Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Juridico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

WHAT "DATA" REALLY ARE IN THE DIGITAL MARKET. SOME REFLECTIONS ON THEIR RELEVANCE AND VALUE UNDER EU LAW

FRANCESCO BATTAGLIA*

1. *Introduction*

The importance of data in the digital ecosystem is well known. Indeed, for a long time, before the digital economy was so dominant, data was described as a form of new oil[1]. At the same time, scholars are discussing the negative impact that such a data-centred economic model may have on the protection of fundamental freedoms, in particular the

* Associate Professor of European Law, University of Rome "La Sapienza".

[1] The expression "data is the new oil" is commonly attributed to mathematician Clive Humby, who first used it in 2006. However, it has been increasingly revived after *The Economist* magazine published an article in March 2017 entitled *The world's most valuable resource is no longer oil, but data* (available online at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data). It was also said that the processing of data produces negative effects comparable to those of the greenhouse effect caused by the use of oil. In particular, it was affirmed that «oil pollutes in two main ways. It spills, and thus defaces beaches, coastlines and waters. It also produces carbon emissions and contributes to the greenhouse effect and climate change. Big Data creates similar injuries to privacy. Like oil, it spills over. Data security breaches - such as the one at Target in 2013, during the Thanksgiving and Christmas shopping season, in which hackers gained access to some 70-110 million customer names, credit and debit card numbers, expiration dates and security codes11 - cause widespread damage, just as oil spills create widespread damage. The impact of Big Data on privacy is similar to that of carbon emissions and climate change. Burning oil contributes to a growing layer of greenhouse gases that traps the sun's heat, causes climate change and makes the physical environment less hospitable to humans and other life forms» (D.D. HIRSCH, *The Glass House Effect: Big Data, The New Oil, and the Power of Analogy*, in *Maine Law Review*, 2014, p. 375).

protection of personal data and the right to privacy[2]. From this point of view, it has been stressed that it is necessary to verify that the fully automated reconstruction of the individual personality, even in its evaluative and predictive aspects, respects the legal value of the human person and the formal principle of its protection. In other words, to define the conditions for the legitimacy of the intrusion into the legal sphere of the individual carried out through the processing of data concerning him or her[3]. Indeed, this is precisely the perspective the EU legislator is trying to take. The aim is not only to create a stricter legal framework for online platforms through instruments such as the Digital Services Act (DSA), the Digital Market Acts (DMA) and the Regulation on Artificial Intelligence (AI Act), but also to identify a core set of fundamental rights tailored to the digital person[4].

However, any analysis of the importance of data in the digital market must take into account that its exploitation has become increasingly massive in recent years and that the systematic processing of data is now the main source of profit for online platforms. This means that the digital market is changing from a data-driven economic model to a true "data market". In this context, users, far from being empowered, have less and less control over their data, which increasingly threatens the protection of their fundamental rights.

Based on the above considerations, this article will focus on the relevance and value of data from an EU law perspective, taking into account the most recent legislation, practice and jurisprudence. To this end, a first consideration will be given to the definition of the legal framework under consideration, and it will be underlined that the "data market" has created a closer convergence among three different branches of EU law, such as data protection law, consumer law and competition law. These are therefore the three areas of EU law around which the analysis will be developed. In particular, with regard to data protection law, the article will analyse the legal basis for data processing in the light of recent initiatives by national authorities and the case law of the Court of Justice. On the other hand, from a competition law perspective, it will examine the role of data in establishing the existence of a dominant position, in particular in the light of the recent *Meta Platofrms* case. Finally, as regards consumer law, it will focus on the value of data and their process of monetization. The aim is to see whether the EU legal framework is evolving in a way that takes due account of the specificities of the digital market and whether recent legislation is able to effectively protect users' fundamental rights.

---

2 In this sense, since the 1970s it was emphasised that the right to privacy was closely linked to the possibility of controlling the activities of information gathering, the manner of its processing and the locations where it was collected. See S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

3 R. MESSINETTI, *La Privacy e il controllo dell'identità algoritmica*, in *Contratto e impresa*, 2021, pp. 150-151.

4 On the developmnet of fundamental digital rights, see A. ADINOLFI, *L'Unione europea dinnanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era della intelligenza artificiale*, Pisa, 2020, pp. 13-36; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Osservatorio europeo*, 2022, pp. 1-15; E. QUINN, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *Verfassungsblog*, 22 December 2022; L. CIANCI, *Dichiarazione europea sui diritti e principi digitali: quid pluris?* in *Diritto pubblico comparato ed europeo*, 2022, pp. 381-390.

2. *The interplay between data protection, competition law and consumer protection*

As mentioned above, the massive exploitation of data has led to a close convergence among some different areas of EU law, i.e. personal data protection, competition law and consumer protection. These areas also tend to overlap in some cases[5]. For this reason, it has been argued that an integrated approach, taking into account different regulatory perspectives, is needed to adequately address the challenges posed by the digital single market[6].

In this sense, already in 2014, the European Data Protection Supervisor (EDPS), in an opinion on privacy and competition in times of big data[7], noted that «EU approaches to data protection, competition and consumer protection share common goals, including the promotion of growth, innovation and the welfare of individual consumers»[8]. In this case, the EDPS emphasised that, in the digital world, certain competition issues, such as mergers between companies or the definition of a dominant position, cannot be separated from the assessment of their impact on data protection and, more generally, on consumer welfare. He therefore recommended closer cooperation between the competent authorities in the three different sectors.

Also in 2014, the relationship between the above disciplines arose when assessing Facebook's acquisition of WhatsApp[9] under Article 2 of Regulation 139/2004[10]. In the context of this procedure, the Commission considered that this acquisition would have led to a concentration of data, which is also relevant from a competition perspective, even if it considered that the transaction the Transaction did not give rise to serious doubts as to its compatibility with the internal market as regards the market for the provision of online advertising services, including its potential sub-segments. In fact, it stated that «regardless of whether the merged entity will start using WhatsApp user data to improve targeted advertising on Facebook's social network, there will continue to be a large amount of Internet user data that are valuable for advertising purposes and that are not within Facebook's exclusive control»[11]. However, the case had a further development in 2016, when WhatsApp changed its terms of use, adding the option to share user data with Facebook for profiling purposes for commercial and advertising purposes. As a result, the Commission fined Facebook 110 million EUR for allegedly

---

[5] W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, in *Journal of Intellectual Property Law & Practice*, 2016, pp. 856-866; 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 *The Antitrust Bulletin*, 2019, pp. 428-446; A. CORREA, *Digitalizzazione e profilazione degli utenti: la Corte di giustizia sul consenso informato e sulla responsabilità degli operatori online*, in *Osservatorio europeo*, 2020, pp. 1-17; M.C. BUITEN, *Exploitative abuses in digital markets: between competition law and data protection law*, in *Journal of Antitrust Enforcement*, 2021, pp. 270–288.

