The Creation of Data Pools as Information Exchanges: Antitrust Concerns

by

Eugenio Olmedo-Peralta*

CONTENTS

* Eugenio Olmedo Peralta, Commercial Law Professor, University of Málaga (Spain), President of the Spanish Academic Network for Competition Law (RADC); email: olmedo@uma.es; ORCID: https://orcid.org/0000-0003-1219-7587.

Suggested Citation: Eugenio Olmedo Peralta, 'The Creation of Data Pools as Information Exchanges: Antitrust Concerns' (2024) 17 YARS pp. 49–88.

Article received: 20 September 2023, accepted: 17 July 2024.

Yearbook of Antitrust and Regulatory Studies, Vol. 17, No. 29, pp. 49–88 • ISSN 1689-9024
https://doi.org/10.7172/1689-9024.YARS.2024.17.29.2

Abstract

In the digital market, data is a critical resource, but its handling reveals a two-sided situation. First, dominant platforms, known as gatekeepers, control major data sources. They may extract data unfairly from dependent partners, or abuse their market position by demanding excessive data for free services, and may also acquire companies solely for their data. The Digital Markets Act counters this by imposing data handling restrictions and portability duties. Conversely, non-gatekeeper companies need data access to compete and innovate. The European Data Act addresses this, by granting data portability rights and promoting data sharing spaces, yet a more extensive data marketplace is needed.

Data pools are essential for companies to access and use data, leading to enhanced derivative data utility. However, they pose risks of collusion, market foreclosure, and abuse of dominance. Exchanges in data pools can infringe competition rules, as seen in the CJEU *Asnef-Equifax* case. Data types vary from raw to processed, and meaningful information, including non-digital data. Commercially sensitive information shared in pools is scrutinized under Article 101(1) TFEU. Specific attention is needed for exchanges involving pricing, production capacities, and commercial strategies, as these directly restrict competition. Public information is exempt from this scrutiny.

To mitigate collusion risks, companies can use blind sharing or limit sensitive information exchanges. Technical data pools, essential for industry and product development, are regulated similarly to patent pools, with access on FRAND terms to prevent market foreclosure. Identifying essential data or market entry as well as ensuring fair access is crucial to address these competition risks.

This paper begins with a brief analysis of the central role that data collection and accumulation play in market functioning and company behaviour. In this realm, a concentrative force arises, leading more powerful companies to accumulate more data, thereby raising significant entry barriers for their competitors. Explored subsequently are the measures adopted from a regulatory standpoint to address these problems through the DMA, DSA, and the Data Act. In this context, the paper explains how data pooling represents a viable approach to address this issue. However, highlighted are also the significant competition risks that may arise from the use of this mechanism, such as facilitating collusive practices, market closure, or other exploitative abuses. Discuss next are potential remedies that can be employed to overcome these risks, and promote the use of data pools as a means to enhance accessibility and access to data. From the author's perspective, it would be necessary to establish a safe harbour (in the form of specific guidelines on data sharing) that

provides certainty about the assumptions and conditions under which data pooling can proceed, without posing a substantial risk to the competitive functioning of markets.

Resumé

Dans le marché numérique, les données constituent une ressource critique, mais leur gestion révèle une situation à double tranchant. D'une part, les plateformes dominantes, connues sous le nom de gardiens de portail, contrôlent les principales sources de données. Elles peuvent extraire des données de manière injuste auprès de partenaires dépendants ou abuser de leur position sur le marché en exigeant des données excessives en échange de services gratuits. Elles peuvent également acquérir des entreprises uniquement pour leurs données. L'Acte sur les Marchés Numériques contrebalance cela en imposant des restrictions sur la manipulation des données et des devoirs de portabilité. Inversement, les entreprises non-gardiennes ont besoin d'accès aux données pour concurrencer et innover. La Loi Européenne sur les Données aborde cela en accordant des droits de portabilité des données et en promouvant des espaces de partage de données, mais un marché des données plus étendu est nécessaire.

Les pools de données sont essentiels pour que les entreprises accèdent et utilisent les données, conduisant à une utilité accrue des données dérivées. Cependant, ils présentent des risques de collusion, d›exclusion du marché et d›abus de position dominante. Les échanges dans les pools de données peuvent enfreindre les règles de concurrence, comme vu dans le cas Asnef-Equifax de la CJUE. Les types de données varient des données brutes aux informations traitées et significatives, y compris les données non numériques.

Les informations commercialement sensibles partagées dans les pools sont examinées en vertu de l'article 101.1 TFUE. Une attention particulière est nécessaire pour les échanges impliquant des prix, des capacités de production et des stratégies commerciales, car ceux-ci restreignent directement la concurrence. Les informations publiques sont exemptées de cet examen.

Pour atténuer les risques de collusion, les entreprises peuvent utiliser le partage aveugle ou limiter l'échange d'informations sensibles. Les pools de données techniques, essentiels pour le développement industriel et de produits, sont réglementés de manière similaire aux pools de brevets, avec un accès selon les termes FRAND pour prévenir l'exclusion du marché. Identifier les données essentielles pour l'entrée sur le marché et garantir un accès équitable est crucial pour aborder ces risques de concurrence.

Cet article commence par une brève analyse du rôle central que jouent la collecte et l'accumulation de données dans le fonctionnement du marché et le comportement des entreprises. Dans ce domaine, une force de concentration se manifeste, conduisant les entreprises les plus puissantes à accumuler davantage de données, élevant ainsi des barrières à l'entrée significatives pour leurs concurrents. Ensuite, les mesures adoptées d'un point de vue réglementaire pour résoudre ces problèmes

à travers le DMA, le DSA et le Data Act sont explorées. Dans ce contexte, nous expliquons comment le regroupement de données représente une approche viable pour aborder cette question. Cependant, nous soulignons les risques importants pour la concurrence qui peuvent découler de l'utilisation de ce mécanisme, tels que la facilitation des pratiques collusoires, la fermeture des marchés ou d'autres abus d'exploitation. En conclusion, nous discutons des remèdes potentiels qui peuvent être employés pour surmonter ces risques et promouvoir l'utilisation des pools de données comme moyen d'améliorer l'accessibilité et l'accès aux données. Du point de vue de l'auteur, il serait nécessaire d'établir un port sûr (sous la forme de lignes directrices spécifiques sur le partage de données) qui offre une certitude sur les hypothèses et conditions sous lesquelles le regroupement de données peut être effectué sans poser un risque substantiel pour le fonctionnement concurrentiel des marchés.

Key words: Data pools; Information exchanges; Data Act; Data Spaces; Digital Markets Act; Competition.

JEL: K21, K24, K12

I. Concentrative Dynamics in the Catching of Data and its Impact on Innovation

In the digital economy, market power rests upon the control over data. Data has supplanted other elements that once underpinned the economic strength of companies, altering the incentive system that defines corporate behaviour in the market. It can be said that in the digital realm, companies no longer solely, or short-term, pursue economic profit, and their strength is not exclusively based on their assets. For many companies, the primary goal is market entry and dominance, leveraging the first-mover advantage to establish themselves as the dominant player in a particular business (market tipping). Profits, if any, may come later. In this context of voracious dynamic competition, and even more fierce innovation, companies are willing to sacrifice profits (even over several fiscal periods) by applying aggressive commercial practices, with the sole objective of consolidating their position as the market-controlling entity.[1]

[1] It is argued here that the best account of this dynamic is still offered by the chair of the FTC in her essay Lina M. Kahn, 'Amazon's Antitrust Paradox' (2017) 126 (3) The Yale Law Journal, 746 ff. In it, the author demonstrates how, for decades, the digital giant Amazon has sacrificed profits in exchange for aggressive business practices in the distribution and marketing of products (predatory pricing, vertical integration, data exploitation, non-equitable contractual conditions, etc.). These behaviours have allowed Amazon to become the manager, and the regulator of the online shopping market, raising significant barriers that prevent (or, at least,

Their benefit lies not in earnings, but in data accumulation and building a fortified dominant position, which creates significant market entry barriers to deter potential competitors.

The greatest asset of companies in the digital economy is data accumulation. The business strategies of major tech companies are aimed at increasing their data capture power by dominating its main sources. This data expansion is sometimes achieved through the development of a new product or service that acts as an information collector (for example, the development of voice assistants, applications, or software).

In other cases, data is obtained indirectly, parasitizing information gathered by other companies and then transferred to the technology platform in their commercial relationships.[2] For instance, this is the practice employed by *Amazon* in its Marketplace, where it obtains information about the sales, customers, and business strategies of professional users utilizing the platform. This is also how digital giants expand their data capture spectrum across various markets. They can do so through data transfer from application developers to the operating system, or the app store where they are marketed, as well as from contracting social media advertising services, or positioning results in search engines. Regulatory and competition authorities have raised alarms about the potential impact of these behaviours on the proper functioning of markets. In the European case, this resulted in the imposition of a series of obligations and prohibitions related to data on platforms designated as

greatly hinder) the entry of competitors, which have real opportunities to offer an alternative. Having achieved this dominant market position, the digital giant can cast its nets to other markets by leveraging data sources from its gatekeeper position. Khan is not the only one who has warned about the effects of this dynamic on competition, and, by extension, on the functioning of the economy in general. Other notable authors, such as Jonathan B. Baker, *The Antitrust Paradigm: Restoring a competitive economy* (Harvard University Press 2019), 11 et seq. highlighted how this trend is generalized in the behaviour of digital giants, leading to a situation that has been aptly and originally termed a 'moligopoly' scenario, see Nicolas Petit, *Big Tech & the Digital Economy, the Moligopoly Scenario*, (OUP 2020), 93 ff.

[2] Regulation (EU) 2019/1150 of the European Parliament and of the Council, on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57-79 (hereinafter: B2P Regulation), is of great importance. This Regulation aims to address the unfair practices arising from the imbalance of bargaining power between digital platforms and professional users that need access to these platforms for part of their activity. In particular, Article 9 refers to data access, establishing a set of information obligations that platform operators must provide to their professional users. However, the B2P Regulation does not correct the often-inequitable nature of the data demands made by platforms on their professional users.

gatekeepers according to the EU Regulation called the Digital Markets Act (hereinafter: DMA).[3]

A third way to increase data capture potential is the execution of an adequate concentration strategy, acquiring other companies, especially emerging ones, that have special potential for data capture in a certain sector, either by marketing data capture devices (connected or not to the Internet of Things; hereinafter: IoT), or by having developed applications or software that enable the collection of data. These concentration strategies are particularly harmful when they entail *killer acquisitions*, that is, the purchase of an emerging company with great growth potential that can become a rival for the buyer, primarily built on the control of an innovation[4]. Considering the acquisition policy carried out by some digital giants in recent decades, it is clear that their behaviour is driven by the aim to control new data sources.[5] A prime example here is *Alphabet's* (*Google*) acquisition of companies like *YouTube*, *DoubleClick*, *Android*, *Motorola Mobility*, *Waze*, *DeepMind*, or *Fitbit*.[6] It is also the case for *Meta* (*Facebook*) and its aggressive acquisition of its main current (*Whatsapp*, *Instagram*) or potential rivals (*Oculus VR*).

