# ADDRESSING THE INTERPLAY BETWEEN COMPETITION LAW AND DATA PROTECTION LAW IN THE DIGITAL ECONOMY THROUGH ADMINISTRATIVE COOPERATION: THE CJEU JUDGMENT IN THE *META PLATFORMS* CASE

*Leonardo Parona*[*]

*Abstract*

The article addresses the issues posed, both at the normative and at the enforcement level, by the interplay between competition law and data protection law, in light of the recent judgment of the Court of Justice in the *Meta Platforms v. Bundeskartellamt* case. The judgment innovates the interpretation of the rules composing the two normative domains, marking a shift from separateness to a logic of complementarity. Nonetheless, while easing the terms of the complex interaction between the two sets of rules and principles, the judgments leaves some questions, in terms of administrative cooperation among the competent enforcement authorities, unanswered. The latter are framed by the Article in terms of missing steps in the way forward, which, also in light of recent developments in EU law (*e.g.* DMA, DSA, AI Act and Data Act), seems to be a steep one.

TABLE OF CONTENTS



[*] Assistant Professor, Roma Tre University.

## 1. Introduction

Considering the fact that, in the digital economy, data undisputedly constitute one of the most valuable goods and a driver of profit-making dynamics, it might seem self-evident that competition law would complement data protection law, in order to prevent companies with access to strategic datasets from abusing their market power to the detriment of users and competitors. The interplay between the two normative realms and their enforcement mechanisms have been nevertheless characterized, at least in the last decade, by significant tensions, if not open contrasts, both in terms of objectives and in terms of competences.

The need to address the interplay between data protection and competition law has been perceived worldwide by public institutions[1] and especially by competition authorities[2]. Within the

[1] A report issued by the UK Parliament anticipated, already more than five years ago, that the degradation of privacy standard perpetrated by dominant online platforms could potentially be framed as an abuse of dominant position, in that it negatively impacted upon the quality of the service provided, leaving no valid alternative to the users (see The UK House of Lords – Select Committee on European Union, *Online Platforms and the Digital Single Market* (10th Report of Session 2015–16, 20 April 2016), para 180).

[2] For instance, the US Federal Trade Commission acknowledged that privacy can constitute a non-price competition parameter which could become especially critical in merger operations; however in the specific case in which the issue arose (the *Google/DoubleClick* case) it concluded that «evidence does not support a conclusion it would do so» (FTC Statement concerning Google/DoubleClick – FTC File No. 071-0170 (2007), 2–3). In similar terms see also the joint report issued in 2016 by the French and the German competition authorities and the position expressed by the Catalan Competition Authority, aimed at fostering cooperation with the Data Protection Authority (see, respectively, the report *Competition Law and Data,* available online at the following Internet address: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2, and Autoritat Catalana de la Competència, *The Data-Driven Economy: Challenges for Competition,* 2016, 42, available online at the following Internet address: https://acco.gencat.cat/web/.content/80_acco/documents/arxius/actuacions

multi-layered normative framework of the European Union, the issue has manifested itself on several occasions, and Member States have already tried to cope with it by looking for a balance in the interaction between potentially non-convergent sets of rules[3].

In this unsettled context, a recent judgment[4] of the Grand Chamber of the Court of Justice of the European Union expressed

/Eco-Dades-i-Competencia-ACCO-angles.pdf). All of them are in line with the holistic approach enshrined in the 2016 Opinion of the European Data Protection Supervisor on coherent enforcement of fundamental rights in the age of Big Data (EDPS, Opinion 8/2016), which launched the Digital Clearing House initiative, *i.e.* a network of authorities based on voluntary collaboration). With regard to Asian countries see for instance S. Van Uystel, Y. Uemura, *Online Platforms and the Japan Fair Trade Commission: the DeNA case as an example of early market intervention,* in B. Lundqvist, M.S. Gal (eds.), *Competition Law for the Digital Economy* (2019), 231 (who show how the Japanese Fair Trade Commission has generally been resistant to applying the Antimonopoly Law to new developments in the market, especially in the digital economy) and V. Sinha, S. Srinivasan, *An integrated approach to competition regulation and data protection in India,* 9(3) *CSI Transactions on ICT* 151 (2021), (who clarify that even the Indian competent authority (the Competition Commission of India) has pointed out the pitfalls of keeping a firewall between the two regulatory realms).

[3] See for instance the case involving Facebook decided a couple of years ago by the Italian Council of State Council of State, Sixth Section, 29 March 2021, n. 2631, which ruled that Facebook's processing of users' data for commercial and profiling purposes represented an unfair commercial practice (the focus being here mainly on the interaction between data protection and consumer law). For an analytical comment of the judgment see S. Franca, *L'intreccio fra disciplina delle pratiche commerciali scorrette e normativa in tema di protezione dei dati personali: il caso Facebook approda al Consiglio di Stato,* 2 *Riv. Reg. Merc.* 362 (2021). In the same line of reasoning, the CJEU more recently established that consumer protection associations may bring legal proceedings (even in the absence of a mandate conferred for that purpose and independently of the infringement of specific rights of the data subjects), against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation (Court of Justice of the European Union, Third Chamber, 28th April 2022, in case C-319/20, *Meta Platforms Ireland Ltd. v. Verbraucherzentralen Bundesverband,* with the comment of E. Mišćenić, *Case note on Meta Platforms Ireland (EuGH v. 28.4.2022 – C-319/20),* 19(5) *Zeitschrift für das Privatrecht der Europäischen Union* 206 (2022)).

[4] Court of Justice of the European Union, Grand Chamber, 4th July 2023, in case C-252/21, *Meta Platforms Inc. et al. v. Bundeskartellamt;* hereinafter "the

some fundamental principles which possibly ease the terms of such complex normative interaction[5], while still posing some challenges in terms of administrative cooperation among the competent enforcement authorities.

The judgment of the Court originates from a request for preliminary ruling of the *Oberlandesgericht* (Higher Regional Court) Düsseldorf, issued in a case where Meta[6] challenged a decision of the *Bundeskartellamt* (the Federal Cartel Office, that is the German competition authority, hereinafter FCO)[7]. The controversy began in February 2019, when the FCO terminated a proceeding against Meta's data processing activities with a decision establishing that the latter abused its dominant position

---

judgment". When references will be made in the footnotes to paragraph numbers without further specifications, they are intended to be referred to this judgment.

[5] Such complex interaction has been at times depicted in critical terms, as if finding a balance between the two normative realms represented an overstretching; for this position see: G.A. Manne, B. Sperry, *The problems and perils of bootstrapping privacy and data into an antitrust framework,* and R. Pepper, P. Gilbert, *Privacy considerations in European merger control: a square peg for a round hole,* both in *Antitrust Chronicle,* 2015, 2, 1 ff. A more conciliative view is expressed by N. Zingales, *Data protection considerations in EU competition law: funnel or straightjacket for innovation?,* in P. Nihoul, P. Van Cleynenbreugel (eds.), *The role of innovation in competition analysis* (2018), 79. A more critical view of this aspect of the judgment is that of O. Brook, M. Eben, *Another Missed Opportunity? Case C-252/21* Meta Platforms V. Bundeskartellamt *and the Relationship between EU Competition Law and National Laws, J. Eur. Comp. L. & Practice,* (Online), 2023.