[6] W. KERBER, *Digital markets, data, and privacy*, cit., p. 857.

[7] EUROPEAN DATA PROTECTION SUPERVISOR, Privacy and competitiveness in the age of big data, 26 March 2014 (available online at https://edps.europa.eu/press-publications/press-news/press-releases/2014/privacy-and-competitiveness-age-big-data_en).

[8] On this issue see V. POZZATO, *2014 Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law*, in *Journal of European Competition Law & Practice*, 2014, pp. 468-470.

[9] European Commission, Case M.7217, *Facebook/ WhatsApp*, 3 October 2014, C(2014) 7239 final.

[10] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), in OJ L 024, 29 January 2004, pp. 1-2.

[11] European Commission, Case M.7217, cit., p. 34.

failing to comply with its obligation to provide accurate information under Regulation 139/2004[12].

At the national level, the Italian Competition and Market Authority (AGCM) investigated the same matter, but approached the issue from a consumer protection perspective, assuming that users' personal data has an economic value[13]. In particular, the AGCM found that WhatsApp had acted aggressively by inducing its users to accept the new terms of service in full, leading them to believe that it would otherwise have been impossible to continue using the application. In this way, the average consumer's freedom of choice or conduct was substantially limited, causing him to take a commercial decision that he would not have taken otherwise.

Finally, the EDPS also intervened in the Facebook/WhatsApp merger. In a 2016 opinion, it criticised the Commission for approving the merger in its capacity as the EU's competition authority without adequately considering the potential consequences for the protection of users' personal data[14]. The EDPS thus recommended closer cooperation between national responsible for competition, data protection and consumer protection authorities so that «in the case of future mergers of a similar nature, individuals might benefit from a more coherent response from [them]»[15]. In his opinion, in fact, «none of these regulatory jurisdictions is hermetically sealed from the others […] Even if they serve different goals […] privacy issues cannot be excluded from consideration under competition law simply by virtue of their nature»[16]. Similarly, the European Data Protection Board (EDPB) called the European Commission and the national authorities to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed[17].

Since the *Facebook/WhatsApp* case, the Commission often stressed the fact that the particular characteristics of digital markets tend to amplify the anticompetitive effects of even fringe acquisitions, in particular because of the advantages generated by data access. Thus, data accumulation issues, in the light of the interplay between competition law, data protection and consumer law has frequently been at the center of EU merger control policy. For example, the investigation on Shazam's acquisition by Apple[18], where the Commission considered for the first time the market of licensing data, was essentially about the negative impact of the acquisition in the light of the dataset possessed by

[12] European Commission, *Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover*, 18 May 2017 (available online at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369).
[13] The investigation and the decision of the AGCM is available at the following lonks: https://www.agcm.it/dotcmsDOC/allegati-news/PS10601_scorrsanz_omi.pdf; su https://www.agcm.it/dotcmsDOC/allegati-news/CV154_vessestratto_omi.pdf.
[14] European Data Protection Supervisor, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 September 2016 (available online here: https://edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf).
[15] *Ibidem*, p. 10.
[16] *Ibidem*.
[17] Statement of the EDPB on the data protection impacts of economic concentration, available here: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_en.pdf.
[18] European Commission, Case M.8788, *Apple/Shazam*, 6 September 2028, C(2018) 5748 final.

Shazam[19]. In several other cases, such as *Google/Fitbit*[20], *Microsoft/Activision*[21], *Booking/eTraveli*[22], *Amazon/iRobot*[23], the Commission has made similar evaluations, but it has rarely found that a transaction was likely to lead to a significant impediment to effective competition because of the potential horizontal effects arising from the combination of user databases and data collection capabilities.

Anyway, given the specificities of the digital market, the European Commission has changed its policy on referrals under Art. 22 of Regulation 139/2004[24] to allow for a more in-depth investigation of digital mergers[25]. In particular, the Commission has decided to revise its practice of refusing Art. 22 referrals where the referring national competition authority did not itself have jurisdiction to review the merger in question, which was based on the experience that such transactions were generally unlikely to have a significant impact on the Single Market. The new policy, in fact, underlines that «market developments have resulted in a gradual increase of concentrations involving firms that play or may develop into playing a significant competitive role on the market(s) at stake despite generating little or no turnover at the moment of the concentration. These developments appear particularly significant in the digital economy, where services regularly launch with the aim of building up a significant user base and/or commercially valuable data inventories, before seeking to monetize the business»[26]. This approach may raise some problems of legal certainty in relation to the different criteria and concepts determining the scope of the merger control rules in force in the Member States, which could lead to uncertainty as to which concentrations fall within the scope. However, the Court of First Instance accepted the Commission's new policy, stating that it was not clear how legal certainty could be increased by applying the previous approach [27].

The European legislator's implementation of the European Commission's new policy is evident in some provisions of the *Digital Markets Act* (DMA)[28]. In particular, in order to strengthen the Commission's control, Art. 14 DMA provides that gatekeepers must notify the Commission of any proposed acquisition, even below the merger

[19] However, the Commission stated that considering that other companies, notably digital music distributors, possessed more significant data covering music consumption patterns than Shazam, the Commission argued that none of the music charts data sets offered in the market, including the data sets offered by Shazam or Apple, was considered "unique" or, in any event, of any particular value compared with other data available on the market.
[20] European Commission, Case M.9660, *Google/Fitbit*, 17 December 2020.
[21] European Commission, Case M.10646, *Microsoft/Activision Blizzard*, 15 May 2023.
[22] European Commission, Case M.10615, *Booking Holdings/Etraveli Group*, 25 September 2023.
[23] European Commission, Case M.10920, *Amazon/Irobot*, 29 January 2024.
[24] Art. 22 of Regulation 139/2004 states that: «One or more Member States may request the Commission to examine any concentration as defined in Article 3 that does not have a Community dimension within the meaning of Article 1 but affects trade between Member States and threatens to significantly affect competition within the territory of the Member State or States making the request».
[25] Communication from the Commission, Guidance on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases, in *OJ* C 113, 31 March 2021, pp. 1-6.
[26] *Ibidem*, par. 9.
[27] Judgment of the General Court (Third Chamber, Extended Composition) of 13 July 2022, *Illumina, Inc.* v *European Commission*, case T-227/21, ECLI:EU:T:2022:447. See P. CALLOL, *Merger control beyond merger thresholds and the multiplication of ex ante merger notification obligations: Illumina Inc v European Commission*, in *European Competition Law Review*, 2023, pp. 117-126.
[28] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), in *OJ* L 265, 12 October 2022, pp. 1-66.

