COMMENTS TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE REVIEW OF THE DIGITAL MARKETS ACT

SUBMITTED BY CONSUMER ASSOCIATION IUS OMNIBUS

I. IUS OMNIBUS

Ius Omnibus (Ius), with its registered office at Second Home Lisboa, Mercado da Ribeira, Av. 24 de Julho, 1200-479 Lisbon, Portugal, is a non-profit association, created in March 2020, with the aim of promoting and defending the rights and interests of consumers in the European Union. It is a consumer protection association registered and recognised by the Portuguese Government and the European Commission as a qualified entity under Directive (EU) 2020/1828, which has filed several class actions in the field of consumer protection.

Ius' interest in participating in this public consultation on the implementation of the Digital Markets Act (DMA) stems from its commitment to the effective defence of consumer rights in digital environments. As an association dedicated to promoting fair and undistorted competition, as well as the collective protection of consumer interests, Ius considers it essential that the implementation of the DMA takes into account its direct impact on innovation, privacy, service quality and the well-being of end users.

In a context of digital transformation, it is crucial that the DMA's regulatory tools ensure that consumers' rights are not directly or indirectly restricted.

II. Previous contributions by Ius and preliminary question on interoperability.

It should be noted that Ius already submitted comments as part of the public consultation launched by the European Commission in January 2025 on the DMA.100204 SP-Apple-Article 6(7).

In this instance, Ius stressed the importance of ensuring that interoperability measures are not limited to technical aspects of the application procedure proposed by Apple, but also take into account the real effects on consumers and the distribution of

applications. The position adopted at that time reflected the need to establish an interoperability regime that protects both developers and end users, preventing gatekeeper control from leading to unjustified restrictions that reduce consumer choice and perpetuate monopolistic practices.

In this regard, Ius considers that the full and proper application of Article 6(7) of the DMA is crucial to ensuring that interoperability translates into a more open digital market and that consumers can freely exercise their right to choose applications, services and content without restrictions imposed by gatekeepers[1].

The subsequent Commission implementing decision[2], the European Commission reflected several of the concerns raised by Ius Omnibus in its decisions, regarding the risks of a purely request-based model for interoperability. It introduced measures to strengthen transparency and predictability in this process, including obligations on documentation, clear timelines, and review mechanisms (pp. 30–32).

The Commission also addressed the perspective of consumers, emphasizing the importance of the end-user journey, ease of installation, and the interaction between Articles 6(7) and 6(4) of the DMA. In addition, it adopted measures to tackle obstacles in the distribution and use of applications, which substantively reflect the positions set out in the contribution of Ius Omnibus (pp. 27–29).

In line with this commitment, Ius welcomes this new opportunity to contribute to the regulatory debate and reaffirms its priority: to ensure that the Commission's decisions under the DMA contribute to a more equitable, innovative and consumer-focused digital market.

III. The public consultation

In the context of the first review of the DMA, the European Commission launched a public consultation on 3 July 2025. The process seeks to gather evidence and observations from all stakeholders on the application of the DMA since its implementation, in order to assess its effectiveness in creating more contestable and equitable digital markets.

The consultation covers issues central to the implementation of the DMA, including: the overall effectiveness of the regulatory framework, the impact of obligations on users and consumers, the possible extension of interoperability to online social networking services, and the review of both the list of essential platform services and the obligations set out in Articles 5, 6 and 7.

---

[1] Ius Omnibus. (2025, January 9). Comments to the Public Consultation launched by the European Commission on Case DMA.100204 SP-Apple-Article 6(7) [Public consultation contribution]. Ius Omnibus. Accessible here.

[2] Commission implementing decision of 19.2.25 pursuant to Article 8(2) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector. Case DMA.100204 – Article 6(7) – Apple iOS and iPadOS – SP – Process. Available here.

IV. Comments

The first review of the DMA provides a crucial opportunity to assess whether the current regulatory framework is fulfilling its objective of limiting the power of gatekeepers and ensuring fairer digital markets. Although the DMA has been a significant regulatory advancement, practical experience shows that major challenges remain in key areas, such obtaining as consent for the use of personal data, effective interoperability of services and applications, access to relevant information for stakeholders, and the possibility of bringing collective actions.