[6] In the text we only refer to Meta for reasons of brevity, however, the proceeding was actually brought against Meta Platforms, Meta Platforms Ireland and Facebook Deutschland.

[7] The proceeding was initiated on 2nd March 2016 on the basis of paragraphs 19(1) and 32 of the *Gesetz gegen Wettbewerbsbeschränkungen* (hereinafter GWB, *i.e.* the law against competition restrictions, an English translation of which is available online at https://www.gesetze-im-internet.de/englisch_gwb/). Under Section 19(1) GWB, principles of the legal system that regulate the appropriateness of conditions in unbalanced negotiations (*i.e.*, between consumers and traders) can be taken as a benchmark when assessing whether business terms are abusive under competition law. The case immediately sparked debate; for some early comments see R. McLeod, *Novel but a long time coming: the Bundeskartellamt takes on Facebook,* 6 *J. Eur. Comp. Law & Practice* 367 (2016); G. Schneider, *Testing art. 102 TFEU in the digital marketplace: insights from the Bundeskartellamt's investigation against Facebook,* 4 *J. Eur. Comp. Law & Practice* 213 (2018); M.N. Volmar, K.O. Helmdach, *Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation,* 2-3 *Eur. Comp. J.* 195 (2018).

on the German market for social networks by imposing, through general contractual conditions and thanks to its market power, certain terms to Facebook's users which violated several GDPR's provisions. The controversial practices, as will be further clarified, consisted in *collecting* users' data generated by various services offered by Meta and third parties[8], *linking* such data to Facebook users' profiles and, finally, *using* such data for several direct and indirect profit-making purposes. Given their unlawfulness, the FCO prohibited Meta from perpetrating such abusive practices and required it to adapt its contractual terms.

While introducing certain policy changes and making some efforts to increase transparency and comply with GDPR's provisions[9], Meta brought an action against the FCO's decision before the Higher Regional Court of Düsseldorf, which, in April 2021, filed the aforementioned request for preliminary ruling. On the one hand, the German court raised doubts as to whether national competition authorities can, in the exercise of their functions, ascertain the legitimacy in terms of compliance with the GDPR, of a company's data processing activities, and eventually sanction the latter on the basis of such finding; on the other hand, it doubted on the interpretation and application of certain GDPR provisions.

The CJEU judgment stemming from such preliminary reference procedure, is both relevant, for the number and complexity of the questions it addresses[10], and innovative from a

[8] In addition to data provided directly by users when signing up for the relevant online services, Meta also collects other user- and device-related data on and off the social network and the services provided by the group.

[9] To be more precise, on 31st July 2019, Meta Platforms introduced new terms of service following a related initiative of the European Commission and of national consumer protection organizations of several Member States. The updated terms expressly state that the user agrees to be shown targeted advertisements instead of paying a monetary price to use Facebook services. Furthermore, since 28 January 2020, Meta Platforms has been offering at a global level the so-called 'Off-Facebook-Activity' service, which allows users to view a summary of the information concerning themselves and obtained in relation to their activities on websites and apps other than Facebook, as well as to disconnect data about past and future activities from their Facebook accounts, if they wish so (see paragraphs 32-33).

[10] As will be further clarified, such questions do not only concern the interplay between data protection law and competition law (questions 1 and 7 of the

methodological and substantial point of view, since it does not follow an all-or-nothing approach, but builds instead a nuanced solution[11], which delineates a balanced interplay between data protection and competition law.

These aspects will be further expounded in the present article by illustrating, first, how the controversy regarding Meta's data processing activities is emblematic of some of the most crucial legal issues characterizing the digital economy [12] (paragraph 2). We will secondly analyze the key passages through which the judgment addresses and untangles the tension between data protection and competition law (paragraph 3). Thirdly, we will discuss some critical issues posed by the judgment, especially in terms of the administrative enforcement of the principles of law established by the CJEU (paragraph 4). Some open questions, as well as some conclusive considerations, will be finally presented in the final paragraph in light of the conducted analysis and of current developments in EU law (paragraph 5).

## 2. Meta's data processing activities within the broader context of the digital economy

The issues raised by the controversy lie, as anticipated, at the heart of a broader debate concerning the delimitation of the respective roles and the possible interplay between competition law and data protection law in the digital economy [13]. Such

---

preliminary ruling), but also a series of issues specifically related to several interpretative issues insisting upon GDPR provisions (questions from 2 to 6).

[11] The CJEU substantially follows the Conclusions presented by Advocate General Rantos and endorses the position of the *Bundeskartellamt*. See *infra,* especially Paragraph 3.

[12] The notion of digital economy is hereinafter referred to in the broad meaning assigned to it by the OECD, *i.e.* as «an umbrella term used to describe markets that focus on digital technologies. These typically involve the trade of information goods or services through electronic commerce. It operates on a layered basis, with separate segments for data transportation and applications» (see OECD The Digital Economy, DAF/COMP(2012)22, 7 February 2013, 5, available at http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf).

[13] Among the extensive literature on this topic, see F. Costa-Cabral, O. Lynskey, *Family ties: the intersection between data protection and competition in EU law,* 54(1) *Comm. Market L. Rev.* 11 (2017); G. Colangelo, M. Maggiolino, *Data Protection in Attention Markets: Protecting Privacy through Competition*, 8(6) *J. Eur. Comp. Law &*

interplay is well summed up by the position expressed by the *Bundeskartellamt*, according to which «where access to the personal data of users is essential for the market position of a company, the question of how that company handles the personal data of its users is no longer only relevant for data protection authorities. It becomes a relevant question for the competition authorities, too»[14].

As it is well known, Meta Platforms operates the social network Facebook as well as several other social networks and services, among which WhatsApp and Instagram. Facebook's business model (but, to a certain extent, the same logic applies also to the other platforms) is based on financing through user-tailored online advertising. More precisely, while access to the social network Facebook and to the rest of the apps and services offered by Meta is free, the company's revenue derives from the price paid by advertisers, who obtain the chance to attract new customers.

This aspect – widely recognized, though still fundamental – deserves a further clarification: although users do not pay a monetary price to access the platform and use its services (rendering the market at issue a *zero-price* one), they do need to accept the specific terms of use by adhering to the consumer agreement, which includes the *privacy policy* unilaterally established by the provider[15]. According to the latter, the user

---

*Practice* 363 (2017). In such interplay among normative bodies, a significant role is also played by consumer law – though not in the present controversy – as observed for instance by I. Graef, D. Clifford, P. Valcke, *Fairness and enforcement: bridging competition, data protection, and consumer law,* 8(3) *Int. Data Privacy Law,* 200 (2018) and W. Kerber, *Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection*, 11 *J. Intell. Prop. Law & Practice* 856 (2016).