notification threshold provided for in Regulation 139/2004, if the merging entities or the target of the concentration provide core platform services or other services in the digital sector or enable the collection of data. Furthermore, Art. 18 of the DMA provides that where a gatekeeper has systematically failed to comply with the DMA, the Commission may adopt an implementing measure imposing on that gatekeeper any behavioral or structural remedies that are proportionate and necessary to ensure effective compliance with the DMA. Such remedies may include, for a limited period, prohibiting the gatekeeper from entering into a concentration in relation to the core platform services or other services provided in the digital sector or from enabling the collection of data affected by the systematic non-compliance. The DMA thus established a legal framework that makes digital concentration more cautious, strengthening the Commission's control over its possible anti-competitive effects.

The above-mentioned provisions are not the only ones in the DMA dealing with how data and competition interact. Indeed, the DMA contains other more specific provisions on this point, imposing both obligations (DOs) and prohibitions (DON'Ts)[29]. In particular, Art. 5, par. 2. states that the gatekeeper shall not do any of the following actions: *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. Furthermore, Art. 6, par. 2, states that the gatekeeper shall not use, in competition with business users, any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users. Finally, Art. 7 DMA contains provisions on interoperability number-independent interpersonal communications services.

Of course, the existence of some overlap among the DMA, the GDPR and the other EU competition laws[30], raises doubts about the duplication of investigative and

[29] The literature on DMA is vast. *Ex multis*, see J.F. RODRÍGUEZ AYUSO, *Administrative Sanctioning Regime for Gatekeepers: Consequences for Non-Compliance with the Digital Markets Act / Regimen administrativo sancionador para los guardianes de acceso: consecuencias para el incumplimiento de la Digital Markets Act*, in *Revista digital de derecho administrativo*, 2024, pp. 329-356; G. COLANGELO, *The European Digital Markets Act and antitrust enforcement: a liaison dangereuse*, in *European Law Review*, 2022, pp. 597-621; A.C. WITT, *The Digital Markets Act: Regulating the Wild West*, in *Common Market LawRreview*, 2023, pp. 625-666; P. AKMAN, *Regulating competition in digital platform markets : a critical assessment of the framework and approach of the EU Digital Markets Act*, in *European Law Review*, 2022, pp. 85-114; A. ANDREANGELI, *The Digital Markets Act and the enforcement of EU competition law: some implications for the application of articles 101 and 102 TFEU in digital markets*, in *European Competition Law Review*, 2022, pp. 496-504; P. AKMAN, *Regulating competition in digital platform markets: A critical assessment of the framework and approach of the EU Digital Markets Act*, in *European Law Review*, 2022, pp. 85-114, P. LAROUCHE, A. DE STREEL, *The European Digital Markets Act : a revolution grounded on traditions*, in *Journal of European Competition Law & Practice*, 2021, pp. 542-560.

[30] Indeed, Competition law had already been used to target several practices by large online platforms, now falling within the DMA, in particular through the prohibition against abuse of dominance in Art. 102 TFEU. See, for example, European Commission, case AT.40462, *Amazon Marketplace*, 17 July 2019, which

sanctioning powers in the hands of different competent authorities, where similar offences fall within the scope of both the GDPR and the DMA, given the very general nature of the coordination clauses among such different regimes[31]. Within the Commission, the newly established AI Office can strengthen this coordination, given that its mandate includes carrying out its tasks, in particular issuing guidance, in a way that does not duplicate the activities of relevant bodies, offices and agencies of the Union under sectoral legislation[32].

The interaction between the legal regimes in question has even been underlined by the Court of Justice, notably in the case of *Facebook Ireland Limited*[33]. In this circumstance, Advocate General Jean Richard de La Tour stressed that the frequent and numerous interactions between the law relating to the protection of personal data, consumer law and competition law are frequent and numerous contribute to making the protection of personal data more effective[34]. Indeed, following this approach, the Court held in *Facebook Ireland Limited* that a possible overlap between the representative action provided for by Directive 2020/1828 and that provided for by Art. 80 of Regulation 2016/679 does not preclude consumer protection associations from taking action against infringements of the rights provided for by the GDPR through rules aimed at protecting consumers or combating unfair commercial practices, such as those provided for by Directive 2005/29 and Directive 2009/22. In other words, this decision, which has been considered revolutionary in terms of its implications for data and consumer protection, allows associations to protect the interests of consumers deriving from data protection legislation, even if their statutes do not grant them powers in the field of personal data

---

is about data combining. On this case, see. V.M.K. REVERDIN, *Abuse of Dominance in Digital Markets: Can Amazon's Collection and Use of Third-Party Sellers' Data Constitute an Abuse of a Dominant Position Under the Legal Standards Developed by the European Courts for Article 102 TFEU?*, in *Journal of European Competition Law & Practice*, 2021, pp. 181-199; T. KNAPSTAD, *Breakups of Digital Gatekeepers under the Digital Markets Act: Three Strikes and You're Out?*, in *Journal of European Competition Law & Practice*, 2023, pp. 394-409.

[31] See G. CONTALDI, *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, 2021, pp. 292-308. With regard to the sanction regime, the DMA only states that the Commision must always take into account fines imposed for identical facts under different legislation. In this sense, recital 86 DMA only affirms that the Commission and the relevant national authorities should coordinate their enforcement efforts in order to ensure that the principle of *ne bis in idem* is respected. Moreover, recital 90 states: «the coherent, effective and complementary enforcement of available legal instruments applied to gatekeepers requires cooperation and coordination between the Commission and national authorities within the remit of their competences. The Commission and national authorities should cooperate and coordinate their actions necessary for the enforcement of the available legal instruments applied to gatekeepers within the meaning of this Regulation and respect the principle of sincere cooperation laid down in Article 4 of the Treaty on European Union (TEU). It should be possible for the support from national authorities to the Commission to include providing the Commission with all necessary information in their possession or assisting the Commission, at its request, with the exercise of its powers so that the Commission is better able to carry out its duties under this Regulation».

[32] Commission decision establishing the European Artificial Intelligence Office, 24 January 2024, C(2024) 390 final.

[33] Judgment of the Court (Third Chamber) of 28 April 2022, Case C-319/20, *Meta Platforms Ireland Limited* v *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV*, ECLI:EU:C:2022:322.