These points are relevant insofar as they directly affect the balance of power between platforms, businesses and consumers, and because they define the extent to which the DMA transforms the existing dynamics in digital markets. Poor or fragmented enforcement risks weakening the scope of the regulation or allowing existing imbalances to persist.

In this context, the following observations focus on identifying gaps or areas that require additional measures in order to strengthen the effectiveness of the DMA and ensure that consumer rights are guaranteed.

1. CONSENT-BASED MODEL UNDER ASYMMETRIC CONSUMER RELATIONS: how gatekeepers turn a right into a formality

Consent is central to the DMA, particularly in Articles 5(2) and 6(10), which prohibit gatekeepers from combining personal data from different services without consent to processing, combination and cross-use within the meaning of the GDPR. In principle, these provisions should strengthen consumer autonomy and limit the indiscriminate accumulation of data that consolidates the power of platforms.

However, experience has shown that this consent, far from being an optimal mechanism for empowerment, has become a mere instrument. In this sense, the DMA reflects the so-called "circularity of consent": the user, in theory, has decision-making capacity, but this is exercised conditioned by the gatekeeper's position of dominance, the lack of real alternatives, and a deliberate overload with manipulative terms and conditions. The asymmetry of information and power is so pronounced that users can rarely understand the value of their data or the consequences of its use, while platforms employ techniques that induce default acceptance. The possibility of refusal is often hidden behind inaccessible interfaces or lengthy processes, so that user consent becomes a formality rather than a free and informed decision.

1.1. The added problem of dark patterns.

This erosion of consent is exacerbated by the use of 'dark patterns': deceptive design patterns that manipulate the architecture of choice and systematically incline the user

towards acceptance. Common examples include hiding the opt-out option behind multiple steps, presenting acceptance as the fastest or most attractive option, or creating false urgency to pressure the user. These practices reduce individual autonomy and, even if consent is formally valid, render it ineffective.

Aware of this risk, the DMA incorporated an anti-circumvention clause in Article 13 aimed at preventing gatekeepers from using dark patterns to circumvent the obligations of the regulation. However, the absence of a uniform definition of dark patterns in the European regulatory framework creates legal uncertainty and loopholes that gatekeepers can exploit. Hence, the Commission has announced the future Digital Fairness Act, which seeks to close these gaps through a horizontal ban on dark patterns and the introduction of the principle of fairness by design.

The concern is not limited to Europe either. In the United States, the Federal Trade Commission (FTC) has identified dark patterns as practices that violate the principle of consumer autonomy by exploiting their cognitive, emotional and socio-economic biases. Its analysis is not only about a lack of transparency in the interface, but also about a form of structural manipulation that substantially alters freedom of choice. From this perspective, dark patterns are a technique that reinforces the dominant position of large platforms and exacerbates the asymmetry between providers and users, undermining the real possibility of freely and informed consent.

The consequences of this dynamic are serious. On the one hand, gatekeepers continue to accumulate and cross-reference data under the cover of formally valid but ineffective consent. On the other hand, this mechanism reinforces network effects and barriers to entry, consolidating the competitive advantage of gatekeepers over smaller players[3].

1.2 Strengthen obligations relating to the mass combination and cross-referencing of data.

Adding to this deficit is the uncertainty recently created by German courts. In the Meta AI case, the Cologne Higher Regional Court (case number 15 UKl 2/25) concluded that Article 5(2)(b) would apply only to individual profiles, excluding the use of "partially anonymised" or aggregated data to train AI systems. This interpretation opens a regulatory loophole: it would suffice to present the data as "partially anonymised" for the gatekeeper to continue exploiting large volumes of information from different services without restriction, thereby strengthening its market position.

This case highlights that there is still significant room for interpretation around key provisions of the DMA, especially those related to data combination.