The first step in this competitive strategy is, therefore, to control important sources of supply of the essential input for competition in the digital market – data. From building a solid dominant position in a specific market, or, in the words of the DMA, after becoming a gatekeeper for a core platform service,[7] the controlling company can use the versatility of the data it captures to extend

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council, on contestable and fair markets in the digital sector, amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L-265/1-66, (known as the Digital Markets Act; hereinafter: DMA).

[4] See Pierre Regibeau, Ioannis Llianos, 'Digital Mergers: A Primer' (2021) (3) Centre for Law, Economics and Society Research Paper Series 1–77; Jörg Hoffmann, Germán O Johannsen, 'EU-Merger Control & Big Data On Data-Specific Theories of Harm and Remedies' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-05; Anca D Chirita, 'Data-Driven Mergers Under EU Competition Law', in John Linarelli, Orkun Akseli (eds), *The Future of Commercial Law: Ways Forward for Harmonisation* (Hart Publishing 2019), 147–183.

[5] In the doctrine, although focusing more on data protection and privacy, see the very interesting overview provided by Reuben Binns, Elettra Bietti, 'Dissolving Privacy, One Merger at a Time: Competition, Data, and Third Party Tracking' (2020) 36 Computer Law & Security Review, 1–19.

[6] To date, the tech giant has carried out more than 250 acquisitions of other companies, recently focusing its expansion on the sector of AI development, data analysis, and robotics software.

[7] According to Article 2(2) DMA, core platform services include online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing services, or online advertising services, including advertising networks, advertising exchange platforms, and any other advertising intermediation services.

its position to other markets. These markets may be vertically connected, adjacent, or complementary to the core platform services. For example, consider how companies like *Amazon* use their dominant position in the digital retail Marketplace to extend their activity to other sectors, such as streaming multimedia content (*Amazon Music*, *Prime Video*), voice assistants (*Amazon Alexa*), or cloud computing (*AWS – Amazon Web Services*).

This dynamic leads to a market scenario that has been conceptualized as *moligopoly*,[8] where a few platforms act as gatekeepers to the markets they control (the core platform services upon which their activity is based) and, while acting virtually as monopolists in that service, compete with only a few companies (oligopoly) in the data market, that is, the other gatekeepers.

The growth potential of these companies is highlighted by the fact that they control relevant data sources from various origins (information about their users, whether professional or private, geolocation, biometric data, etc.). Being the dominant platform of a core platform service (a gatekeeper), the company benefits from a position that is difficult to contest, where users have little incentive to switch platforms. Moreover, precisely because of their dominance, they can impose inequitable conditions on their counterparts, especially regarding forcing them to grant access to data about their activity.

Data's importance in establishing market power in the digital realm is rooted primarily in two key considerations.[9] Firstly, the versatility of data applications is crucial. Information about a specific sector, customer group, market operations, geolocation of objects or individuals, etc., can be used in numerous ways. This versatility grants companies controlling such information significant power not only in their specific operating market, but potentially in other markets as well (possibility of market leveraging). For instance, *Google*'s acquisition of *FitBit*, thus gaining access to substantial biometric and physical activity data of its users, combined with its other services like maps and navigation, allows Google to gather data relevant not only to its core services (search engine, streaming videos), but also to potentially benefit in markets where it is not yet present, such as the insurance sector. Similarly, the economic and financial information that *Amazon* may acquire could enable it to successfully enter markets where it is not currently active, like the banking

[8] Nicolas Petit, *Big Tech & the Digital Economy*, 153 ff.

[9] Although it may seem reductive, it suffices here to refer to the Crémer Report, European Commission, Directorate General for Competition, Competition Policy for the Digital Era, final report (2019), 73 et seq. In summary, it is highlighted that data are a non-rival, replicable, and transmissible resource; they allow parallel use by different users, without diminishing the value for any of them, or consuming their utility; likewise, they permit the exclusion of users by limiting access to the data; their acquisition requires investments (hence the need to ensure their remuneration); they have a ubiquitous nature (what matters is the access to the data not their location or place of storage); and, finally, they produce significant scale and scope effects.

sector. Hence, the potential of data is not only a competitive threat in the market where a company operates, but can also be used as a springboard into markets where the controlling tech giant is not yet present, offering superior products and services compared to traditional dominant companies.[10]

The second significant characteristic of data when it comes to building a dominant position is that its utility improves as more data is accumulated, diversified in its sources, and varied in its variables. In other words, the combination of data enhances its value. This is why tech giants are pursuing aggressive strategies to enter markets initially unconnected to their core business activities. An example is Amazon's aggressive strategy to make Alexa the leading voice assistant system. Although Amazon's core activity of online retail sales has no direct connection with selling hardware incorporating a voice assistant system, its venture into hardware, and the development of advanced artificial intelligence and voice command response systems, are enabling the gatekeeper to capture valuable, diverse data about its users.

Innovation depends on the acquisition of vast amounts of data and their potential combination. This is true not just in the digital sector, but also in more traditional sectors like medicine, manufacturing, construction, etc. The information derived from analysing and processing large datasets obtained from different sources enables the creation of new and improved products and services. Therefore, access to data is critical not only for competing in current markets, but also for fostering dynamic competition. Data are the raw materials for growth.

Addressing the previously described situation requires action in two opposing directions:

- On the one hand, it demands the imposition of limitations on the use of data by digital giants. Given their potential to monopolize data sources, sometimes through anticompetitive or unfair practices, regulatory intervention is justified. Such intervention will particularly focus on limiting the use and combination of data they can access.
- On the other hand, it is necessary to empower and facilitate potential competitors (non-gatekeepers) to access data sources, combine data, and participate in the growth and innovation opportunities derived from them. Therefore, regulations should promote the development of a data market where companies (again, non-dominant) can exchange and share useful data for their activities. Only then will data contribute to enabling these entities to enter the market, develop disruptive products and services, and compete with gatekeepers

[10] Consider, in the insurance sector, a more precise actuarial calculation of risk; or a better development of the credit profile, and the risk of default of clients in the banking industry.

The following section will analyse in depth how the European Union is tacking both of these issues through recent legislations. The subsequent Section III will consider the characteristics of data pools, and their potential to enable the exchange and access to large amounts of data for companies that have fewer opportunities to do so. However, as considered in Section IV, data exchanges between companies (and, in particular, data pools) can give rise to anticompetitive behaviours, such as collusive practices or abuses of a dominant position. After critically analysing the implications of these data-sharing agreements from the perspective of competition law, the paper concludes by indicating the advisability of establishing a safe harbour through guidelines, or other soft law instrument, applicable to data exchanges. In this way, companies will have clear reference to when, and to what extent they can exchange their data without risking engaging in anticompetitive conducts.

II. The Design of a Market Fit for Data Trading: Limitation for Some, Simplification for Others

In the market for data, some have had excessive access, while others lack the real capacity to access data at an adequate scale. Technology giants, designated as gatekeepers, have established strong positions of dominance in various digital markets, largely building their position on controlling data sources. In contrast, smaller companies, without the ability to control and combine data, face challenges in entering such markets, and creating a viable alternative to these digital giants. This situation has justified the regulatory intervention recently developed by the European Union to address both of these circumstances.

1. Limitations on the Use and Combination of Data Imposed on Gatekeepers in the DMA

The Digital Markets Act (DMA) was designed to implement measures to overcome the primary market failure identified in the digital sector – the construction of virtually indisputable dominant positions by certain digital platforms.[11] In its development, by imposing obligations and prohibitions on

[11] It is not the purpose of this paper to carry out a detailed analysis of the DMA which is already the subject of extensive literature. The Author of this paper has addressed it in other studies such as Eugenio Olmedo-Peralta, 'Redefiniendo el ámbito de aplicación de la Ley de Mercados Digitales: ¿a quién? ¿cómo? y ¿para qué?', in Julio Costas Comesaña et al (eds), *Nuevas tendencias en el derecho de la competencia y de la propiedad industrial III*, (Marcial Pons 2022), 87–115; or in 'La construcción de un régimen jurídico para el sector digital más

companies designated as gatekeepers, the DMA aims to enhance fairness and contestability in these markets.

On 6 September 2023, following notifications by the platforms, the European Commission adopted its first decision that designates gatekeepers in accordance with the DMA. It identified *Alphabet*, *Amazon*, *Apple*, *Bytedance*, *Meta*, and *Microsoft* as gatekeepers in certain core platform services[12] for DMA purposes, thereby subjecting them to the duty to comply with the obligations and prohibitions established by the Regulation. Additionally, four market investigations were opened to consider the exclusion of certain services from this notion (*Bing*, *Edge*, and *Microsoft Advertising* for Microsoft; and *iMessage* for Apple), and, likewise, for the possible designation of other services as gatekeepers (*Apple's iPadOS*), despite not meeting the thresholds. Conversely, the Commission decided to exclude services like *Gmail*, *Outlook.com*, and *Samsung Internet Browser*[13] from consideration as core platform services, despite surpassing the thresholds.

Articles 5 and 6 of the DMA stipulate the obligations and prohibitions placed on gatekeepers.[14] Relevant to this discussion, it is highlighted that among the duties imposed on designated gatekeeper platforms, some are expressly related to data control, namely:

---

allá del Reglamento de Mercados Digitales', in Juan Ignacio Ruiz Peris et al (eds) *Mercados digitales y competencia* (Tirant lo Blanch 2023), 153–208. See the detailed analysis developed by Rupprecht Podszun, *Digital Markets Act, Article-by-Article Commentary* (Nomos, 2024); Juan Ignacio Ruiz-Peris, 'La nueva Digital Markets Act, una respuesta híbrida de la Unión Europea a los gatekeepers GAFA' (2021) Revista Aranzadi de Derecho y Nuevas Tecnologías, 57; Juan Ignacio Ruiz-Peris, 'Gatekeepers, discriminación autopreferente exclusionaria y reforzamiento de la posición de dominio: La nueva propuesta europea de Digital Markets Act', in Jaume Martí Miravalls (ed) *Competencia en mercados digitales y sectores regulados* (Tirant lo Blanch 2021), 29–64.