[34] Opinion of Advocate general Richard De La Tour delivered on 2 December 2021, Case C-319/20, *Facebook Ireland Limited* v *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2021:979, par. 81.

protection, since the violation of rules on consumer protection or unfair commercial practices may well be linked to the violation of a rule on the protection of personal data.

Since Facebook Ireland Limited, the Court has identified complementarities and synergies between the three legal regimes in an increasing number of judgments, most recently in the Meta Platforms case of 2023, which is analyzed below[35]. These cases show how their interaction can be mutually reinforcing, even if some friction is possible because they are three different areas of law. For example, when it comes to access to data, competition law aims to open up markets by facilitating access to data, while the data protection regime is based on the need to maximise control over one's own data and thus limit its disclosure[36].

3. *Some developments in the legal basis for data processing*

Having discussed the overlap between the three systems, it is necessary to analyse the issue from the perspective of each discipline, to reach then a synthesis.

With regard to data protection, the main aspect to be considered when analysing the relevance and value of data in the context of the Digital Single Market is the lawfulness of the processing. On this point, leaving aside the much debated issue of consent[37], we will focus on an issue that has recently seen some interesting innovations in the light of the relationship between data protection and competition law: the legitimate interest.

This condition is regulated by Art. 6, par. 1, lett f), GDPR, which states that «processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child».

Legitimate interest is a very sensitive criterion because it has to be constantly balanced against the interests, rights and freedoms of the data subject. Indeed, three cumulative conditions for a legitimate interest must meet: first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence[38].

---

[35] Judgment of the Court (Grand Chamber) of 4 July 2023, Case C-252/21, *Meta Platforms and Others*, ECLI:EU:C:2023:537. On this point, see *infra* paragraph 4.

[36] P. NEBBIA, *The interaction of competition, consumer and data protection laws: a few comments inspired by the recent case law of the Court of Justice of the European Union*, in *ERA Forum*, 2023, p. 524.

[37] With regard to consent, we believe that this is the most critical element in the context of the Digital Single Market, as there is a clear imbalance between the data subject and the controller, and it is a significant factor to be taken into account when assessing whether users have freely given their consent. On this point, see F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023, pp. 286-300; C. KOOLEN, *Transparency and Consent in Data-Driven Smart Environments*, in *European Data Protection Law Review*, 2021, pp. 174-189; Y. POULLET, *Consentement et RGPD: des zones d'ombre!*, in *Droit de la consummation*, 2019, pp. 3-37.

[38] Judgment of the Court (Second Chamber) of 4 May 2017, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* v *Rīgas pašvaldības SIA "Rīgas satiksme"*, ECLI:EU:C:2017:336, point 28.

Legitimate interest has become the main legal basis used by social networks to process data for the purpose of displaying personalised advertising, especially following the decision of the Irish Data Protection Commission (IDPC) to exclude "contractual necessity" under Art. 6, par. 1, lett. b) GDPR, as a legal basis for this purpose.[39] However, this practice has already been the subject of decisions by both national data protection authorities and the Court of Justice.

In July 2022, the Italian authority issued an order against Tik Tok concerning its decision to change its privacy policy in order to use the legitimate interest of the owner, rather than the consent, as a legal basis for the processing of user data for direct marketing purposes[40]. The Authority considered such measure contrary to the e-Privacy Directive for several reasons, in particular because *a)* the legitimate interest pursued by the data controller and third parties (the advertising partners) was not clear; *b)* the privacy policy did not specify whether special categories of personal data were also processed; *c)* the explanation of the balancing test was too general and did not allow for an assessment of its compliance with the criteria set out in the case law of the Court of Justice.

Once again, the Italian authority addressed the legal basis for data processing in a case against OpenAI relating to its ChatGPT service. First, in March 2023, the authority ordered the platform to temporarily restrict the processing of Italian users' data until it complied with Italian and European privacy laws, as there appeared to be no legal basis to support the mass collection and processing of personal data to train the algorithms relied on by the platform.[41]. Susequently, in April 2023, the authority found possible to proceed with the reassessment of the circumstances underpinning the temporary limitation decision in the light of the willingness expressed by the company to put in place concrete measures to protect the rights and freedoms of users[42]. Among these measures, OpenAI should have changed the legal basis for the processing of users' personal data for the purpose of algorithmic training, by removing any reference to contract and relying on consent or legitimate interest as legal bases[43]. Finally, in January 2024 the authority opened a formal investigation against OpenAI because the available evidence pointed to the existence of breaches of the provisions contained in the GDPR.

The above-mentioned initiatives opened the debate on the lawfulness of processing data for personalised advertising, as they did not exclude the possibility of relying on a

[39] In May 2018, Meta Ireland had changed the terms of service for its Facebook and Instagram services. It also indicated that it was changing the legal basis for processing users' personal data, which had previously been based on consent, to rely on the contract legal basis for most of its processing operations, including personalised advertising. The IDPC found this behaviour contrary to the GDRP and, in two separate decisions, imposed a fine of 390 million euro on META (Decision Nos. IN-18-5-5 and IN-18-5-7, 31 December 2022).

[40] Garante per la protezione dei dati personali, Provision n. 9788429, 7 July 2022, n. 9788429. With regard to direct marketing, recital 47 GDPR states that «The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest». However, even in this case, the legitimate interest has to fulfil the three criteria mentioned above.

[41] Garante per la protezione dei dati personali, Provision n. 112, 30 March 2023.

[42] Garante per la protezione dei dati personali, Provision n. 114, 11 April 2023. Following this decision, the EDPS decided to launch a dedicated task force to foster cooperation and to exchange information on possible enforcement actions conducted by data protection authorities.

[43] Furthermore, it should have made available, on the Company's website, at least to users who are connected from Italy, an easily accessible tool by which to exercise their right to object to the processing of their own data as acquired when using the service for the purpose of training algorithms, where the legal basis chosen under point 5 above is the Company's legitimate interest.

legal basis other than consent, namely legitimate interest[44]. The latter is in fact more flexible than consent and is therefore preferred by platforms, but it provides a lower level of security for users because it is based on the principle of controller accountability. In fact, given the low propensity of online platforms to be transparent about their data processing activities, it is unlikely that a system based on data controller accountability can effectively safeguard the interest or the fundamental and freedoms of the data subject. At the same time, from the perspective of balancing the economic interests of the platform with the interests of the users, it is difficult to imagine a form of legitimate interest when data are collected on such a large scale and without precise indication of the sources used. After all, this approach seems to have been followed by the Court *Meta Platforms* with regard to personal data collected by social networks for the purpose of personalised advertising. In that circumstance, the Court ruled that the interests and fundamental rights of users override the interest of operators in personalised advertising, even though the services of an online social network are free of charge. Therefore, processing by that operator for such purposes cannot fall within the scope of Art. 6, par. 1, lett. f) of the GDPR[45]. In other words, the Court emphasised that platforms' interests cannot be considered legitimate if their behaviour gives rise to the feeling that users' private lives are being continuously monitored.