This reasoning is problematic. Limiting the ban solely to individual profiles and leaving out aggregated or partially anonymised uses opens the door too widely for

[3]Car, P., & Cassetti, F. (2025). *Regulating dark patterns in the EU: Towards digital fairness* (EPRS ATA 2025-767191). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf

gatekeepers to continue exploiting their privileged position in terms of data access. The German decision appears to reduce the scope of the rule and render the prohibition meaningless, since in practice most AI training relies on large volumes of aggregated data, which, although they do not directly identify individual users, are still the result of accumulation across different services.

The risk of this type of interpretation is clear: it creates legal uncertainty, with national courts applying divergent criteria and, as a result, gatekeepers exploring regulatory loopholes to further exploit their advantage in terms of data accumulation.

The recent disciplinary proceedings against Meta by the European Commission exemplify the problem of consent in the digital economy, especially when managed by gatekeepers. Meta implemented a 'pay-or-consent' model, whereby users must choose between accepting the massive use of their personal data for personalised advertising and training of artificial intelligence systems, or paying a subscription for an ad-free version of the service. Although this model can be interpreted as an expression of freedom of choice, the reality is that the paid alternative is not equivalent to the standard model in terms of cost or functionality, which leads most users to consent to the intensive use of their data.

The European Commission concluded that this model violated Article 5(2) of the DMA and fined Meta €200 million, emphasising that the regulation requires offering an alternative service with limited use of personal data that is, in essence, equivalent to the standard.

Beyond the specific infringement observed, the problem is of a structural nature. The 'pay-or-consent' model shifts the burden of exercising their rights onto users, establishing a consent that, despite complying with legal formalities, is materially ineffective. When this logic is combined with interfaces designed using dark patterns and with the growing dependence on quasi-essential digital services, the dominant platform reinforces structural inequality towards the consumer. This legitimises the massive exploitation of personal data, undermines effective competition, erects barriers to entry and erodes privacy guarantees in the digital environment, consolidating the market power of these operators and weakening the autonomy of users.

Also, the German case against Google under Section 19a GWB[4] is of great importance for the topic. The Bundeskartellamt required Google to obtain explicit and informed user consent before combining personal data across its different services. This obligation goes beyond the DMA by strengthening safeguards against potentially misleading or manipulative consent banners and reinforcing user control over data processing. While the measure enhances transparency and consumer protection, it also raises practical challenges, such as how to design consent requests that are genuinely

[4] Bundeskartellamt, Decision of 5 October 2023, Case B6-46/22 – *Google (Data Processing Terms)*, pursuant to Section 19a(2) GWB.

clear and free, and how to reconcile these national requirements with the broader EU framework under the DMA and the GDPR.[5]

It is therefore essential that the EC intervene with specific guidelines clarifying how the prohibition on data combination should be understood. These guidelines should make it clear that the aggregation and use of supposedly 'de-identified' data between different services of the same gatekeeper may also violate the DMA, insofar as they reinforce the concentration of data power and create barriers to entry for other competitors. In addition, they should specify which anonymisation standards are acceptable and which safeguards must be applied for user consent to be truly valid.

A more robust interpretative framework would prevent contradictory decisions from arising and ensure that the prohibitions in the Regulation are interpreted consistently across the Union. This would better fulfil the objective of the DMA: to prevent gatekeepers from exploiting data accumulation as a tool to reinforce their market position, both in traditional services and in emerging areas such as AI.

Ultimately, the Meta case demonstrates that the application of the DMA cannot be left solely to national courts without prior guidance from the European Commission. The Commission should be proactive in issuing guidelines, clarifying the limits of practices such as data aggregation and ensuring that the regulation retains its full force. Only in this way can restrictive interpretations be prevented from ultimately weakening the transformative effect that the DMA aims to have on European digital markets[6].

In this context, the revision of the DMA should prevent consent from being reduced to a mere formality devoid of content. To this end, it would be necessary to:

- Requiring that the information provided to users be clear, understandable and standardised, transparently explaining the uses and risks associated with data processing.
- Establishing accessible configuration options free from dark patterns that manipulate the user's decision.
- Prohibiting access to basic or essential services from being dependent on the acceptance of data sharing.
- Giving the European Commission a more active role in supervising and harmonising consent criteria, avoiding fragmented interpretations that weaken the scope of the regulation.

