZMAN, R. GROSS, A. ACQUISITI, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, in *Journal of Privacy and Confidentiality*, 4, no. 2, 2013, pp. 7-41.
[46] FEDERAL MINISTRY OF JUSTICE, *Competition Act (Gesetz gegen Wettbewerbsbeschränkungen – GWB)*, https//www.gesetze.-im-internet.de (accessed 16 November 2022).
[47] FEDERAL MINISTRY OF JUSTICE, *German Civil Code (BGB)*, https//www.gesetze-im-internet.de (accessed 16 November 2022).

the GDPR, and iii) that the opting-out options provided for in Facebook's privacy settings did not constitute a form of voluntary consent[48]. The rest of the legal bases used by Facebook in its processing activities are also analysed in this same light[49]. After that, the Bundeskartellamt draws out the normative-causal connection between both areas: the infringements of the GDPR were strictly correlated with Facebook's market power[50]. The Bundeskartellamt added to that argument that there is also a causal relationship between unlawful data processing conditions and market dominance regarding the impediment effects of the terms of services and data privacy policies to the detriment of competitors[51].

In the particular case of consent, the Bundeskartellamt highlights the relevance of the lack of voluntary consent of Facebook's end users when registering into the social network, in light of the clear imbalance between these data subjects and the controller. Moreover, the FCO reads Recitals 42 and 43 of the GDPR as a relevant presumption applicable not only in the field of data protection but also for the case of antitrust. Thus, users had no genuine or free choice to refuse or withdraw consent without suffering any type of detriment to their positions vis-à-vis the provision of Facebook's services, i.e., they would have been hindered from using the service altogether if they had not agreed to the social network's terms and conditions. To wrap the argument up, the German competition authority even goes as far as saying that «in any event, the very fact that the company has a dominant position in the market means consent is not given voluntarily»[52]. In a similar vein, Facebook's market-dominating position also pre-empts the finding that not one of the legal bases put forward by the social network was admissible in the context of dominance[53].

Notwithstanding the close relationship between the imbalances in power and the effectiveness of consent, the Bundeskartellamt only infers their causal relationship through the lens of dominance, as measured from a narrow interpretation of Facebook's

[48] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, paras 639-665.
[49] B6-22/16, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, paras 668-870.
[50] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, paras 873, 876, 880 and 898; R. PODSZUN, *The Facebook Decision: First Thoughts by Podszun*, https//www.d-kart.de (accessed 26 November 2022).
[51] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 885.
[52] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, paras 644-646 and 877.
[53] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 878.

dominant position as designed through the previous exercise of a narrow market definition. In the broadest terms, the FCO only takes recourse to users' lack of choice on the level of data protection they wish on the social network and whether they would accept those same terms when accessing the service if they had that particular choice. Lack of choice is proven through a user survey showing they do not have an alternative to consent, and, in any case, they are unlikely to read the social network's privacy policy anyway. On top of that, strong lock-in effects based on incompatibility and identity-based network effects strengthen the authority's line of reasoning regarding a lack of alternatives on the user's side[54].

The appeal of the decision before the Higher Regional Court Düsseldorf triggered the addressing of a preliminary ruling to the ECJ in Case C-252/21 (*Meta Platforms v. Bundeskartellamt*[55]) which produced Advocate General (AG) Rantos' opinion on the circularity of these same arguments presented by the FCO[56]. AG Rantos believes that the competition authority can rely on the concepts of opt-in and lock-in (as well as dominance) to establish the elements which can be considered to establish whether consent was granted freely and effectively in terms of interpreting the GDPR. In this sense, the market power of the controller is equated to a clear imbalance between the digital platform and the end user[57]. In turn, compliance with the GDPR may also be considered incidentally in the broader analysis of the economic and legal context of the conduct regarding the abuse of a dominant position[58]. However, AG Rantos discards the presumption that an infringement of the GDPR's provisions and principles automatically implies an abuse of a dominant position based on the one-stop-shop principle under Articles 51 to 67 of the GDPR[59].

If the ECJ is to embrace this approach, the circularity of the argument regarding consent may well be even supported with further elements on top of the already existing complex and undefined concept of power imbalances, although the FCO's decision may be impinged concerning its key elements, i.e., the interaction and causality between the privacy infringements and competition law harms.