[12] Specifically, the core platform services affected are as follows:
- Social networks: TikTok, Facebook, Instagram, and LinkedIn
- Intermediation: Google Maps, Google Play, Google Shopping, Amazon Marketplace, App Store, Meta Marketplace
- Advertising: Google, Amazon, Meta
- Number-independent interpersonal communication services: WhatsApp and Messenger
- Video sharing: YouTube
- Search engine: Google Search
- Browsers: Chrome and Safari
- Operating systems: Google Android, iOS, and Windows PC OS.

[13] Consequently, for now, Samsung escapes being designated as a gatekeeper under the DMA.

[14] Article 5 DMA lists a series of pure or unconditional obligations, while Article 6 DMA refers to obligations 'that can be specified in greater detail' by the Commission.

- Refrain from processing, for the purpose of providing online advertising services, the personal data of end-users using third-party services that utilize the gatekeeper's core platform services (Article 5(2(a) DMA).
- Refrain from combining personal data from relevant core platform services with personal data from any additional core platform services or any other services provided by the gatekeeper, or with personal data from third-party services (Article 5(2(b) DMA).
- Refrain cross-using personal data from the relevant core platform service with other services provided separately by the gatekeeper, including other core platform services, and vice versa (Article 5(2(c) DMA).
- Refrain from logging in end-users to other services of the gatekeeper for the purpose of combining personal data (Article 5(2(d) DMA).
- Obligation to share data with advertisers and publishers, providing each advertiser or publisher offering online advertising services (or authorized third parties) with daily and free information about each advertiser's ad, regarding: a) the price and commissions paid by that advertiser; b) the remuneration received by the publisher with their consent; and c) the measures from which the prices, commissions, and remunerations are calculated (Article 5(9) and 10 DMA).
- Prohibition of using, in competition with professional users, any data that is not publicly accessible generated or provided by such professional users in the context of their use of the relevant core platform services or services provided alongside or in support of these services, including data generated or provided by the customers of such professional users (Article 6(2) DMA).
- Obligation to provide advertisers and publishers (or third parties authorized by them) with free access to the gatekeeper's performance measurement tools and the necessary data for advertisers and publishers to carry out their independent verification of the ad inventory (Article 6(8) DMA).
- Obligation to allow end-users and authorized third parties, upon their request, effective and free portability of data provided by the end-user or generated by their activity in the context of using the relevant core platform service (Article 6(9) DMA).
- Obligation to provide professional users (and third parties authorized by them) with effective, high-quality, continuous, real-time access to aggregated or disaggregated data, and the use of such data, including personal data, provided or generated in the context of the use of core platform services or services provided jointly or in support of these. In relation to personal data, the gatekeeper will provide such access to personal data or its use only when such data are directly related

to the use that end-users have made with respect to the products or services offered by the relevant professional user through the relevant core platform service, and when the end-user opts for such exchange by giving their consent (Article 6(10) DMA).

– Obligation to provide third-party online search engine providers with FRAND (fair, reasonable, and non-discriminatory) access to data on rankings, queries, clicks, and views in relation to free and paid search generated by end-users in their online search engines. Any such data on queries, clicks, and views that are personal data will be anonymized (Article 6(11) DMA).

The imposition of these obligations and prohibitions on gatekeepers serves a dual purpose. Negatively, it aims to curb the increase in market power of post-merger companies, and further combination of data. Positively, it introduces portability obligations, and recognizes data access rights, as a prerequisite for potential rivals to compete with digital giants.

Although originally envisaged as a new competition tool, the DMA is a regulatory instrument, aimed at solving the market failure of excessive concentration of power by major platforms, and consequently, imposes a series of prohibitions and obligations directly. Unlike antitrust rules, it does not establish a prohibition of certain behaviours that, after verification, lead to the imposition of remedies and sanctions. The DMA applies *ex ante*, with the designation of gatekeepers and their subjection to these duties and prohibitions. Non-compliance with such duties directly entails a sanctioning regime, without the need to demonstrate the effects that the offending behaviour may have on the competitive functioning of the market.[15]

2. Gatekeepers Duty to Report on Mergers

As previously noted, major digital companies can build their dominant positions not only through the development of practices involving the capture, concentration, and abusive combination of data in their activities. Their dominance in data can also stem from a strategy of mergers with other digital

[15] Thus, Article 29 DMA states that after conducting the necessary proceedings to confirm non-compliance, the EC will adopt a non-compliance decision when it is established that an obligation or prohibition has been breached. In such a decision, the gatekeeper will be ordered to cease the non-compliance and to provide explanations on how it plans to comply with the decision. Furthermore, upon confirmation of the infringement, the Commission may impose on the gatekeeper fines that do not exceed 10% of its total worldwide turnover in the preceding financial year, an amount that can be increased to 20% in the event of repeat offenses within an eight-year period (Art. 30 DMA).

companies, especially when these have the potential to control relevant data sources.[16]

However, applying general merger control rules, some of these operations may fall outside the scope of the merger analysis performed by a competition authority for not exceeding the turnover threshold required by the EU Merger Regulations to be considered an operation with a community dimension,[17] or the market shares alternatively determined in national merger control regulations. In the digital field, however, the initial screening to discern whether a merger should be subject to pre-emptive review should not be based solely on quantitative criteria, but take into account, above all, qualitative elements. Otherwise, there is a substantial risk of false negatives: failing to subject an operation to a merger control assessment for not being considered to have a community dimension,[18] yet concluding from substantive analysis that the operation could produce a significant obstruction of effective competition in the market.

To avoid this situation, Article 14 of the DMA expands the scope of operations subject to the duty of notification.[19] Designated gatekeepers must inform the

[16] Whether it is due to a medium's ability to capture large amounts of data, or the specifics (uniqueness) of particular data that can be obtained, in this case, the value of the data depends more on their uniqueness than on their quantity.

[17] See Article 1(2) and 1(3) of Council Regulation (EC) 139/2004 on the control of concentrations between undertakings (hereinafter: EU Merger Regulation) [2004] OJ L24/1, as well as the referral rules that also allow the EC to deal with matters that do not have a community dimension (Articles 22 and 4(5)).

[18] In this case, because the companies involved (especially the acquired company) do not exceed the turnover threshold required to subject them to merger control.

[19] This extension of the scope of the thresholds of the EU Merger Regulation is not exclusive to the DMA. Recently, other regulations have also included, within the scope of merger control, operations that initially fell outside the consideration of their community scale. Thus, Regulation (EU) 2022/2560 of the European Parliament and of the Council, on foreign subsidies that distort the internal market [2022] OJ L330/1-45, has expanded the set of cases where a concentration must be notified to the EC with the aim of enabling better control of foreign subsidies, which may distort competition in the single market. Specifically, according to Article 20 of this Regulation, a concentration subject to a notification duty will be deemed to occur when, in a concentration:

a) at least one of the companies that merge, the acquired company, or the joint venture is established in the Union and generates a total turnover in the Union of at least €500,000,000; and
b) the following companies have received combined financial contributions from third countries in the three years preceding the conclusion of the agreement, the announcement of the public offer, or the acquisition of a controlling interest, exceeding €50,000,000:
   i. In the case of an acquisition, the acquirer or acquirers and the acquired company;
   ii. In the case of a merger, the merging companies;
   iii. In the case of a joint venture, the companies creating the joint venture and the joint venture itself.

Commission of any concentration when the merged entities, or the resulting company from the merger, provide core platform services, or any other services in the digital sector, or allow data collection, regardless of whether it is notifiable to the Commission under the Merger Regulation or to a national competition authority in accordance with their own merger control rules. Like the general notification duty derived from the Merger Regulation, such notifications must be made prior to the execution of the merger.

In particular, it is important to remember that this rule imposes an additional notification duty for mergers that affect services that allow data collection. The focus is, therefore, on establishing certain control over concentrative operations that may expand the gatekeepers' capacity to dominate data supply sources and exclude their use by other operators.

Through this notification, the Commission will be informed about the companies affected by the operation, their global and Union turnover, their areas of activity, and the transaction value of the contract or an estimate thereof. A summary of the merger must be attached, indicating its nature and justification, and pointing out the affected Member States. Regarding the affected core platform services, their annual turnover in the Union, the number of annual active professional users, and the number of monthly active end-users must be indicated.

When, as a result of these mergers, a core platform service exceeds the thresholds determined in Article 3 of the DMA, the access gatekeeper must inform the Commission of such circumstance, for the purpose of developing the corresponding market investigation and, if applicable, proceed to designate the gatekeeper as a gatekeeper also in that new core platform service.

However, the DMA requires a critical consideration. It is important to note that this provision imposes a duty of notification to the Commission for merely informational purposes, but does not establish a true procedure for controlling the operation. That is, once the information is received, it is not stipulated that the European Commission must enter into a substantive analysis of such operation, to determine its compatibility with the functioning of the market, which would imply suspending the operation until its authorization. If the merger does not reach a community dimension, the Commission will not acquire such powers. Nonetheless, it is established that the Commission will transmit the information received about the merger to the Member States,[20] so that their national competition authorities – which take action under lower thresholds justifying merger control – can use this information to open corresponding national control procedures or so that, if applicable, they can request the Commission to examine the merger, making use of the *Dutch*

[20] Certainly, safeguarding the legitimate interests of businesses, with regard to the protection of their trade secrets.

clause provided in Article 22 of the EU Merger Regulation. It is fair to state that this last option is more reasonable, due to the potential impact these mergers may have on the European digital market. Thus, although initially, an operation of these characteristics may impact exclusively the market of some Member State, the digital products or services, affected by the core platform service, will have great potential to extend their marketing scope to other territories of the Union, without incurring significant investments.

3. Promoting Access to Data and the Creation of Data Marketplaces: Measures from the Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)

A further regulatory solution requires action in the opposite direction regarding data access by companies that are not designated as gatekeepers. With regards to these companies, the development of innovations, and the promotion of competition, requires an appropriate regime that facilitates data access and exchange. To achieve this, it is necessary to trigger the development of data marketplaces and granting users the right to access to, and transfer of their data to prevent their capture by the dominant companies that generate that data.

On 13th December 2023, the European Parliament and the Council of the European Union adopted Regulation (EU) 2023/2854, on harmonised rules on fair access to and use of data (hereinafter: Data Act).[21] This Regulation is part of the *European Data Strategy*,[22] the general outlines of which were published in February 2020, aiming to build a genuine single data market and make Europe a global leader in the digital economy. This required introducing measures to facilitate data access, promoting European data spaces, and recognizing the rights to access, and the portability of machine-generated data. The legislative process on the Data Act was accompanied by other legislative initiatives, notably the approval of the EU regulation known as the Data Governance Act (hereinafter: Data Governance Act).[23]

The Data Act aims to provide the legal basis for non-gatekeeper companies to access data generated by devices, platforms, applications, and software based on their users' utilization.[24] These are some of the main sources of

[21] OJ L, 22.12.2023.

