From market dominance to data dominance: reimagining competition law for the digital age

Ina VIRTOSU
PhD in EU Law, University of Macau, SAR Macau, China
yb67199@connect.um.edu.mo, ivirtosu3@gmail.com

Abstract
In the digital economy, data has emerged as the key source of competitive advantage - a currency that determines market control and innovation potential. It now plays a role similar to what capital or labour once did in shaping competitive advantage. However, traditional competition law - built around measures such as market share, pricing, and output - often fails to reflect the realities of data-driven markets. Digital platforms thrive on access to user data, network effects, and complex ecosystems that amplify their market power in ways conventional tools struggle to assess. This paper explores the idea of "data dominance" as an emerging form of market control and argues for an updated approach to competition policy that recognizes this shift. It looks at how data concentration can act as a barrier to entry for smaller firms, how interoperability and data portability can encourage fairer competition, and why stronger coordination between competition and data protection laws is essential. The discussion concludes by suggesting practical ways regulators can adapt enforcement strategies to ensure digital markets remain open, innovative, and centred on the public interest.

Keywords: Data monopolies, interoperability and data portability, exclusive access, data gatekeeper.

1. Introduction: the shift from industrial to digital market power
Competition law has long focused on addressing the influence of dominant players in traditional industries. In the industrial era, regulators assessed market control primarily through tangible measures such as production capacity, output, and market share [1]. This approach was effective when physical goods and manufacturing defined market power. However, the rise of the digital economy has fundamentally changed the landscape. Today, a firm's competitive advantage depends less on physical assets and more on its control over data. Access to user information, behavioral patterns, and digital footprints has become central to shaping market outcomes, giving rise to a new type of market power: "data dominance" [2]. Leading digital platforms such as Google, Amazon, Meta, and Alibaba illustrate this transformation. These companies collect and analyze vast volumes of user data, which allows them to refine services, improve targeting, and maintain self-reinforcing ecosystems [3]. This feedback loop - more users generating more data, which enhances service quality and attracts more users - creates barriers for new entrants and consolidates market power [4]. Given these developments, the question arises: is traditional market share still a meaningful measure of dominance in the digital age? Scholars and regulators increasingly argue that competition law must adapt to account for the role of data as a critical source of power [1, 5]. This paper explores this shift, examining how data monopolies can act as barriers to entry, the role of interoperability and data portability in fostering competition, and the importance of aligning competition law with data protection frameworks to ensure open, fair, and innovative digital markets [2, 6].

2. The rise of data dominance

2.1. Data as a strategic asset

The digital economy has fundamentally reframed the foundations of market power. Whereas industrial-era dominance depended on tangible assets such as factories, supply chains, or distribution networks, today's leading firms derive much of their influence from the scale and scope of data they collect. This shift has made data a central strategic resource - one that not only supports day-to-day operations but also shapes long-term competitive dynamics.

In digital markets, data increasingly determines which firms are able to innovate quickly, anticipate market trends, and deliver services that adapt to individual user preferences. Rather than merely recording transactions, data allows companies to develop predictive capabilities, understand user behavior in real time, and refine algorithms that grow more accurate with each interaction [1]. The ability to turn raw information into actionable insights has become a defining feature of market leadership.

Major platforms illustrate this transformation clearly. Google's search engine improves continuously because its algorithms learn from billions of daily queries - identifying patterns, refining rankings, and optimizing targeted advertising. This constant feedback loop is possible only because of the company's unmatched volume and diversity of data [3]. Similarly, Amazon integrates browsing histories, purchasing data, logistics information, and even voice assistant interactions to personalize recommendations, manage inventory, and predict demand across its vast retail ecosystem. These services become more effective - and more indispensable - as the underlying datasets grow.

What makes data particularly powerful as a strategic asset is that it accumulates over time and becomes increasingly difficult for smaller firms to replicate. A new entrant may build a sophisticated platform, but without access to similarly deep and varied datasets, its algorithms will remain less accurate and its services less responsive. As the OECD notes, data-rich incumbents benefit from an "experience advantage": each interaction enhances the quality of their products, which in turn attracts more users and generates even more data [2]. This cycle reinforces the position of dominant firms and widens the competitive gap.