[54] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, paras 883 and 902.
[55] OBERLANDESGERICHT DÜSSELDORF (Germany), 22 April 2021, C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, http://curia.europa.eu (accessed 17 November 2022).
[56] Advocate General Rantos, 20 September 2022, C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*.
[57] AG Rantos, C-252/21, *Meta Platforms and Others*, para 75.
[58] AG Rantos, C-252/21, *Meta Platforms and Others*, paras 24-33.
[59] AG Rantos, C-252/21, *Meta Platforms and Others*, footnote 18.

3.1.2 The Quantification of Non-Competition Interests: Non-Material Damages as an Expression of Ineffective Consent

In line with Facebook's allegations, the Bundeskartellamt had to respond to whether the lack of an economic quantification of the abusive conduct is needed to demonstrate the conduct's actual or potential harm produced to users due to the unlawfulness of Facebook's personal data processing terms[60]. Pre-emptively, the competition authority highlights that an economic quantification of this type of abusive behaviour is hardly possible[61]. However, the FCO's findings do not quite go in line with this preliminary warning.

Instead, the Bundeskartellamt redirects the burden of demonstrating actual or potential user harm to material and non-material harms. On one hand, the conduct's economic quantification relies on the risk of data breaches, i.e., material financial harm may be adverted when Facebook discloses data to third parties which can, in turn, lead to practices such as identity theft, extortion or fraud[62]. On the other hand, users may also suffer non-material Damages due to the vast data pools which may be conformed with the information they deliver online based on the particular depth, scope, and quality of these pools as opposed to their subjective expectations when navigating online and accessing the social network[63]. In this sense, the FCO adopts a similar view towards user harm to GDPR liability under Article 82 when damages are claimed in the form of redress[64].

Unlike the decision's close approach to the interplay between ineffective consent and antitrust, the FCO diverts to reason that the end user's subjective perceptions and their lack of interest in reading privacy policies are relevant to account for a tangible economic quantification of the conduct. Interestingly, these two elements distance the quantification

[60] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 906.
[61] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 908.
[62] K. KEMP, *Concealed data practices and competition law…*, cit. pp. 644-647.
[63] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 910; L.K. JOHN, *Uninformed Consent*, https//www.hbr.org (accessed 27 November 2022).
[64] L. HORNKOHL, *A Guide on Civil Liability for Data Protection Violations: Non-material Damages (and more)*, https/www.eulawlive.com (accessed 26 November 2022); A.M. MCDONALD, L.F. CRANOR, *The Cost of Reading Privacy Policies*, in *Journal of Law and Policy for the Information Society*, 4, no. 3, 2008, pp. 543-568; WHITTINGTON, C.J. HOOFNAGLE, *Unpacking Privacy's Price*, cit. pp. 1359-1360; G. HULL, *Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data*, in *Ethics and Information Technology*, 17, 2015, p. 91.

of abusive behaviour from a possibility to a chimaera.

In any case, the Bundeskartellamt rounds up the argument by saying that welfare effects (in the form of net consumer benefits in favour of the end users produced by Facebook's services) may not counter the «harm» produced by the infringement of privacy protection, insofar as economic assets are not in play, but fundamental rights of freedom related to the end user's willingness to disclose personal data are concerned, instead[65].

3.2 The Italian Approach: The Consumer Protection Perspective

The Autorità garante della concorrenza e del mercato (AGCM) adopted twin decisions based on Apple's and Google's unlawful personal data processing concerning the registration into their services[66]. Similar to the German decision, the Italian competition authority relied on its consumer protection mandate to issue a decision protecting consumer self-determination and freedom of choice[67]. The decisions interpreted the digital platforms' processing terms in light of Articles 24 and 25 of the Italian Consumer Code[68], corresponding with Articles 8 and 9 of the Unfair Commercial Practices Directive.

The Italian competition authority found that Google's registration into a Google account (and, therefore a Google ID) to access the rest of Google's services as well as Apple's process compelling end users to create an Apple ID, if they were willing to access the Apple Store and other Apple-related services, constituted a misleading commercial practice.

