Market Failures in Business-to-Business (B2B) Data Exchanges and Measures to Address Them with Regulation and Competition Remedies: A European Perspective on Existing Law and Legislative Policy*

Fallos en el mercado de intercambio de datos entre empresas (B2B) y medidas para abordarlos desde la regulación y los remedios de competencia: una perspectiva europea de lege lata *y* de lege ferenda

EUGENIO OLMEDO PERALTA**
Universidad de Málaga, Malaga, Spain
olmedo@uma.es | https://orcid.org/0000-0003-1219-7587

◆

Received: September 4, 2023 | Accepted: October 13, 2023 | Published: October 31, 2023

Abstract: Access to data is critical for the development of products and services which are competitive in the digital market. But developing and gathering data is subject to certain dynamics which lead to data accumulation in the hands of a few companies hoarding data. Even if data are destined to be shared and exchanged among companies, there are major market failures preventing an efficient business-to-business data market to develop. This situation leads to a suboptimal use of data; also, a large part of the social usefulness that may be derived from data goes unused. Data-hoarding conducts by companies—especially as to gatekeepers—leads to underuse, to the detriment of market competition and innovation. In developing its Data Strategy, the European Union tries to address these market failures in two ways: by regulating the digital sector, and specifically laying down rules on data exchanges. Therefore, portability obligations and rights are imposed, exchanges are promoted as well as the creation of common data spaces and data pools. At the regulatory level, gatekeepers are subject to a series of duties and restraints aimed at opening up the market and avoiding the consolidation of indisputable

* This article has been translated from Spanish into English by Mariano Vitetta.

** European Ph.D. in Commercial Law, Università di Bolonia, Italy. Full Professor of Commercial Law, Universidad de Málaga, Spain.

positions. Competition authorities may additionally impose remedies in proceedings for antitrust violations with the purpose of promoting an open data market.

Keywords: Data; market failures; Data Act; Digital Markets Act; gatekeepers; portability; business-to-business; B2B; data sharing; data pools.

Resumen: El acceso a datos resulta crítico para el desarrollo de productos y servicios que resulten competitivos en el mercado digital. Sin embargo, su generación y captación se somete a dinámicas que llevan a la acumulación de datos en manos de pocas empresas que los acaparan. A pesar de que los datos están llamados a ser compartidos e intercambiados entre las empresas, se aprecian importantes fallos de mercado que impiden el desarrollo de un mercado interempresarial de datos eficiente. Ello da lugar a un uso sub-óptimo de los datos y a que se desaproveche buena parte de la utilidad social que puede obtenerse de ellos. Las conductas de acaparamiento de datos por las empresas —especialmente cuando se trata de guardianes de acceso— lleva a su infrautilización en detrimento de la competencia en el mercado y de la innovación. En el desarrollo de su Estrategia de Datos, la Unión Europea trata de abordar estos fallos de mercados a través de dos vías: por medio de la regulación del sector digital, y más concretamente estableciendo normas relativas al intercambio de datos. Se imponen así obligaciones y derechos de portabilidad, se fomentan los intercambios y la creación de espacios comunes de datos y pools de datos. A nivel regulatorio, los guardianes de acceso o gatekeepers quedan sometidos a una serie de obligaciones y prohibiciones dirigidas a la apertura del mercado y evitar la consolidación de posiciones indisputables. Complementariamente, las autoridades de competencia pueden también imponer remedios en los expedientes que instruyan ante infracciones antitrust con el objetivo de promover un mercado abierto de datos.

Palabras clave: Datos; fallos de mercado; Reglamento de Datos; Reglamento de Mercados Digitales; guardianes de acceso; portabilidad; business to business; B2B; intercambio de datos; consorcios de datos.

1. The Role of Data in the Digital Economy. The Need for a Business-To-Business Data Market

The possibilities for creating and marketing competitive products and services in the digital economy depend to a large extent on the amount of data which the developer or manufacturer may access.

Marketing of software, mobile apps, social media, communication services, brokerage platforms, and a large array of digital services will only be successful if relevant data can be accessed real time and in a significant manner for proper operation. An example is the development of a driving-assistance mobile app which, based on geolocation, shows us the best routes for our transfers at every moment. This product can only be developed

if important data can be accessed, such as the real-time status of traffic in the different areas of the city or the existence of works affecting traffic. But, in addition, if the app wants to provide a better service, it will have to take into account other elements which in a predictive manner may affect traffic when we are in a given area. To provide the service with greater precision, data such as entry and exit times to high-traffic locations (sports stadiums, schools, etc.) will be required, as well as information on unforeseen circumstances impacting traffic flow, such as accidents that fully or partially obstruct the initially preferred route. Our app will only be successful if we have enough and adequate access to the data we need for its operation.

