Disruptive Business Models in Data-Driven Markets: Rethinking EU Competition Law through the Lens of Privacy

Beatrice Lupacchini[1*]

[1] Faculty of Law, Department of Law, University of Macerata, Macerata, Italy

[*]Corresponding author: b.lupacchini1@unimc.it

Abstract

This research highlights how the disruptive business models of digital platforms have altered the structure of digital markets and the very logic of competition, shifting the core value from price and output to data control and monetization. Against this background, the current EU competition law framework, largely grounded in the "more economic approach", consumer welfare, and allocative efficiency proves increasingly inadequate to address the systemic risks of data-driven markets. The paper advances an alternative framework in which personal data protection is recognized as a fully-fledged competitive parameter, shaping both service quality and consumer autonomy. This proposal is anchored in recent legal and regulatory developments: the Meta/Bundeskartellamt proceedings and the Court of Justice's case law, which acknowledge privacy as a relevant factor in competition analysis, as well as the ex ante obligations introduced by the Digital Markets Act. Together, these elements support a multidimensional vision of EU competition law, responsive to the challenges of the digital economy.

Research purpose:

Disruptive business models of digital platforms have reshaped market power and competition dynamics, exposing the limits of current EU antitrust law. This research proposes innovative solutions that integrate personal data protection as a competitive parameter, aiming to enhance market contestability and safeguard consumer through a multidimensional approach to competition law.

Research motivation:

The research stems from the recognition that traditional competition law tools are insufficient to address the disruptive transformations brought by digital platforms. By shifting competition from price and output to data control and user influence, these models demand a reassessment of how privacy protection can be integrated into antitrust analysis.

Research design, approach, and method:

The approach adopted is legal-comparative, with particular attention to European competition law and the framework on personal data protection. The research combines theoretical inquiry with case law analysis, focusing in particular on the Meta/Bundeskartellamt proceedings and the jurisprudence of the Court of Justice, as well as on the regulatory innovations introduced by the Digital Markets Act.

Main findings:

The analysis demonstrates that personal data today constitute an essential dimension of service quality and, consequently, a relevant parameter of competition. Privacy, traditionally confined to the domain of data protection law, emerges as a competitive variable directly affecting the welfare of the digital consumer. Recent jurisprudence of the Court of Justice and the ex ante regulation introduced by the Digital Markets Act confirm the necessity of a multidimensional conception of competition law, capable of incorporating non-economic values such as the protection of privacy.

Practical/managerial implications:

Recognizing privacy as a competitive parameter enables more effective repression of exploitative practices rooted in data appropriation and consumer harm, while ensuring a more accurate understanding of digital market dynamics. This approach represents an essential update of the antitrust enforcement toolkit, aligning it with the structural challenges of data-driven business models and reinforcing market contestability.

Keywords: Digital Markets Act (DMA), disruptive business models, European competition law, gatekeepers, privacy and protection of personal data

N. D. Nguyen and P. T. K. Ngoc (eds.), *Proceedings of the International Conference on Emerging Challenges: Business Dynamics in Disruptive Economy (ICECH 2025)*, Advances in Economics, Business and Management Research 377,
https://doi.org/10.2991/978-94-6239-622-7_25

1. INTRODUCTION

It is beyond dispute that the business models of digital platforms qualify as disruptive. In the original definition developed by Clayton Christensen (Christensen, 1997), disruption refers to the process through which an innovation, introduced by a firm initially operating at the margins of the market or targeting segments neglected by incumbents, progressively gains market share until it supplants established models and comes to dominate the market.

In the current context of digital markets, the phenomenon of disruption has undeniably assumed a structural dimension. Platforms such as Google, Apple, Meta, Microsoft, and Amazon (the so-called GAMMA) have implemented business models that not only generated new markets in which they secured enduring dominance, but also "reshaped" the very logic of competitive dynamics (OECD, 2015; Zuboff, 2019).

Unlike traditional offline markets, where competitive rivalry has historically centred on price and output, the digital economy derives its distinctive value from the capacity to gather, process, and monetise personal data. Such monetisation takes place both through the personalisation of advertising, such as the behavioural advertisement or microtargeting advertisement (OECD, 2020a) and through the training of artificial intelligence algorithms (OECD, 2024a). Personal data of users—which convey personal and even highly personal information, protected in the European union as fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights—have thus become the core of the transformation characterising the data-driven digital economy. In practice, the erosion of consumers' privacy, resulting from the systematic exploitation of such data for commercial purposes represent the "structural condition" for the profitability of these business models.

This profound disruptive transformation has compelled EU competition law to reconsider its instruments.

The analytical framework developed within the "more economic approach"—privileging consumer surplus, allocative efficiency, and price-oriented assessment—appears increasingly inadequate to address the realities of data-driven markets. Phenomena such as network effects, information asymmetries, lock-in strategies, and data concentration generate new forms of market power that fall outside the scope of traditional analytical tools (Crémer, De Montjoye & Schweitzer, 2019; Kerber, 2024). Moreover, the so-called model of apparent gratuity – under which users transfer their personal data in lieu of a monetary consideration—destabilises the very foundations of antitrust analysis, which was originally designed to operate within monetised markets (Akerlof, 1970; Costa-Cabral & Lynskey, 2017; Economides & Lianos, 2018). The harm to digital consumers under such—disruptive—business models does not manifest itself in higher prices or reduced output, but rather in diminished control over personal information, opaque consent mechanisms, dark patterns, and a general decline in privacy policy standards (Costa-Cabral & Lynskey, 2017; Deutscher, 2018; Stucke, 2022).

Although the issues at stake are of central importance, competition law has thus far been slow to integrate privacy into its analytical framework (European Data Protection Board, 2014; European Commission, 2018; Kerber, 2024). In this context, an urgent question arises: should privacy and data protection be conceptualised as dimensions of competition? And if so, in what manner?

While the European Union relies on the General Data Protection Regulation (EU) 2016/679, the so called "GDPR", (European Union, 2016), to ensure a robust safeguard of personal data, its application does not suffice in digital markets. The regulatory framework does not distinguish between dominant and non-dominant undertakings and fails to capture the competitive implications of data concentration (European Data Protection Board, 2014; European Data Protection Board, 2025). Competition law, for its part—conceived to address practices of dominance and exploitative conduct—has consistently excluded the protection of privacy from its analytical framework (Court of Justice of the European Union, 2006; European Commission, 2014, 2018, 2020).

The present contribution seeks to fill this gap by advancing the view that the protection of personal data should be recognised as a fully-fledged competitive parameter.

Framed as a dimension of service quality, privacy protection has a direct impact on the welfare of European consumers, and its diminution may constitute the benchmark for the activation of antitrust enforcement (Botta & Wiedemann, 2018; Lamadrid & Villiers, 2017; Deutscher, 2018).