Following the spirit of Article 8 of the Unfair Commercial Practices Directive, the AGCM held that when end users registered into their services did not have any other choice but to assume and consent to the commercial conditions imposed by both digital firms regarding the processing of their personal data. On one hand, the terms and conditions as well as the privacy policy were imposed on the users when they registered, given that

[65] B6-22/16, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, para 913.
[66] Italian Competition Authority, PS11147 – *Google Drive-Sweep 2017*, order. n.29890, 29 November 2021, in Bulletin no. 47/2021 p. 196; Italian Competition Authority, PS11150 - *iCloud*, order. n.29888, 29 November 2021, in Bulletin no. 47/2021 p. 153.
[67] M. BOTTA, K. WIEDEMANN, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, in *Antitrust Bulletin*, 64, no.3, 2019, pp. 428-446.
[68] NORMATTIVA, Legislative Decree No. 206/2005 concerning Consumer Code under Art. 7 Law 229/2003, https//www.normattiva.it (accessed 17 November 2022).

consent could only be withdrawn once the user was registered -and her personal data was already stored and combined with the rest of Google's and Apple's services-, in line with an opt-out system. On the other hand, contrary to the GDPR's provisions, the registration systems pre-selected the options which favoured the intensive processing and use of personal data. For instance, in the case of Apple, when the data subject was accessing the ecosystem, the registration system pre-selected the boxes concerning marketing activities via email to be performed through the combination of the data subjects' device identifier and the rest of the personal data processed within the device[69].

Both factors contributed to the finding that end users were not able to express their consent in a free and specific manner to enable the processing of their personal data[70]. Similar to the case of the Bundeskartellamt, the AGCM did not address in detail the particular power imbalances between the platforms and the data subjects. Instead, it preferred to outline throughout the twin decisions that the digital platforms' power relied on the lack of equally attractive alternatives in the market and the lock-in effects suffered by end users thereof[71].

Although the chosen legal instrument by the AGCM to pursue the conduct was its national consumer protection regime, the decisions pose two main questions in terms of antitrust. First, should a firm -digital or else- be subject to opening up the market, if it is not integrated into a regulated market, even if it has dedicated its efforts and long-run investments into building up its ecosystem. And second, is a competition authority -even if it is acting upon its consumer protection mandate- legitimised to instrumentalise the lack of equally attractive alternatives in the market against the undertaking. The DMA has answered both of these questions in the affirmative, by transforming the digital sector into a quasi-regulated market where contestability and fairness should be addressed *ex-ante* regarding particular economic operators[72].

3.3 An Unreliable Meter for the Unlawfulness of Consent

The Italian and German competition authorities have been some of the few to address the unlawfulness of consent from the perspective of a national competition authority when

[69] PS11150, *Apple*, para 91.
[70] PS11147, *Google*, para 76; PS11150, *Apple*, paras 88-90.
[71] G. MALGIERI, A. DAVOLA, *Data-Powerful*, cit. p. 9.
[72] M. RHOEN, *Big Data and Consumer Participation in Privacy Contracts: Deciding Who Decides on Privacy*, in *Utrecht Journal of International and European Law*, 31, n. 80, pp. 51-71.

applying competition law. However, their analysis demonstrates that the balancing of consent through the lens of the business models of the dominant digital platforms will always produce an unfavourable outcome against them, by rendering the unlawfulness of their privacy policies, which is later paired up with a declaration of the existence of an abuse of a dominant position.

If we take the *FCO v. Facebook* case, circularity is not only present when interpreting the provisions of the GDPR but also when navigating its particular impact on end users. The unlawfulness of Facebook's data processing terms and conditions stemmed from the lack of voluntary consent in the hands of the data subjects, in line with the authority's constructed presumption set out from Recitals 42 and 43 of the GDPR. Therefore, consent is pre-empted invalid in the context of dominance due to the lack of choice and lock-in effects suffered by the end users. There will not be a rebuttable argument to counteract this first step of the analysis: the conduct is unlawful due to dominance in terms of the GDPR, and in the realm of the GDPR there is no further balancing in terms of the potential efficiencies produced by the conduct. Whether the processing of personal data is lawful or unlawful, there is no middle ground on that. In any case, the necessity of the processing could only be assessed in light of the legal basis set out in Article 6(1)(f) of the GDPR, whereas when analysing Article 6(1)(a) of the GDPR the same analysis does not apply.

In turn, these same elements are operationalised by the German competition authority into the analysis of the abusiveness of the conduct standing from an exogenous perspective. Given that the presumption is applicable, then the rest of the legal requirements cascade and transform into an abuse in terms of competition law. By this token, the presumption asserts the existence of an imbalance in power between the data subject and controller, negating control of personal data and arising in the form of the data subject's vulnerability. Thus, all of the legal requirements set out in the GDPR go hand in hand to find the existence of an abuse of a dominant position from the perspective of the German competition law regime. In this same vein, the Italian competition authority does not resolve the conundrum either. Instead, the AGCM adds on the condition of both Apple's and Google's terms and conditions upon registration as an opt-out system as a presumption linked to the aggressiveness of the conduct, in terms of the consumer protection viewpoint.