[14] Bundeskartellamt, *Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive*, 19 December 2017, available online at the following Internet address: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/ 2017/19_12_2017_Facebook.html. As will be further clarified, this consideration is shared by the Court of Justice.

[15] By signing up to Facebook, the user accepts the *user agreement,* which refers to the company's general terms as far as data and cookies policies are concerned (the *privacy policy*) (paragraph 28). It is worth adding that in the latest months (after the judgment of the Court was issued) in certain geographical area, included EU Member States, Facebook is making it explicit that if users do not wish to have their data used for targeted advertising, they will have to pay a

discloses a series of personal and non-personal data, which are then monetized directly and indirectly by the provider, mainly through profiling activities[16]. Moreover, it is worth adding that, besides the data directly provided by the users when signing up for a given service (such as Facebook), Meta also collects other user- and device-related data on and off that specific service or social network (off-Facebook data), which are linked to the various user accounts. The aggregate view of such data intuitively allows detailed conclusions to be drawn about the users, whose data therefore provide a gateway to extract consumer information concerning both actual and potential purchasing power and preferences[17]. Being instrumental to targeting online advertising, data represent a key revenue source; one that has been defined, as it is well known, in terms of "new currency"[18].

The aforementioned business model is technically possible thanks to the online collection of huge quantities of data (Big Data), their interpolation, and the automated creation on such basis of detailed personal profiles of social network users[19].

---

monthly subscription of 12,99 €. By paying such price, Facebook declares that users' data and information will no longer be used, and that advertising will no longer be shown to the user. Meta's announcement is available online: https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/.

[16] The indirect monetization of personal data can be qualified as a hidden cost paid by the user, as explained by M.S. Gal, D.L. Rubinfeld, *The hidden costs of free goods: implications for antitrust enforcement,* 80(3) *Antitrust Law J.* 562 (2016) and F. Polverino, *Hunting the wild geese: competition analysis in a World of "Free",* 1 *Concorrenza e mercato* 545 (2012).

[17] These practices constitute typical examples of «digital market manipulation», which «causes or exacerbates economic harms», as observed by R. Calo, *Digital market manipulation,* 82 *Geo. Wash. L. Rev.* 1026, 1027 (2013).

[18] The evocative expression is frequently used both in scientific discussions and in the political debate; see recently C.A. Makridis, J. Thayer, *Data is the New Currency,* in *The Wall Street Journal,* 31st June 2023, observing that, at least in the US, antitrust law still fails to account for how companies exploit users' information to dominate markets. For an early use of the expression see W.D. Eggers, R. Hamill, A. Ali, *Data as the new currency. Government's role in facilitating the exchange,* 13 *Deloitte Rev.* 19 (2013). More generally on the topic see A. Marciano, A. Nicita, G.B. Ramello, *Big data and big techs: understanding the value of information in platform capitalism,* 50 *Eur. J. L. & Eco.* 345 (2020).

[19] This point is clear in the reasoning of the Court at paragraph 27. Another important case in which algorithmic manipulation has been assessed as a type of conduct that may raise competition concerns is represented by the *Google*

Platforms such as those provided by Meta (and especially Facebook) operate in (*rectius* constitute themselves) two-sided markets[20]. This kind of – digital – markets feature networks effects, meaning that the platform's value, and therefore the provider's revenues, increase the more participants are active on the platform and the more data they put into it.

Such dynamics, which trigger monopolistic tendencies, raise the question whether a new market power definition shall be provided[21]. The accumulation of Big Data in the hands of a single company (or group, as in the case of Meta) therefore represents a matter of concern for competition authorities, which in fact, in the last couple of years, have worldwide initiated several investigations against the major platforms[22]. This is so from two

---

*Search* case, addressed by the European Commission in 2017 (Commission Decision C(2017) 4444 final), on which see K. Bania, *The European Commission's decision in* Google Search. *Exploring old and new frontiers of competition enforcement in the digital economy,* in B. Lundqvist, M.S. Gal (eds.), *Competition Law for the Digital Economy*, cit. at 2, 264. The decision is relevant for our discussion in that it started a paradigm shift in the evaluation on anti-competitive conducts, considering also non-monetary and data-driven transactions between a search engine and its users as parameters to be weighed in a competition analysis. At paragraph 158 of such Decision, the Commission recognized that «even though users do not pay a monetary consideration for the use of general search services, they contribute to the monetization of the service by providing data with each query. In most cases, a user entering a query enters into a contractual relationship with the operator of the general search service».

[20] As clarified in the economic literature, in a two-sided market two sets of agents or customer groups interact through an intermediary (which in the digital economy is an online platform), and the decisions of one set of agents affect the outcomes of the other set of agents. The intermediary benefits by the presence of the two sets of agents on the platform and optimizes its profits by pricing the two groups differently. In our case, one group (users) pays through data, whereas the other (advertisers and companies in general) pays the price required in order to advertise products or services online. On this topic see L. Filistrucchi, D. Geradin & E. van Damme, *Identifying two-sided markets,* 36 *World Competition* 33 (2013); M. Rysman, *The economics of two-sided markets,* 23(3) *J. Econ. Perspectives* 125 (2009); J.-C. Rochet, J. Tirole, *Platform competition in two-sided markets,* 1 *J. Eur. Econ. Ass'n* 990 (2003).

[21] The question is formulated by H.K. Schmidt, *Taming the shrew: is there a need for a new market power definition for the digital economy?,* in B. Lundqvist, M.S. Gal (Eds.), *Competition Law for the Digital Economy*, cit. at 2, 29.

[22] For an analysis of the topic and an overview of the main cases see M. Wörsdörfer, *What happened to "Big Tech" and antitrust? And how to fix them!,* 21

distinct but related points of view: on the one hand, Big Data are an indicator of market power (and possibly dominance); on the other hand, Big Data (and the monopoly over them) can be used in several ways that are detrimental to competition [23]. These anticompetitive practices may consist in exclusionary conducts (*i.e.* excluding actual or potential competitors [24]) or in the imposition of unfair conditions on users (as it was the case in the controversy).

These underlying economic dynamics, as will be further discussed, are crucial in the legal analysis conducted by the Court of Justice.

Having outlined the broader context of the digital economy, it is now possible to turn our attention to the specific circumstances of the case at issue. Meta's processing of personal data is based on three different, but related, operations, the criticalities of which derive from their undeniable interconnectedness[25], an aspect which is underlined by the CJEU but which, adopting an atomistic approach, has in the past been at times underestimated[26].

---

*Philosophy of Management* 345 (2022) and V. Robertson, *Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data,* 57 *Comm. Mrkt. L. Rev.* 185 (2020).