By this decision, the Court thus clarified an importanto point, namely that the legal basis for the processing of personal data must also be assessed in the light of its impact on users' privacy, taking into account that the protection of personal data and privacy are two rights that do not overlap under the Charter of Fundamental Rights. However, some issues remain unresolved, particularly regarding the effectiveness of consent, which cannot remain the golden rule for data processing as it has proven to be ineffective in the digital ecosystem[46]. In essence, without a discipline that truly empowers users to control their data and eliminates practices such as repeatedly requesting consent, upholding the principle of user self-determination will be difficult.

4. *Data and competition law in the recent case-law on abuse of a dominant position*

From a competition law perspective, the interplay between the disciplines involved raises some interesting questions about the role of data in determining a company's market position. This point is important not only to reflect on the value of data, but also on the quality of its processing. Indeed, as underlined by the Commission, in data-intensive digital markets characterised by increasing corporate concentration, the dominant player has little incentive to adopt a business model that enhances consumer privacy[47].

[44] See O. POLLICINO, G. DE GREGORIO, *European Data Protection and Social Media: The Quest for Consistency in the Internal Market*, in *medialaw.eu*, 6 February, 2023; O. POLLICINO, *Generative AI and the rediscovery of the legitimate interest clause* (available at https://iep.unibocconi.eu/generative-ai-and-rediscovery-legitimate-interest-clause); L. MEGALE, *Il Garante della Privacy contro ChatGPT: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione dei diritti?*, in *Giornale di diritto amministrativo*, 2023, pp. 403-413.
[45] Judgment of the Court (Grand Chamber) of 4 July 2023, Case C-252/21, cit., par. 117.
[46] O. POLLICINO, *Generative AI*, cit.
[47] European Commission, Case M.9660, cit., pp. 104-105.

The Court of Justice addressed this issue in June 2023 in the case concerning the policy used by Meta Platforms to collect and process data[48]. This ruling clarified some key elements of the interplay between the disciplines involved, as well as other related aspects, in particular the value of data in the digital market[49].

The Court pointed out that data have become a significant parameter of competition between undertakings in the digital economy. It follows that, in the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR[50]. Indeed, in view of the different objectives pursued by the rules established under Art. 102 TFEU and the those provided by the GDPR, where a national competition authority identifies an infringement of competition law in the context of the finding of an abuse of a dominant position, it does not replace the supervisory authorities. This approach is clearly in line with previous case where the Coturt stated that the breach of another area of EU or national law beyond competition law can be a factor in determining a violation of the competition rules as well[51].

In our opinion, even if this decision does not deeply analyze the substantive interactions between competition law and GDPR, it is aimed at a greater user protection. In this sense, keeping a strict separation between data protection and competition "would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union"[52], lowering users'

---

[48] Judgment of the Court of 4 July 2023, Case C-252/21, cit.

[49] The case originates from a decision of the Bundeskartellamt, which was then the subject of a court dispute, leading to a preliminary reference before the Court of Justice. In particular, the German Competition Authority, in February 2019, closed an investigation through which it had found that the data processing carried out by Facebook Ireland constituted an abuse of its dominant position on the social network market for private users in Germany, since, at the time of registration, Facebook required users to accept Terms of Use that authorised the *social network* to collect their data also from third-party sites, so-called *off-Facebook* data. On the same issue, the AGCM had already pronounced itself (measure no. 27432 of 29 November 2018 and measure no. 28562 of 9 February 2021), which, however, addressed the issue from the perspective of consumer protection. According to the Italian Authority, Facebook would have carried out an aggressive practice, having exercised undue influence on the consumers themselves, who would have been subjected, without express and prior consent, to the transmission and use for commercial purposes of data concerning them. I. GRAEF, *Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment*, in *Maastricht Journal of European and Comparative Law*, 2023, pp. 325–334; M.C. BUITEN, *Exploitative abuses in digital markets: between competition law and data protection law*, in *Journal of Antitrust Enforcement*, 2021, pp. 270-288; M.-O. MACKENRODT, *Data Processing as an Abuse of Market Power in Multi-Sided Markets - The More Competition-Oriented Approach in the German Federal Supreme Court's Interim Decision KVR 69/19 - Facebook*, in *GRUR International,* 2021, pp. 562-570; M. MIDIRI, *Platforms and Data Power (Facebook Doesn't Pass the Rhine)*, in *Information and Computer Law*, 2021, pp. 111-136; 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 *The Antitrust Bulletin*, 2019, pp. 428-446; G. SCHNEIDE, *Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook*, in *Journal of European Competition Law & Practice*, 2018, pp. 213-225.

[50] Judgment of the Court of 4 July 2023, Case C-252/21, cit., par. 48.

[51] Judgment of the Court (First Chamber), 6 December 2012, Case C-457/10 P, *AstraZeneca AB and AstraZeneca plc* v. *European Commission*, ECLI:EU:C:2012:770; Judgment of the Court (First Chamber), 14 March 2013, Case C-32/11, *Allianz Hungária Biztosító Zrt. and Others* v. *Gazdasági Versenyhivatal*, ECLI:EU:C:2013:160.

[52] Judgment of the Court of 4 July 2023, Case C-252/21, cit., par. 51.

protection. Indeed, digital platform capitalism, precisely because of its data-driven nature, is structurally anti-competitive and it tends to create monopolies. Therefore, a rigid separation between data protection and competition law would weaken consumer protection.

In this context, the judgment does not create any particular risk of overlapping competences between supervisory authorities, because it addresses the interactions between enforcers in a straightforward and consistent manner[53]. Essentially, following the model proposed by the advocate general[54], the Court established a cooperation mechanism based on the principle of sincere cooperation, where the national competition authority cannot depart from decisions issued by the competent national supervisory authority under the GDPR. Furthermore, when the national competition authority «doubts as to the scope of the assessment carried out by the competent national supervisory authority or the lead supervisory authority, where the conduct in question or similar conduct is, simultaneously, under examination by those authorities, or where, in the absence of investigation by those authorities, it takes the view that an undertaking's conduct is not consistent with the provisions of the GDPR, the national competition authority must consult and seek their cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment»[55].