4. Articles 5(2) and 6(10) in the DMA: The Overriding Effective Consent of the End User

The DMA will be applicable starting from March 2024, and it incorporates the already-existing circularity of consent into its framework. In the words of the DMA, the GDPR's provisions must apply «without prejudice» to the provisions of the regulatory instrument. Thus, the incorporation of the GDPR's notion of consent in Articles 5(2) and 6(10) brings with it the complexity to strike a balance between an analysis of unlawfulness as opposed to an analysis of abusiveness stemming from undefined power imbalances. Within this context, the paper addresses the question of whether the GDPR is implicitly placed in superior standing as opposed to the DMA or vice versa as well as whether the introduction of Article 6(1)(a) of the GDPR into the DMA's text adds any support to the difficult task of ensuring the compliance of the regulatory instrument[73].

4.1 What is the Relationship Between the DMA and the GDPR?

The DMA and the GDPR are provisions of secondary law, as opposed to antitrust, which derives from primary law, namely Articles 101 and 102 TFEU. To the extent that the DMA and the GDPR have adopted the form of a regulation, they are directly applicable in the Member States, regardless of the existing hierarchy between secondary and primary law. However, the recent developments in Eu law seem to indicate otherwise.

The authorities which will enforce these provisions might overlap in some instances. The European Commission is the sole authority empowered to enforce the DMA (although, in practice, a dedicated taskforce will assume those powers[74])[75], whereas it is also the enforcer of Articles 101 and 102 TFEU at the Eu level, alongside NCAs, under the powers vested by Regulation 1/2003[76]. Aside from these fields of law, the GDPR's enforcement relies on Data Protection Authorities (DPAs) at the national level where each Member State will provide for one or more independent public authorities to monitor the application of its provisions[77].

---

[73] IRISH COUNCIL FOR CIVIL LIBERTIES, *Meta's internal use of data and the DMA*, https//www.iccl.ie (accessed 22 November 2022).
[74] F. YUN CHEE, *EU wants 40-man antitrust team to enforce new tech rules, official says*, https//www.reuters.com (accessed 22 November 2022).
[75] *DMA*, Recital 91 and Articles 20-32.
[76] Council, 16 December 2002, 1/2003, Regulation on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty in OJ L1/1.
[77] *GDPR*, Article 51.

4.2 Competition law v. DMA/GDPR

In terms of the interaction between antitrust and any regulatory framework, the ECJ has confirmed that the scope of Article 102 TFEU cannot be restricted by its existence, i.e., a restriction imposed under the regulation on electronic communications[78]. This same reasoning applies to the regulatory framework presented by the DMA and the GDPR. Thus, their provisions must not restrict the scope of Article 102 TFEU, regardless of the fact that it is still unclear whether the GDPR and the DMA may add some nuance to the reading and interpretation of Article 102 TFEU, without necessarily restricting its scope. In this sense, it could well be admissible that the gaps left for enforcement in digital markets could be filled up with rules belonging to the GDPR and the DMA. In line with the paper's previous discussion, these gaps arise regarding digital platforms' data processing policies and their interpretation in light of their lawfulness[79].

However, the recent ECJ ruling on *DB Station* questions this straightforward assumption in the field of railway regulation, namely Directive 2001/14[80]. The preliminary ruling is based on the claimant's capacity to receive compensation for harm derived from an infringement in the scope of the railway infrastructure regulation where Article 102 TFEU was also invoked by the claimant. The ECJ stated that the German national regulatory authority could directly apply Article 102 TFEU due to its exclusive competence to hear and determine any dispute falling within Directive 2001/14[81]. The Court extended the regulatory authority's competence onto antitrust without any legal basis, whilst restricting its scope[82].