[23] See H.K. Schmidt, *Taming the shrew: is there a need for a new market power definition for the digital economy?*, cit. at 21, 42 and B. Lundqvist, *regulating competition in the digital economy. With a special focus on platforms,* in B. Lundqvist, M.S. Gal (Eds.), *Competition Law for the Digital Economy*, cit. at 2, 2. For a general analysis of the topic see M. Stucke, A. Grunes, *Big Data and competition policy* (2016) and A. Ezrachi, M. Stucke, *Virtual competition: the promise and perils of the algorithm-driven economy* (2016).

[24] In this perspective, it has been proposed to qualify data as an essential facility, the monopoly over which, together with exclusionary conducts, amounts to a violation of competition law. For this theory see I. Graef, *Data protection and online platforms. Data as essential facility?* (2016), especially Chapter 7.

[25] Such interconnectedness also derives from the circumstance that Meta Platforms Inc. is the outcome of a series of merger and acquisition operations occurred in the last ten years, which have significantly accrued the quantity of data concentrated in the hands of one single gatekeeper.

[26] Atomistic approaches to the digital economy might be praised for their clarity and for serving a didactic function; they appear nonetheless unfit to realistically depict how digital economy actually works. According to S.Y. Esayas, *Privacy-as-a-quality parameter of competition. Some reflections on the skepticism surrounding it,* in B. Lundqvist, M.S. Gal (eds.), *Competition Law for the Digital Economy*, cit. at

Such activities, which have been briefly referred to in the Introduction, are the following: *i)* the *collection* of data, both within Meta's own services and apps, and on third party websites; *ii)* the *linking* of the latter with the former, in order to gain greater knowledge and insight on each user's preferences; *iii)* the *use* of such data for fine-tuning services and for tailoring advertising (*i.e.* profiling)[27].

As long as they take place within the EU, Meta's data processing activities must comply with the GDPR, the well-known core principles of which, enshrined in Article 5, are: lawfulness and fairness; purpose limitation; minimization; accuracy or data quality; storage limitation; data security; accountability. On the basis of such regulation, personal data processing is in principle prohibited, unless it is specifically permitted and except for data that have been anonymized (leaving here aside the issues of re-identification that affect anonymization processes). We could in other words say that, opposite to EU and national rules on the freedom of economic enterprise – that represent the backbone competition law builds upon – according to which every business activity is allowed unless specifically forbidden, data protection law works the other way round: a specific legal justification shall

---

2, 126, 150 such approaches rely on two underlying assumptions: «(i) distinguishing among different processing activities and relating every piece of personal data to a particular processing is possible; and (ii) if each processing is compliant, the data privacy rights of individuals are not endangered». The Author, however, agreeably observes that «these assumptions are untenable in an era where companies process personal data for a panoply of purposes, where almost all processing generates personal data and where data are combined across several processing activities».

[27] See paragraph 28. Profiling, which is *per se* a controversial practice, generates in turn a series of other problems, which cannot however be dealt with within the scope of the present article. We refer, in particular, to the so-called "filter bubble" and the "creepiness effect". The former refers to the consequence of content personalization, according to which users are only exposed to contents that they are interested to, and that they agree with (determining, among other things, political polarization); see on this E. Pariser, *The Filter Bubble: how the new personalized web is changing what er read and how we think* (2011). The latter refers to the feeling of being observed and tracked by others, who assess and capitalize at the cost of the users' privacy; see on this L. Barnard, *The cost of creepiness: how online behavioral advertising affects consumer purchase intention* (2014).

in fact be provided to allow a company to process data within its economic activity[28].

The questions addressed to the Court of Justice in the request for preliminary ruling insist upon several aspects of the issues that have just been mentioned. Focusing here on the ones that matter the most for the interplay between data protection and competition law in a public law perspective, we shall briefly recall that the German Court asked: i) whether a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking, that the latter's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with the GDPR, and, if so, whether Article 4(3) TEU must be interpreted as meaning that such a finding by the competition authority, having incidental nature, is also possible where the same or similar terms are being simultaneously investigated by the competent data protection authority (questions 1 and 7)[29]; ii) whether the consent given by the user of an online social network to the operator of such a network may be considered valid, according to Article 4(11) GDPR, and, in particular, whether it can be considered freely given, where that operator holds a dominant position on the market for online social networks (Question 6)[30].

The remaining questions formulated by the referring court (Questions 2-5) exclusively concern data protection law, not imping upon the interplay between the former and competition law, which in fact remains, with regard to this set of questions, on the background. They insist, more precisely, upon the interpretation of Articles 6(1)(b)-(f), 9(1), and 9(2)(e) of the GDPR, which respectively establish the lawfulness requirements for data processing activities in general and with regard to special categories of personal data (such as those revealing, on the one

[28] N. Zingales, *Data protection considerations in EU competition law: funnel or straightjacket for innovation?*, cit. at 5, 108.

[29] These questions therefore insist upon the interpretation of Article 51 et seq. of the GDPR (comprised within Chapter VI of the GDPR, dedicated to independent supervisory authorities), read in conjunction with Article 102 TFEU and 4(3) TEU.

[30] Besides Article 4(11), already mentioned in the text, the questions insist upon the interpretation of point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR, respectively concerning the lawfulness of processing activities and the processing of special categories of personal data.

hand, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and, on the other hand, genetic data, biometric data and data concerning health or a natural person's sex life or sexual orientation)[31]. In its answer to this latter set of questions, the Court narrowly interprets the legal bases (other than consent) for data processing.

As anticipated, in the following paragraph the analysis will be conducted from a public law perspective and it will, therefore, focus on the former set of questions, illustrated above under points i) and ii).

### 3. The interplay between data protection law and competition law in the judgment of the Court

The Court's analysis departs from the acknowledgment of the circumstance that both the facts of the controversy and, consequently, the questions formulated by the referring Court, require to address, and possibly shed light on, several interactions between data protection and competition law.

In this regard, it is necessary to recognize that a certain conduct carried out by a company such as Meta may alternatively: comply with both data protection law and competition law; comply with the former but still violate the latter, or vice-versa; or, finally, violate both normative bodies. To be more explicit, it is possible to say that, considering the different objectives of the two legal disciplines, data processing may breach competition rules while complying with the GDPR[32], and that, conversely, unlawful conducts under the GDPR do not automatically violate competition law. What is undeniable, according to the Court, is therefore that, in circumstances as the ones presented by the case at issue, the two normative domains objectively overlap, however, a clash between the two sets of legal norms and enforcement

[31] Except for few aspects, Meta's contractual terms and practice were found to be in violation of several GDPR provisions by the *Bundeskartellamt*, whose decision was found to be based on a correct interpretation of EU law by the Court of Justice, which, in turn, deemed Meta's exploitation of personal data in violation of the GDPR. See paragraph 64 ff.