[22] Commission Communication, *A European Strategy for Data*, COM(2020) 66 final.

[23] Regulation (EU) 2022/868, of the European Parliament and of the Council, on European data governance and amending Regulation (EU) 2018/1724 (hereinafter: Data Governance Regulation) [2022] OJ L 152/1-44.

[24] See Björn Lundqvist, *Regulating Access and Transfer of Data* (CUP 2023) 102 et seq.

Big Data today, largely controlled by gatekeepers. Data generation directly derives from these products or devices (including those connected to the IoT or to virtual assistants), or through related services.[25] These related services refer to any digital service (including software) embedded in a product, or interconnected with it, such that its absence would prevent the product from performing some of its functions. Since these products and devices generate a vast amount of data essential for competing in that market, or in secondary markets, measures must be devised to allow access to such data.[26] For this purpose, the Regulation makes these data available to its recipients, also allowing public bodies to access them for general interest reasons, when necessary (such as, for reasons of public interest).

The provision is carried out by imposing a series of obligations and portability rights aimed at allowing recipient companies to access such data under fair, reasonable, non-discriminatory, and transparent conditions (seen here as *FRAND+* conditions). Additionally, specific measures are considered to foster the reuse of data generated by the public sector, to promote innovation, and the development of new products and services.

This legal framework must be compatible with data protection, privacy, and security rules, encouraging the creation of a framework of trust for data use and transmission.

While these measures are useful for correcting perceived market failures, they are not definitive. The final goal is to develop an effective market for data, where data exchange and its shared use are facilitated. For that reason, an appropriate regime for the conclusion of contracts, and the creation of data pools as large (private or public) repositories allowing data exchange and combination, is necessary.

The scope of the Data Act includes business-to-consumer (B2C) and business-to-business (B2B) data exchanges. It imposes the obligation on manufacturers as well as designers of related products and services, to design them in a way that allows users easy access to data generated from their use, and to exercise their right to data portability in favour of another company.

This is achieved, first, by imposing pre-purchase information duties on professional users regarding the product or related service. Subsequently, users have a recognized right to access and use the data generated through these products or related services. More practically, users are given the right

[25] On the lock-ins created by connected devices, see Josef Drexl, 'Data Access and Control in the Era of Connected Devices' Study on behalf of the European Consumer Association BEUC (2018), 34.

[26] For more in-depth analysis of the objectives and measures of the Regulation, see Rupprecht Podszun, Philipp Offergeld, 'The EU Data Act and the Access to Secondary Markets', Study for the Ludwig-Fröhler-Institut für Handwerkswissenshaften (2022).

to share these data with third parties, allowing the user to transfer them to another user, whether individual or professional, without delay and free of charge. These third parties commit to a fair and lawful use of the received data, treating the data only for the purposes and conditions agreed upon with the users, and subject to a series of prohibitions.[27] Data recipients must not:

a. Coerce, deceive, or manipulate the user in any way, harming or undermining the user's autonomy, decision-making, or options, nor use a digital interface with the user;
b. Use the received data for profiling individuals, unless necessary to provide the requested service;
c. Make the received data available to another third party, in raw, aggregated, or derived format, unless necessary to provide the requested service;
d. Make the data available to a company that provides core platform services, one or more of which have been designated as gatekeepers under the DMA;
e. Use the data to develop a product competing with the product from which the accessed data originate, nor share the data with another third party for such purpose;
f. Prevent the user, particularly through contractual commitments, from making the received data available to other parties.

The rules of the Data Act should be read in conjunction with the provisions of the DMA, particularly concerning the obligations of platforms designated as gatekeepers to enable effective portability of such generated data,[28] as previously considered. Furthermore, platforms classified as gatekeepers will not benefit from the right to data portability provided by the Data Act, thus not being seen as "eligible third parties" for the data transfer covered in this legislation.[29] This disqualifies them from urging, or commercially incentivizing a user (in whatever way) to provide access for their services to data obtained through exercising their right to access and portability; to urge or commercially incentivize a user to request the data holder to make the data available to one

[27] Cf. Article 6 of the Data Act which stipulates that data made available must be treated only for the purposes and conditions agreed upon with users.

[28] This portability obligation refers to any data generated by the end-user and is not limited to the portability considered by the General Data Protection Regulation (GDPR), which exclusively refers to personal data. On this point, see Simonetta Vezzoso, 'The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU' (2021) 17 (2) European Competition Journal, 400 et seq.

[29] Thus, Article 5(3) of the Data Act stipulates that 'Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, shall not be an eligible third party under (…)'.

of their services; or to receive data that a user has previously obtained by exercising these rights.

Generally, access to such data will not be free of charge. Given that the obtainment and initial processing of the data requires significant investments, the data holder is entitled to a reasonable compensation for making the data available. When determining the amount of such reasonable compensation, a limitation is established benefiting those recipients that are a micro-enterprise or a SME, whereby the compensation cannot exceed the costs directly related to the process of making the data available.

Considering that data-related relationships often arise in situations with a power imbalance, the Regulation introduces a series of measures to prevent abuses by a stronger negotiating power, from the perspective of unfair competition. Thus, a list of specific contractual clauses is considered abusive, when unilaterally imposed on micro-enterprises or SMEs. The scope of this rule is limited, covering only smaller businesses. In cases where an imbalance in negotiating power affects larger companies (e.g., a large company versus a digital platform with a gatekeeper status), controlling abuse will be subject to general rules on unfair commercial practices. As considered by Directive 2005/29/EC,[30] the Data Act starts with a general prohibitive clause that considers any contractual clause abusive by its nature that manifestly departs from good commercial practices, in terms of data access and use in contravention of the principles of good faith and fair trade. Subsequently, a dual list of black clauses[31] – clauses that will always be considered abusive – and grey clauses[32] – whose abusiveness is presumed unless proven otherwise – is introduced.

---

[30] Directive 2005/29/EC of the European Parliament and of the Council, on unfair business-to-consumer commercial practices [2005] OJ L-149/22, esp. Article 5.

[31] A contractual term is unfair if its object or effect is to:

a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;
b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations;
c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

[32] A contractual term is presumed unfair if its object or effect is to:

a) inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;
b) allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;

To enable effective data exchanges, technical obstacles must also be eliminated, promoting the creation of standards, and facilitating the creation of industry-adopted protocols that allow data mobility. This necessitates the involvement of intermediaries and data processing services in the cloud. The ultimate objective of the Regulation in this respect is to eliminate material obstacles that may hinder the effective exercise of this portability right.

III. Data Pools as a Tool for Data Intermediation and Combination

The above analysis has justified the importance of data access for participation in digital markets, and synthesized some legislative measures that are being implemented in order to encourage data sharing and prevent their monopolization by digital platforms. However, from a practical perspective, intermediaries are required to facilitate data exchange and to support transactions. This intermediation can be structured through data pool contracts.

A data pool contract is one where two or more parties (partners in the pool) agree to share their data in a consortium. This sharing can occur by transmitting the data to a medium that remains under the joint control of the partners, or is controlled by a third-party intermediary (trustee, escrowee, or administrator) acting on behalf of the partners. It can also go in a more decentralized way, by allowing each of the partners to let the others access certain data that remain under their control or giving them the possibility to exploit certain data sources, with, or without the intervention of a third party.[33]

---

c) prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;
d) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
e) enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.

[33] European Commission, Joint Research Centre, JRC Science for Policy Report, Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance (2023), 59–61; ALI-ELI, Principles for a Data Economy – Data Transactions and Data Rights – the latest draft was proposed by ELI in 2021 and can be accessed at: https://www.principlesforadataeconomy.org.

Through this contract, the parties acquire the right to use the shared data, and assume the obligation to share the data they already have, or generate with the other parties. The development of this activity is subject to a series of controls and limitations that the parties will establish in the contract.[34]

Thus, a data pool is an associative contract through which (1) the parties pool the data they possess (all or some individualized data), (2) in exchange for the possibility of accessing the data of others (reciprocity), and (3) with the common goal of benefiting from having access to a larger quantity of data (quantitative improvement), and (4) to deeper data they have access to thanks to the benefits obtained from combining its different sources (qualitative improvement).

Depending on who is granted access to the data in the pool, private and public data pools can be distinguished. This paper focuses more on private data pools that involve creating closed data platforms that only companies that have entered into the agreement can access. In contrast, public data pools involve creating open data schemes, allowing access to companies or entities, be it public or private, which meet certain requirements that are the basis for the creation of the pool.[35]

In terms of their configuration, data pools can be structured in three different ways: (1) first, a medium can be created, under the joint control of the partners, to which the data are transmitted, and through which the parties can access them (a structure similar to a joint venture); (2) second, a mediated pool can be created, where the data are transmitted to a medium controlled by a third party (trustee, escrowee, or administrator) who acts on behalf of, and for the parties; (3) three, data pools can be configured in a decentralized way, granting the parties simply the possibility of reciprocal access to the data, or the possibility of reciprocally exploiting certain data sources, without the intervention of a third party (following a cross-licensing system).

For the purposes of these reflections, the central point of data pools is that they are formed as a fundamental tool for sharing and combining data. Thanks to data pooling, it is possible to create new products and services, improve existing products and services, train algorithms and artificial intelligences, reduce costs and improve efficiency in the activity of companies, and develop personalized products that are more in line with the needs of the buyer.[36]

---

[34] For a deeper consideration of the implications of pool contracts, Eugenio Olmedo-Peralta, 'Data Pools Contracts: An Approach to Their Legal Regime and Economic Function', in Luis María Miranda Serrano, Javier Pagador López (ed) *Commercial Contracting: Digitization and Protection of the Client/Consumer* (Marcial Pons 2023) 93–122.

[35] This second category includes so-called 'data spaces' promoted by the Data Governance Act for sectors such as health, or data integrated in vehicles.

[36] See European Commission, Directorate General for Competition, Competition Policy for the Digital Era, (n 11), 94–95.

At the same time, the pooling of data by partners in a data pool can generate a series of significant risks, especially concerning competition in the market.

IV. Competition Concerns: Information Exchanges and Blocking Strategies

The pooling of data in a data pool can pose risks from an antitrust law perspective. This form of intermediation and cooperation can facilitate the development of collusive practices among the partners, lead to the closure of the market to current or potential rivals, or grant companies controlling the pool a position allowing them to engage in abusive practices, particularly limiting innovation.[37] Furthermore, the formation of these pools may be the result of a previous (anti-)competitive strategy by the partner companies, which fosters the creation of a data pool standard under their control.[38]

Competition issues arising from data pools stem from various sources. On the one hand, data processing allows for the acquisition of information, which can be used for illicit coordination of market behaviours. On the other hand, access to data shared in a data pool that is essential for an industry, can be crucial for other companies' entry into that market. Thus, for the development of certain sectors (for example, autonomous vehicles), it is indispensable for economic operators to pool data, which they will need access to in order to develop their activities. These pools may eventually become a sort of industry-required standard or, as some have considered, an essential resource to compete in the market.[39]

---

[37] Michael Mattioli, 'The Data Pooling Problem' (2017) 32 (1) Berkeley Technology Law Journal, 190 et seq.