Moreover, data advantages are not just quantitative. Their qualitative dimension - encompassing metadata, behavioral insights, and cross-service linkages - adds layers of value that cannot be easily duplicated. For example, Google Maps does not rely solely on geographic information; it incorporates years of real-time traffic flows, route corrections, and mobility patterns. These insights create a dataset so deep that it effectively insulates the service from meaningful competition. This illustrates why data has become both a driver of innovation and a structural barrier to entry.

2.2. Network effects, self-reinforcing ecosystems and data monopolies

One of the reasons why data dominance has become so powerful in digital markets is the strength of network effects. The basic idea is simple: the more people who use a platform,

the more useful it becomes. But in digital markets, this dynamic goes even further. Each user interaction - every click, search, message, or purchase - produces new data. Platforms feed this information back into their algorithms, improving recommendations, personalisation, and overall service quality. As noted in research published by Björn Lundqvist, this creates a self-reinforcing cycle: more users generate more data, better data leads to better services, and improved services attract even more users [4].

Large platforms like Meta and Alibaba show how powerful these feedback loops can be. Meta's business model depends heavily on the detailed data it gathers from billions of social interactions, allowing it to offer highly targeted advertising that few rivals can match. Alibaba combines data from e-commerce sales, payment services, and logistics into a tightly integrated ecosystem. Because each of these services provides information for the others, the platform becomes increasingly valuable over time. Even if a competitor launches a superior product, it may struggle to compete without access to an equally rich flow of user data. This exclusive control over data can create a type of monopoly that looks quite different from the traditional dominance associated with industrial markets. Instead of relying on physical assets or financial scale, digital monopolies are built on information [5]. Competing firms may find themselves locked out simply because they cannot access the same depth or breadth of data.

Competition authorities have started to pay closer attention to these issues. The European Commission's investigation into Amazon's use of third-party seller data raised concerns about whether the company was leveraging sensitive information to advantage its own retail operations [3]. Google's use of search and advertising data has also attracted scrutiny, both in Europe and the United States, warning about the competitive implications of such data concentration.

The emergence of data-driven market power challenges many of the basic tools used in competition law. Market share alone often fails to capture the strength of a digital platform. To understand dominance today, regulators increasingly need to look at several factors when assessing market power in data-driven markets. One key issue is whether dominant firms limit or block access to datasets that smaller competitors genuinely need in order to operate on equal footing. Another important aspect is the way platforms combine multiple services, such as payments, logistics, cloud storage, or advertising into a tightly linked ecosystem that makes it extremely difficult for users or business partners to switch to alternatives. A further concern is the role of algorithmic learning. Continuous improvements driven by large volumes of data can steadily reinforce a platform's advantage [2]. Together, these features show how market power today can solidify through information flows rather than through traditional control of physical or financial resources. These considerations suggest a need for modernized approaches to antitrust enforcement that account for data as a core source of market power rather than a byproduct of sales.

3. Data monopolies as barriers to entry: why challengers struggle to catch up?

In today's digital markets, strong incumbents can leverage their data advantage to shut out competitors - not just through scale, but via strategic control of information. Below, we explore how this works in practice, the risks it poses to competition, and real-world examples.

3.1. Concentration of data and competitive lock-out

In digital markets, an early lead in data collection can quickly translate into a long-term competitive advantage. What begins as a simple difference in scale often becomes a structural barrier that keeps new entrants at a distance. Dominant firms do not merely have more users; they possess richer, deeper, and more granular datasets that improve their algorithms and services in ways rivals cannot easily match [6]. By aggregating transactional, behavioral, and meta-data from users and third parties, incumbents build a knowledge base that is difficult for newer or smaller competitors to replicate [7]. This data concentration acts as a powerful barrier to entry: without access to similar datasets, challengers cannot match the incumbents' insights or refine their business models with the same precision. Moreover, incumbents may design contracts or technical systems so that access to sensitive data is limited or controlled. This unequal access means that data becomes an "essential input" for meaningful competition, yet one that is effectively denied to rivals [8].