From a methodological standpoint, this research adopts a legal-comparative approach, combining theoretical inquiry with the analysis of case law and regulatory innovation implemented by European Union. The case-studies examined include the German proceedings launched by the German competition authority (Bundeskartellamt) against Meta, concerning personal data processing practices (Bundeskartellamt, 2019; Oberlandesgericht Düsseldorf, 2019; Bundesgerichtshof, 2020), as well as the subsequent landmark judgment of the Court of Justice of the European Union delivered in preliminary ruling proceedings (Court of Justice of the European Union, 2023). In addition, the analysis considers the innovative scope of the recent European Digital Markets Act (European Union, 2022), which provides for specific regulation of the disruptive business models of gatekeeper platforms, emphasising the role of personal data processing in competitive dynamics. At the theoretical level, the study argues that European competition law should adopt a multidimensional approach, moving beyond the narrowly economic paradigm that has so far prevailed, in order to incorporate non-economic values such as personal data and privacy protection (Ezrachi, 2018; Lianos, 2018). At the practical level, the research proposes an analytical framework enabling competition authorities to integrate privacy considerations within the tools available for antitrust enforcement. Such an approach is necessary to ensure that competition law, while continuing to serve its essential function of safeguarding open and contestable digital markets, also adapts its instruments to address

the challenges generated by disruptive business models (Maggiolino, 2018; Whish & Bailey, 2024).
Although elaborated within the framework of European law, this theorisation may also prove valuable in comparative perspective. It offers an analytical framework capable of being transposed to other jurisdictions, given the global scope of the practices of major digital platforms (GAMMA) and the consequent need for a more uniform international response.

2. LITTERATURE REVIEW AND RESEARCH GAP

In academic discourse, the role of personal data and the relevance in competitive dynamics is far from novel. An expanding body of scholarship has emphasised how data have become the fundamental strategic asset of digital markets, often described as 'the new oil' or 'the new oxygen' of the digital economy (European Parliament, 2020). Contemporary data-driven business models rest upon mechanisms of extraction and monetisation, thereby generating what has been aptly described as a false gratuity: services are ostensibly offered free of charge, while in reality users 'pay' through the disclosure of their personal information (Meta, 2025). The disruptive business models of digital platforms benefit from dynamics that enable them to create and preserve dominance.
Network effects increase the attractiveness of a platform as the number of users grows, and the related phenomenon of lock-in prevents consumers from switching to alternative digital service providers (OECD, 2022a). These dynamics are compounded by high switching costs including both technical burdens and the loss of data or content uploaded onto a given platform, which significantly discourage users from turning to alternative providers (Kerber, 2024). Furthermore, profound informational asymmetries and the resulting imbalances of power arise between the contracting parties: on the one hand, consumers, as the weaker party, lack the necessary information regarding the processing and collection of their personal data; on the other hand, platforms, as the stronger party, exercise such power as to be able unilaterally to determine the conditions and terms of privacy. This situation undermines the ability of consumers to make genuinely free, autonomous, and informed choices (Akerlof, 1970; Kerber, 2024).
Taken together, these dynamics reduce the contestability of digital markets by discouraging the entry of new competitors—who face severe difficulties in attracting users—while simultaneously reinforcing the concentration of power in the hands of a small number of platforms (Costa-Cabral & Lynskey, 2017; Economides & Lianos, 2018).
Scholarly analysis has further noted that, in the digital economy, competition progressively shifts from competition within the market—namely, competition for users within a given segment—to competition for the market—namely, competition for dominance over entire market segments. This gives rise to 'winner-takes-all' dynamics, in which dominant firms succeed in exercising control over entire ecosystems and vast quantities of users' personal data (Geroski, 2003; Stucke, 2022).
These effects do not merely lead to an increase in the levels of market concentration, but also entail a qualitative transformation in the very nature of consumer choice. Users are not aware of the economic value of their personal data nor of the ways in which such data are processed by platforms. Indeed, platforms do not offer users the possibility to decide how much and which data to provide or to choose the specific modalities of processing; moreover, the terms and conditions of use and privacy policies are often lengthy and complex, to the point that an average consumer may not adequately understand them (Acquisti, Brandimarte & Loewenstein, 2015). From the perspective of the applicable legislation, the General Data Protection Regulation (European Union, 2016) has provided a solid framework for the protection of personal data, with provisions applying to all digital platforms (European Union, 2012, 2016); however, it proves insufficient to capture the competition dynamics related to personal data, which are issues that undeniably fall within the domain of competition law (EDPB, 2014, 2025).
Moreover, the relationship between data protection and competition law has attracted sustained scholarly attention. Costa-Cabral and Lynskey (2017) analyse the existing "family ties between" the two legal domain, whereas Economides and Lianos (2018) interpret privacy intrusions as a specific form of exploitation arising from market failures. The Report by Crémer, De Montjoye and Schweitzer (2019) further stressed the inadequacy of traditional antitrust tools in capturing these dynamics, advocating a fundamental reconsideration of enforcement strategies. More recent contributions, particularly those of Kerber (2024) and Stucke (2022), have drawn attention to the economic implications of data concentration, identifying it both as a structural barrier to entry and as a source of consumer harm.
Legal scholarship has therefore examined in depth the interaction between the two regulatory domains and the structural limitations of European competition law, highlighting its inability to incorporate dimensions other than purely economic ones. The centrality of personal data within competitive dynamics is by now well established; what is still lacking, however, is an explicit qualification of privacy as a parameter of competition.

3. DIGITAL MARKETS AND THE LIMITS OF COMPETITION LAW

EU competition law has historically been conceived as a framework designed to safeguard market structure and to remedy market failures, in line with the Ordoliberal tradition of the Freiburg School (Vanberg, 2018). However, in the 1990s, the pressures of globalization and the demand for a rational economic theory upon which to ground theories of harm and competitive assessment transformed EU antitrust into a discipline increasingly shaped by economics. This so-called "more economic approach" (Witt, 2018) shifted the analytical focus towards consumer welfare, understood in terms of consumer surplus, and allocative efficiency. Consequently, the core conceptual tools of EU competition law, such as the definition of the relevant market, the assessment of market power, and the analysis of competitive effects, were progressively framed in predominantly economic terms (Iacovides & Stylianou, 2024). While these categories have long

proved effective in interpreting traditional industrial markets, they appear increasingly ill-suited to data-driven digital markets, which function according to dynamics that escape the confines of classical economic models (OECD, 2018).

The notion of the relevant market has always constituted the analytical starting point for assessing the position of firms (European Commission, 2024a). It rests on the substitutability of products or services, identified through the behaviour of the average consumer in response to variations in price or essential product characteristics. In digital markets, however, this traditional approach loses much of its descriptive power. The price criterion, long relied upon as the benchmark for substitutability, is no longer pertinent where digital services are offered free of charge, or more precisely appear to be free. The counter-performance lies in the users' disclosure of personal data and the attention they devote to the platforms (Evans, 2020). It follows that market definition can no longer be confined to substitutable goods or services assessed in terms of price. It should instead take into account other elements that guide consumer choice.

Beyond innovation, a crucial factor is the volume of personal data collected by the platform and, consequently, the level of data protection offered through its privacy policies and terms and conditions, which cannot be readily captured in economic terms.