[38] See Josef Drexl, 'Designing Competitive Markets for Industrial Data: Between Propertisation and Access' (2017) JIPITEC 8, 292. Also, see Commission Communication, *Standardization priorities in the ICT sector for the Digital Single Market*, COM(2016) 0176 final.

[39] While preliminary, it is fair to view the application of the essential facilities doctrine to data pools as not appropriate, considering the inherently duplicable nature of data, the multiple ways in which they can be accessed, and the possibility of building competing data consortia, as no one controls an indispensable non-duplicable resource for the market. In this case, it will be a market failure that must be approached through other regulatory instruments, theories of harm, or applicative tools. In this sense, cf. European Commission, Competition Policy for the Digital Era, (n 11), 98 et seq.; European Commission, Joint Research Centre, Business-to-Business data sharing: An economic and legal analysis, JRC Technical Report, (2020), 36–38. In doctrine, see Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law Int'l, 2016); Giuseppe Colangelo, Mariateresa Maggiolino, 'Big Data as Misleading Facilities' (2018) 13 (2–3) European Competition Journal, 249–281.

Recognizing that competition problems arising from the creation of data pools can have different origins and configurations, various regulatory instruments must be combined for their assessment. Therefore, it is necessary to consider the rules of the Data Governance Act, as well as the Data Act. In addition, similar situations can be guided by other rules, such as the new Guidelines on Horizontal Cooperation Agreements of 2023[40] (hereinafter: Horizontal Guidelines), the new Block Exemption Regulations for Research and Development Agreements[41] or for Specialization Agreements,[42] as well as established doctrine regarding patent pools (technology consortia)[43] and information exchanges.

Considered next are the main risks that the use of these data pools can generate from a competition law perspective.

1. Risk of Collusion

Data processing enables the extraction of information. Through a data pool, information can be derived from data provided by external companies. If processing these data yields insights into the commercial activities or competitive strategies of other companies, especially when they are direct competitors or operate in the same or related markets, which is typically why there is interest in creating the pool, there's a risk of coordinated behaviours that could fall within the scope of the prohibition of collusive practices.

[40] Commission Communication, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements [2023] COM(2023) 4752 final, OJ C259/1-125 (hereinafter: Horizontal Guidelines).

[41] Regulation (EU) 2023/1066 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European Union to certain categories of research and development agreements [2023] OJ L143/9-19.

[42] Regulation (EU) 2023/1067 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European Union to certain categories of specialization agreements [2023] OJ L143/20-26.

[43] Regulation (EU) 316/2014 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European Union to certain categories of technology transfer agreements [2014] OJ L93/17-23 (which excludes them from its scope of application, and, consequently, will require individual evaluation based on the criteria set out in the Guidelines), and Commission Communication, Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements [2014] (2014/C 89/03), OJ C89/3-50.

Generally, information exchanges as a practice facilitating collusion have been repeatedly addressed by competition authorities[44] and by scholars.[45] On one hand, as data pools form the infrastructure for developing an information exchange system, they can increase transparency of corporate behaviours, facilitating alignment of market practices.[46] On the other hand, a data pool can be used as a tool to monitor the development of a prior, explicit or tacit coordination.[47] Thus, once parties have aligned their behaviours, sharing data through the pool allows its partners to check how their contractual counterparts (in case it's explicit), or other parties aligning their behaviours tacitly, are following what had been previously agreed upon.

What uniqueness do information exchanges through data pools present? Compared to other exchange mechanisms, data pools enable real-time data transfers between parties. If this type of information is included in the data pool, partners can have real-time information on prices, production, capacity, and investments being made by others. When assessing the potential anti-competitive nature of activities conducted through a data pool, the nature of the shared data and the characteristics of the affected market should be

[44] See CJEU judgments in Case c-74/14 *Eturas and others*/*Commission* EU:C:2016:42; Case C-8/08, *T-Mobile Netherlands and others*/*Commission* EU:C:2009:343; Case C-286/13, *Dole Food and Dole Fresh Fruit Europe* /*Commission* EU:C:2015:184; Case C-609/13, *Duravit and others* /*Commission* EU:C:2017:46; Case C-883/19, *HSBC Holding and others*/*Commission* EU:C:2023:11; Case, T-180/15, *ICAP and others*/*Commission* EU:T:2017:795; Case C-199/92, *Hüls*/*Commission* EU:C:1999:358; joined cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P, and C-219/00 P, *Aalborg Portland and others*/*Commission* EU:C:2004:6; GCEU judgment in Case T-240/17, *Campine and Campine Recycling*/*Commission*, EU:T:2019:778.

[45] Antonio Capobianco 'Information Exchanges under EC Competition Law' (2004) (41) Common Market Law Review, 1247–1276; Okeoghene Odudu, 'Indirect Information Exchange: The Constituent Elements of Hub and Spoke Collusion' (2011) Vol 7, N 2, European Competition Journal, 205–242; Florian Wagner-von Papp, 'Information Exchange Agreements', in Ioannis Lianos, Damien Geradin (eds) *Handbook on EU Competition Law – Substantive Aspects* (Edward Elgar 2013), 130–173; Carmen Estevan de Quesada, *Las prácticas facilitadoras: Control de la colusión en los mercados oligopolísticos* (Tirant lo Blanch 2013) 155 et seq.

[46] Thus, the Horizontal Guidelines (paras. 377 and 378) expressly consider that 'By artificially increasing transparency between competitors in the market, the exchange of commercially sensitive information can facilitate coordination of undertakings' behaviour and result in restrictions of competition. First, information exchanges are likely to facilitate collusion if they allow an undertaking to signal to its competitors, through any means, the conduct that it would find desirable for those competitors to follow, or the conduct that the undertaking itself would adopt in reaction to the same competitors' conduct. Second, the exchange of commercially sensitive information may in itself allow undertakings to reach a common understanding on the terms of coordination, which can lead to a collusive outcome on the market. The exchange can create mutually consistent expectations regarding the uncertainties present in the market. On that basis, undertakings can then reach a common understanding on their behaviour on the market, even without an explicit agreement on coordination'.

[47] Paras. 379 and 380 of the Horizontal Guidelines.

considered.[48] In most cases, the immediate and automatic nature of data exchanges facilitates collusion to a greater extent than if information exchanges took place through periodic reports or other means of sharing.

The new Horizontal Guidelines rightly consider that problems of coordination prohibited by Article 101 TFEU can also arise from regulatory initiatives. In particular, this may occur when a data exchange happens in compliance with data portability duties established by the General Data Protection Regulation (GDPR), the DMA, the Data Act, or the Data Governance Act. In such cases, companies affected by these regulatory norms must implement necessary precautions to avoid the exchange of sensitive information, and limit their activity to the information required by the applicable legislation.

1.1. Ways to Organize Information Exchanges

Information exchange can be organized in various ways:

- It can consist of a direct exchange among competitors, whether the exchange occurs unilaterally, bilaterally, or multilaterally. In the context of this paper, this form would be realized through the creation of disintermediated pools, or following cross-licensing schemes.
- As a direct information exchange through a third party. In the case of data pools, this situation is considered when the pool is managed by a third-party administrator, such as an online platform that allows for the combination and processing of data, with, or without the use of its own algorithm.
- Through a market research organization, as was the case in the paradigmatic *Asnef-Equifax* case.[49]
- Via suppliers or customers of the parties to the exchange, or through a website. In this case, it is necessary to consider the possibility of sharing sensitive information that facilitates collusion through specialized platforms like in the *Booking.com* or *Idealista* cases.

[48] For sure, collusion is more likely in oligopolistic markets than in markets with greater competition.

[49] Judgment of the CJEU (Third Chamber) of 23 November 2006, Case C-238/05, *Asnef-Equifax v. Ausbanc* EU:C:2006:734 (preliminary ruling request) where the Court ruled that Article 81(1) EC (now Article 101(1) TFEU) 'must be interpreted as meaning that a system for the exchange of information on credit between financial institutions on customer solvency does not, in principle, have as its effect the restriction of competition within the meaning of that provision, provided that the relevant market or markets are not highly concentrated, that that system does not permit lenders to be identified and that the conditions of access and use by financial institutions are not discriminatory, in law or in fact'.

1.2. Possible Content of the Exchanged Information: Types of Data

The notion of information exchange can encompass a wide variety of scenarios. The Horizontal Guidelines consider that the doctrine on these exchanges applies to:

1. Exchange of raw, unorganized digital content, which may need processing to be made useful (raw data).
2. Pre-processed data that has already been prepared and validated.
3. Manipulated data to produce meaningful information, in any form.
4. Any other type of information, including non-digital information.

Information exchange can occur through physical means, or digital or immaterial methods, and can affect actual or potential competitors. Although not explicitly mentioned in the Guidelines, this notion of information exchange should include the ways in which parties grant access to data sources. This is the case, for example, when one or more platforms allow other agents to directly access data generated by a device (sensors, IoT devices), software, or application.

More significant for the classification of the effects of their exchange from the perspective of the collusion prohibition, it is necessary to distinguish: (1) commercially sensitive information, (2) public information, (3) data necessary for industry, technology or product development, and (4) information that must be mandatorily communicated.

Commercially Sensitive Information. This refers to confidential information about a company's commercial policies, the formulation of its strategies, or the objectives pursued. Sharing this type of information could constitute a violation of the prohibition of collusive conduct, if it can influence the commercial strategy of competitors. To determine the anti-competitive effect of sharing commercially sensitive information, the nature of the affected products, the size and number of companies participating in the exchange, and their market share should be considered.[50] Thus, as a potential restriction of competition by effect, it would be necessary to demonstrate that sharing this information allows coordinating the behaviour of rivals in terms of price, quality, production, or innovation.

This type of information includes data related to a company's cost structure, production capacity, actual production, market shares, customers, strategic plans to operate in certain markets, or other elements of their business strategy

[50] Thus, the more the market structure approaches an oligopoly, the more plausible the anticompetitive impact of this information exchange. Conversely, the greater the competition, and the smaller the market share of the affected companies, the lower the risk of an anticompetitive effect (CJEU, *Asnef-Equifax 7Ausbanc*, para. 57).

that the parties would not be interested in exchanging as their market success depends on it.