3.2. Exclusive access, vertical integration, and self-preferencing

One of the clearest barriers is *exclusive access to high-value datasets*. Some platforms collect data that is non-replicable - either because of their massive user base, the sensitivity of what they track, or because users rarely multi-home across competing services [9]. This exclusivity means that newcomers, even if they have innovative ideas, cannot simply "scale up" their data collection to the level of an established platform. The value lies not only in volume, but in diversity and historical depth: a new mapping service may copy basic geographic data, but replicating years of behavioral patterns, traffic corrections, and search history embedded in Google Maps is virtually impossible.

A second barrier comes from *vertical integration* across complementary services. Many leading platforms operate at multiple layers of the digital ecosystem. For instance, Amazon combines marketplace hosting, retail operations, logistics, cloud computing, and advertising. Likewise, China's giants - such as Alibaba and Tencent - run broad ecosystems linking e-commerce, payments, messaging, cloud services, and digital media. This integration lets them pool data from different touchpoints, creating insights and synergies that standalone competitors cannot match. The richer data enhances each piece of the business, and in return, those improved services draw users ever deeper into the platform's ecosystem [2].

This vertical integration also enables *self-preferencing* - when a platform uses its exclusive data to benefit its own products. Amazon, for example, has faced serious scrutiny from the European Commission for using non-public seller data from its Marketplace to inform its retail business. According to the Commission, Amazon uses this data to adjust pricing and

to decide which product categories to expand into, thereby disadvantaging third-party sellers [10]. In the U.S. and EU, critics argue that Amazon privileges its private-label offerings or favours its own products in search ranking by leveraging this data [11]. Similarly, Google's use of search-query and click-through data has raised concerns that it may use behavioral insights from its search business to benefit its advertising platforms - a potential unfair leveraging of data from one service to advantage another.

For startups and small firms, these data-driven dynamics are especially challenging. Many rely on dominant platforms for visibility or distribution - app developers depend on app stores, online stores depend on marketplace access, and advertisers depend on search and social platforms. This dependence gives incumbents significant leverage: a change in API access, data sharing terms, or algorithmic ranking can materially disrupt a small firm's business overnight. Additionally, young companies often lack the resources to build datasets that rival those of incumbents, limiting their ability to train competitive models or finely target customers. Even in jurisdictions that support data portability or user consent, the technical and financial costs of switching platforms - for both users and businesses - remain prohibitively high.

3.3. Case studies

These tensions are vividly illustrated in major competition cases. In 2017, in the Google Shopping decision, the European Commission concluded that Google had abused its dominance in general search by systematically giving preferential placement to its own comparison-shopping service while demoting rival services in its search results [12]. This preferential positioning was not simply a matter of visibility. Because Google controlled vast quantities of granular search-query and click-through data - information about what users searched for, which results they clicked on, and how they behaved thereafter - it could continuously refine and optimize its shopping service. Competing comparison-shopping sites, by contrast, had access only to limited data about their own users, leaving them unable to match Google's algorithmic improvements. The case illustrates how informational advantages can amplify the effects of self-preferencing, making it difficult for even well-designed competing services to gain traction [13].

A similar pattern emerges in the investigations into Amazon Marketplace. In 2020, the European Commission issued a Statement of Objections accusing Amazon of exploiting non-public seller data from its marketplace to compete directly against the very sellers who relied on the platform [10]. This data included real-time information about sales volumes, pricing strategies, shipping performance, and consumer demand - insights unavailable to other retailers. According to the Commission, Amazon used this information to guide decisions about which private-label products to launch, how to price them, and where to place them within search results. Beyond product selection, concerns were raised that Amazon's "Buy Box" algorithm, which determines which seller receives the most prominent placement, might implicitly favor Amazon's own retail offerings or sellers who used Amazon's logistics services.

In the United States, similar issues surfaced in congressional investigations into digital platforms. The U.S. House Judiciary Committee's 2020 report on competition in digital

markets highlighted allegations that Amazon's access to sensitive marketplace data allowed it to identify bestselling products and replicate them with private-label alternatives, while also using its control over platform infrastructure to shape market outcomes in its favor [14]. Although the legal standards differ from the EU, the competitive concerns are comparable: when a dominant platform both hosts and competes with third-party sellers, exclusive access to transaction-level data can tilt the competitive landscape.