As opposed to Advocate General Ćapeta's Opinion on the case[83], the ECJ held that the exclusive competence of the regulatory body was based on the technical constraints specific to the railway sector. According to the definition of Directive 2001/04, railway infrastructure is deemed as a natural monopoly and, as such, the incumbent must be

[78] Court of Justice, 27 March 2012, C-209/10, *Post Danmark A/S v Konkurrencerådet*, para 25; Court of Justice, 10 July 2014, C-295/12, *Telefónica SA and Telefónica de España SAU v European Commission*, para 128; Court of Justice, 6 September 2017, C-413/14, *Intel Corp. v European Commission*, para 136.
[79] Advocate General Kokott, 13 October 2022, C-449/21, *Towercast*, paras 2 and 44.
[80] European Parliament and Council, 26 February 2001, 2001/14/EC, Directive on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification, in OJ L75/29.
[81] *DB Station & Service*, para 74.
[82] M. SOUSA FERRO, *Op-Ed: "DB Station (C-721/20): What have they done to EU Law?" by Miguel Sousa Ferro*, https//www.eulawlive.com (accessed 22 November 2022).
[83] Advocate General Ćapeta, 7 April 2022, C-721/20, *DB Station & Service*, paras 24 and 63.

regarded as in a dominant position concerning railway undertakings. Therefore, those powers enable the regulatory body to meet the technical requirements of the railway infrastructure[84]. By this same token, to ensure non-discriminatory access under fair conditions of competition to the railway infrastructure, the regulatory body must be able to take into account the competitive situation of rail transport. In this sense, the ECJ highlights that, if a claim is brought to the regulatory body's attention where the infringement of Article 102 TFEU is also invoked, the regulatory body's decision to dismiss the claim based on a lack of competence would run counter to the objectives of the regulation[85]. This same reasoning would also apply even when the regulatory body would act in its own motion, when necessary[86].

Based on this finding, the ECJ then establishes that to ensure the full effectiveness of Article 102 TFEU, national courts may apply competition law concurrently to the regulatory body's own application of the prohibition of abuse but will have to consider (and even wait for) the latter's analysis on the lawfulness of the conduct as a relevant element when assessing the abusive conduct. In the Court's own words, however, these requirements will not apply when the discussion is centred on the parallel application of Article 102 TFEU via the European Commission and a regulatory body. The Court highlights that the Commission's intervention «does not present a risk of several, potentially divergent, decisions»[87]. Thus, descending the dichotomy to the interaction between antitrust and the DMA, a divergent interpretation of the same concepts even if they pursue distinct objectives is not preoccupying for the full effectiveness of Article 102 TFEU insofar as both regimes will be enforced from the realm of the Commission. The same would not apply to the interaction between antitrust and the GDPR, nor between the enforcement and interpretation of the DMA and GDPR provisions, given that their interaction takes place outside of the competence of the European Commission.

If we strictly attend to the *DB Station* ruling, a regulatory framework based on technical and specific requirements which tends to ensure competitive conditions could well interfere with the scope of Article 102 TFEU. However, interference may not always equal a restriction of the scope of Article 102 TFEU, it may also mean that the prohibition may be informed and supplemented through the legal intricacies of a specific regulatory

[84] *DB Station & Service*, paras 57-58 and 61.
[85] *DB Station & Service*, paras 68, 69, 72 and 74.
[86] *DB Station & Service*, para 65.
[87] *DB Station & Service*, para 33.

legal background[88].

Up until this moment, the ECJ has found that a restriction of the scope of Article 102 TFEU occurs when unlawfulness from the sectoral regulation is translated into the finding of abusiveness of a dominant position. In other words, the ECJ has not admitted that *prima facie* unlawfulness of an anticompetitive conduct may be drawn out from the finding of an infringement of sectoral regulation in a prior proceeding held by the regulatory body within its competence and powers. Instead, throughout its preliminary rulings and judgements, the Court has incorporated the interaction between regulation and competition into the broader context in which the particular practice has been implemented, i.e., into the legal and economic context of the conduct[89]. In the particular case of the intersection between privacy and competition, AG Rantos also proposes to divert the discussion to the «all things considered» analysis[90].

4.3 DMA v. GDPR

The DMA is not aimed to repeal the provisions of the GDPR or any other Union act of law. That's the reason behind the fact that the DMA's provisions apply «without prejudice» to the GDPR. From a hierarchical perspective, both instruments are secondary laws and should not enter into direct conflict when they are applied. As opposed to the dichotomy between the DMA and antitrust, the GDPR and DMA are not complementary to each other, but they run parallel courses of action throughout the regulation of digital markets regarding business models and the data that is produced within them. In principle, the DMA's provisions and compliance cannot interfere with the GDPR's concepts and interpretation, and the same applies to the GDPR.