Therefore, it falls within the scope of the prohibition of collusive behaviour if the exchanged information reduces uncertainty about the future, or recent actions of rival companies. Also problematic is the exchange of information that parties must protect, through trade secrets or otherwise, in order to maintain or improve their competitive position in the market.

The most typical case of this form of information exchange relates to prices or criteria used for price determination.[51] In particular, sharing data about the algorithm used for price determination will involve exchanging commercially sensitive information, which will likely fall within the scope of Article 101 TFEU prohibition.

As different degrees of commercially sensitive information can be delineated, based on their usefulness for promoting anti-competitive coordination of behaviours, the Horizontal Guidelines identify within this category particularly sensitive commercial information.

1.a. *Particularly Sensitive Information*. Certain categories of confidential commercial data deserve special treatment, given their particular potential to promote coordinated behaviour of companies to the detriment of competition. This determination should consider the content of the information, its objectives, the operating conditions of the affected market, the goods or services concerned, and the legal and economic context in which the exchange occurs. Sharing this type of data will be classified as a restriction by object and, therefore, will amount to an infringement of Article 101 TFEU (or equivalent national competition laws) without the need to demonstrate its anti-competitive effect on the market[52]. Given the severity of this classification, clarity is needed on what kind of information deserves this consideration. Therefore, the Horizontal Guidelines include a list of practices, as a blacklist, on types of data that, when exchanged between companies (within a data pool or not), will constitute a competition restriction by object. These are:

a) The exchange with competitors of current prices and intentions for future price setting by a company.
b) The exchange with competitors of current and future production capacities of a company.

---

[51] In this regard, para. 385 of the Horizontal Guidelines states that 'Information on pricing is generally considered commercially sensitive and Article 101(1) may apply even if the exchange does not have a direct effect on the prices paid by end users'.

[52] In particular, there is no need to demonstrate the connection between the exchanged information and the prices applied to products or services, with the nature of the contacts being relevant.

c) The exchange with competitors of a company's current or future commercial strategy.
d) The exchange with competitors of a company's forecasts related to current and future demand.
e) The exchange with competitors of a company's forecasts about future sales data.
f) The exchange with competitors of future product features that are relevant to consumers.

2. *Public Information*. In contrast to the above types of information, the exchange of public information does not raise competition issues, nor is it likely to constitute an infringement of the prohibition of collusive behaviour. Public information is defined as information that, in general, can be accessed equitably by all competitors and consumers.

3. *Technical data pools*: Access to data pools that contain information related to the industry or necessary for the development of products or technology is essential in order to compete in a certain sector, as the shared data, and access to the platform where they are shared, are indispensable for the development of products or services. An example would be data pools where precise data are shared for the development or operation of intelligent vehicles[53].

4. *Mandatory Information*. This refers to data that must be shared by companies in compliance with a legal duty. For example, in Spain, this would be the obligation to publish annual accounts in the Commercial Registry, or on the website of publicly traded companies. It is also the case for other data that must be made publicly available as a matter of obligation, as occurs with capacities and wholesale production costs in the electricity sector. Since these are data easily accessible by competitors and consumers themselves, they do not pose problems for competition, and their sharing will not generate collusion risks.

1.3. Ways to Limit the Risk of Collusion

Depending on the type of data shared, and the way the pool is organized, there might be a greater or lesser likelihood of competition issues arising. In certain cases, for the proper functioning of the consortium, and to derive the expected benefits from data pooling, it may be necessary to share information that could potentially involve commercially sensitive data. In this scenario, it is essential to adopt measures aimed at limiting the harmful potential of data

[53] Since the main type of competition problems that can arise from this type of data pools relates to abuse of dominance through exclusion, they will be analysed in depth in the following section of this paper.

sharing, implementing strategies based on data anonymization or aggregation, in order to prevent the identifiability of its source. While not exhaustive, there are various ways to do this.

Blind Sharing: A primary method to limit the potential use of shared data in a pool for collusion, is to share the data in a completely anonymous or blind manner. Through this approach, data can be shared via a pool for the development of a particular sector, such that companies send their data to a platform managed by an independent third party not active in that sector, and receive back aggregated data, without indication of its specific origin, that is, without knowing which company or companies the data came from.[54]

Limiting Access to Information: Another option is based on restricting access to certain information, through screening the shared data or establishing internal silos, which protect access to certain information the availability of which could be especially problematic. In this way, partners sharing data in the pool would implement measures to limit access to (sensitive) information, or to control or restrict how such data are used.

These measures are designed to ensure that each partner in the pool can, in principle, have access only to their own data, and the data resulting from its aggregation and combination with other users' data, provided that the data from other partners in the pool cannot be individualized. To achieve this, it is necessary to implement technical and practical measures to ensure that each participant cannot obtain commercially protected information from other partners.

1.4. Possible Defences of the Pool

If it is considered that an information exchange via a data pool constitutes a collusive practice, it is necessary to analyse if such conduct can be justified under any legally established exemptions.

1. *General Exception under Article 101(3) TFUE*. First, it should be assessed whether the agreement to share data in the pool can be covered by the general exemption under Article 101(3) TFEU. To apply this rule, it is essential that the requirements set forth in it are met, namely, that the agreement contributes to improving the production or distribution of goods or to promoting technical or economic progress; that it allows consumers a fair share of the resulting benefit; that it does not impose on the participating companies restrictions which are not indispensable to achieving these objectives; and that it does not afford the companies participating in the pool the possibility of eliminating competition in respect of a substantial part of the products concerned.

[54] Margrethe Vestager, 'Big Data and Competition' speech delivered on 29-9-2016 at EDPS-BEUC Conference on Big Data, Brussels. These measures are referred to by Björn Lundqvist (n 66), 15.

It is argued here that the first condition (contribution to the improvement of production, distribution, or technical or economic progress) will be met in most data pools, as they are generally created to obtain an advantage from the combination of data from different companies, which will enable the development of new products, and the improvement of current capabilities. Likewise, in most cases, this combination of data can result in consumer and user benefits, provided there is no excessive exploitation of their data.

The problematic points for the application of this general exemption will derive from the two negative conditions of the provision. Thus, for the pool to be declared compatible with the market, it must not impose on the partners or other interested third parties any restrictions that are not indispensable to achieve the intended objectives. Externally, this requirement will prevent the pool from excluding or limiting the participation of other companies that might be interested in joining, especially when access to the data may provide a competitive advantage in the market. Internally, it will be required that the data shared are limited to what is strictly necessary to achieve the pool's objectives, without being used as a means to exchanging other information, which will only be used in the market for a commercial purpose. In this sense, a screening of the information contributed to the pool by each partner should be carried out, sharing only the data that are strictly necessary for the consortium's objectives. In many cases, meeting such requirements can compromise the internal economy of the pool.

The possibility of market closure, as analysed later in the paper, is also problematic for the formation of data pools and may hinder the application of this generally applicable individual exemption, especially when the shared data can be considered essential technical data, or data necessary to pursue an activity in a particular market.

In applying the Article 101 (3) TFEU exemption, the use of an efficiency defence has been promoted, trying to justify the utility of the pool agreement, and the benefit derived from it. This efficiency defence can also be used in cases of abuse of a dominant position, which will be referred to in subsequent sections. For it to be admitted, it must be adequately justified that the agreement promotes competitiveness among participating companies, resulting in improvements in their activity, technological development as well as new products and services.[55] Thus, in certain cases, when markets have

[55] See CJEU (Fifth Chamber) Case C-7/95 P, *John Deere Ltd*/*Commission* EU:C:1998:256, esp. para. 88 where it is recognized that 'in principle, where there is a truly competitive market, transparency between traders is likely to lead to intensification of competition between suppliers, since the fact that in such a situation a trader takes into account information on the operation of the market, made available to him under the information exchange system, in order to adjust his conduct on the market, is not likely, having regard to the atomised nature of the supply,

sufficient competition, having more information about the market could allow companies to better profile their competitive strategy and make optimal decisions[56]. However, this conclusion needs to be questioned, especially in cases where companies use algorithms or artificial intelligence for processing the accessed data, and for designing their competitive strategies. The use of similar algorithms that can coordinate the activities of the partners, or AI systems based on self-learning that allow alignment, would lead to a high risk of coordinated behaviour, with an anti-competitive outcome.

2. *Consideration as an ancillary restraint*. In cases where data sharing through a pool is necessary for the execution of conduct that is not considered anti-competitive or is covered by a block exemption,[57] the pool agreement will likewise avoid from being considered anti-competitive. The same applies when the creation of a data pool is indispensable for the execution of a merger that has been authorized by the relevant competition authority.[58] In these instances, the accessory follows the principle, meaning that if the merger or agreement is valid under competition law, so too should be the necessary measures for its execution, in the context of this paper, the creation of a data pool where essential data for the successful completion of the relevant lawful operation are shared.[59]

---

to reduce or remove for the other traders all uncertainty about the foreseeable nature of his competitors' conduct'. However, the conclusion must be the opposite in oligopolistic markets, so, in each case, the particular circumstances of the market, and of the companies participating in the data exchange, must be considered.

[56] Thus, European Commission, Competition Policy for the Digital Era, (n 11), 96, where it is expressly indicated that outside the cases expressly considered by sectoral rules: 'Possible efficiency gains will therefore need to be analysed closely case by case – sometimes in the context of Article 101(1), but mostly in the context of Article 101(3)'.

[57] For example, consider a research agreement that falls within the scope of Commission Regulation (EU) 2023/1066 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European Union to certain categories of research and development agreements [2023] OJ L 143/9-19, and which requires for its implementation the sharing of a set of data through the creation of a pool in which the companies in the agreement participate. This could also be the case for other horizontal agreements such as joint purchasing, joint production, or joint marketing agreements.

[58] Commission Communication on the direct restrictions linked to the realization of a concentration and necessary for that purpose (2005/C 56/03) [2005] OJ C56/24-31. See also Luis María Miranda-Serrano, 'En el Derecho antitrust también lo accesorio sigue la suerte de lo principal: a propósito de la recepción por el Tribunal Supremo de la doctrina de las restricciones accesorias' (2013) 13 Revista de Derecho de la Competencia y la Distribución, 15–50; Mario A. Pérez Molina, 'Enjuiciamiento antitrust de las restricciones accesorias insertas en operaciones de concentración de empresas en la Unión Europea' (2014) 15 Revista de Derecho de la Competencia y la Distribución, 169–188.

[59] For example, if the exchange of information is necessary for the development of a vertical cooperation agreement, which falls within the scope of Commission Regulation (EU) 2022/720 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European

3. *A Possible Specific Exemption through a Block Exemption Regulation*. There is currently no block exemption regulation that generally considers the creation of data pools as agreements with anti-competitive potential that are compatible with the European market. There are, however, examples of sector-specific regulations that have considered exempting certain information exchange systems.