With these safeguards, consent can become an instrument of empowerment, in line with the spirit of the DMA, rather than perpetuating the current situation in which

[5] Carugati, C. (2025). *Digital Competition's submission on the Digital Markets Act review*. Digital Competition.

[6] Díez Estella, F. (2025, april 25th). Del abuso de posición dominante a la regulación digital. Almacén de Derecho. https://almacendederecho.org/del-abuso-de-posicion-dominante-a-la-regulacion-digital

gatekeepers benefit from formal consent that legitimises practices contrary to competition and privacy protection[7].

2. INTEROPERABILITY: the pending task of public enforcement

The experience with Apple shows that a system based on requests to the gatekeeper, while it may be seen as a first step forward, in reality leaves a large margin of discretion intact in the hands of the company. This means that Apple retains the ability to decide how, when and under what conditions interoperability is granted.

Such processes do not remove the structural barriers affecting the distribution of applications and content. Developers continue to face limitations in accessing the ecosystem, and consumers remain subject to a framework in which they cannot freely install any application or software, but only those that Apple validates and on the terms it imposes. The 'walled garden' effect remains, reinforcing dependency and reducing real alternatives.

Furthermore, a system that relies on the initiative of the gatekeeper inevitably slows down innovation. Each interoperability request involves a process that can be slow and has uncertain results. This discourages small developers, who do not have the resources to sustain procedures, and reinforces the network effect.

Ultimately, it is end users who suffer, as they see their options limited and are faced with a closed ecosystem.

A more robust framework is needed: interoperability should be guaranteed by clear and directly enforceable obligations on gatekeepers, without depending on their willingness.

The process should be transparent, with defined deadlines and independent control mechanisms, so that it does not become an instrument of self-preference or covert exclusion. It would also be necessary to strengthen supervision by the Commission and encourage consumers and developers to challenge unfair decisions by gatekeepers.

For the DMA to achieve its objective, it is essential to establish a system that limits the ability of these platforms to condition access, ensuring that users have the effective freedom to decide which applications to use and how to configure their devices.

3. AVOIDING SELF-PREFERENCING IN GATEKEEPERS' CPS

When addressing this issue, it is necessary to mention the Google Shopping case, which is a clear example of how self-preferencing negatively affects consumers. The European Commission found that Google systematically gave preferential treatment to its own price comparison service, displaying it in prominent positions, while even the highest-ranked rivals were relegated to later pages. In practice, this drastically reduced

[7] Evirom. (2025, june 17th). Meta AI y tus datos personales: ¿Qué ha pasado y cómo protegerte? Evirom. https://www.evirom.com/meta-ai-privacidad-usuarios-2025/

the visibility of relevant alternatives and limited users' ability to compare offers on equal terms.

Another recent illustration of this concern can be found in the judgment of the Regional Court of Mainz (LG Mainz) of 25 August 2025 (Case 12 O 123/24). In this case, brought by the telecommunications provider 1&1. The court examined the process of setting up Android smartphones and found that Google had unfairly favoured its own email service, Gmail, over rival providers such as GMX and Web.de. During the setup process, users were guided in a way that strongly suggested or even nudged them towards choosing Gmail, while competing services were either presented less prominently or not offered in equal terms.

The court considered this a form of self-preferencing that was incompatible with the objectives of the DMA, as it limited users´ ability to make an informed, unbiased choice between competing email providers. Crucially, the decision stressed that such conduct not only harms competitors by restricting their access to potential users, but also reduces consumer welfare by depriving individuals of genuine alternatives and by entrenching the market power of gatekeepers.

The consequences are clear: consumers had fewer real choices, faced higher prices or lower quality services, and saw their freedom of choice restricted. In addition, this bias reinforced the gatekeeper's power, weakening competition and preventing third-party innovation from reaching the market. As economic analysis highlights, self-preferencing leads users to end up choosing the gatekeeper's own products, even when better alternatives exist. The damage caused by such practices not only affects competitors who see their market share reduced but also negatively affects the entire market and ultimately harms consumers.