However, the most valuable data is generated and hoarded by a few platforms. This data is neither sufficiently exchanged nor shared. It remains exclusively available to the companies that generate it. That is why, in a very unfortunate expression, it has been asserted that data is the oil of the digital economy. While it is true that, like oil, data is a resource creating wealth and is essential for gaining competitiveness in the market, the differences outweigh the similarities. This is basically because data is a non-appropriable and non-rivalrous resource. The fact that an individual or company possesses and uses a given dataset does not prevent this same set from being created and used by another. Moreover, the common or shared use of data does not limit its utility for the company that generated it. Consequently, data can be reused repeatedly without any detriment to its usefulness.

Due to this feature, data is destined to be shared and exchanged among companies. Moreover, the very value of data depends on its quantity and diversity, but also on the relative difficulty of obtaining it. As we amass larger volumes of data across various metrics stemming from different sources, the value of the information we derive increases. Thus, the combination of data generated by multiple companies enhances its value, generating significant synergies. Conversely, from the perspective of competition, data loses value as it becomes more accessible and widely known among firms. Consequently, data that is harder to acquire and less accessible to most companies will be more valuable than data that is readily obtainable. Therefore, companies making significant investments in instruments to obtain data will try to monetize them as much as possible and, in many cases, they will not be interested in sharing their data with other companies, as its value diminishes with broader access.

Due to its very nature, companies cannot acquire an exclusive and intrinsic control over data. That is, the fact that one company obtains a specific piece of data about the environment or about a user's behavior regarding a certain product does not prevent another company from also collecting and using that data. There are no exclusive rights

over the data generated. As data does not result from a creative effort, no intellectual property right may be claimed over it.[1] However, this data holds value. Companies that generate and control data will seek to implement actions to retain this value, considering that the value will increase as data is increasingly useful, more varied, and more difficult to be obtained by other companies. Without the possibility of using intellectual property rights for that, companies will employ technical or contractual measures to achieve *de facto* exclusivity of control over certain data. This protection requires the adoption of measures to guarantee data confidentiality, including strategies to avoid sharing data with actual or potential rivals.

This dynamic fuels the problem of a lack of a truly efficient data market, in which companies generating and obtaining data exchange it to create added value, increase its utility, and foster innovation in the development of new products and services. Data remains concentrated in the hands of few companies, and this monopolization prevents potential competitors from entering the market (raising entry barriers) or even the development of new products or services (stifling innovation).

In this context, it becomes necessary, first, to identify the market failures that prevent sufficient levels of data exchange and, second, to analyze the legal measures that could be adopted to overcome them. As is true of virtually every sector with operation problems, these market failures may be solved in two ways: by means of economic market regulation or by applying competition law, specifically by implementing *ex post* remedies in response to infringements of the regulations.

[1] There is no intellectual or industrial property right which allows for appropriation, giving an exclusive right over data. The only related right—but which also does not protect data *per se*—is the right *sui generis* over databases, regulated under article 133 of the Spanish Intellectual Property Law, transposing Directive 96/9/CE of the European Parliament and the Council, of 11 March 1996 on the legal protection of databases. However, this right is aimed at protecting the substantial investment, quantitatively or qualitatively assessed, made by the manufacturer whether of financial means, use of time, effort, energy, or others of a similar nature, to obtain, verify, or present their content. This right, therefore, is granted to protect databases if the producer invests substantially in obtaining, verifying, and presenting data. What it aims to protect is, therefore, the investment in data compilation and not its creation as a byproduct of another financial activity. *See* STJUE (Gran Sala) of 9 November 2004, in the matter of C-338/02, "Fixtures Marketing Ltd. v. Svenska Spel AB", especially section 19 (and, likewise, the other judgments of 9 November 2004, in the matters C-46/02, "Fixtures Marketing Ltd v. Oy Veikkaus AB"; C-203/02, "British Horseracing Board Ltd v. William Hill"; and C-444/02, "Fixtures Marketing Ltd v. OPAP").