The Meta judgment did not, however, resolve all questions about the relationship between the two areas of law. Firstly, as cited, it does not go in depth on the substantive interactions between competition law and GDPR, in particular where both sets of rules apply. Secondly, with regard to the cooperation between national authorities, more details should be provided to avoid an effective cooperation.

5. *The role of data in the first disputes on the application of the Digital Services Act and Digital Market Act*

The exploitation of data is at the center of the first disputes on the application of the DSA and the DMA pending before the Court of justice.

With regard to the DSA, our interest is to the referrals under Art. 263 TFEU submitted by Zalando and Amazon over their designation as Very Large Online Platforms (VLOP)[56]. Both referrals pursue the same objective but they have different approaches. Zalando contests the applicability of the DSA to itself and the lawfulness of Article 33, which is the legal basis of its designation as VLOP. Amazon, on the other hand, challenges the lawfulness of the obligations resulting from the designation, specifically Articles 38 and 39 of the DSA.

[53] See 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*, in *Journal of European Competition Law & Practice*, 2023, pp. 1-5.

[54] Opinion of advocate general Rantos delivered on 20 September 2022, Case C-252/21, *Meta Platforms and others*, ECLI:EU:C:2022:704.

[55] Judgment of the Court of 4 July 2023, Case C-252/21, cit., p. par. 58.

[56] Action brought on 27 June 2023, *Zalando* v. *Commission*, Case T-348/23; Action brought on 5 July 2023, *Amazon Services Europe* v. *Commission*, Case T-367/23.

As first plea, Zalando argues that the DSA is not applicable to it, as it is already not an intermediary service and consequently neither a hosting service nor an online platform within the meaning of the DSA. However, such a position does not seem appropriate, because Zalando sells both its own products and those partners. By the way, it is worth noting that the jurisprudence of the Court on the qualification of such services is not uniform, as showed by the cases of *UberPop*[57] and *Airbnb*[58]. Thus, the judgement could be the occasion to clarify aspects where the legislation is lacking, and the case-law is not always coherent. As a second plea, intead, Zalando affirms that, even if part of the service qualifies as an online platform, it does not reach the threshold of 45 million monthly active users, for the calculation of which the DSA does not set out any specific criteria, referring to following delegated acts. Indeed, a comparison between the DSA and the DMA shows that the latter is partly based on the same threshold, but it specifies the calculation criteria in detail in a separate annex. On this point, a recent document published by the Commission clarifies that the average monthly active recipients of the service in the Union must be calculated in accordance with the delegated acts that it can adopt under Art. 33, par. 3 of the DSA. This document therefore indicates that the Commission will address this issue in the near future. However, in the absence of such a delegated act, Art. 33 of the DSA applies[59].

Differently to Zalando, as mentioned above, Amazon has not challenged the act by which the Commission designated it as a VLOP, but rather the effects that such a designation entails, namely those under Articles 38 and 39 of the DSA, which are about recommender systems and advertising transparency. As regards Art. 38, which States that VLOP that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling, Amazon argues that such a provision is detrimental also to users. In its view, in fact, without the ability to customise, it would face significant hurdles in meeting customer expectations, which would undermine the core function of marketplaces to facilitate transactions and result in a poor shopping experience for customers using the opt-out. The effect would be that «many customers who opt out will not be fully aware of the consequences and the impact of such a decision. Those customers, [state Amazon], will not link a subsequent bad shopping experience to their previous decision to opt out from recommender systems. Instead, they will assume that that negative shopping experience reflects a general deficiency on the part of the applicant. As a result, those customers might not opt back in for recommender systems at a later stage and will reduce their use of the Amazon Store. The resulting loss of market share would, according to [Amazon], be irreparable. Customers who have stopped using an online retailer or an online marketplace because of a negative shopping experience will be unlikely to return to those services»[60]. In other words, according to this theory, the user would tend to unknowingly refuse the processing of his personal data for profiling purposes, which would lead to negative

[57] Judgment of the Court (Grand Chamber) of 20 December 2017, Case C-434/15, *Asociación Profesional Elite Taxi* v. *Uber Systems Spain*, ECLI:EU:C:2017:981.
[58] Judgment of the Court (Grand Chamber) of 19 December 2019, Case C-390/18, *Criminal proceedings against X*, ECLI:EU:C:2019:1112.
[59] Questions and Answers on identification and counting of active recipients of the service under the Digital Services Act, available online here: https://digital-strategy.ec.europa.eu/it/library/dsa-guidance-requirement-publish-user-numbers.
[60] Order of the President of the General Court of 27 September 2023, Case T-367/23 R, *Amazon Services Europe Sàrl* v. *European Commission*, ECLI:EU:T:2023:589, parr. 30-31.

effects on the service used that he would not be able to attribute to his choice, but to an inefficiency of the platform. Such a theory seems to be developed around the idea of the "consumer unable to choose", who should have limited decision-making power because he is not able to understand the negative effects of his choices on his consumption experience. Such an argument, however, does not take into account that «the guiding principle at the basis of EU data protection law is that of a self-determined decision of an individual who is capable of making choices about the use and processing of his or her data»[61]. Hence, following the idea of users' self-determination, the President of the General Court, in the order dismissing the request of interim measures, rejected Amazon's argumentation and it stated that «there is nothing to prevent [Amazon] from taking precise and effective measures to inform its customers fully of the benefits of the recommender systems and the risks that will ensue from opting out of them so that they are fully aware of the consequences and the impact of their decision in the event of opting out. If [Amazon] were to take such measures, customers who have a negative experience after opting out would be aware that it was caused by that choice, and that they could reactivate the recommender system in order to restore the degree of satisfaction to which they were accustomed. It is therefore not certain that customers will reduce their use of the Amazon Store if they have the choice of opting out of the recommender system»[62].

With regard to Art. 39 of the DSA, instead, Amazon argues that the advertisement repository put in place pursuant to that provision reveals strategic and confidential information, such as campaign duration, campaign reach and targeting parameters, allowing competitors and the applicant's advertising partners to draw market insights on an ongoing basis, to the detriment of itself and its advertising partners. Such an obligation will, consequently, disrupt its current business relations with its advertising partners, which will make Amazon Store less attractive for advertisers and impose a significant implementation burden and ongoing costs[63].

It is therefore interesting to see how the Court will balance the users' interest in transparency with the economic interests of digital platforms. Indeed, it is clear that in the digital ecosystem it is essential to resolve the tension between the need to meet people's need for privacy and, on the other hand, the need not to disrupt an economic system based on the processing of personal data. It is a balance that the DSA has, to a certain extent, attempted to achieve, albeit not entirely satisfactorily. In this context, the two cases analysed are likely to be the first acts of a longer legal battle that online platforms, especially VLOP, will engage in in order to challenge and thus evade the

---

[61] Opinion of Advocate General Szpunar delivered on 4 March 2020, Case C-61/19, *Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, ECLI:EU:C:2020:158, par. 37.