The nature of platform "power" that must be captured by competition law has also evolved. Market power has traditionally been defined as «*the ability of a firm to maintain prices above competitive levels for a significant period of time without losing customers to the extent that such a strategy becomes unprofitable*» (Whish & Bailey, 2024). In digital markets, however, market power does not necessarily manifest itself through the imposition of supra-competitive prices (OECD, 2022b). A more appropriate notion of digital market power should therefore build upon the definition articulated in the seminal *Hoffmann-La Roche* judgment: «*a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained in the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of consumers*» (Court of Justice of the European Union, 1979).

If one accepts the notion of "power" as the ability to produce effects on others by inducing them to conform to one's will without resorting to physical coercion (Maggiolino, 2018), it becomes clear how this concept materialises in digital markets. Platforms exercise this power to exclude rivals, thereby obstructing the development of effective competition. At the same time, they influence consumer choices and affect consumer welfare in a manner that goes beyond the mere parameter of price. This occurs through privacy notices that are insufficient or excessively complex, through mechanisms of consent collection and management that curtail genuine freedom of choice, and more broadly through practices that undermine the overall quality of the digital user experience (Kerber, 2024).

If consumer choices are not authentic, the very foundation of entrepreneurial merit collapses. Within the ordoliberal paradigm, consumers are regarded as the ultimate judges of market offers and are called upon to «*serve the market's own selective mechanism*» (Maggiolino, 2018). When they are manipulated, the proper functioning of competition is distorted. This reflects a fundamental shift: power is no longer exercised to raise prices, as in traditional markets, but rather to extract ever greater amounts of personal data, thereby appropriating from consumers a genuine informational surplus.

The inadequacy of traditional antitrust tools, primarily centred on price, becomes particularly evident when assessing the position of the digital consumer, who is exposed to forms of harm different from those ordinarily recognised in classical competition analysis. Although consumers appear formally free to choose among competing platforms, their autonomy is in practice severely constrained by structural factors. Network effects and lock-in mechanisms discourage users from switching to alternative providers: leaving a social network, for instance, entails the loss of one's network of contacts, uploaded content, and accumulated interactions over time (Crémer, De Montjoye & Schweitzer, 2019). This dynamic reduces the incentives for new entrants, aware of the difficulty of attracting a sufficient user base, and thereby strengthens dominant positions while closing markets (OECD, 2018).

To these barriers must be added profound informational asymmetries and a marked imbalance of power between the parties. Users are typically unaware both of the real economic value of the data they disclose and of the ways in which such data are exploited. The algorithmic logics underlying the collection, processing, and monetisation of information remain opaque and inaccessible, with the result that user choices are neither fully informed nor genuinely free (Costa-Cabral & Lynskey, 2017). In such circumstances, the classical notion of contractual freedom—an implicit premise of a properly functioning competitive market—loses its substance: genuine freedom of choice cannot exist without adequate and transparent information. These dynamics disprove the argument that consumers would continue to prefer the services of dominant platforms (GAMMA) solely on the basis of their innovative merits. User persistence is explained, at least in part, by the structural constraints mentioned, which in fact compel them to remain within the platform's ecosystem. This observation also calls into question one of the assumptions of classical competition theory. Adam Smith, considered the father of economic liberalism (Smith, 1776), conceived markets as governed by the interaction between supply and demand within a system of natural liberty. In his vision, competition, through the "invisible hand," would channel individual self-interest towards the promotion of collective welfare.In the digital age, however, it is legitimate to ask whether Smith's "invisible hand" has not been supplanted by a new form of coordination: the so-called "digital hand" (Smith, 1776). Digital markets are driven by dynamics profoundly different from those envisaged by Smith or by ordoliberal theory. Rather than being characterised by a plurality of firms competing under conditions of consumer freedom of choice, the digital economy is marked by the concentration of both economic and informational power in the hands of a few dominant platforms, which consolidate their position through exclusionary or exploitative strategies that

threaten not only the competitive process but also the freedom of users to make autonomous and informed choices. It follows that it is legitimate to question whether, in the current architecture of digital markets, consumer choices can truly be considered free and conducive to their welfare, or whether they primarily serve to consolidate the entrenched dominance of the major online platforms (Ezrachi & Stucke, 2016).

4. RESULTS AND DISCUSSIONS: CONCEPTUALIZING PERSONAL DATA AS A COMPETITIVE PARAMETER AND A DIMENSION OF CONSUMER WELFARE

The challenges outlined above constitute the foundation of this research's proposal for an innovative framework: to integrate privacy protection into competition law analysis in cases of abuse of dominance—at the same time—preserving its essential function of safeguarding the proper functioning of markets (Lamadrid & Villiers, 2017).

Although this conceptual exercise has been partially undertaken by the European Commission in the field of merger control (European Commission, 2024b), a significant institutional and scholarly gap remains with respect to the theory and case law on abuse of dominance (OECD, 2018a).

At the outset, it is necessary to clarify what is meant by "privacy". The term refers to the protection of personal data, informational self-determination, and the effective ability of individuals to exercise choice regarding how and under what conditions their personal information is shared (Solove, 2006). This understanding is enriched by the theory of "contextual integrity", which maintains that privacy is preserved when flows of information conform to the normative expectations embedded within specific contexts (in the case at hand, the provisions of the GDPR). Conversely, a violation of privacy occurs when these contextual norms are disregarded or breached (Nissenbaum, 2010).

Antitrust assessment has traditionally relied on variables such as price, output, and the quality of goods and services. In its Guidance on Article 102 TFEU, which prohibits abuse of dominance in European markets, the European Commission expressly stated that: «*In applying Article 82, the Commission will focus on the types of conduct that are most harmful to consumers. Consumers benefit from competition through lower prices, better quality and a wider choice of new or improved goods and services*»(European Commission, 2009).

The theoretical proposal advanced here is that privacy should be treated as a dimension of service quality, and therefore as an integral component of the competitive process itself (OECD, 2018a). In digital markets, where services are ostensibly provided free of charge, price ceases to be a meaningful metric. What becomes decisive instead is the extent of data collection and the level of privacy protection offered, as demonstrated by empirical studies (Cisco, 2019; RSA, 2019; Kim, Wang & Roh, 2021; Dengler, Prüfer, 2021; Gupta et al., 2023; Rodríguez-Priego, Porcu, Prados Peña, & Crespo Almendros, 2023; D'Annunzio & Menichelli, 2022).

Against this backdrop, this research advances the following proposal.

A higher level of privacy protection corresponds to an enhancement in the qualitative standard of the service provided; conversely, its reduction entails a deterioration in service quality. Privacy policies thus constitute an indispensable structural component of any digital service. From this perspective, the reduction of privacy standards can be further conceptualised as a form of consumer harm: a commercial practice that lowers privacy standards diminishes the overall quality of services and directly undermines consumer welfare by infringing upon fundamental rights.