The experience of China also sheds light on how data-driven ecosystems can entrench market power. For much of the past decade, China's digital markets have been organised around "walled garden" models - closed platforms that restrict interoperability and tightly control the flow of user data. Chinese regulators have repeatedly flagged these practices as obstacles to competition and innovation, noting that platform operators often use data exclusivity to lock users into their ecosystems [15].

A well-known example is the long-standing divide between Tencent's WeChat ecosystem and Alibaba's network of e-commerce and payment services. WeChat, which integrates messaging, payments, social media, and thousands of mini programs, historically restricted the sharing of links to Alibaba's Taobao and Tmall marketplaces. Alibaba similarly limited the use of Tencent's WeChat Pay within its platforms, ensuring that users who shopped on Taobao or used Alipay remained within Alibaba's environment [16]. These restrictions did not merely inconvenience users - they prevented meaningful cross-platform data flows, reinforcing path dependence and making it harder for consumers or sellers to switch.

These closed ecosystems fostered entrenched dominance. Once users accumulated transaction histories, contacts, social graphs, loyalty points, and payment information within a single platform, switching costs increased significantly. Smaller competitors lacked access to equivalent datasets, limiting their ability to offer personalised or data-driven services of comparable quality [17]. As a result, the leading platforms were able to translate data advantages into durable market power.

Regulators in China responded by adopting a more interventionist approach. In 2021, the State Administration for Market Regulation issued the Anti-Monopoly Guidelines for the Platform Economy, which explicitly targeted practices such as blocking competitor links, discriminatory access, and the coercive use of data [18]. Later that year, authorities went further by requiring major platforms to stop blocking each other's URLs and to allow users to access rival services more freely [15]. These measures represented a clear effort to open previously closed ecosystems and to reduce the competitive advantages arising from data concentration.

The regulatory shift toward promoting interoperability and data portability in China reflects a broader understanding: when platforms control large, multi-service ecosystems, data exclusivity becomes a structural form of dominance. By encouraging openness, Chinese authorities aim to create conditions in which smaller firms can compete more effectively, and consumers can exercise genuine choice. The Chinese case illustrates that without

regulatory intervention, data-driven ecosystems may evolve into irreversible market structures.

Taken together, these examples underscore the growing centrality of data in assessing market power. Unlike traditional barriers, which were often physical or financial, the barriers in digital markets are increasingly informational and algorithmic - built on exclusive access, reinforced by integration, and executed through opaque digital tools. For regulators aiming to preserve competitive and dynamic markets, understanding these data-centered dynamics is no longer optional - it is essential.

4. Interoperability and data portability: opening up closed digital ecosystems

4.1. Understanding interoperability and data portability

Interoperability and data portability have become essential tools for addressing structural barriers in digital markets. *Interoperability* refers to the capacity of different platforms, devices, or services to communicate and exchange information with one another. When systems interoperate, users can interact across services without being confined to a single provider's closed environment. *Data portability*, on the other hand, gives users the ability to transfer their data from one service to another in a structured and usable format. The right to portability first appeared as a privacy tool under Article 20 of the GDPR, but policymakers have increasingly recognised its competition-enhancing potential [19].

Although conceptually distinct, the two tools share a common goal: shifting control over data and digital interactions away from dominant platforms and toward consumers and smaller market participants. In markets where a handful of firms control essential services, these mechanisms offer a way to weaken the lock-in effects that can entrench dominance.

A similar dynamic is visible in smart-home and IoT environments. IoT ecosystems often rely on tightly coupled hardware and software combinations that restrict interoperability between devices and services [20]. Such multilateral bundling and tying practices can limit consumer choice and may even raise competition-law concerns under Article 102 TFEU, precisely because the absence of interoperability reinforces user lock-in and dependence on a single provider.

4.2. How interoperability and portability promote competition, innovation, and consumer choice

Interoperability and data portability are powerful tools for stimulating competition and fostering innovation. By enabling different services to communicate and allowing users to transfer their data, these tools lower barriers to entry for new firms. For example, interoperability in messaging services ensures that users on one platform can interact with users on another, reducing the network advantage of large incumbents. The article 6 (7) of EU Digital Markets Act (DMA) obliges designated "gatekeepers" to provide interoperability in core platform services such as messaging and operating systems, helping new entrants gain access to critical networks without needing to replicate an entire ecosystem [21].