[62] Order of the President of the General Court of 27 September 2023, Case T-367/23 R, cit. parr. 36-37.

[63] On this point, the President of the General Court, in the Order on interim provisions, stated that «a judgement ordering annulment would be rendered illusory and deprived of practical effect if the present application for interim measures were to be dismissed, since that dismissal would have the effect of allowing the immediate disclosure of the information at issue, thereby effectively prejudging the future decision in the main action, namely that the action for annulment would be dismissed», thus «the interest defended by the applicant must prevail over the interest in the dismissal of the application for interim measures, a fortiori where the grant of the interim measures requested amounts to no more than maintaining the status quo for a limited period» (Ibidem, parr. 82-83).

obligations arising from the DSA, which are likely to be much more burdensome than assumed when the legislation was adopted[64].

Similar considerations can be drawn by examining the first referral regarding the DMA, namely the application of Bytedance Ltd against the Commission Decision of 5 September 2023 designating it as a gatekeeper pursuant to Article 3 of the DMA. Also in this case, in fact, the applicant submits that its designation as a gatekeeper will cause it serious and irreparable harm since it provides strengthened transparency rules on data exploitation systems[65].

In particular, the applicant argues that Article 15 of DMA will require it, so far as concerns its product TikTok, to disclose detailed confidential information regarding its commercial strategy. In particular, It will have to publish detailed information concerning the way in which it profiles TikTok users that would go to the heart of TikTok's business in the European Union and would cause it significant competitive harm compared with a number of competitors which are not gatekeepers and none of which are required to disclose similar information. Actually, Article 15 of DMA only requires that the applicant *a)* has to submit to the Commission an independently audited description of any techniques for profiling of consumers that It applies to or across its core platform services, which will be transmitted to the European Data Protection Board (EDPB); *b)* shall make publicly available an overview of the above mentioned audited description, which will be prepared by the gatekeeper itself, taking account of the need to respect its business secrets.

Furthermore, Bytedance Ltd challenges the restrictions provided by Articles 5 and 6 of the DMA, in particular those regarding the combination and cross-use of personal data, laid down in Article 5, par. 2, of that regulation. The later, however, does not prohibit the combination and cross-use of the end user's personal data, but merely makes those actions subject to the prior consent of the user. Thus, also in this case, is clear the tension between the need, on the one hand, to foster transparency and user self-determination, and, on the other hand, the need of the platforms to maintain their core business which could be undermined giving free choices to users, because they will tend to refuse consent.

6. *Data as payment: the use of cookie paywalls*

In the perspective of the present analysis, a last relevant issue is that of the economic value assumed by data.

---

[64] It is worth noting that the Commission has already started an intensive monitoring and control activity based on the powers conferred on it by the DSA. For example, it has requested information from several companies, such as Meta, Tik Tok, X and Youtube, on the risk mitigation measures they have put in place under the DSA to deal with certain situations, such as the protection of minors or the dissemination of illegal or misleading content. These requests could lead to proceedings under Article 66 of the DSA, which provides that « The Commission may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 73 and 74 in respect of the relevant conduct by the provider of the very large online platform or of the very large online search engine that the Commission suspect of having infringed any of the provisions of this Regulation».

[65] Order of the President of the General Court of 9 February 2024, Case T-1077/23 R, *Bytedance Ltd* v. *European Commission*, ECLI:EU:T:2024:94.

It is well known that many digital services are provided free of charge, but in exchange, users are asked to consent to the collection and processing of their data. This has sparked a debate on the "monetization" of data, with two main arguments emerging. From a "person-oriented" perspective, some argue that it is not possible to make a contract for the exchange of personal data and services. This is because certain personal data cannot be negotiated without violating the dignity of the person. On the other hand, others argue that the significant value of personal data in market transactions cannot be ignored[66].

The debate on the value of data may be intensified by the growing use of cookie paywalls, which require users to authorize tracking via cookies or subscribe to gain access to the website. Essentially, it is an "consent or pay" model that is a consequence of operators' financial dependence on exploiting users data.

Indeed, this issue has already been addressed by several authorities in the Member States[67], which have questioned whether the "consent or pay" system complies with Article 7, par. 4, of the GDPR, which states that «when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract».

In general, such investigations concludes that payment may constitute an alternative to consent, provided that the fee requested as alternative to consent is reasonable and proportionate and that the other conditions set out in the GDPR are met, including the data protection impact assessments that must be carried out under its Article 35, par. 1[68].

Anyway, the definition of proportionate or reasonable payment through personal data is unclear, given that, as stated by the Directive 2019/770, personal data is a fundamental right and cannot be considered a commodity[69]. Moreover, it is worth noting that many online journals using cookie paywalls do not provide full access to the site's

---

[66] On the monetization of data, see S.-A. ELVY, *Paying for Privacy and the Personal Data Economy*, in *Columbia Law Review*, 2017, pp. 1369-14-60.

[67] See, for example, the analysis conducted by the Austrian Authority (available online at https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-vraag-ik-als-organisatie-toestemming-zonder-cookiewall-7112), as well as that of the Dutch Authority (https://autoriteitpersoonsgegevens.nl/nl /nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies). In France, on the other hand, the *Commission nationale de l'informatique et des libertés* (CNIL), had initially rejected the cookie wall practice in its entirety, as «les utilisateurs ne sont pas en mesure de refuser le recours à des traceurs sans subir des conséquences négatives» (délibération n. 2019-093 du 4 juillet 2019). However, after a ruling by the *Conseil d'Etat, in the* opinion of which the CNIL had «excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit souple' (Conseil d'Etat, no. 434684 du 19 June 2020, ECLI:FR:CECHR:2020:434684.20200619), the CNIL has adopted new guidelines in which it essentially recognises that the *consent-or-pay* mechanism may comply with the GDPR, provided that the alternative payment is within reasonable limits (CNIL délibération no. 2020-091 et no. 2020-092 du 17 septembre 2020).

[68] Art. 35, par. 1, states that «where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks».

[69] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, in OJ L 136, 22 May 2019, pp. 1-27.

content when users grant consent to process their personal data. After giving consent, in fact, they can only read the first few lines of the articles and must pay to view the full text. In other words, the cookie paywall is not an equivalent alternative to the subscription, which is the only way to access the full text. Instead, it seems to be a method of inducing users to accept data processing, despite the limited benefits in terms of service usage.