However, the DMA incorporates the GDPR's concepts –namely consent- into the provisions which will be applicable for gatekeepers in the form of legal exceptions to their application. In this sense, the public policy concerns that the DMA wants to address are overridden by the public policy concerns that the GDPR wants to pursue, i.e., the

[88] Court of Justice, 14 March 2013, C-32/11, *Allianz Hungária Biztosító Zrt. and Others v Gazdasági Versenyhivatal* (*Allianz Hungary)*, paras 47-51.
[89] Court of Justice, 6 December 2012, C/457/10, *AstraZeneca AB and AstraZeneca plc v European Commission*, paras 105-113; Court of Justice, C-32/11, *Allianz Hungary*, paras 46-48; Court of Justice, 30 January 2020, C-307/18, *Generics (UK) Ltd and Others v Competition and Markets Authority*, paras 87-90.
[90] AG Rantos, C-252/21, *Meta Platforms and Others*, para 23.

protection of privacy[91].

4.3.1 Article 5(2) DMA of the DMA: A Low-Intensity Ban on the Combination, Cross-Use and Processing of Personal Data

Going back to the idea of how consent has been interpreted across different fields of law, Article 5(2) of the DMA establishes the self-executing obligation to prohibit any combining, processing, and cross-using of personal data of end users the gatekeeper holds with the data it processes from third-party services or other of its services integrated into its ecosystem. The provision draws out its inspiration from the *FCO v. Facebook* case that presumed an abuse in light of imbalances of power between the end users and the data controller.

Unlike the strategy that digital platforms such as Google and Apple are attempting to introduce to differentiate between first-party data and third-party data[92], the DMA presumes that data produced from one of the designated gatekeepers should not be used outside of those same services and onto differentiated core platform services of its own, in line with the purpose limitation principle introduced by the GDPR. In this regard, the efforts of digital firms to differentiate between the data they produce, infer, and observe in their ecosystems as opposed to the data they may obtain through data brokers or third-party websites, apps and environments, are completely disregarded. Instead of protecting the generation of first-party data within the same ecosystem, the DMA bars the combination, processing, and cross-use of an end user's personal data even when two separate services from the same gatekeeper are provided based on the same dataset[93].

However, the prohibition will not apply when the end user has been presented with the specific choice and has given consent to the processing, combination and cross-use within the meaning of the GDPR, namely Articles 4(11) and 7. On top of that, the prohibition applies without prejudice to the possibility of justifying the conduct under the legal bases set out in Article 6(1), points (c) to (e). In this sense, the DMA disregards the rest of the

[91] *DMA*, Recital 35.
[92] THE PRIVACY SANDBOX, *Protecting your privacy online*, https//www.privacysandbox.com (accessed 26 November 2022); APPLE DEVELOPER, *Upcoming AppTrackingTransparency requirements*, https//www.developer.apple.com (accessed 26 November 2022).
[93] I.D. MITCHELL, *Third-Party Tracking Cookies and Data Privacy*, 2012, https//www.papers.ssrn.com (accessed 28 November 2022); N. ECONOMIDES, I. LIANOS, *Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective*, in *Journal of Competition, Law and Economics*, 17, no. 4, 2021, pp. 765-847.

legal bases provided for in Article 6(1) as a clear expression of its normative preference regarding the position of the designated gatekeepers[94]. Even though the end user consents or not to override the prohibition, the gatekeeper's services must remain untouched in terms of quality, unless the processing of data is a direct consequence of an increase in the quality of the service provided[95].

4.3.2 Article 6(10) of the DMA: The Other Side of the Coin

Consent is interpreted inversely when establishing positive obligations in favour of business users and third parties engaging in competition with the gatekeeper regarding the provision of aggregated and non-aggregated data in the context of their interaction within the gatekeeper's ecosystem, including personal data. End users are not handed over the capacity to curtail the effectiveness of the obligation altogether, but they can decide which personal data they want other business users to use - as opposed to the data the gatekeeper holds in the capacity of the ecosystem holder - through an opt-in system, regardless of the fact that status quo biases may counsel otherwise and act in favour of the gatekeepers in any case[96].