Evidence from the smart-home sector also supports this logic. Effective smart-home systems depend on interoperable devices capable of exchanging sensor data, analysing behaviour, and adapting in real time [22]. Smart home's technical architecture presupposes seamless data flows across devices and services. This illustrates how interoperability not only enhances user experience but also enables third-party developers to build complementary services within an open ecosystem. Conversely, when such systems are closed, innovation becomes more difficult and users face higher switching costs.

Data portability complements this effect by empowering consumers to move their information between services with minimal friction. The EU Data Act (2023) extends portability beyond personal data to include certain non-personal data generated by connected devices and digital services, enabling businesses and users to switch providers more easily [21]. By reducing switching costs, portability strengthens competitive pressure on dominant platforms, encouraging them to improve service quality, pricing, and innovation.

Together, interoperability and portability foster innovation by allowing third-party developers to build on top of existing platforms without negotiating special access. Startups can enter markets with differentiated services, offering alternative functionalities, better user experiences, or enhanced privacy features. For consumers, these mechanisms enhance choice: users can move to platforms that better match their preferences without losing valuable data or social connections. Regulators have emphasised that such structural tools increase the contestability of digital markets, which is critical for maintaining dynamic and innovation-driven ecosystems [24].

4.3. Challenges and risks: privacy, security, and technical complexity

Despite their promise, implementation of interoperability and portability raises substantial challenges. One concern relates to privacy and data protection. If data flows too freely between services, users may face greater risks of unauthorised access or misuse. The European Data Protection Board has warned that interoperability obligations must be carefully aligned with GDPR safeguards to prevent weakening privacy standards [22]. Messaging interoperability, for example, requires robust encryption and clear allocation of responsibilities across interconnected providers.

Another challenge involves cybersecurity. When multiple systems become interlinked, vulnerabilities in one can quickly spill over to others. Ensuring secure data exchanges requires significant investment in technical infrastructure, monitoring, and governance frameworks. Smaller firms may struggle to meet these requirements, raising concerns that compliance costs could inadvertently reinforce the market position of dominant players [25].

A final set of challenges concerns costs and technical feasibility. Achieving true interoperability may require redesigning legacy systems, developing standardised APIs, or adopting uniform data formats [26]. These changes can be complex and expensive, particularly for services built on proprietary architecture. Even when mandated by

regulation, the pace and quality of implementation may vary across industries, limiting the immediate competitive impact.

Taken together, these challenges show that interoperability and data portability are neither simple nor automatic solutions. However, they remain central to ongoing attempts to open digital ecosystems and ensure that competition can take place on the merits rather than through structural advantages rooted in data concentration. As regulatory frameworks such as the DMA and Data Act become operational, their success will depend on balancing openness with user protection and technical security.

5. Bridging competition law and data protection: a new regulatory frontier

Digital markets increasingly sit at the intersection of competition law and data protection, two regulatory regimes that share overlapping objectives but can sometimes produce conflicting incentives. Competition law seeks to prevent market dominance, abuse of market power, and anti-competitive conduct, while data protection law, exemplified by the EU General Data Protection Regulation (GDPR), focuses on safeguarding individual privacy and controlling how personal data is collected, processed, and transferred [19]. The rise of data-driven business models has highlighted both the synergies and tensions between these regimes.

One major tension arises between *data minimization principles* and the need for data sharing to foster competition. GDPR mandates that organizations limit data collection and use personal information only for specific, legitimate purposes. While this is essential for protecting privacy, it may restrict the availability of data that competitors need to develop rival services or train AI systems, potentially reinforcing incumbent advantages [27]. Conversely, competition authorities may seek to mandate data access or portability to reduce barriers to entry and encourage innovation. These objectives can conflict if sharing data undermines privacy safeguards or exposes individuals to risk.

Addressing these tensions requires co-regulatory approaches. Collaboration between competition authorities, consumer protection agencies, and data protection regulators can help reconcile privacy and competition goals. The UK Digital Regulation Cooperation Forum (DRCF) provides a practical example: the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), and sectoral regulators coordinate investigations and share expertise to ensure that regulatory interventions account for both market fairness and privacy concerns [28]. Similarly, the EU Digital Markets Act (DMA) mandates interoperability and data access requirements for gatekeepers while explicitly emphasizing compliance with GDPR standards, demonstrating how structural competition measures can be aligned with data protection obligations [29].