By contrast, more stringent guarantees in the field of data protection and privacy strengthen consumer welfare, albeit in non-economic terms, by safeguarding informational self-determination and ensuring broader protection of personal and highly sensitive data. This theoretical move allows for the integration of a non-economic value into antitrust analysis.

A measure of caution is, however, required: not every reduction in privacy standards represents a competitive harm sufficient to justify intervention by competition authorities. As Lamadrid has persuasively observed, if competition law were to intervene in every case of privacy infringement, it would risk transforming into an all-encompassing instrument for addressing any emerging social concern, thereby losing coherence and straying from its fundamental purpose of safeguarding the competitive process (Lamadrid & Villiers, 2017). In this sense, the inclusion of privacy as a competitive parameter—at least in the theoretical framework advanced here—is intrinsically linked to market dynamics and cannot be dismissed as a mere consequence of competitive behaviour. Privacy is compromised precisely as a result of the concentration of power in the digital economy and of the structural effects that limit competition. The characteristic analysed above, such as network effects, informational asymmetries, switching costs, and lock-in mechanisms collectively erode market contestability, depriving consumers of any genuine choice between providers and services. There is no real freedom to decide whether to disclose personal data, nor to use an alternative platform, when a single dominant operator effectively constitutes the only available digital service in the market. Further support for this theorisation lies in the added value that would derive from genuine competition on levels of personal data protection. In today's digital markets such competition is virtually absent (Grunes & Stucke, 2015). Dominant platforms unilaterally set privacy standards to their own advantage, without being subjected to any competitive pressure from rivals (which are effectively non-existent). By contrast, competition on the parameter of privacy would induce firms to guarantee higher levels of data protection in order to attract consumers, much as traditional competition on price aims to expand consumer demand. The absence of competition on this parameter results in lower levels of personal data protection, accompanied by uncertainty and opacity in data-processing practices, which have already been scrutinised by competition authorities (Bundeskartellamt, 2019, 2025).

By contrast, in a dynamic market where multiple platforms offered substitutable services—i.e., services that satisfy the

same consumer needs—firms, unable to compete on price, would be forced to compete on innovation and on the levels of privacy protection they provide. Faced with two alternative services offering different privacy guarantees, users would be more likely to choose the one ensuring higher levels of protection, thereby excluding from the market those platforms that adopt weaker standards. Such dynamics would generate a virtuous cycle in digital markets, driving upward convergence in privacy protection.

However, in order to validly include privacy within the set of competitive parameters, it is essential to address not only theoretical considerations but also practical solutions. Integrating privacy as a competitive parameter necessarily requires the adoption of methodologies that go beyond the traditional approach to market definition. Conventionally, the relevant market is delineated through the SSNIP test (*small but significant non-transitory increase in price*) (OECD, 2013; European Commission, 2024a), which relies on hypothetical price variations to assess substitutability from the consumer's perspective. Yet in digital markets, where services are often provided at a nominal price of zero, price ceases to be a meaningful indicator. This calls for the use of alternative methodologies, such as the SSNDQ test (*small but significant non-transitory decrease in quality*) (OECD, 2013), which evaluates substitutability and competitive constraints by considering variations in the quality of products or services (European Commission, 2024a).

Following this line of reasoning, recent scholarship has put forward an even more tailored instrument: the SSNDP test (*small but significant non-transitory decrease in privacy*), designed to capture deteriorations in the level of privacy afforded to users (Deutscher, 2018). As Deutscher has discussed, this framework recognises privacy as a dimension of quality with direct relevance for competition analysis.

The use of such a test, however, entails the need to clearly define the concepts of diminution of privacy and its significance. This is not an easy task, considering that privacy preferences are fluctuating and subject to the subjective evaluation of individual consumers: some consumers may not perceive personalised advertising, based on their previous searches, as harmful, but rather as useful for completing a transaction and satisfying their needs. Indeed, they may even regard general advertising, not based on their personal data, as intrusive (OECD, 2018a). The literature has highlighted the so-called privacy paradox: while consumers declare that they value higher standards of data protection, in their market choices they often tend to prioritise access to services at zero monetary price over the protection of their privacy (Solove, 2020; 2025).

The present research develops this line of reasoning further and mitigates the aforementioned shortcomings. It proposes the GDPR as an objective benchmark: violations of its provisions may be regarded as verifiable and significant evidence of privacy degradation. It thereby provides for an assessment of consumer behaviour in the event of a significant reduction in privacy, which entails a violation of GDPR provisions, and evaluates consumer choice among digital services that differ precisely in the level of privacy they provide or in their compliance with the law. This ensures an anchoring to parameters that are neither variable nor subject to individual evaluation.

Moreover, the recognition of privacy as a competitive parameter would allow for the construction of new theories of harm specifically adapted to digital markets, thereby justifying the activation of competition law in cases of exploitative abuse of dominance. Such abuse arises when a firm "takes advantage of the opportunities arising out of its dominant position in order to reap trading benefits which it would not have obtained under conditions of normal and sufficiently effective competition" (Court of Justice of the European Union, 1978). This is precisely what occurs in digital markets, where firms exploit their undue power over consumers placed in a structurally weaker position.

Finally, the inclusion of privacy in antitrust analysis (OECD, 2024a) must also be situated within the broader debate on the multidimensional (Ezrachi, 2018) or polycentric (Lianos, 2018) nature of competition law's objectives. This debate, particularly vivid in Europe, calls upon antitrust law to incorporate additional non-economic concerns into its analytical framework, alongside privacy, such as environmental sustainability (OECD, 2021), democracy (OECD, 2024b), and labour market considerations (OECD, 2020).

Whereas the Chicago School (Bork, 1967) and the European approach of the 1990s (Odudu, 2010) had reduced the aims of competition law to the narrow promotion of consumer welfare understood in terms of allocative efficiency (Bartalevich, 2016), this article highlights how such an economic calculus proves inadequate—and indeed undesirable—in digital markets. Consumer welfare, and the factors that constitute it, must be conceived in broader terms, encompassing values that are not strictly economic. Within this framework, data protection cannot be relegated to an external field merely because it resists quantification.

• THE EUROPEAN APPROACH: POSITIONS OF THE COMMISSION AND THE COURT OF JUSTICE

The theorisation of privacy as a parameter of competition analysis has developed within a framework long marked by institutional resistance, both at the level of the European Commission and of the Court of Justice. In its ASNEF/Equifax judgment, the Court held that «*the issues relating to the sensitivity of personal data are not, as such, a matter of competition law, but may be resolved under the relevant provisions governing data protection" (Court of Justice of the European Union, 2006). Similarly, in its 2014 decision approving the Facebook/WhatsApp merger, the Commission emphasised that "privacy-related concerns fall outside the scope of the assessment under the Merger Regulation, but can be addressed under data protection rules*» (European Commission, 2014).

The same approach was reiterated in Apple/Shazam (European Commission, 2018) and Google/Fitbit (European Commission, 2020).