Thus, self-preference is not merely an abstract competition problem, but a practice with very concrete and adverse effects on freedom of choice and consumer welfare. Recital 52, which addresses this issue, should be equipped with real mechanisms to ensure compliance[8].

4. STRENGTHEN TRANSPARENCY FOR ADVERTISERS.

Although this recommendation directly affects businesses and not consumers, the lack of transparency in sectors such as digital advertising is also of particular concern with indirect effects for consumers. Gatekeepers exercise almost complete control over the conditions under which advertisers and publishers participate in the advertising ecosystem, but these conditions are opaque, complex and very difficult to negotiate. This creates a scenario in which advertisers and publishers do not clearly know how prices are determined, what the true reach of their campaigns is, or what data is

[8] Peitz, M. (2022). *The prohibition of self-preferencing in the DMA*. Centre on Regulation in Europe (CERRE). https://cerre.eu/wp-content/uploads/2022/11/DMA_SelfPreferencing.pdf

relevant for measuring results. The immediate consequences are additional costs and a reduced ability to compare and choose between service providers.

The Regulation already requires gatekeepers to provide access to measurement data and tools that allow for independent verification of service provision. However, in practice, these requirements are not met or are only partially met. The lack of transparency results in an information asymmetry that favours the gatekeeper and limits the ability of professional users to switch providers or negotiate better terms.

This problem is particularly serious because digital advertising is one of the pillars of many gatekeepers' business models. By controlling both data collection and advertising distribution channels, platforms are in a privileged position to impose unclear or discriminatory conditions, reinforcing their market power and reducing opportunities for smaller players.

The DMA needs to be enforced to a high standard. It is not enough to require access to data; it is necessary to ensure that the information is complete and standardised. In addition, there must be accessible and rapid dispute resolution mechanisms so that advertisers and publishers can challenge terms without fear of reprisals or excessive costs.

The possibility of external auditing of measurement and revenue-sharing systems should become mandatory, and penalties must be clear and dissuasive.

5. PRIVATE ENFORCEMENT OF THE DMA

5.1 Collective redress

Comparative experience shows that this mechanism is essential: neither consumers nor most SMEs have sufficient resources, information or incentive to take action individually. The costs of litigation are too high and the potential benefits too small when divided on a case-by-case basis. Without collective action, most infringements would go unchallenged.

Directive (EU) 2020/1828 on representative actions has opened the door for qualified entities to defend collective interests, and some Member States have already taken steps in this direction: Germany has incorporated into its legal system a system that allows for redress actions for infringements of the DMA. Innovative models such as the assignment of rights have also been developed.

However, there are gaps: 1) the transposition of the Directive has been uneven, creating differences between countries and making it difficult to coordinate cross-border proceedings; 2) the text of the DMA does not establish a specific procedural framework for collective actions, leaving open questions such as how actions are coordinated in different Member States, what the scope of redress is, etc.

It would be necessary to:

- Ensure that qualified entities can act without excessive obstacles

- Regulatory recognition of the possibility of claiming and receiving compensation
- Establish coordination mechanisms between national courts and the European Commission to avoid overlaps
- Adequate funding for these actions, so that consumer associations and SMEs can sustain long and complex proceedings against platforms. For example, through European litigation support funds
- Promote the creation of a European register of collective actions in the field of DMA that centralises information and facilitates coordination between courts.

Finally, we would point out that these collective actions in the field of the DMA will be predominantly 'follow-on' in nature: many claims will depend on previous decisions by the Commission (primarily designation of gatekeepers) or administrative or judicial bodies, as well as on the existence of evidence developed in public proceedings. Consequently, firm and effective public enforcement, involving investigation, clear sanctioning decisions and active supervision, is a prerequisite for private actions to be more than merely formal, but to have a real deterrent effect on gatekeepers.

6. BROAD ACCESS TO INFORMATION

It is essential that the parties have sufficient and timely access to the relevant files and data.

In practice, access remains very limited. The Commission and gatekeepers often invoke trade secret protection and confidentiality as grounds for restricting the disclosure of information.