Building on these initiatives, there is increasing interest in a unified "Digital Fairness Framework". Such a framework would integrate competition law, data protection, and consumer protection objectives, creating a holistic regulatory lens through which digital platforms are evaluated [30]. It could include guidelines for balancing data sharing with privacy, mechanisms for ensuring fair access to platform data without compromising security, and standards for algorithmic transparency that simultaneously protect consumers

and maintain market contestability. A coherent framework would not only reduce regulatory fragmentation but also provide clearer guidance for firms, enabling them to innovate responsibly while maintaining fair competitive practices.

Ultimately, bridging competition law and data protection represents both a challenge and an opportunity. As digital markets continue to evolve, coordinated regulation can ensure that platforms compete on merits rather than on data lock-in, while safeguarding the privacy and rights of consumers. Regulatory experimentation in the EU and UK demonstrates that practical, integrated approaches are possible, and a broader adoption of a "Digital Fairness Framework" could serve as a model for other jurisdictions seeking to harmonize these critical policy objectives.

6. Reimagining competition law for the digital age: updating the toolbox

Digital markets have evolved beyond the scope of traditional economic models, and competition law must evolve in tandem to remain effective. Dominance is increasingly determined by control over vast datasets, the integration of complementary services into unified ecosystems, and the dependence of users and smaller firms on a few dominant platforms. Market share alone no longer captures the full extent of power in digital environments. Updating regulatory tools is essential to preserve contestability, stimulate innovation, and protect consumer welfare.

6.1. New metrics for assessing dominance

Traditional indicators of market power, such as sales figures, market share, or pricing behavior, no longer capture the full dynamics of digital markets. Assessing dominance in data-driven environments requires metrics that reflect how platforms accumulate, integrate, and leverage information. These metrics include:

a) Data access refers to the breadth, depth, and exclusivity of the datasets a firm control. In smart-city and IoT contexts, controlling sensor networks, cloud systems, and behavioural data provides a durable informational advantage that competitors cannot easily replicate [22, 31]. These informational advantages can determine a platform's ability to refine and train algorithms, personalise services, target advertising and predict user behaviour, giving incumbents a structural lead that rivals cannot easily match [27].

b) Ecosystem control concerns the way dominant firms integrate complementary services into a single, interconnected environment. Such integration strengthens network effects, increases user lock-in, and allows the platform to shape the terms of access for third parties, thereby reinforcing its overall position in the market. In smart-home ecosystems, bundling and tying of devices and services restricts interoperability and locks users into a single provider's system [20]. Control over technological architecture becomes as critical as market share in shaping competitive dynamics.

c) Dependency relationships capture the extent to which smaller firms, app developers, or consumers rely on a particular platform for visibility, distribution, or essential digital infrastructure. Smart-city research demonstrates how users and service providers

increasingly depend on a few integrated platforms for essential services [32]. High levels of dependency can create asymmetrical bargaining power and limit the capacity of challengers to operate independently [2].

Incorporating these dimensions allows competition authorities to identify structural sources of power that traditional metrics overlook. Even when market share appears modest, control over data, ecosystems, and dependencies may reveal a deeper, more entrenched form of dominance characteristic of today's digital platforms.

6.2. Proactive and forward-looking regulation

Modern digital markets demand a proactive approach to competition enforcement. Waiting until anti-competitive conduct has caused irreversible harm is costly and often ineffective.

Studies of algorithmic and data-driven systems show how predictive analytics and automated service optimisation can reinforce incumbency without overt anti-competitive agreements [22]. These findings highlight the necessity for authorities of forward-looking tools to monitor data aggregation, algorithmic behaviour, and platform integration. Early intervention can prevent the solidification of market power that may take years to reverse [27].

Data-sharing obligations for key intermediaries are also essential. Where exclusive datasets form barriers to entry, regulated access - balanced with privacy and security requirements - can lower entry costs, stimulate innovation, and prevent the entrenchment of gatekeepers [31].

Proactive regulation also includes establishing data-sharing obligations for gatekeepers, particularly for datasets essential to entry and competition. By enabling responsible access while preserving privacy and security, authorities can reduce barriers for new entrants and foster innovation.