The interpretation of effective consent in the context of Article 6(10) of the DMA should also follow the meaning of the GDPR, irrespective of the fact that the DMA already places opt-in systems as a preferable choice architecture for granting consent online as opposed to opt-out systems, which were also thoroughly analysed in the *FCO v. Facebook* case. In this regard, free choice, and effective consent in the terms of the GDPR are tied up to the idea that only opt-in systems can produce effective consent, whereas significantly higher costs are placed on consumers through this normative preference[97]. As opposed to the overriding effect of the GDPR on the force of Article 5(2) of the DMA, Article 6(10) of the DMA complements the public policy concerns pursued by the regulatory

[94] D. GERADIN, K. BANIA, T. KARANIKIOTI, *The interplay between the Digital Markets Act and the General Data Protection Regulation*, https//www.papers.ssrn.com (accessed 2 October 2022).
[95] *DMA*, Recital 37; S. ESAYAS, *Privacy-As-A-Quality Parameter: Some Reflections on the Scepticism*, in *Stockholm University Research Paper*, no. 43, 2017, https//www.papers.ssrn.com (accessed 28 November 2022).
[96] R. GRADWOHL, *Privacy in Implementation*, in *Social Choice and Welfare*, 50, n. 3, 2018, pp. 547-580; D. L. RUBINFELD, M. S. GAL, *Access Barriers to Big Data*, in *Arizona Law Review*, 59, 2017, pp. 339-381; J. CAMPBELL, A. GOLDFARB, C. TUCKER, *Privacy Regulation and Market Structure*, in *Journal of Economics & Management Strategy*, 24, no. 1, 2015, pp. 47-73.
[97] F. CATE, M. E. STATEN, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"*, https//home.uchicAGo.edu (accessed 25 November 2022); E.J. JOHNSON, S. BELLMAN, G.L. LOHSE, *Defaults, Framing and Privacy: Why Opting In-Opting Out*, in *Marketing Letters*, 13, no.1, 2002, pp. 5-15.

instrument aimed at gatekeepers with a particular - and exclusively admissible - architecture choice in mind, which will have to be implemented by design[98].

5. Overall Examination of the Circularity of Consent in the DMA

Stemming from the fact that consent and its interplay with free choice are not yet well delineated in the field of privacy protection, especially in the context of dominant players, its interpretation within the DMA's scope will also render to be a difficult task. As far as the GDPR is concerned, stating the criteria where freely given, specific, informed, and unambiguous consent where the data subject suffers from the specific vulnerability regarding power imbalances with the data controller/processor is a hard task at hand. The elements of vulnerability and power imbalances are defined circularly: vulnerability is explained through the presence of power imbalances, whereas power imbalances are defined by the exploitation of a vulnerability.

However, the circularity of the argument does not stop there. In the field of antitrust, vulnerabilities have been directly identified with the existence of power imbalances. In turn, power imbalances are defined according to the existing competitive conditions and dominant position of the undertaking which generates the possibility of bargaining powers to start in the first place. By this token, a presumption has been drawn out from the existence of dominance to the finding that, in the context of dominance, end users cannot consent according to the GDPR's requirements.

Regarding the enforcement of the DMA's provisions, the GDPR's interpretation in the field of privacy protection is factored into the compliance by design imposed on gatekeepers, although the prohibition of Article 5(2) precisely originates in this same circular understanding. Nonetheless, the prohibition may be overridden through the obtention of the end user's consent in the equivocal terms of the GDPR, which render the starting point and the exemption of the prohibition as based under the same assumption: either processing, combining and cross-using personal data is per se prohibited under the DMA or the burden of proof to show that end users can choose freely is placed at a disproportionately high threshold. In the context of Article 5(2), the prohibition is not unapplied when consent is granted effectively - even if the gatekeeper manages to prove it -, given that the gatekeeper's behaviour will still fall in the scope of the DMA.

[98] *DMA*, Recital 65.

Moreover, the anti-circumvention obligation under Article 13(4) of the DMA rounds the argument up elevating the regulatory instrument to a catch-it-all tool where any attempt of the designated gatekeeper to ensure that end users may consent to their activities may undermine the prohibition's effective compliance[99].

Although the DMA initially considers applying the GDPR on its terms, the circularity of the argument in the field of privacy protection displaced to the regulatory instrument makes it extremely difficult to make that possible. The DMA's normative technique only adds to the already existing complexity of the interpretation of consent in the digital context, which is yet awaiting a response in terms of a unified approach towards power imbalances.