[32] In *AstraZeneca v. Commission* (C-457/10, paragraph 132), the Court of Justice recalled that, in the majority of cases, an abuse of dominant position consists of conducts which are otherwise lawful under branches of law different from competition law, such as data protection law, as enshrined in the GDPR.

mechanisms does not constitute an inevitable outcome, but only one possible unwanted effect, which can both be prevented and, eventually, mitigated.

### 3.1. The relevancy of data protection violations in competition proceedings and the possibility for a competition authority to ascertain them

As far as the first question is concerned[33], the Court of Justice moves from the general consideration that the competences assigned by the two normative bodies to national authorities (*i.e.* competition authorities as the *Bundeskartellamt* on the one hand, and data protection authorities on the other) are distinct. Such distinctness, which entails the performance of distinctive tasks and the pursuance of diverse objectives, might be intended as a first – though not *per se* decisive – guarantee against the risk of conflicts.

Until few years ago, distinctness was however conceived by European Institutions in terms of strict separateness of the two domains, with the consequence that «privacy-related concerns flowing from the increased concentration of data within the control of Facebook […] [did] not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules»[34].

A firewall between the two regulatory domains had therefore to be preserved, according to that view. The rigid respect of enforcement competences, however, was to a certain extent detrimental to a full and effective application of EU law[35].

---

[33] The one introduced *supra* at point i) of Paragraph 2.

[34] That was, in particular, the position of the European Commission in the decision concerning the *Facebook/WhatsApp* case, of 3 October 2014 (C(2014) 7239 final, paragraph 87). Such position was more recently confirmed by the Court of Justice (CJEU, Grand Chamber, *Facebook v. Gegevensbeschermingsautoriteit,* 15 June 2021, C-645/19) which established that under the GDPR national supervisory authorities are only competent for the performance of the tasks explicitly assigned to them, and exclusively on the territory of the Member State. In earlier rulings on a related topic (*i.e.* privacy threats deriving from the accumulation of data in one single hand as a result of mergers) the Court of Justice contented itself with indicating that privacy as such was beyond the scope of competition law (see for instance *Asnef-Equifax v. Asociación de Usuarios de Servicios Bancarios,* C-238/05, paragraph 63).

[35] For a critical comment of the approach aimed at maintaining such separation in the interpretation and enforcement of the two regulatory realms see G.

Only gradually access and collection of data – including personal data – via digital platforms began to be considered an indicator of market power and, therefore, to be included among the parameters of competition relevant in the digital economy[36]. Not doing so, as wisely observed by the Court in the judgment here commented, would in fact disregard the reality of how businesses work in the digital era and undermine competition law's effectiveness[37].

To state, as the Court does, that rules on the protection of personal data shall be taken into consideration by competition authorities when examining an abuse of a dominant position, does not however imply that the competences attributed to the latter authorities shall be extended. The solution envisaged by the Court of Justice is balanced also under this point of view; in fact, to ensure consistency, it recalls the duty to cooperate and tries to further articulate it in procedural terms. The latter aspect – besides the criticalities that will be discussed in Paragraph 4 – is especially important, and it was arguably not strictly required to the Court, which could have simply referred to the general principle of sincere cooperation as enshrined in Art. 4(3) TEU[38].

---

Buttarelli, *Strange bedfellows: data protection, privacy and competition,* 34(12) *The Comp. & Int. Lawyer* 1 (2017), observing both in the US and in Europe a tendency to «work in silos». For a more critical view of the inefficiencies of this regulatory approach see I. Scott, T. Gong, *Coordinating government silos: challenges and opportunities,* 1 *Glob. Pub. Pol'y & Gov.* 20 (2021); R. O'Leary, *From silos to networks: hierarchy to heterarchy,* in M.E. Guy, M.M. Rubin (eds.), *Public administration evolving: from foundations to the future* (2015), 85; F. Froy, S. Giguère, *Breaking out of policy silos: doing more with less* (2010).

[36] See the position of the European Commission in the *Microsoft/LinkedIn* case (Commission Decision C(2016) 8404 final) and the judgment of Court of Justice, First Chamber, 14th March 2013, *Allianz Hungária Biztosító Zrt v. v Gazdasági Versenyhivatal,* in the case C-32/11. On the topic see S.Y. Esayas, *Privacy-as-a-quality parameter of competition. Some reflections on the skepticism surrounding it,* cit. at 26.

[37] See paragraphs 50 and 51. Since data represent a key source of competitive advantage in providing service through online platforms, data protection law becomes an essential component in the regulation of the competitive process, with the consequence that, in turn, compliance or noncompliance with data protection rules constitutes a significant competitive differentiator.

[38] In his Conclusions, Advocate General Rantos contents himself with referring to the general principle of loyal cooperation and to the right to good administration, which implies in turn a duty of diligence and care (paragraphs 28-29 of the AG Conclusions, presented on the 22nd September 2022). On the

As observed as well by AG Rantos[39], the Court underlines that the issue at stake is not currently addressed by EU law[40], and, more precisely, that it cannot be ruled under GDPR provisions on the cooperation among data protection authorities[41], nor under competition law rules concerning the cooperation among national authorities and the EU Commission[42], since they have a precise and distinct scope of application.

In the absence of specific rules on cooperation, the Court first recalled the general duty of Member States, including their administrative authorities, to «take any appropriate measure to ensure fulfilment of the obligations» arising from acts of the EU institutions, and «refrain from any measure which could jeopardise the attainment of the European Union's objectives»[43].

Secondly, it introduced a substantial limitation, by stating that a competition authority can consider and interpret the GDPR within a proceeding of its competence only when this is necessary to issue a decision falling within the scope of its tasks[44].

Thirdly, if such necessity threshold is surpassed, even in the absence of risks of potential divergences, the competition authority must consult the data protection supervisory authority that would be competent under the GDPR to address the issues at stake. Such duty becomes more stringent when there is an actual risk of contrasting interpretations concerning the same or similar contractual terms or practices. More precisely, the competition authority must always ascertain whether analogous conducts have already been the subject of prior decisions by a data protection authority. In the presence of such decisions, although the

---

principle of cooperation see M. Klamert, *The Principle of Loyalty in EU Law* (2014), especially 235 ff. on the duties to consult and inform.

[39] Paragraph 29 of the AG Conclusions.

[40] See paragraphs 42, 43 and 53. It is worth noting that some national authorities have already coordinated their activities in a spontaneous manner, as it is the case with the Italian Competition, Communications and Data Protection authorities (see AGCM, AGCOM, Garante Privacy, *Indagine conoscitiva sui Big Data,* 10th February 2020, available at www.agcm.it).

[41] The issue is partially addressed by chapters VI and VII of the GDPR, which establish 'one-stop-shop' mechanisms for the exchange of information and for mutual assistance between supervisory authorities.

[42] See Chapter IV of UE Regulation n. 1/2003.

[43] Paragraph 53, citing *UPC Nederland* (C-158/11) and *Sea Watch* (C-14/21 and C-15/21).