A turning point in the debate on the interplay between competition law and data protection came with the *Meta/Bundeskartellamt* case (Bundeskartellamt, 2019). In 2019, the German competition authority found that Meta had abused its dominant position by making access to its services conditional on users' acceptance of contractual terms authorizing the collection and combination of data from Facebook, Instagram, WhatsApp, and third-party websites with embedded plug-ins. The Bundeskartellamt held that such conduct infringed the principle of informational self-determination and the GDPR, while also constituting exploitative abuse of dominance, since users lacked any meaningful alternative neither the ability to reject the terms nor to switch to competing providers (Kerber & Zolna, 2022)[1].

On appeal, the Oberlandesgericht Düsseldorf adopted a markedly more restrictive stance than the progressive competition authority, ordering the suspension of the Bundeskartellamt's decision (Oberlandesgericht Düsseldorf, 2019). In subsequent proceedings challenging this suspension, the German Federal Court of Justice overturned the judgment of the Court of Appeal and endorsed the reasoning advanced by the Bundeskartellamt (Bundesgerichtshof, 2020).

The Federal Court held that Facebook's dominant position exacerbated the "clear imbalance" between the platform and its users, depriving the latter of genuine freedom of choice and rendering their consent to the processing of personal data merely formal rather than substantive (Podszun, 2020). In so doing, the Court confirmed the relevance of privacy as a parameter of competitive assessment.

The divergence between the two judicial approaches could hardly have been more pronounced. As a result, the Oberlandesgericht Düsseldorf referred the matter to the Court of Justice of the European Union (CJEU, 2021), seeking guidance on a number of questions that highlight the intricate relationship between competition law and data protection (CJEU, 2023).

As a preliminary matter, the central question concerning the incorporation of data protection into competition analysis is whether antitrust authorities may assess potential infringements of the GDPR by a dominant undertaking in the context of competition enforcement. In its landmark judgment (CJEU, 2023), the Court of Justice held that a competition authority, in the exercise of its functions and insofar as it is instrumental to the assessment of a possible competition law infringement, *must* examine «*the compliance or non-compliance of such conduct with the provisions of the GDPR*» (paras. 37–43), provided that the cooperation mechanisms laid down by the Court are respected and that the competition authority does not substitute itself for the data protection authorities in their primary role (Lupacchini, 2025).

Secondly, it was necessary to determine the relevance of the GDPR within competitive dynamics. On this point, the Court stated that «*the compliance or non-compliance of such conduct with the provisions of the GDPR may, depending on the circumstances, constitute an essential indication among the relevant factors of the case in order to establish whether such conduct involves recourse to methods governing the normal play of competition and to assess the consequences of a given practice on the market or for consumers*» (para. 47).

Moreover, departing from the earlier position that data protection should not be regarded as a matter of antitrust concern, the Court emphasised that «*access to personal data and the possibility of processing such data have become a significant parameter of competition between undertakings in the digital economy*» (para. 51).

This judgment of the Court of Justice marks a watershed in European competition law, giving concrete effect to the interconnection between the two legal domains and establishing the GDPR as a normative benchmark for assessing data-related anticompetitive conduct. On the one hand, a breach of privacy—in this case, of the Regulation's provisions—constitutes competition on a basis other than merit and thereby justifies the activation of antitrust enforcement (Lupacchini, 2025). On the other hand, the Court makes explicit that the protection and processing of personal data amount to a competitive parameter in their own right.

The 2023 ruling thus anchors in positive law an approach that had previously been elaborated only at the theoretical level, but which now receives authoritative confirmation in European jurisprudence.

• BEYOND ANTITRUST: NEW REGULATION FOR DIGITAL DISRUPTION (THE DIGITAL MARKETS ACT)

The recognition of the structural deficiencies of digital markets, and in particular of the strategic role of personal data in reinforcing market power and harming consumers, has led European institutions to complement traditional antitrust instruments with an ex ante regulatory framework, the so-called Digital Markets Act (European Commission, 2022). The European response to disruptive, data-driven business models is thus characterised by a radical change of approach: moving away from the exclusively *ex post* control of harmful conduct, which has long defined the enforcement of competition law, towards the establishment of ex ante rules designed to regulate business models in a manner that promotes contestability and fairness in the marketplace (Manzini, 2021). This framework makes it possible to respond more effectively to the distinctive features of digital markets, marked by speed, unprecedented concentrations of power, and the risk of irreversible anticompetitive effects detrimental both to markets and to consumers.

The Digital Markets Act was conceived out of the recognition that the data-related practices of large digital platforms could not be adequately addressed through the classical instruments of European competition law (such as abuse of

[1] The decision of the Bundeskartellamt is innovative in that it recognized that violations of data protection rules may be relevant under competition law, insofar as they affect the contractual imbalance between a dominant undertaking and its users. The underlying idea was that user consent was not genuinely free, but conditioned by the dominant position of the platform, thus amounting to an exploitative abuse within the meaning of § 19 GWB (German Competition Act) and, in parallel, of Article 102 TFEU.

dominance prohibition enshrined in article 102 TFEU). These provisions are constrained by lengthy investigations, protracted enforcement timelines, and uncertain outcomes, limitations that are particularly acute when dealing with the complex assessments characteristic of data-driven markets. The underlying rationale was therefore to establish a preventive framework aimed at curbing the power of the so-called gatekeepers (art. 3), namely those platforms that constitute indispensable gateways to the digital economy and that, by controlling data, users, and technological infrastructures, are capable of shaping the very functioning of markets themselves.

The innovative scope of this regulation lies in the formulation of ex ante obligations and prohibitions, directly and immediately applicable, which reshape the disruptive business models of digital platforms. They focus in particular on access to and control over users' personal data, the possibility of greater choice among services available on the market, and both vertical and horizontal interoperability of digital services. Within this framework, the centrality of data protection clearly emerges; the DMA recognises that the market power of gatekeepers largely derives from the exclusive use and concentration of vast amounts of data and, through targeted prohibitions, seeks to restore users' control over their data and their genuine choices. Among the obligations laid down by the Digital Markets Act is, first and foremost, the requirement of interoperability between systems and services (Article 6(7)). Complementing this is the prohibition of self-preferencing practices (Article 6(5)), aimed at preventing platforms from favouring their own services (in terms of ranking and positioning) over those of competitors. Other significant obligations include the possibility for end users to uninstall pre-installed applications and to easily modify default settings (Article 6(3)–(4)), as well as the obligation for gatekeepers to ensure effective data portability and real-time access to information generated by users (Article 6(9)). In addition, with specific regard to number-independent interpersonal communication services (NIICS), article 7 establishes an interoperability obligation among messaging services available on the market, in order to avoid the segmentation of related markets.

Among the most significant provisions is Article 5(2) DMA, which occupies a particularly central role. First, it prohibits gatekeeper platforms from:

a) processing, for the purpose of personalised advertising, the data of users originating from third-party services that make use of the gatekeeper's core platform services. This prevents the gatekeeper from exploiting data collected indirectly (e.g. through complementary or third-party services) for profiling or targeting purposes;

b) combining personal data obtained from one core platform service with data from other CPS or from other services offered by the gatekeeper, as well as with data obtained from third-party services. This restriction is intended to prevent the gatekeeper from building an "excessive" user profile by leveraging its multi-service position;

c) engaging in cross-use of personal data, namely, data collected in one core platform service may not be used in other separate services, nor vice versa, without limitation. This seeks to avoid dominance in one service being converted into unfair competitive advantages through the use of data.