With regard to the use of cookie paywalls, a passage from the above-mentioned judgment in *Meta Platforms* is significant, in which the Court states that «users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations»[70]. However, the Court did not go further on this point, leaving the above questions unanswered. It thus remains to be seen whether the European legislator will be able to address this issue effectively when adopting the new e-Privacy Regulation. Actually, the text of the current draft does not contain any interesting novelty in this respect, as it just states that in the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements, while at the same time specifying that «consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment»[71]. Such a general provision was criticized also by the EDPS, who affirmed that «the Proposal lacks ambition with regard to the so-called 'tracking walls'»[72], also underlining that «tracking walls undermine the idea that consent must be freely given [because they» often oblige the user to consent to the use of third-party tracking cookies, which are unnecessary for the performance of the service concerned»[73].

7. *Data Governance Act: From a Data Driven Market to a Data Market*

The Data Governance Act (DGA), adopted in June 2022[74], introduces significant legal innovations regarding the mentioned issue of data value and the process of data monetization. According to the vice-president of the Italian Authority for the Protection

[70] Judgment of the Court of 4 July 2023, Case C-252/21, cit., par. 150.

[71] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final, recital 18.

[72] European Data Protection Supervisor, Opinion 6/2017, 24 April 2017, p. 10.

[73] *Ibidem*, p. 17.

[74] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), in *OJ* L 152, 3 Jube 2022, pp. 1.44.

of Personal Data[75], the DGA, along with the Data Act[76], represents the first attempt to establish rules on data monetization. In other words, it is a further step in the evolution of digital market, which is no longer just a 'data-driven market' but is now moving towards being also a 'data market'. Unlike the laws analysed here, the DGA does not aim to regulate the use of data in the digital market, but rather to establish legal guidelines for such a 'data market'. It also creates new entities that are expected to play a key role in the data economy, such as intermediaries.

Generally speaking, the DGA aims to improve conditions for data sharing in the internal market, particularly for reusing data held by public sector bodies. In particular, it lays down *a)* conditions for the re-use, within the Union, of certain categories of data held by public sector bodies; *b)* a notification and supervisory framework for the provision of data intermediation services; *c)* a framework for voluntary registration of entities which collect and process data made available for altruistic purposes; and *d)* a framework for the establishment of a European Data Innovation Board.

However, while such legislation may enhance data sharing among companies to prevent their concentration in a few large companies, the idea of establishing a 'data market' raises some legal complications, particularly in terms of upholding the principles enshrined in the GDPR. Indeed, the coordination between the GDPR and the DGA is not always straightforward. This is because the GDPR was not designed to act within a data market and also because the DGA provides much broader rules, since it applies to all data and not only to personal data. In this sense, for example, the DGA introduces new notions, such as 'data holder' and 'data user', which are not provided by the GDPR.

Namely, 'data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data. Such a notion is not clear enough, above all because it does not clarify the conditions under which data ownership can be recognised, since this is a less straightforward concept than the concept of data subject referred to in the GDPR[77]. On this point, the EDPB and the EDPS, through a joint opinion, affirmed that the definition of 'data holder' is not in line with the overarching principles of the GDPR, as well as with the letter of the GDPR. In this regard, they noted that «legal uncertainties may arise from the fact that the GDPR does not mention the data subject's right to grant access or to share his personal data with third parties and even less so an equivalent right for the legal person which seems possible to extrapolate from the definition of 'data holder'. Rather, the GDPR guarantees to every individual the right to the protection of personal data concerning him or her, which refers to a comprehensive set of rules for the processing

[75] It is available at the following link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9769786.

[76] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), in *OJ* L, 22 December 2023, pp. 1-71.

[77] See J. BALOUP; E. BAYAMLIOĞLU; A. BENMAYOR; C. DUCUING; L. DUTKIEWICZ; T. LALOVA-SPINKS; Y. MIADZVETSKAYA; B. PEETERS, *White Paper on the Data Gover- nance Act*, KU Leuven - Centre for IT & IP Law (CiTiP), Working Paper 2021.

of personal data that are binding for each entity processing the data (data controller/joint controller) or processing the data on behalf of the data controller (processor)»[78].

'Data user' is, instead, defined by the DGA as a natural or legal person who has lawful access to certain personal or non-personal data and has the right to use that data for commercial or non-commercial purposes. Also on this notion, the EDPB and the EDPS highlighted some legal ambiguity, in particular with regard to its interplay with the notions of controller, joint controller or processor under the GDPR.

By the way, regardless their legal uncertainty, the notions of 'data holder' and 'data user' represent a change in the EU's approach to data. Previous legislations on personal data, in fact, had never linked the concept of 'ownership' directly to data, but rather to the processing of data. This could lead to a more market-oriented approach to data that could weaken its human rights dimension.

8. *Conclusions*

Data is of growing importance in the Digital Single Market. This market is no longer just a 'data-driven market' but it is also evolving towards being a 'data market'. This is resulting in a closer interplay between data regulation, competition law and consumer protection.

On the one hand, as shown in *Meta Platforms*, data has clearly acquired an economic value. In this context, as emerged in the first disputes on the application of DSA and DMA, platforms consider data processing as an indispensable source of profit which, in their view, should not be subject to rigid provisions. On the other hand, however, it is also clear that a purely market-oriented approach undermines users' right and, in this sense, the current legislation is not able to effectively safeguard users' interests and to promote their digital self-determination.

In this context, the EU legislator has undertaken an extensively activity to promote greater integration between these branches of EU Law, including increased synergies among regulators. Such a legislative activity has introduced some significative innovations in the field of data, particularly through DMA, DSA, DGA and Data Act. However, this analysis has shown that several uncertainties remain, even because the European legislator not properly addressed the tension between the need to protect users' rights and the economic needs of companies. Such a tension has clearly emerged in the disputes in the disputes on the application of the DMA and the DSA, where the applicants have openly stated that users' freedom of choice may be in contrast with their business model, which cannot be implemented without data.

The analysis of cookie paywalls leads to similar considerations. In fact, as we have seen, this is a strategy where consent to data processing is not really an alternative to subscription, because consent often only gives access to part of the online content. One gets the impression that companies tend to collect both consent and subscriptions because they are different sources of income.

In this context, the legislative measures adopted by the EU represent a cautious intervention that only partially takes into account the specificities of the digital market.

[78] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 10 March 2021.

The European legislator seems to have prioritised market aspects, such as the circulation of data, over the protection of users. In this sense, the most recent proposals, such as the e-privacy regulation, which have not been analysed here, also seem to be moving in this direction.