6.3. Policy recommendations for fair and transparent markets

To maintain contestability, regulators should adopt a multi-faceted strategy:

- Fair access requirements, which ensure that smaller firms, developers, and third parties can access platform infrastructure and data under non-discriminatory conditions [23].

- Algorithmic transparency, requiring disclosure of ranking criteria, recommendation systems, and personalization algorithms that influence market outcomes. This prevents subtle self-preferencing that may disadvantage competitors.

- Accountability for self-preferencing practices to monitor how dominant platforms leverage data from one service to benefit another, including preferential treatment of their own offerings.

- Cross-sector coordination, which integrates competition law with data protection and consumer regulation to balance innovation, fairness, and user rights [24].

These measures aim to create a regulatory environment where firms compete on merit rather than the structural advantages of data or ecosystems.

6.4. Sustaining innovation and protecting consumers

A modernized competition framework encourages innovation while protecting consumer welfare. By maintaining contestable markets, platforms are incentivized to improve product quality, enhance privacy standards, and offer differentiated services. Consumers benefit from wider choice, competitive pricing, and access to higher-quality services. At the same time, preventing entrenched dominance ensures that technological progress is not stifled by a few powerful actors controlling essential data or ecosystems. The approach aligns with the principles articulated in OECD studies, which emphasize that sustaining dynamic and competitive digital markets requires policies that consider both structural advantages and the long-term effects on innovation and consumer outcomes [33].

Ultimately, competition law in the digital age must move beyond reactive measures, using nuanced metrics and proactive policies to address the unique challenges of data-driven markets. By focusing on data access, ecosystem control, dependency relationships, transparency, and accountability, regulators can create an environment where competition thrives, innovation is rewarded, and consumers are protected.

7. Conclusion: toward fair and inclusive digital markets

The digital economy has transformed the sources and mechanisms of market power. Data has emerged as a central asset, allowing firms to consolidate influence across multiple services, reinforce network effects, and create ecosystems that are difficult for newcomers to enter. Traditional competition frameworks, which focus primarily on market share, pricing, and output, are increasingly inadequate for assessing dominance in these environments. The rise of data-driven platforms underscores the need for competition law to evolve, integrating a nuanced understanding of data access, ecosystem control, and dependency relationships as core indicators of market power [27, 33].

Modernized regulatory tools, such as interoperability requirements, data portability rights, algorithmic transparency, and monitoring of self-preferencing practices, can address these new forms of dominance. Coordinated approaches that bridge competition law with data protection and consumer protection frameworks - illustrated by the EU Digital Markets Act - demonstrate how policymakers can harmonize multiple objectives while maintaining fairness and security.

Looking forward, ensuring open, dynamic, and inclusive digital markets will require proactive regulation that anticipates emerging risks rather than reacting to harm after this fact. Societies must foster environments where competition is driven by innovation and quality, not by structural advantages rooted in exclusive control over data. Policies must empower consumers, support smaller firms and startups, and incentivize platforms to

innovate responsibly. A unified "Digital Fairness Framework" that aligns competition, data protection, and consumer interests can provide a guiding principle for future regulation, helping digital markets remain both competitive and socially beneficial.

In sum, the evolution of competition law for the digital age is not merely a legal necessity but a societal imperative. By embracing forward-looking, coordinated, and data-aware policies, regulators can ensure that technological ecosystems continue to expand while remaining accessible, fair, and conducive to innovation for all participants.

References

[1] J. Haucap, "Competition and competition policy in a data-driven economy," *Intereconomics*, vol. 54, no. 4, pp. 214-221, 2019.

[2] OECD, OECD handbook on competition policy in the digital age, OECD Publishing, 2022, https://www.oecd.org/en/publications/2022/02/oecd-handbook-on-competition-policy-in-the-digital-age_50b6e951.html

[3] V. M. K. Reverdin, "Abuse of dominance in digital markets: Can Amazon's collection and use of third-Party sellers' data constitute an abuse of a dominant position under the legal standards developed by the European Courts for Article 102 TFEU?" *Journal of European Competition Law & Practice*, vol. 12, no. 3, pp. 181-196, 2022.