All of this is prohibited unless the user has been presented with a specific choice option (a specific consent under the DMA) and has given consent in accordance with the provisions of the GDPR (Articles 4(11) and 7 GDPR). It follows that, in addition to the consent required under Article 6 of the GDPR for the processing of personal data, the DMA introduces further levels of consent (specific option). These levels are based on the granularity of the type of processing rather than on the category of personal data being processed.

The purpose is to strengthen consumer control over their personal information, on the assumption that consent constitutes the gateway through which platforms gain access to users' data. Admittedly, concerns regarding possible phenomena of consent fatigue cannot be overlooked; nonetheless, this measure is regarded as appropriate and proportionate.

A further step is taken in Recitals 36 and 37, which provide that, where users do not give consent to the processing of personal data as envisaged therein, gatekeepers may not block access to the platform. They must, instead, offer «*a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user's consent*».

This less personalised offer «*should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service. Not giving consent should not be more difficult than giving consent. When the gatekeeper requests consent, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner. In particular, consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user, as defined in Regulation (EU) 2016/679. At the time of giving consent, and only where applicable, the end user should be informed that not giving consent can lead to a less personalised offer, but that otherwise the core platform service will remain unchanged and that no functionalities will be suppressed*».

In this context, the business models of digital platforms are profoundly tested in relation to their sources of profitability: a reduction in the volume of personal data collected through the provision of an equivalent alternative inevitably translates into lower financial revenues for the platform. This, in turn, may lead to consequences that are difficult to balance. On the one hand, there would be a clear gain in terms of enhanced privacy protection for consumers. On the other hand, as persuasively argued in the study by Choe, Matsushima and Shekhar (2024), when the quantity of data collected decreases, the platform is likely to respond by raising access prices or introducing new fees, in order to compensate for the loss of value resulting from the diminished monetisation of data.

This is precisely what occurred with Meta, which introduced the so-called *pay-or-consent* model: users are presented with a binary choice between consenting to the processing of their personal data for personalised advertising purposes or, alternatively, paying a monetary fee in order to access the platform without personalisation.
According to the European Commission, such a mechanism contravenes the provisions of the Digital Markets Act: the user's freedom to give genuinely valid consent is severely undermined when the only alternative is between disclosing personal data and, in the event of refusal, bearing a financial burden. For this conduct, a fine of EUR 200 million was imposed (European Commission, 2025). It should not be overlooked, however, that the legitimacy of the model also finds partial support in paragraph 150 of the *Meta* judgment, Case C-252/21, in which the Court of Justice recognised—albeit in narrowly defined terms—the possibility of resorting to similar schemes (Court of Justice of the European Union, 2021).
This case, in all its complexity, highlights a crucial point: the level of privacy protection offered in digital markets can no longer be regarded merely as a matter of compliance with the GDPR, but rather constitutes an essential element of the proper functioning of the competitive process. Its protection therefore has direct implications for competition law and can no longer be relegated to an external matter or considered the exclusive domain of data protection regulation.
Privacy thus emerges, in an undeniably clear manner, as a genuine parameter of competition. From this perspective, the DMA represents a decisive turning point: it inaugurates a competition policy capable of responding to the demands of the digital era, in which the protection of personal data and the safeguarding of the competitive process are no longer treated as separate domains, but as dimensions intimately interconnected within a unified framework of European economic governance.

5. LIMITATION AND FUTURE RESEARCH

Despite the progress made in recognising privacy as a parameter of competition, several significant limitations remain that call for further reflection and development.
A primary limitation lies in the challenge of demonstrating a robust causal link between the erosion of data protection standards and an actual anticompetitive effect. Not every reduction in the level of privacy protection necessarily derives from the exercise of market power; in some cases, it may simply reflect contractual choices or neutral market dynamics. This evidentiary uncertainty complicates the legal qualification of exploitative abuse and requires the elaboration of more precise analytical tools capable of distinguishing competitive harm from mere regulatory non-compliance. Much will depend on how competition authorities construct the theory of harm and on the contribution of legal scholarship to this debate.
A further limitation concerns the risk of excessive *legal formalism* in the use of the GDPR as a benchmark for assessing privacy degradation. Not every infringement of the GDPR has competition law relevance, just as not every antitrust concern entails a violation of data protection rules. Exclusive reliance on GDPR compliance as an index of competitive harm would not be correct; it would risk automatising competition law enforcement whenever privacy issues arise. The matter, instead, requires careful attention and solid connections to competitive dynamics and their consequences on privacy, and vice versa.
The adoption of the proposal advanced here is also exposed to an additional phenomenon. Large platforms may formally adapt their business models to the new rules on privacy and competition while in fact continuing to maintain substantial competitive advantages. Such strategies may take the form of new lock-in mechanisms or alternative modes of data monetisation, thereby reducing the actual impact of regulation on the functioning of digital markets and on the protection of personal data.
Equally relevant is the rapid and unpredictable pace of technological evolution. The rise of generative artificial intelligence is testing existing legal paradigms, including the DMA itself. This may entail the necessity of applying the thesis advanced here to disruptive technologies heavily based on the exploitation of personal data. In this context, a twofold challenge emerges. On the one hand, regulators and enforcers must possess solid knowledge of the functioning of such AI models. On the other hand, the delicate task arises of reconciling privacy with other parameters, in particular technological innovation. The need for delicate trade-offs may arise: overly stringent policies on data protection risk restraining data-driven innovation (such as machine learning systems and AI), which contributes to overall welfare. This could constrain technological innovation and expose it to calls for regulatory opportunity.
Furthermore, stricter data protection rules may incentivise undertakings to develop alternative business models to replace revenues lost from the monetisation of personal data, such as the imposition of fees for accessing services without the processing of personal data for targeted advertising purposes. In such cases, a higher level of privacy protection may paradoxically result in a reduction of welfare for those consumers compelled to bear costs in order to secure the non-processing of their data.
Finally, a clear regulatory asymmetry emerges between different jurisdictions at the international level. The European approach, based on the integration of the GDPR and the DMA, applies primarily to gatekeepers operating within the internal market, while practices of data collection and exploitation often have a global dimension. The absence of effective international coordination, and the divergent approaches adopted in other regions (such as ASEAN countries), may fragment the effectiveness of the European regulatory response.
The limitations identified do not call into question the recognition of privacy as a parameter of competition; rather, they require further research at both the European and the international levels.