[44] Paragraph 54.

competition authority cannot depart from them, it can nonetheless draw its own (and potentially different) conclusions, considered that the same facts might be diversly qualified under the perspective of competition law[45].

Fourthly, shall the competition authority have doubts as to the scope of the assessment carried out by a data protection authority, the former shall consult and seek further cooperation from the latter. The same duty applies when the conduct under scrutiny, or a similar one, is being simultaneously examined by the two authorities. Such consultation is aimed at dispelling doubts and, eventually, determining whether the competition authority should wait for the data protection one to issue a decision, before stating its own assessment[46].

Besides imposing a duty to seek cooperation on part of the competition authority, the CJEU also qualifies the respective obligations of the data protection authority. The latter shall, in fact, respond to requests for information and cooperation «within a reasonable period of time», and inform the former of the intention to initiate a proceeding (eventually in cooperation with other national data protection authorities or with the European Data Protection Board). Shall a data protection authority not reply within a reasonable time, then the proceeding competition authority seeking cooperation would be allowed to continue its own investigation, in the same way as it would do in case no objections to the investigation had been raised[47].

Applying the principles just elaborated to the referred case, the CJEU upheld the *Bundeskartellamt*'s interpretation of the normative framework and, therefore, its conduct. In fact, before adopting the contested decision, the German competition authority contacted both the federal and the regional data protection supervisory authorities (as well as the Irish one) and waited for their responses. The latter confirmed that no investigations were being conducted in relation to facts similar to those at issue in the main proceedings and raised no objection to the competition authority's action. Finally, in the reasoning of the decision sanctioning Meta, later challenged in court, the

[45] Paragraph 56.
[46] Paragraph 58.
[47] Paragraph 59.

*Bundeskartellamt* expressly referred to the outcome of such administrative cooperation[48].

### 3.2. The issue of consent: is it freely given when the data processing undertaking holds a dominant position?

As far as the second question is concerned[49], the interpretation of the interplay between the two normative realms offered by the Court also paves the way to a balanced solution with regards to the validity of consumers' consent to online data processing activities. That is so, more precisely, with reference to the specific issue of consent being freely given by a user (under Article 4(11) GDPR[50]) to a platform operator holding a dominant position in the market for online social networks.

As recalled by the Court, according to recital 42 of the GDPR, consent cannot be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or subsequently withdraw consent without detriment[51]. Recital 43 adds that consent cannot be considered valid if there is a clear imbalance between the data subject and the controller and that it is presumed not to be freely given if it is not possible for the user to give separate consent to different personal data processing operations. A further normative parameter relevant under this point of view in the analysis of the Court is represented by Article 7(4) GDPR, under which the circumstance that a contract's performance is conditional upon the consent to personal data processing activities

[48] Paragraphs 60-61.

[49] The one introduced *supra* at point ii) of Paragraph 2.

[50] In its judgment of 11th November 2020, *Orange Romania* (C-61/19, paragraphs 35-36 and the case-law there cited), the Court of Justice clarified that the wording of Article 4(11) of the GDPR, which defines the consent of the data subject, appears even more stringent than Article 2(h) of Directive 95/46, in that it requires a «freely given, specific, informed and unambiguous» indication of the data subject's wishes in the form of a statement or by «a clear affirmative action» signifying agreement to the processing of personal data relating to him or her. Moreover, as the EDPB pointed out, the adjective "free" implies real choice and control for data subjects (see EDPB Guidelines 5/2020, paragraph 13). The same paragraph specifies, inter alia, that consent cannot be considered freely given if, on the one hand, the data subject feels compelled to consent or will endure significant negative consequences in case he or she refuses to consent, and, on the other hand, consent is presented as a non-negotiable part of terms and conditions.

[51] Paragraph 143.

that are not necessary for the performance of the contract itself, must be taken into due account[52]. Finally, according to the first paragraph of the same provision, where processing is based on consent, it is the controller who bears the burden of demonstrating that the data subject has specifically consented to the processing of personal data.

In light of this – briefly recalled – normative framework, the CJEU observes that the fact that the operator of an online social network holds a dominant position does not *per se* prevent users from validly giving their consent to the processing activities of their personal data carried out by that operator[53]. Nonetheless, such circumstance undoubtedly bears significant consequences in terms of the possible existence of an imbalance favoring the latter, since the former's freedom of choice might be affected by a limitation, if not a complete impairment, of the possibility to freely refuse or withdraw consent[54].

Although the point is among the ones requiring further verification by the referring court, the CJEU finds that the controversial data processing activities at issue in the case do not appear to be «strictly necessary for the performance of the contract between Meta Platforms Ireland and the users of the social network Facebook»[55]. This is especially evident for the processing of off-Facebook data, but the same applies to other data processing operations, with reference to which users – according to applicable EU law, as interpreted by the Court – must be free to express individual refusals, instead of being obliged to refrain entirely from using the service[56].

Conclusively, the Court affirms that, although holding a dominant position does not automatically vitiate users' manifestations of consent to data processing activities, this aspect is nevertheless «an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for the operator to prove»[57].

---

[52] Paragraph 145.
[53] Paragraph 147.
[54] Paragraphs 148-149.
[55] *Id*.
[56] Paragraphs 150-151.
[57] Paragraph 154.

### 4. The missing steps: looking for administrative cooperation procedures

The previous paragraphs have illustrated the answers provided by the Court, which, as anticipated at the outset, address in a complementary – instead of opposing – perspective, fundamental issues of coordination that affect the interplay between competition law and data protection law both at the normative and at the enforcement level. The latter aspect, which can be more precisely framed in terms of administrative cooperation, is however thorny[58], raising questions that exceed the scope of the interpretative ones referred to the Court, but which complement them; they ought therefore to be addressed here for the sake of completeness.

Differently from issues of administrative enforcement and cooperation that are encompassed within one single regulatory domain, the interaction and coordination among enforcement authorities operating in distinct sectors have been to a significant extent neglected by EU law and scholarship[59]. This represents a direct consequence of the traditional "vertical silos" normative approach based on the separateness of the various domains we

---

[58] The view that this aspect represents a possible point of weakness of the judgement is shared by I. Graef, Meta platforms: *How the CJEU leaves competition and data protection authorities with an assignment, Maastricht J. Eur. Comp. L.* 1, Online First, (2023) especially 9-10, observing that while the Court opens the door for establishing further synergies between the two legal domains, it also leaves competition and data protection authorities with an assignment to coordinate their respective competences and interpretations of the law.