This has the opposite effect to that intended by the DMA: it weakens the ability of third parties to understand decisions, discourages private enforcement and maintains information asymmetries.

On the one hand, consumers and SMEs, who are potential victims, do not have access to data that would enable them to prove the damage suffered or identify practices that contravene the DMA. This applies even in the case of entities qualified to bring collective actions, which face significant barriers to obtaining evidence.

Disclosure policy must move towards a more balanced model:

- Data rooms could be set up for interested parties to consult information without the possibility of filtering it.
- Standardise the timeframes within which the Commission and gatekeepers are required to provide information.

Similarly, it is crucial to ensure access to algorithms and data linked to DMA obligations. Various analyses warn that, although the DMA and DSA contain multiple provisions in

this area, their practical application lacks clarity regarding deadlines, quality and continuity of access.

The DMA sets compliance windows after gatekeeper designation, yet leaves broad discretion over how obligations are implemented, creating uncertainty about what counts as timely compliance. Both laws, and specifically the DMA in this case, lacks operational detail, leaving scope and quality of access undefined and raising the risk that obligations could be met in a merely formal sense without ensuring meaningful benefits for businesses or end users.[9]

Some gatekeepers have circumvented or limited obligations, for instance by offering degraded forms of interoperability or introducing technical barriers that undermine continuity of access.[10]

For consumers, this means promised improvements—such as greater choice of services, easier switching between platforms, and consistent availability of features—may be delayed or delivered only in partial form. Without clearer standards on compliance deadlines and stronger criteria for the quality and continuity of access, the consumer-facing benefits of the DMA and DSA risk being significantly reduced.

Among other noteworthy proposals, the use of secure data rooms and the application of a structured test to balance the interest in transparency with the protection of trade secrets, privacy and security are highlighted.

At the same time, it is noted that access to the file provided for in Article 34 DMA is mainly granted to the parties concerned, leaving out consumers, SMEs, or researchers who may also be affected by illegal practices. This limitation reduces the effectiveness of Articles 6(10) and 6(11) DMA, which provide for access to data generated by the use of the platform and information on rankings, queries, clicks and views, and Article 19 DMA, which empowers the Commission to request information, including algorithms, since without adequate disclosure mechanisms, these obligations are largely meaningless.

The academic literature further emphasises that the Implementing Regulation to the DMA (DMA-IR) restricts the scope of access to file primarily to gatekeepers and undertakings formally concerned by proceedings. Third parties, even when directly affected, are not recognised as beneficiaries of these rights. Access is, in practice, "narrow, fragmented and at the discretion of the Commission", creating a sharp imbalance between those subject to obligations and those harmed by potential infringements. The article also stresses that confidentiality is interpreted broadly, allowing extensive redactions and limiting the utility of documents disclosed. While the DMA-IR foresees the use of non-confidential versions of submissions and decisions, the

[9] CERRE. (2023). Access to data and algorithms: For an effective DMA and DSA implementation. Centre on Regulation in Europe.
[10] Article 19. (2024). Digital Markets Act: Trends, gaps, and insights from the first year of enforcement.

quality of these is often so reduced that meaningful scrutiny by external actors becomes impossible.

Moreover, the Commission retains wide discretion in deciding whether to grant access under special modalities such as confidentiality rings or data rooms, which the literature describes as important but insufficient tools, since their availability is neither systematic nor guaranteed for all stakeholders. This reinforces the asymmetry: gatekeepers can access the full record in order to defend themselves, but consumers, SMEs, or qualified entities cannot access the same material to pursue damages or monitor compliance.

It is also highlighted that the Commission's publication duties under the DMA (for example, concerning compliance reports or market investigation findings) are framed in general terms, with no uniform requirements regarding timeliness, format or quality of the published information. As a result, disclosure may be delayed, overly selective, or fragmented, undermining the transparency objectives of the DMA.[11]

Therefore, a balanced access policy must also include specific guarantees for third parties with a legitimate interest, ensure minimum standards of quality and format for the data provided, and establish clear limits on automatic invocation of confidentiality, so that access to information, algorithms and data is not merely formal, but effective.[12]

7. ANALYSE NOTIFIED CONCENTRATIONS IN AN AUTONOMOUS MANNER

Article 14 DMA and Recital 71 impose an obligation on gatekeepers to notify the EC of any concentration operation in which they are involved, provided that it affects digital platform services or sectors linked to data collection. This obligation is independent of whether or not the transaction exceeds the thresholds set out in the Merger Regulation or in national merger control rules.