6. CONCLUSION

The analysis has shown that the business models of digital platforms fully embody the disruptive nature that defines them, while at the same time acquiring an additional dimension: not merely incremental innovations, but systemic transformations that have fractured the very foundations upon which European competition law has traditionally rested. The extraction and exploitation of personal data have redefined the parameters of competition, giving rise to markets where value is no longer measured in terms of price or quantity, but rather through control over information and the ability to steer user choices. The consumer is no longer a rational actor expressing preferences in the market, but has become a source of data from which economic value (consumer surplus) is extracted; competition is no longer played out solely *in* the market, but increasingly *for* the market, insofar as the control of a platform entails dominance over the entire digital data ecosystem.

It follows that competition law is called upon to reinvent itself: no longer a unidimensional discipline anchored exclusively to economic indicators, but one that is flexible enough to include values not directly or economically measurable, such as privacy and the protection of personal data. This, however, remains functional to its purpose: ensuring that markets are open and contestable, while addressing the challenges posed by data-driven business models.

On this basis, the paper advances the theorization of data protection and thus privacy, as a parameter of competition, conceptualized as a subcategory of service quality. A reduction in the level of personal data protection amounts to a diminution of one of the competitive parameters directly impairing consumer welfare in digital markets. The benchmark chosen to anchor such reductions to verifiable criteria is Regulation (EU) 2016/679: non-compliance with its requirements on data processing not only diminishes the qualitative dimension of the service, but also constitutes a breach of the European regulatory framework. Recent jurisprudence of the Court of Justice has opened the door to such an interpretative approach.

Equally, the regulatory turn embodied in the Digital Markets Act reflects the growing awareness that the digital economy requires legal instruments capable of capturing the multidimensional nature of competition, with a precise focus on the processing of personal data and its value in competitive dynamics.

This paper thus aligns with the strand of scholarship emphasizing that European competition law is now called upon to reinvent itself: no longer a unidimensional discipline confined to economic indicators, but one attentive to broader values, ranging from the protection of personal data to the safeguarding of genuinely contestable markets, responsive to the challenges posed by data-driven business models.

This is the very essence of disruption: not a mere technological shift, but a radical transformation of the legal and economic order, requiring European law to redefine its paradigms in order to remain faithful to its foundational mission of securing free and pluralistic markets.

All this, of course, is not enough. Looking ahead, the central challenge lies in the adaptive capacity of the law. The speed with which digital business models evolve demands a legal framework capable of responding within a reasonable timeframe, avoiding both regulatory inertia and an overproduction of static rules that risk obsolescence almost immediately.

It follows that the European Union should pursue a regulatory framework that is adaptive and dynamic, designed to anticipate the disruptive strategies of digital platforms and to prevent technological innovation from solidifying into unchecked concentrations of power, while remaining anchored to the fundamental values underpinning the European legal system. In the conclusion, it can be observed that disruptive business models are implemented on a global scale. The European Union increasingly positions itself as a genuine regulatory laboratory. Instruments such as the Digital Markets Act may serve as models capable of being exported to other jurisdictions, as is already partially occurring in Australia. This underscores the importance of striving for a global and more coherent regulatory response. Nevertheless, in ASEAN countries reliance on soft law and voluntary approaches to regulating digital markets reflects a distinctive regulatory philosophy, one that recognises digital platforms as key drivers of innovation and as enablers for SMEs to access markets. A global vision—while remaining sensitive to the specific priorities and regulatory traditions of each jurisdiction—appears both desirable and necessary.

REFERENCES

Acquisti, A., K. Brandimarte, G. Loewenstein (2015), “Privacy and human behaviour in the age of information”, Science, Acquisti, A., Brandimarte, K., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *Science, 347*(6221), 509–514.

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics, 84*(3), 488–500.

Bartalevich, D. (2016). The influence of the Chicago School on the Commission’s guidelines, notices and block exemption regulations in EU competition policy. *Journal of Common Market Studies, 54*(2), 267–283.

Bork, R. H. (1967). The Goals of Antitrust Policy. *The American Economic Review* 57, 2.

Botta, M., & Wiedemann, K. (2018). EU competition law enforcement vis-à-vis exploitative conducts in the data

economy: Exploring the terra incognita. *New York University School of Law Working Paper*.

Bundesgerichtshof. (2020, June 23). *Decisione, causa KVR 69/19, Facebook,* ECLI:DE:BGH:2020:230620BKVR69.19.0.

Bundeskartellamt. (2019). *Decision B6-22/16 – Facebook, 6 February 2019*.

Bundeskartellamt. (2023). *Entscheidung Missbrauchsaufsicht: Verfahren B7-70/21* [Decision in abuse control proceedings].

Christensen, C. M., Raynor, M., & McDonald, R. (2015). What is disruptive innovation?. *Harvard Business Review*, 93.

Christensen, C.M. (1997). The innovator's dilemma: When new technologies cause great firms to fail. *Brighton: Harvard Business School Press*.

Cisco. (2019). *Consumer privacy report: The growing imperative of getting data privacy right*. https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf

Costa-Cabral, F., & Lynskey, O. (2017). Family ties: The intersection between data protection and competition in EU law. *Common Market Law Review, 54*(1), 11–50.

Court of Justice of the European Union. (1978). *Case 27/76, United Brands Company and United Brands Continentaal BV v Commission*, ECLI:EU:C:1978:22, para. 249.

Court of Justice of the European Union. (1979). *Hoffmann-La Roche v. Commission*, Case 85/76, ECLI:EU:C:1979:36, paragraph 461.

Court of Justice of the European Union. (2006). *Case C-238/05, Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios*, ECLI:EU:C:2006:734, para. 63.

Court of Justice of the European Union. (2023, July 4). *Case C-252/21, Meta Platforms and Others (Terms of service of a social network)*.

Crémer, J., De Montjoye, Y., & Schweitzer, H., (2019). Competition Policy for the Digital Era. *European Commission Report*.

D'Annunzio, A., & Menichelli, E. (2022). A market for digital privacy: Consumers' willingness to trade personal data and money. *Journal of Behavioral and Experimental Economics, 99*, 101900.

Dengler, S., & Prüfer, J. (2021). Consumers' privacy choices in the era of big data. *Games and Economic Behavior, 130*, 499-520.

Deutscher, E. (2018). How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets. *EUI Working Papers, Law 2018/13*. European University Institute.

Economides, N., & Lianos, I. (2018). Restrictions on privacy and exploitation in the digital economy: A market failure perspective. *Antitrust Law Journal, 81*(3), 673–711.

European Commission. (2009). *Communication from the Commission: Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings* (Text with EEA relevance), (2009/C 45/02). *Official Journal of the European Union*, C 45/7.

European Commission. (2014). *Case M.7217, Facebook/WhatsApp, Decision of 3 October 2014*.

European Commission. (2018). *Decision Apple/Shazam, Case M.8788, C(2018) 5748 final of 6 September 2018*, para. 262.

European Commission. (2020). *Decision Google/Fitbit, Case M.9660, C(2020) 8750 final of 17 December 2020*, paras. 263–266.

European Commission. (2022). *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 (Digital Markets Act)*. *Official Journal of the European Union*, L 265, 1–66

European Commission. (2024a). *Commission Notice on the definition of the relevant market for the purposes of Union competition law* (C/2024/1645). *Official Journal of the European Union*, C 2024/1645.