As a historical reference, in the insurance sector, Regulation 267/2010[60] exempted certain categories of agreements, decisions, and concerted practices in the insurance sector aimed at cooperation in the area of aggravated risk registers, and their corresponding information systems.[61] These included joint compilations of the average costs of risks, as well as tables on the frequency of certain types of accidents. The application of this exemption was conditional on the data pool being limited to aggregated and non-binding actuarial data, not including financial information from the participating companies. It was also conditional upon allowing access to the pool under FRAND conditions to other companies in the sector and potential new entrants. As of 31st March 2017, this Regulation is no longer in force; since then, these types of data

Union to certain categories of vertical agreements and concerted practices [2022] OJ L134/4-13, the block exemption would cover the information exchange, considering that it is directly related to the implementation of the vertical agreement, and that it is necessary for the improvement of the production or distribution of the products or services affected by the agreement. A similar conclusion must be reached when the information exchange implies an ancillary restriction linked to the execution of an authorized merger.

[60] Regulation (EU) No 267/2010 on the application of Article 101, paragraph 3, of the Treaty on the Functioning of the European Union to certain categories of agreements, decisions, and concerted practices in the insurance sector [2010] OJ L83/1-7.

[61] Para. 9 of the Regulation justified the exemption considering that 'Collaboration between insurance undertakings or within associations of undertakings in the compilation of information (which may also involve some statistical calculations) allowing the calculation of the average cost of covering a specified risk in the past or, for life insurance, tables of mortality rates or of the frequency of illness, accident and invalidity, makes it possible to improve the knowledge of risks and facilitates the rating of risks for individual companies. This can in turn facilitate market entry and thus benefit consumers. The same applies to joint studies on the probable impact of extraneous circumstances that may influence the frequency or scale of claims, or the yield of different types of investments. It is, however, necessary to ensure that such collaboration is only exempted to the extent to which it is necessary to attain these objectives. It is therefore appropriate to stipulate in particular that agreements on commercial premiums are not exempted. Indeed, commercial premiums may be lower than the amounts indicated by the compilations, tables or study results in question, since insurers can use the revenues from their investments in order to reduce their premiums. Moreover, the compilations, tables or studies in question should be non-binding and serve only for reference purposes. The exchange of information not necessary to attain the objectives set out in this recital should not be covered by this Regulation'.

exchange agreements, and the creation of data pools in the insurance sector, must be analysed in light of the Horizontal Guidelines.

Although there is currently no block exemption regulation that directly allows considering the compatibility of data pools with the competitive functioning of the market, the future approval of general regulations, or specific ones for certain sectors, which would establish a safe harbour for certain data exchange systems is possible. This would be applicable where these are necessary and where potential greater economic benefits justify possible risks of limiting competition. For now, any analysis of the compatibility of data exchanges through a pool must be judged within the framework, perhaps overly generic, of the Horizontal Guidelines.

2. Risk of Market Foreclosure

Technical data pools, or pools of precise data necessary for operating in a specific sector, or for the development of products or technologies, can create barriers to market entry. These are essentially real-time updated data repositories, access to which becomes indispensable for market participation. A typical example is the access to data pools on autonomous vehicles, necessary for both the design and development of new vehicles and their operation. In the pharmaceutical sector, access to certain medical data pools, providing information on the progression of diseases or patient responses to treatments, is also crucial.

In these cases, situations similar to patent pools[62] appear. Access to these data pools is essential for operating in a particular market, and their generation and control are due to the combined effort of different companies, each holding some rights over the information shared in the data pool.[63] This, similarity, should lead to the consideration of whether the effects on competition from these practices can be assessed using an analogous application of the Guidelines on Technology Transfer Agreements.

[62] On patent pools and the setting of standard essential patents, take into account the recent publication of a Proposal for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU)2017/1001, 2023/0133 (COD) of 27.4.2023. In the doctrine, see Carmen Rodilla-Martí, *Consorcios de estandarización, patentes esenciales y cláusulas FRAND* (Tirant lo Blanch 2016); Björn Lundqvist, *Regulating Access and Transfer of Data*, (CUP 2023), 90 considers the opportunity to apply the logic of the Guidelines on Technology Transfer.

[63] However, there are also important differences between patent and data pools. Thus, patent rights shared in the first type of pools are strong industrial property rights; while the data shared in data pools will not have such legal protection, despite being covered by the protection afforded by the legislation on business secrecy.

Given the necessity of accessing the data in these pools to compete in the market, it is vital to promote a system that unites the entire sector to share data (all-industry sharing of data), as access to this data is fundamental for technological development, innovation, and research and development activities.[64]

Poor management of such data can lead to a significant risk of market closure, resulting in the exclusion of actual or potential competitors, either in the same market where the data are generated, or in connected markets.

When data in the pool are essential for accessing a particular sector or technology, the risk of market closure can occur in the same market affected by the exchanged data, or in a related secondary market. Firstly, market closure in the same market where data are shared can occur when the data exchange puts competitors that do not have access to it (because they are not part of the pool) at a competitive disadvantage compared to those who participate in the data exchange.

Secondly, data exchange through a data pool can lead to an anti-competitive closure of the primary market to third parties operating in another related market.[65] This impact on other markets can occur, particularly in vertically connected markets, where having data about the functioning of a market upstream or downstream, can be crucial for determining the commercial strategy in another market. For instance, the advantages for raw material suppliers in accessing data about the activities of their main customers, allowing them to plan their production and adapt inputs to their demand. In this case, if some suppliers have access to this information, while others do not, an anti-competitive market closure for the latter would occur.

To address the problems arising from market closure, the most suitable remedies are those that allow access to the data contained in the pool. Considering that the information shared in the data pool is strategic for competition in the market (in the same market or in a connected market), the solution to the potential problem of anti-competitive closure involves granting access to the data pool to companies that request it.

Reasoning by analogy with the rules that regulate access in similar situations of market closure (such as standard setting, essential facilities, etc.), it can be inferred that access should be granted under FRAND terms.[66] This means that access to the data pool must be allowed to any company that requests it, without discrimination among them, provided a legitimate interest is shown.

---

[64] Björn Lundqvist 'Data Collaboration, Pooling, and Hoarding under Competition Law' (2018) 61 Stockholm Faculty of Law Research Paper Series.

[65] In digital markets involving data, there is a considerable number and variety of markets that may emerge as interconnected or linked.

[66] European Commission, Competition Policy for the Digital Era, (n 11), 97.

Moreover, a transparent procedure must be followed if the creation of the data pool establishes a standard in the industry, and data interoperability must be promoted, making it useful for companies that were granted access, which can incorporate it into their production structure. Finally, such access must be granted under fair, reasonable, and non-discriminatory terms.[67]

Furthermore, imposing obligations and recognizing data portability rights, whether from a regulatory perspective (as analysed), or in a competition proceeding, can facilitate access to such data and open the market.

However, it should be noted that the obligation to share and grant access to data in the consortium arises only when the data are strategic for competition, that is, when access to the pool is absolutely indispensable for competing in the market. Denying competitors access to these essential data pools would erect entry barriers, as business rivals (actual or potential) would not be able to operate in the market in competition with those who have access to the data. Conversely, refusing access to data pools that do not have such a character is permissible.

3. Risk of Other Kind of Exploitative Abuses

Competition law intervention in the data market should only occur when the use of data by one or more companies is detrimental to the market, in such a way, that the harm derived from their conduct outweighs the benefits that can be obtained from such data.[68] In these cases, measures and remedies must be adopted to establish appropriate competition conditions in the market. However, mere control of large, even enormous, amounts of data does not justify public intervention. Simple dominance over data does not necessarily and automatically imply market power, and its exploitation may not constitute abusive behaviours.[69]

However, there can be situations where, due to the unique characteristics of the data, the difficulty to obtain them through parallel means, or because they are indispensable for operating in a specific market, the holders of the

[67] Regarding the challenge of concretely defining what should be understood as FRAND terms in practice, reference is made again to Carmen Rodilla Martí, *Consorcios de estandarización* (n 64), 153 et seq.

[68] Fabiana Di Porto, 'Abuses of Information and Informational Remedies: Rethinking Exchange of Information Under Competition Law?' in Fabiana Di Porto, Josef Drexl (eds) *Competition Law as Regulation* (Edward Elgar Publishing 2014), 298.

[69] Margrethe Vestager, 'Competition in a Big Data World' speech delivered on 17/1/2016 at DLD Munich.

data or, in the context of this paper, the parties controlling the pool, might engage in exploitative behaviours to the detriment of other agents.

Such exploitative behaviours may occur when a data pool becomes indispensable (a pool that has become a standard or essential pool) for operating in a particular market, or developing a certain technology, and for which licensing under FRAND conditions is necessary. In this case, the participants of the data pool could exploit their dominant position derived from controlling these data, by progressively increasing the fees to be paid in order to use the pool's data, as access to them becomes more crucial for competing in the market. This would be developing abusive behaviours similar to patent abuses in the field of intellectual property.[70]

Another possible exploitative behaviour, derived from market power based on control of the data pool, might involve demanding an excessive amount of data contribution from new partners wishing to enter the pool. This behaviour would consist of requiring new entrants to contribute data that, in terms of quality, quantity, or diversity of sources, is quantitatively or qualitatively more extensive than data provided by the other partners. Entry into the essential pool would be conditional on accepting non-reciprocal conditions that could be considered excessive.

V. Conclusive Remarks: the Need for Safe Harbours to Promote the Development of Data Pools

In the digital era, the development of new products and services based on data requires access to large amounts of information from various sources as well as the combination of such data to gain deeper and more useful insights. Data pools are a highly conducive means for this purpose.

However, when addressing market competition and the creation of such consortia, the varying positions of companies must be taken into account. On one side, there are large digital platforms that, in some cases, may qualify as gatekeepers and already control a substantial portion of the market's available data. Granting these companies even greater access to data can be problematic, which is why the DMA (Digital Markets Act) and the Data Act impose limitations on their ability to access data from other sources. Instead, gatekeepers are subject to a series of obligations and prohibitions meant to allow other companies, whether competitors or not, to access more data. On the other hand, measures need to be implemented to enable these other companies to access larger quantities of data, and to break down entry barriers resulting from their amassing by other agents.

[70] European Commission, Competition Policy for the Digital Era, (n 11), 97.

Although the general assessment should be that data pools are positive for dynamic market competition, as they allow for the development of new products and services, and improve market efficiency, they can also give rise to certain competition issues. These problems may, in particular, stem from possible collusion arising from information exchanges, or from the abuse of a dominant position built upon control of the data in the pool.