Recital 71: *"Gatekeepers should inform the Commission, prior to their implementation, of all their planned acquisitions of other undertakings providing core platform services or any other services provided in the digital sector or other services enabling data collection*."

This presents a significant gap: it does not establish what the Commission should do with the information received. In practice, the notification obligation risks becoming a mere formality, as the EC has no clear procedure for assessing the impact of the transaction or for following up on the information provided. Currently, the only

[11] Hornkohl, L. (2024). Transparency Unveiled: Access to Information in Digital Markets Act Proceedings on EU Level. Nordic Journal of European Law, 7(2). https://journals.lub.lu.se/njel/article/view/26289

[12] Edelson, L., Graef, I., & Lancieri, F. (2023, march). *Access to data and algorithms: For an effective DMA and DSA implementation*. Centre on Regulation in Europe (CERRE). https://cerre.eu/wp-content/uploads/2023/03/CERRE-Access-to-Data-Algorithms.pdf

obligation is to share the information with national competition authorities and publish it annually, which does not guarantee substantive or preventive control.

This is problematic because many acquisitions made by large platforms, even if they do not reach the notification thresholds, can have a significant impact on competition and consumer rights. For example, so-called killer acquisitions, where large established market players acquire small, innovative startups not necessarily due to their current turnover, but because of their future potential to compete or innovate, can strategically eliminate potential competitive threats. Since the year 2000, big digital platforms within the scope of the DMA have acquired nearly 700 small companies worldwide, but only a few were notified to the European Commission due to turnover thresholds not being met. This leads to increased market concentration and reduced competition, as many of these acquisitions have not been thoroughly scrutinized by competition authorities.

The current EU framework mainly relies on turnover thresholds for merger notification, which inadequately captures acquisitions of startups with growth potential but limited current revenues. This gap allows acquisitions that may harm competition by removing nascent competitors through "killer acquisitions", where targets often discontinue their products post-acquisition, undermining market quality and innovation. Furthermore, the burden of proof currently lies with competition authorities, which struggle to predict competitive dynamics of fast-evolving digital markets. The proposal is to amend the DMA to empower the European Commission to scrutinize any acquisition by gatekeeper platforms where it pertains to their respective CPS regardless of turnover and to shift the burden of proving that a merger is not harmful onto the acquiring platform. This approach would leverage the market players´ superior knowledge to improve merger control effectiveness in dynamic and complex digital markets[13].

The Guidelines should introduce an ex-post control mechanism for transactions notified under Article 14, or, when a gatekeeper notifies a merger, a simplified review procedure should be activated, accompanied by a precautionary suspension preventing the transaction from being carried out. This procedure should be agile, with short deadlines, but robust enough to enable the Commission to identify whether there are serious risks to competition or consumer interests.

However, even the existence of ex post control could prove insufficient, as this mechanism does not allow for the preventive determination of which transactions may cause real harm to consumers. It is therefore advisable that, in addition to the mandatory notification by gatekeepers, Article 14 be accompanied by an automatic control procedure that is activated immediately upon each notification. This procedure should include a precautionary suspension preventing the transaction from being executed until the Commission has completed a preliminary review within a short time frame. This would ensure more effective preventive control, preventing potentially

[13]Mariniello, M. (2025). *Reinforcing EU merger control against the risks of acquisitions by big tech*. Bruegel Policy Brief. https://www.bruegel.org/policy-brief/reinforcing-eu-merger-control-against-risks-acquisitions-big-tech

harmful concentrations from materialising before the Commission can assess their effects on competition and consumer rights[14].