[59] EU law and scholarship, in fact, devote far greater attention to the latter aspect, and this emerges as well from the judgment of the Court when focusing on enforcement mechanisms and their coordination as envisioned by the GDPR and Regulation 1/2003 (see *supra* notes …). For an exception see P. Larouche, A. De Streel, *Interplay between the New Competition Tool and Sector-Specific Regulation in the EU: expert study* (2020). More generally, on the topic of the enforcement of EU law see M. Scholten (ed.), *Research Handbook on the Enforcement of EU Law* (2023); S. Montaldo, F. Costamagna, A. Miglio (eds.), *EU Law Enforcement: The Evolution of Sanctioning Powers* (2021); M. Maggetti, F. Di Mascio, A. Natalini (eds.), *Handbook of Regulatory Authorities* (2022). See for instance the coordinated enforcement action on the role of data protection officers https://edps.europa.eu/press-publications/press-news/press-releases/2023/coordinated-enforcement-action-role-data-protection-officers-0_en.

have referred to at an earlier stage, and, in turn, it weakens enforcement[60].

At the Member State level, such issues have instead been taken into some consideration by legal scholars whom, with regard to independent administrative authorities, have expounded the topic of their potentially overlapping competences[61]. That scholarship, however, mostly concerned the interactions and possible conflicts among either sector specific authorities (such as for instance financial market authorities and communications authorities) or between one of the latter and an authority provided with general competence, *i.e* mainly the national competition authority[62]. Relationships among authorities provided with general competences (such as data protection and competition ones, as in the case at issue) remained instead significantly understudied also at the national level[63].

---

[60] See *supra,* Paragraph 3.1, especially note 35 and accompanying text.

[61] See for instance, in the Italian literature, S. Cassese, *L'Autorità garante della concorrenza e del mercato nel "sistema" delle autorità indipendenti*, 1 *Giorn. dir. amm.* 1 (2011); G. della Cananea, *Complementarità e competizione per le autorità indipendenti*, in C. Rabitti Bedogni, P. Barucci (Eds.), *20 anni di antitrust. L'evoluzione dell'Autorità garante della Concorrenza e del Mercato*, Vol. I, (2010), 309, especially 315. M. Clarich, *Le competenze delle autorità indipendenti in materia di pratiche commerciali scorrette,* in *Giur. comm.*, 2010, 5, 688 ss. For more general contributions on the topic, in the Italian literature, see S. Cassese, C. Franchini, *I garanti delle regole* (1996); F. Merusi, *Democrazia e autorità indipendenti* (2000); A. La Spina, G. Majone, *Lo Stato regolatore* (2000); G. Tesauro, M D'Alberti, *Regolazione e concorrenza* (2000); M. Clarich, *Autorità indipendenti. Bilancio e prospettive di un modello* (2005); M. D'Alberti, A. Pajno (eds.), *Arbitri dei mercati. Le autorità indipendenti e l'economia* (2010).

[62] On the topic see N.W. Averitt, R.H. Lande, *Using the "consumer choice" approach to antitrust law*, 74 *Antitrust L.J.* 175 (2007) and, in the Italian literature: F. Cintioli, *La sovrapposizione di competenze delle autorità indipendenti nelle pratiche commerciali scorrette e le sue cause (dopo gli interventi dell'Adunanza plenaria del 2012 e del 2016)*, in Vv. Aa., *Scritti in onore di Ernesto Sticchi Damiani* (2018), 199; L. Lorenzoni, *Il riparto di competenze tra Autorità Indipendenti nella repressione delle pratiche commerciali scorrette*, 1 *Riv. It. Antitrust* 83 (2015); L. Torchia, *Una questione di competenza: la tutela del consumatore fra disciplina generale e discipline di settore*, 10 *Giorn. dir. amm.* 953 (2012); L. Arnaudo, *Concorrenza tra autorità indipendenti. Notarelle bizzarre intorno ad un parere del Consiglio di Stato*, 6 *Giur. comm*. 916 (2010).

[63] For a recent exception see P. Manzini, *Antitrust e privacy: la strana coppia,* in P. Manzini (ed.), *I confini dell'antitrust. Diseguaglianze sociali, diritti individuali, concorrenza* (2023), 123 ff.

The judgment of the CJEU addresses this gap in EU law[64], offering an answer that is based on the complementarity of the functions entrusted to competition authorities and data protection ones, and on the coordination of enforcement actions. As we have seen, on the one hand, this answer entails that, competition authorities can ascertain GDPR violations within their inquiries, as long as they coordinate their action with the competent data protection authorities (see Paragraph 3.1); on the other hand, the solution envisioned by the Court makes it clear that violations of competition rules (such as abuses of dominant positions) complement the normative framework according to which data protection authorities exercise their functions (see Paragraph 3.2).

The Court of Justice's affirmation of the duty to cooperate, which functionally stems from the need to ensure a coordinated enforcement of EU sectoral rules and normatively derives from the general principle enshrined in article 4(3) TEU, is indeed a step forward in addressing some of the most urgent problems affecting the legal regime of online platforms in the digital economy[65]. Nonetheless, both history and practice suggest that cooperation between administrative authorities, which are institutional actors operating within complex systems[66], is better ensured within

[64] Previous caselaw of the CJEU mainly addressed the issue of contrasts, rather than coordination, and interpreted contrasts among authorities in a narrow way. See for instance Court of Justice, Second Chamber, 13th September, 2018, *AGCM v. Wind Tre,* in the case C-54/17, where it established that issues of competences typically arise in case of «conflict» between applicable provisions, a term which «refers to the relationship between the provisions in question which goes beyond a mere disparity or simple difference, showing a divergence which cannot be overcome by a unifying formula enabling both situations to exist alongside each other without the need to bring them to an end» (Paragraph 60).

[65] In this sense, the envisioned cooperation might represent a successful strategy of «coalition capacity» among administrative authorities; the expression is borrowed from G. Napolitano, *Conflicts and strategies in administrative law,* 12 *Int'l J. Const. L.* 357 (2014), at 366.

[66] The expression is borrowed from G. della Cananea, *Complexity and Public Authorities. A View from Italy,* in M. De Donno, F. Di Lascio (eds.), *Public Authorities and Complexity. An Italian Overview* (2023), XI.

procedures whose requirements and terms are established by written law[67].

Several gaps and practical uncertainties affect the CJEU judgment's effective implementation under this point of view. Just to mention the most evident issues, that is the case of: the conditions upon which the duty to initiate a cooperation becomes stringent in a given case; the form and time of consultations and information exchanges; the mandatory (or non-mandatory) nature of the obligation to wait for a reply; the binding or non-binding force carried by the competent authority's opinion; the possible avocation of the case by one authority and the establishment of conjunct enforcement actions.

Filling these gaps is indeed a complex task and it has a bearing on delicate institutional balances; it would be therefore unthinkable to even attempt an answer in the present article. What can be nonetheless observed here is that sharp-edged solutions seem utterly unfit for addressing these issues: a chronological or first-arrived-first-served criterion of coordination, the simple interchangeability of data protection and competition authorities, as well as a – highly improbable – fusion of the two, are all options that seem both normatively untenable and practically unworkable.