In this sense, Article 6(10) of the DMA hints at a possible solution, in light of similar efforts from NCAs which have proposed the same solution to this conundrum: if the choice architecture is designed as an opt-in, power imbalances may be alleviated and data subjects may be free-er to decide on whether they wish to have their personal data processed, collected and cross-used by the designated gatekeeper or by third parties. Even in this case, power imbalances are not defined regarding end users, but regarding business users in the form of the existing bargaining power between competitors leading to unfair practices and conditions imposed on them[100]. In the abstract, the objective of unfairness is tied to the «detriment of prices, quality, fair competition, choice and innovation in the digital sector» which end users may suffer[101]. According to the DMA, imbalances in power between the data subject and the data controller must be interpreted in light of a potential detriment to these parameters of competition, irrespective of its *ex-ante* and efficiency-adverse approach. No further detail is rendered about the dimension and scope that these effects must potentially project in the digital arena to become relevant from the regulatory perspective. It is also unclear whether a detriment in these parameters of competition will always be interpreted in terms of a decrease[102].

All things considered, the paper has shown how the DMA does not apply «without prejudice» to the provisions of the GDPR, namely the notion of consent. Instead, the

---

[99] O. ANDRIYCHUK, *The Digital Markets Act: A Comparative Analysis of the Main Normative Theories*, in Digital Legal Talks, 2022.

[100] *DMA*, Recitals 4, 33 and 62.

[101] *DMA*, Recital 4.

[102] D. LYPALO, *Can Competition Protect Privacy? An Analysis Based on the German Facebook Case*, in *World Competition*, 44, no. 2, 2021, pp. 169-198; K. Kemp, *Concealed data practices and competition law: why privacy matters*, in *European Competition Journal*, 16. nos. 2-3, 2020, pp. 628-672.

DMA projects a set of normative preferences in terms of the end user's capacity to control their personal data in the environment of the core platform services provided by the designated gatekeepers, i.e., only opt-in systems can facilitate free and voluntary choice and effective consent within the meaning of the GDPR will be seldom admissible given the dynamics of digital markets. In this sense, the DMA is not privacy-agnostic and is not coherently designed according to its intention to not repeal -or at least, not influence- the force of the GDPR's provisions in the context of consent.

6. Conclusions

The DMA works on the premise that it applies to a designated set of economic operators and core platform services to ensure contestability and fairness in those settings where antitrust has failed to protect the competitive conditions of the digital markets or at least has not done so as smoothly and quickly as would be desired according to the challenges posed by digital players. However, the regulatory instrument acknowledges that it must be applied hand in hand with other acts of the Union to be effective when it is enforced. The GDPR stands out as one of the key sets of rules that must not be curtailed, given the spectacular role of data in the business models implemented by the designated gatekeepers in their ecosystems.

The cornerstone of the interaction between privacy and antitrust is placed on how to interpret the GDPR's requirements of voluntary and free consent in the context of dominance. From the privacy perspective, the interpretation of the criteria to deem consent effectively rendered by the data subject is not undisputed. The lack of unified criteria when interpreting the notion of an existing imbalance in power between the data subject and the data controller/processor underlies the complexity to incorporate privacy considerations into antitrust, in general. In the particular case of consent, the *FCO v. Facebook* cases and the *AGCM v. Apple/Google* cases exemplify the circularity of the argument: given that imbalances in power are defined in the GDPR as the ability to exploit the data subject's vulnerability and the latter is defined regarding the existence of power imbalances, the ecosystem holder's dominance in the market is factored in as a decisive element to outweigh the analysis in favour of the finding of abusiveness.

The DMA builds up its provisions based on this same assumption, namely in Articles 5(2) and 6(10). In the case of the former, a prohibition on the combination, processing and cross-using of personal data is established against the designated gatekeeper, unless the end users consent to these activities according to the requirements of the GDPR. Article 5(2) starts and is exempted based on two incompatible presumptions: the prohibition is applicable because consent cannot be granted freely in the context of dominance and the prohibition is overridden due to the presence of consent in the form of a legal exception applying to idiosyncratic and particular cases. Circularity on the dichotomy between dominance and consent is not undermined but reinforced in this regard. In the case of the latter, a similar driving force inspires Article 6(10) of the DMA, building up on the circularity, and conditioning consent to be expressed through opt-in systems, or else consent will not be admissible in terms of the representation of free end user choice when handing over the control over their personal data.

Thus, the paper demonstrates overall that the DMA is inspired by particular normative preferences and choices which taint its fairness and contestability purposes, undermining the effectiveness of its provisions as well as the unified interpretation of effective consent under the GDPR.