The antitrust assessment of these behaviours requires comparing each situation with competition law. However, it cannot be claimed that current legislation is completely adequate or able to sufficiently address the competition problems that may arise around data pools. In 2023, new Guidelines on Horizontal Cooperation Agreements were approved, clarifying the EU framework for assessing data pools as systems that enable information exchanges between companies. Nonetheless, the Guidelines could have been more ambitious, by offering a more detailed treatment of the specific features of data exchanges (since data is not the same as information) through data pools. It might even have been more appropriate to maintain the general character of the Horizontal Guidelines, but to accompany them with additional guidelines, or another soft law instrument, specific to the data sector. This leads to the suggestion to create and additional act of EU soft law on data sharing, which can assess the effects on competition specifically of these types of agreements, offer companies security about what kind of data they can share in a data pool, and how these can be configured without risking a violation of competition rules.

In light of the need for guidance from competition authorities, the creation of a safe harbour that allows companies to conduct an antitrust assessment of the data they share in a data pool becomes necessary.[71] This could be achieved by means of the adoption of specific Data Sharing Guidelines. For example, the guidelines could establish that shared data must be anonymized or aggregated, to protect consumer privacy and prevent the misuse of sensitive information. They could also specify that data exchanges must be transparent and equitable, ensuring that no company gains an unfair advantage over its competitors.

However, the above discussions have shown that it becomes increasingly problematic to analyse competition issues by analogy to other acts governing more or less similar situations. Thus, applying a similar logic to that used in the Block Exemption Regulations for Research and Development Agreements or Patent Pool Agreements, with respect to data exchanges in a pool is complex. Importantly, it cannot be assumed that the data in a pool is a resource that has no alternatives, as it is always possible to use other data, or obtain similar data by other means, to achieve a more or less analogous result. Similarly, it is not appropriate to classify the data in a pool as an essential facility, as alternative

[71] Björn Lundqvist 'Competition and Data Pools' (2018) 7 (4) Journal of European Consumer and Market Law, 146–154.

data-based systems can be built, or other data compilations can be used for a more or less similar result (naturally, except when the pool has become the standard necessary to operate in a particular industry or market).

Specialized Data Sharing Guidelines would promote innovation and dynamic competition. It would enable smaller companies to access valuable data that they otherwise could not obtain. This would level the playing field, allowing for fairer competition and fostering innovation. Smaller companies could use this data to develop new products and services, improve their processes, and offer better experiences to their customers. A clear framework for data sharing can facilitate collaboration between companies and the development of new technologies. In many cases, companies may need to share data to develop emerging technologies, such as artificial intelligence and machine learning. Without a clear guide, these collaborations can be difficult to establish and maintain.

Along with that, such tailor-made soft law would help to mitigate legal risks associated with data sharing. Currently, companies may be reluctant to share data due to the fear of violating competition or privacy laws. Legal uncertainty can deter companies from engaging in data-sharing practices that could be beneficial to the market overall. Guidelines that clearly define the conditions under which data can be exchanged would provide companies with the legal certainty they need. A legally recognized safe harbour would allow them to know when, and how they can share data without it being an anticompetitive behaviour. This would reduce the risk of legal sanctions and encourage more companies to participate in data sharing.

The former would also lead to a significant improvement in data quality. When companies share data, they can combine their resources to obtain more complete and accurate datasets. This is especially important in sectors such as healthcare, scientific research, and artificial intelligence, where data quality can have a direct impact on outcomes and the ability to innovate. The fear to break competition rules might prevent parties from entering into such agreements, and this makes the existence of a safe harbour more necessary.

Funding

This paper has been drafted as a part of the Research Project: Marco jurídico para la competencia dinámica en mercados digitales y para la innovación a través de Inteligencia Artificial (CODIG-IA), ref. PID2021-122536OB-I00 (PI Eugenio Olmedo Peralta), funded by MCIN/AEI/10.13039/501100011033 and the European Union "NextGenerationEU"/PRTR; so as a part of the Research Project: Consumidores y pequeños profesionales en la contratación en Mercados Digitales: prácticas anticompetitivas, desleales y explotación de dependencia económica (CoMeDi), Ref. ProyExcel_00665. Proyectos de Excelencia, Programa de Ayudas a la I+D+i, en régimen de concurrencia competitiva, Plan Andaluz de Investigación, Desarrollo e Innovación (PAIDI 2020) (PIs: Olmedo Peralta / Benavides Velasco).

The cost of editing selected articles published in the Yearbook of Antitrust and Regulatory Studies in the 2022–2024 is covered by funding under the program "Development of scientific journals" of the Ministry of Education and Science under agreement No. RCN/SN/0324/2021/1. Task title: "Verification and correction of scientific articles and their abstracts". Funding value: 36 298,00 PLN; The task consists of professional editing of articles published in English.

Declaration of Conflict of interests

The author declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

Declaration about the scope of AI utilisation

The author did not use AI tools in the preparation of this article.

Literature

American Law Institute and European Law Institute (ALI-ELI), *Principles for a Data Economy – Data Transactions and Data Rights*-, last draft by ELI proposed on 2021, available at: https://www.principlesforadataeconomy.org

Baker JB, *The Antitrust Paradigm: Restoring a competitive economy* (Harvard University Press 2019)

Binns R and Bietti E, 'Dissolving Privacy, One Merger at a Time: Competition, Data, and Third Party Tracking' (2020) 36 Computer Law & Security Review 1

Capobianco A, 'Information exchanges under EC competition law' (2004) 41 Common Market Law Review, 1247

Chirita AD, 'Data-Driven Mergers Under EU Competition Law', in O Akseli and J Linarelli (eds), *The Future of Commercial Law: Ways Forward for Harmonisation* (Hart Publishing 2019)

Colangelo G and Maggiolino M, 'Big Data as Misleading Facilities' (2017) 13(2–3) European Competition Journal, 249

Di Porto F, 'Abuses of Information and Informational Remedies: Rethinking exchange of Information Under Competition Law?', in F Di Porto and J Drexl (eds) *Competition Law as Regulation* (Edward Elgar 2014)

Drexl J, 'Designing Competitive Markets for Industrial Data: Between Propertisation and Access' (2017) 8 JIPITEC 25

— 'Data Access and Control in the Era of Connected Devices' Study on behalf of the European Consumer Association BEUC (2018)

Estevan de Quesada C, *Las prácticas facilitadoras: Control de la colusión en los mercados oligopolísticos* (Tirant lo Blanch 2013)

European Commission, DG Competition, *Competition Policy for the Digital Era* final report (2019) Crémer J, de Montjoye YA and Schweitzer H (aut)

European Commission, JRC, *Business-to-Business data sharing: An economic and legal analysis* JRC Technical Report (2020) Martens, de Streel, Graef, Tombal and Duch-Brown (aut)

— *Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*, JRC Science for Policy Report (2023) Micheli, Farrell, Carballa-Smichowski, Posada-Sánchez, Signorelli, Vespe (aut)

Graef I, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer Law Int'l 2016)

Hoffmann J and Johannsen GO, 'EU-Merger Control & Big Data On Data-Specific Theories of Harm and Remedies' (2019) 19-05 Max Planck Institute for Innovation and Competition Research Paper 1

Khan LM, 'Amazon's Antitrust Paradox' (2017) 126(3) The Yale Law Journal 710

Lundqvist B, 'Competition and Data Pools' (2018) 7(4) Journal of European Consumer and Market Law 146

— 'Data Collaboration, Pooling and Hoarding under Competition Law' (2018) 61 Stockholm Faculty of Law Research Paper Series 1

— *Regulating Access and Transfer of Data* (CUP 2023)

Mattioli M, 'The Data Pooling Problem' (2017) 32(1) Berkeley Technology Law Journal, 179

Miranda Serrano LM, 'En el Derecho antritrust también lo accesorio sigue la suerte de lo principal: a propósito de la recepción por el Tribunal Supremo de la doctrina de las restricciones accesorias' (2013) 13 Revista de Derecho de la Competencia y la Distribución 15

Odudu O, 'Indirect Information Exchange: the constituent elements of hub and spoke collusion' (2011) 7 European Competition Journal 205

Olmedo Peralta E, 'Redefiniendo el ámbito de aplicación de la Ley de Mercados Digitales: ¿a quién? ¿cómo? y ¿para qué?', in A Tato, J Costas, P Fernández and F Torres (eds) *Nuevas tendencias en el derecho de la competencia y de la propiedad industrial III* (Marcial Pons 2022)

— 'La construcción de un régimen jurídico para el sector digital más allá del Reglamento de Mercados Digitales', in JI Ruiz Peris, F González Castilla and C Estevan de Quesada (eds) *Mercados digitales y competencia* (Tirant lo Blanch 2023)

— 'Los contratos de pools de datos (data pools): aproximación a su régimen jurídico y función económica' in LM Miranda Serrano and J Pagador López (eds) *Contratación mercantil: digitalización y protección del cliente/consumidor* (Marcial Pons 2023)

Pérez Molina MA, 'Enjuiciamiento antitrust de las restricciones accesorias insertas en operaciones de concentración de empresas en la Unión Europea' (2014) 15 Revista de Derecho de la Competencia y la Distribución 169

Petit N, *Big Tech & the Digital Economy, the Moligopoly Scenario* (Oxford UP 2020)

Podszun R and Offergeld P, 'The EU Data Act and the Access to Secondary Markets' Study for the Ludwif-Fröhler-Institut für Handwerkswissenshaften (2022)

Podszun R (ed) *Digital Markets Act, Article-by-Article Commentary* (Nomos 2024)

Regibeau P and Lianos I, 'Digital Mergers: A Primer' (2021) 3 Centre for Law, Economics and Society Research Paper Series 1

Rodilla Martí C, *Consorcios de estandarización, patentes esenciales y cláusulas FRAND* (Tirant lo Blanch 2016)

Ruiz Peris JI, 'La nueva Digital Markets Act, una respuesta híbrida de la Unión Europea a los gatekeepers GAFA' (2021) 57 Revista Aranzadi de Derecho y Nuevas Tecnologías 1

— 'Gatekeepers, discriminación autopreferente exclusionaria y reforzamiento de la posición de dominio: La nueva propuesta europea de Digital Markets Act', in J Martí Miravalls (ed) *Competencia en mercados digitales y sectores regulados* (Tirant lo Blanch 2021)

Vestager M, “Big Data and Competition”, speech delivered on 29/9/2016
— “Competition in a Big Data World”, speech delivered on 17/1/206
Vezzoso S, ‘The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU’ (2021) 17(2) European Competition Journal
Wagner von Papp F, ‘Information Exchange Agreements’, in I Lianos and D Geradin (eds) *Handbook on EU Competition Law – Substantive Aspects* (Edward Elgar 2013)