Finally, in addition to the uncertainties of procedural nature affecting the coordination duty affirmed by the CJEU, the solution envisioned in the judgment also raises concerns of a more general and systemic nature, impinging upon the principle of legal certainty and on the coherence of the legal system. Under this latter point of view, it cannot for instance be excluded that, based on the solutions adopted following the CJEU's judgment, a company might first be found – incidentally – not in violation of the GDPR by the inquiring competition authority, then persist in its – putatively legitimate – data processing practices, but finally be found at a later stage nonetheless in violation of data protection rules by the competent authority. The proceeding authorities' efforts of coordination envisioned by the CJEU's judgment could of course prevent the occurrence of this kind of situations and, especially, of their inconsistent outcome. However, both the aforementioned procedural uncertainties and the inapplicability in

[67] See on the topic J. Freeman, J. Rossi, *Agency Coordination in Shared Regulatory Space,* 125(5) *Harv. L. Rev.* 1131 (2012), and F. Cortese, *Il coordinamento amministrativo. Dinamiche e interpretazioni* (2012), especially 135 ff.

these matters of a *ne bis in idem* principle, do not ensure that this case constitutes a mere hypothetical, representing – rather – a risk.

Antinomies and incoherencies are of course not a novelty to our legal systems, but they can be nonetheless exacerbated by the normative and enforcement conundrums that characterize the regulation of the digital economy. When multiple authorities, tasked with distinctive competences and pursuing different objectives, apply the same normative framework but reach conflicting outcomes, a *vulnus* is clearly inflicted to the legal system's coherence (as well as to citizens and enterprises' legitimate expectations).

That is why the solution envisaged by the CJEU, while representing a fundamental step towards the right direction, must be followed by further steps of the legislators (both European and of the Member States) and of national administrations, that will need to give form, procedure, and substance to administrative cooperation.

## 5. The complex way forward

Current European Union law developments interact in different ways with the principles established in the commented judgment: in part they represent complementary steps in the direction envisioned by the Court of Justice; in part they pose further challenges at the enforcement level. By mentioning recent EU law, reference goes here, in particular, to the regulations composing the EU Digital Services Package (*i.e.* the Digital Markets Act and the Digital Services Act, hereinafter DMA and DSA) [68] and to the draft regulations on artificial intelligence (hereinafter AI Act)[69] and data (hereinafter Data Act)[70].

---

[68] 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 (DMA) and Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (DSA). See on the topic A. Manganelli, A. Nicita, *Regulating Digital Markets. The European Approach* (2022).

[69] European Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence, COM(2020)842 final. On the topic see G. Resta, *Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale?,* 2 *Dir. informaz. e informatica* 323 (2022) and B. Marchetti, L. Parona, *La regolazione dell'intelligenza*

Especially the DMA seems to be built upon the same principles established by the Court – or *vice versa*, considered that the judgment was issued after the entry into force of the DMA[71]. The key provision under this perspective is represented by Article 5(2), according to which gatekeepers (among which Meta is included, being therefore subject to the supervision of the European Commission[72]) shall not «(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» unless the user has been presented with the specific choice and has given consent. Such requirements are instrumental both to competition, aiming at ensuring that gatekeepers «do not unfairly undermine the contestability of core

*artificiale: Stati Uniti e Unione europea alla ricerca di un equilibrio,* in *DPCE Online,* Monographic Issue, 236 (2022) and the literature there cited.

[70] European Commission Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on the fair access to and use of data, COM(2022)68 final.

[71] Although there is no express reference to this in the reasoning of the judgment, it is possible to argue that the Court interpreted the normative framework applicable to the controversy in light of the principles established by the DMA (we shall recall that the DMA entered into force 1st November 2022, the judgment was issued on 4th July 2023, and the facts of the controversy date back to February 2019). On the DMA see A.C. Witt, *The Digital Markets Act – Regulating the Wild West,* 60 *Comm. Mrkt. L. Rev.* 625 (2023).

[72] Gatekeepers are undertakings providing core platform services (according to Article 2) designated as such by the European Commission under the procedure individuated by Article 3. On 6th September 2023 the Commission qualified Meta among the gatekeepers (together with Alphabet, Amazon, Apple, ByteDance and Microsoft). The qualification in terms of gatekeeper is subject to periodical revision (at least every two years) and gatekeepers are required to comply with DMA's provisions within 6th May 2024.

platform services», and to a more effective protection of users' data[73].

This provision patently resonates with the principles established by the Court of Justice in relation to the need to «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 […] without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent»[74].

These commonalities are indeed welcome, in that they consolidate a complementary vision of the interplay between data protection and competition law in the digital economy. Some reasons of concern emerge, however, with regard to the interaction and coordination of the different enforcement competences established by these and other EU regulations and by national laws.

Both the DMA and the DSA bluntly address the issue by stating – as it is usually the case – that they apply «without prejudice» to other EU law rules[75]. Furthermore, some provisions of the DMA and of the DSA indeed encompass various forms of cooperation; nonetheless, on the one hand, they do not lay down detailed procedural rules, but rather establish a general duty to cooperate and to exchange information, and, on the other hand, they mainly follow a vertical silos approach, circumscribing cooperation among the national authorities competent for each sector[76].

These aspects *per se* deserve further attention[77]. They shall be, moreover, closely scrutinized in that they add a layer of complexity to enforcement competences: data protection and competition rules, as it is well known, are mainly enforced through *ex post* controls carried out either by national authorities or by the EU Commission and the EU Data Protection Board

[73] See Recital 36 of the DMA.

[74] *Id.*

[75] See respectively Article 1(6) of the DMA and Article 2(4) of the DSA.

[76] See respectively Recital 90 and Article 37 ff. of the DMA, Recitals 125-126 and Article 49 ff. of the DSA, and Article 23 of the proposed AI Act.

[77] For an early comment on some of these issues see J. Blockx, *The Expected Impact of the DMA on the Antitrust Enforcement of Unilateral Practices,* 14(6) *J. Eur. Comp. L. & Practice* 325 (2023)

(depending on the relevancy of the violation); the DMA and the DSA confer enforcement competences – to be exercised both through *ex ante* controls and *ex post* investigations – to the European Commission[78]; whereas, finally, national authorities will foreseeably represent the main enforcers of the AI Act.

The challenges posed by the digital economy, as exemplified by the controversy at issue in our case, call for considerable synergy efforts on part of the regulators and of the enforcing authorities; the outlined scenario, however, intuitively renders cooperation among such authorities complicated, both in theory and in practice. In light of the reasoning of the Court and of the analysis conducted in the previous Paragraphs, the way forward indeed needs to be represented by stronger administrative cooperation; such way, though, is steep and paved with obstacles.

[78] The DMA, in particular, is enforced by the European Commission, with national authorities being only allowed to initiate investigations into potential infringements and then having to pass information to the Commission according to Article 38(7) and recital 91 of the DMA. On the topic see A.C. Witt, *The Digital Markets Act – Regulating the Wild West,* cited at 71, 643 ff.