[4] B. Lundqvist, "An access and transfer right to data - from a competition law perspective," *Journal of Antitrust Enforcement*, vol. 11, Supp. 1, pp. i57-i71, 2022.

[5] H. Schweitzer and A. Metzger, "Data access under the draft data act, competition law and the DMA: Opening the data treasures for competition and innovation?", *GRUR International*, vol. 72, no. 4, pp. 337-356, 2023.

[6] A. Ma, "Convergent antitrust regulation in China, EU, and US digital markets: mirror of an intensifying geopolitical competition," *Asian Review of Political Economy*, vol. 11, no. 1, pp. 45-68, 2024.

[7] OECD, Big data: Bringing competition policy to the digital era, OECD Publishing, 2016.

[8] E. Calvano & M. Polo, "Market power, competition and innovation in digital markets: A survey," *Information Economics and Policy*, vol.54, pp.1-18, 2021.

[9] R.-B. Esteves & F. Carballo-Cruz, "Can data openness unlock competition when an incumbent has exclusive data access for personalized pricing?" *Information Economics and Policy*, vol. 64, 2023.

[10] European Commission, Statement of objections to Amazon for use of non-public independent seller data, Press Release, 10 Nov. 2020.

[11] K. Cox, Amazon's use of marketplace data breaks competition law, EU charges, Ars Technica, 2020.

[12] European Commission, Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to its own comparison shopping service, Press Release, 27 June 2017.

[13] Court of Justice of the European Union, Judgment in Case C-48/22 P - Google & Alphabet v Commission (Google Shopping), Curia, 10 Sept. 2024.

[14] U.S. House Judiciary Committee, Investigation of competition in digital markets: Majority staff report and recommendations, 116th Congress, Oct. 2022.

[15] State Administration for Market Regulation, Restrictions on blocking external links, Press Release, Sept. 2021.

[16] R. Creemers, "China's emerging data governance framework", Stanford University Cyber Policy Center, 2021.

[17] Y. Feng and R. Mansell, "Platform power and data governance in China," *Journal of Information Policy*, vol. 12, 2022.

[18] State Administration for Market Regulation, Anti-monopoly guidelines for the platform economy, 7 Feb. 2021.

[19] European Parliament and Council, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016.

[20] I. Virtosu, I. & C. Li, "Bundling and tying in smart living," *Smart Cities and Regional Development (SCRD) Journal*, vol. 6, no. 2, pp. 97-110, 2022.

[21] European Parliament and Council, Digital Markets Act (DMA), Regulation (EU) 2022/1925, 2022.

[22] B. Davidovic, Z. Bogdanovic, K. Djordjevic & A. Labus, "Designing adaptable smart home environment based on resident's activity," *Smart Cities and Regional Development (SCRD) Journal*, vol. 2, no. 2, pp. 51-58, 2018.
[23] European Commission, The Digital Markets Act: Ensuring Fair and Open Digital Markets, 2022.
[24] European Data Protection Board, Opinion on Interoperability and Data Sharing in the Digital Markets Act, 2022.
[25] J. Bessen, The new goliaths: How corporations use software to dominate industries, kill innovation, and undermine regulation, Yale University Press, 2022.
[26] A. Newman, Digital interoperability and the politics of standardization, Oxford University Press, 2020.
[27] European Commission, Shaping Europe's digital future: Data, competition, and AI, 2020.
[28] UK Government, Digital Regulation Cooperation Forum: Framework for Co-Regulation of Digital Markets, 2021.
[29] European Parliament and Council, Data Act, Regulation (EU) 2023/2854, 2023.
[30] K. Wolfgang, "Digital markets, data, and privacy: Competition law, consumer law, and data protection," MAGKS Papers on Economics, Philipps-Universität Marburg, 2016.
[31] A. Labus, "An IoT system for healthcare in the smart city," *Smart Cities and Regional Development (SCRD) Journal*, vol. 6, no. 2 pp. 77-89, 2022.
[32] M. Romanelli, "Rediscovering urban intelligence within cities by technologies," *Smart Cities and Regional Development (SCRD) Journal*, vol. 5, no. 3, pp. 115-122, 2021.
[33] OECD, Digital platforms, market power, and competition policy, OECD Publishing, 2022.