8. INCORPORATING ARTIFICIAL INTELLIGENCE INTO THE DMA ANALYSIS

The Commission is also seeking comments on its implications for the AI sector. On whether the DMA can effectively contribute to a competitive and fair AI sector in the EU.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) does not address the obligations of developers in view of their rapid growth and eventual gatekeeper position in the market.

In this regard, we consider it necessary to open the debate on the appropriateness of treating certain artificial intelligence services as core platform services (CPS) for the purposes of the DMA. The integration of AI models and functionalities into large-scale digital services poses risks similar to those that justify the regulation of gatekeepers: data accumulation, network effects, lack of algorithmic transparency and discriminatory practices that may prevent the entry of new competitors.

The Commission itself, through the DMA High Level Group, has already expressed its concern about the impact of AI on fairness and competition in digital markets. However, since then, there have been no significant regulatory advances or concrete initiatives to address this issue within the framework of the DMA. This inaction creates a vacuum that gatekeepers can exploit, consolidating dominant positions through AI services that are not subject to the ex-ante obligations of transparency, interoperability or data access provided for in the regulation.

If this situation continues, there is a real risk that AI will become an additional lever of concentration and competitive exclusion, disproportionately affecting SMEs, start-ups and consumers. The speed of technological development contrasts with the slowness of the regulatory response and may lead to an irreversible consolidation of market power in the hands of a few players[15].

In any case, we welcome the steps being taken by the Commission towards a comprehensive analysis of the implications of AI in relation to the major players in

[14]Helminger, J., & Hornkohl, L. (2024). *Transparency unveiled: Access to information in Digital Markets Act proceedings*. *European Journal of Law and Technology*. https://journals.lub.lu.se/njel/article/view/26289

[15] Yasar, A. G., Chong, A., Dong, E., Gilbert, T. K., Hladikova, S., Maio, R., Mougan, C., Shen, X., Singh, S., Stoica, A.-A., Thais, S., & Zilka, M. (2023). *AI and the EU Digital Markets Act: Addressing the risks of bigness in generative AI*. *arXiv*. https://arxiv.org/abs/2308.02033

digital markets. Specifically, the consultation asks about an obligation imposed by the DMA that may be of particular importance in the short term when AI systems have become more widespread and integrated into digital markets: the audit obligation outlined in Article 15.

The audited description of profiling techniques will provide valuable information for assessing the risks and opportunities that the new gatekeeper will face. In these cases, it is recommended that the Commission have detailed implementing rules adapted to the vicissitudes of artificial intelligence systems. It is therefore recommended that Articles 15(2) and 46(1)(g) of the DMA be used when the designation of a gatekeeper is prompted by the use of artificial intelligence, regardless of the CPS in which it operates.

Therefore, the Commission's policy should:

- Assess the possibility that AI-based services may be designated as CPS when they meet gatekeeper criteria and have structural effects similar to those of current regulated services.
- Issue clear guidance on how DMA obligations should apply to AI functionalities integrated into existing platforms, ensuring that they are not left outside the regulatory framework.
- Establish specific commitments and defined deadlines for developing legislative or regulatory proposals that clarify the scope of the DMA in relation to AI.
- Promote transparency and data access mechanisms that allow for independent auditing of AI systems, preventing confidentiality or trade secrets from being used as an absolute barrier to scrutiny[16].

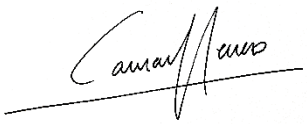
We hope that our comments can provide the Commission with valuable insights and recommendations that reflect a genuine concern for consumer welfare and the proper functioning of a market guarded by gatekeepers.

For Ius Omnibus,

[16] European Commission. (2024, May 22). *High-Level Group for the Digital Markets Act: Public statement on artificial intelligence*. https://digital-markets-act.ec.europa.eu/high-level-group-digital-markets-act-public-statement-artificial-intelligence-2024-05-22_en

Lena Hornkohl, President of Ius Omnibus

Carmen Herrero Suárez, Vice-President of Ius Omnibus



Carmen Estevan de Quesada, Board Member of Ius Omnibus