European Commission. (2024b). *Competition policy brief: Non-price competition. EU merger control framework and case practice* (Issue 1). Publications Office of the European Union. ISBN 978-92-68-14914-0. ISSN 2315-3113.

European Commission. (2025). *Decision on Meta Case DMA.100055* [Digital Markets Act case].

European Data Protection Board. (2014). *Preliminary opinion: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy*.

European Data Protection Board. (2025). *Position paper on interplay between data protection and competition law*.

European Parliament, European Parliamentary Research Service. (2020). *Is data the new oil? Competition issues in the digital economy* (PE 646.117).

European Union. (2012). *Charter of Fundamental Rights of the European Union*. Official Journal of the European Union, C 326, 391–407.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88.

European Union. (2022). *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 (Digital Markets Act)*. *Official Journal of the European Union*, L 265, 1–66

Evans, D. S. (2020). The economics of attention markets. *SSRN*. https://doi.org/10.2139/ssrn.3044858

Ezrachi, A. (2018). EU competition law goals and the digital economy. *Oxford Legal Studies Research Paper* No. 17/2018).

Ezrachi, A., & Stucke, M. E. (2016). Virtual competition. *Journal of European Competition Law & Practice, 7*(9), 585–586.

Geroski, P. A. (2003). Competition in markets and competition for markets. *Journal of Industry, Competition and Trade, 3*(3), 151–166. https://doi.org/10.1023/A:1025422324414

Grunes, P., & Stucke, M. E. (2015). No mistake about it: The important role of antitrust in the era of big data. *University of Tennessee Legal Studies* Research Paper No. 269.

Gupta, R., Iyengar, R., Sharma, M., Cannuscio, C. C., Merchant, R. M., Mitra, N., & Grande, D. (2023). Consumer views on privacy protections and sharing of digital health information. *JAMA Network Open, 6*(3), e231305.

Iacovides, M., & Stylianou, K. (2024). The new goals of EU competition law: Sustainability, labour rights, and privacy. *European Law Open*.

Kerber, W. (2024, March 25). Competition policy and data protection law: The complexity of its interplay from an economic perspective. *SSRN*.

Kerber, W., & Zolna, K. K. (2022). The German Facebook case: The law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics, 54*(2), 217–250. https://doi.org/10.1007/s10657-022-09755-9

Kim, Y., Wang, Q., & Roh, T. (2021). Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. *Telematics and Informatics, 56*, 101483.

Lamadrid, A., & Villiers, S. (2017). Big data, privacy and competition law: Do competition authorities know how to do it? *Competition Policy International*.

Lianos, I. (2018). Polycentric competition law. Current Legal Problems, 71(1), 161–216. *Oxford University Press*.

Lupacchini, B. (2025). La protezione dei dati personali è un problema antitrust? Profili giuridici e implicazioni nei mercati digitali. *Diritto ed Economia dei Mezzi di Comunicazione, 1*.

Maggiolino, M. (2018). *I Big Data e il diritto antitrust*. Milano: Egea.

Manzini, P. (2021). Equità e contendibilità nei mercati digitali: La proposta di Digital Market Act. *AISDUE. Eu Focus "Servizi e piattaforme digitali"*, Annali AISDUE, 3(2).

Meta, MENLO PARK, Calif., Jan. 29, 2025 /PRNewswire/ -- Meta Platforms, Inc. (Nasdaq: META) today reported financial results for the quarter and full year ended December 31, 2024.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. *Stanford University Press.*

Oberlandesgericht Düsseldorf. (2019, August 26). *Cases VI-Kart 1/19 (V).*

Odudu, O. (2010). The wider concerns of competition law. *Oxford Journal of Legal Studies, 30*(3), 599–613.

OECD. (2013). *The role and measurement of quality in competition analysis: Key findings, summary and notes* (OECD

Roundtables on Competition Policy Papers, No. 141). OECD Publishing.

OECD. (2015). *Hearing on disruptive innovation: Issues paper by the Secretariat* (DAF/COMP(2015)3). OECD Competition Committee.

OECD. (2018a). *Quality considerations in digital zero-price markets* (DAF/COMP(2018)14). OECD Publishing.

OECD. (2018b). *Rethinking antitrust tools for multi-sided platforms*. OECD Publishing.

OECD. (2020a). *Competition in digital advertising markets*. OECD Publishing.

OECD. (2020b). *Competition issues in labour markets* (OECD Roundtables on Competition Policy Papers, No. 244). OECD Publishing.

OECD. (2021). *Sustainability and competition* (OECD Roundtables on Competition Policy Papers, No. 262). OECD Publishing.

OECD. (2022a). *OECD handbook on competition policy in the digital age*. OECD Publishing.

OECD. (2022b). *The evolving concept of market power in the digital economy* (OECD Competition Policy Roundtable Background Note). OECD Publishing.

OECD. (2024a). *AI, data governance and privacy: Synergies and areas of international co-operation* (OECD Artificial Intelligence Papers, No. 22). Paris: OECD Publishing.

OECD. (2024b). *The interaction between competition and democracy* (OECD Roundtables on Competition Policy Papers, No. 316). OECD Publishing.

OECD. (2024c). *The intersection between competition and data privacy* (OECD Roundtables on Competition Policy Papers, No. 310). OECD Publishing.

Podszun, R. (2020). The consumer as a market player: Competition law, consumer choice and data protection in the German Facebook decision. *GRUR – Gewerblicher Rechtsschutz und Urheberrecht*, 2020(4), 375–384.

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), OJ L 265, 12.10.2022, 1–66.

Rodríguez-Priego, N., Porcu, L., Prados Peña, M. B., & Crespo Almendros, E. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services, 72*, 103284.

RSA. (2019). *Data privacy & security survey 2019: The growing data disconnect between consumers and businesses*. https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf

Smith, A. (1776/1904). *An inquiry into the nature and causes of the wealth of nations* (E. Cannan, Ed.). London: Methuen & Co.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Solove, D. J. (2020). The myth of the privacy paradox. *GW Law Faculty Scholarship & Other Works*.

Solove, D. J. (2025). On privacy and technology. *Oxford University Press*.

Stucke, M. E. (2022). The rise of the data-opolies. In *Breaking away: How to regain control over our data, privacy, and autonomy* (online ed.). *Oxford Academic*.

Vanberg, V. (1998). Freiburg School of Law and Economics. In P. Newman (Ed.), *The New Palgrave Dictionary of Economics* (Vol. 2). London: Palgrave Macmillan.

Whish, R., & Bailey, D. (2024). *Competition Law* (11th ed.). Oxford University Press.

Witt, A. C. (2019). The European Court of Justice and the more economic approach to EU competition law – Is the tide turning? *Antitrust Bulletin, 64*(2), 172–213.

Zuboff, S. (2019). The Age of Surveillance Capitalism. The Fight for a Human Future and the New Frontier of Power. *New York, Public Affairs*.