2. The European Policy for the Digital Age and the European Data Strategy

Over the last decade, EU institutions have prioritized the adoption of regulatory measures to address market failures in the digital society and, in particular, to promote the creation of a data market. These initiatives are based on the findings and critical points mentioned by the studies and reports developed by the end of the last decade on the legal and financial problems of digital markets. In Europe, these reports include the two versions of the *European Data Market Study*[2] and the so-called *Crémer* report (Crémer et al., 2019). In other regions, significant reports include those from the *Stigler Committee* (Stigler Committee, 2019), *Chicago Booth* (Morton et al., 2019), the *Furman* report (Furman et al., 2019), the one of the French *Conseil d'Analyse Économique* (Jean et al., 2019), or that of *CERRE* (Franck and Peitz, 2019).

Based on these and other studies, the European Union designed its regulatory plan by means of Communication "Building a European Data Economy" (European Commission, 2017), highlighting the importance of creating an operative data market, removing the obstacles for the free circulation of data resulting from reasons other than the protection of personal data in the European Union. It also prioritizes the elimination of unjustified restrictions on data localization for storage or processing. The document identifies the following as key points requiring regulatory intervention:

— Satisfying the need to improve access to anonymized machine-generated data

— Facilitating and incentivizing data sharing

— Protecting investments and assets created for the development of the digital economy.

— Preventing the disclosure of confidential data and strengthening the protection of personal data.

— Minimizing lock-in effects.

— Promoting measures to incentivize companies to share data, encouraging the development of technical solutions for reliable data identification and sharing.

— Defining default contractual terms to serve as a foundation for data exchanges.

[2] The results of the first study were presented in February 2017 (IDC and Open Evidence, 2017), offering the first findings on the dimension and trends of the data economy in Europe and the bases for the measurement of results were established. After this first analysis in 2020, the results of the second study were presented for the period between 2017 and 2020 (Cattaneo et al., 2020).

These measures were formalized in February 2020 in the *European Data Strategy* (European Commission, 2020), setting out the main lines for the construction of a single data market that would enable Europe to take a leading role in the digital economy. The core idea in this strategy is to democratize access to data creating an agile market in which data may circulate for the benefit of competition and innovation. This purpose would be attained, on the one hand, by creating European data spaces and, on the other hand, by guaranteeing the right to access and portability of machine-generated data. The strategy also emphasizes the need to maintain competitive data markets data markets by monitoring potentially abusive conducts by major digital platforms controlling the markets (especially those designated as gatekeepers) and checking the fairness of contractual terms used in data-based commercial relationships particularly in cases of contractual imbalance.

The *European Data Strategy* has deployed an intense legislative agenda, which has resulted in these regulations:

— Regulation (EU) 2022/868, on Data Governance (informally known as "Data Governance Act").

— Regulation (EU) 2023/2854, on harmonized rules on fair access to and use of data (or Data Act).

— Regulation (UE) 2022/1925, on Digital Markets (DMA).

— Regulation (EU) 2022/2065, on Digital Services.

The normative framework is further supported by previously adopted regulations, which provide the foundation necessary for these new measures to take effect. In the realm of private-sector relationship, notable regulations include:

— Regulation 2016/679, the General Data Protection Regulation (GDPR).

— Regulation (EU) 2018/1807 on the free flow of non-personal data.

— Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (or Platform 2 Business, P2B Regulation).

This intense regulatory activity is based on the fact that the development of the data market has come to a halt due to a lack of trust among relevant undertakings, given the existence of contradictory economic incentives, and the presence of technological barriers preventing the enjoyment of the potential of data-based innovation. To address these issues, the goal is to provide a regulatory framework that enables and promotes

data reuse while strengthening Europe's data economy, observing both data protection regulations as well as European values.[3]

The proper configuration of an operational data market must have an impact on the channeling of greater data flows among economic agents, as well as on the promotion of fair and equitable conditions in exchanges. This requires addressing relationships among the various stakeholders in the market, whether they are business-to-business (B2B), business-to-government (B2G), government-to-business (G2B), or government-to-government (G2G), and with a scope that encompasses all economic sectors.

3. Identification of the Main Failures in the Business-to-Business (B2B) Data Market

At the economic level, extracting commercial value from data relies on achieving economies of scale and scope, which require data acquisition, analysis, combination, and processing. On the one hand, the larger the set of accessible data, the more users will be reached, offering them products or services of their interest (economies of scale). On the other hand, the re-use of data and the control of diversified sources allows to increase benefits based on the combination of data relative to diverse parameters and which complement each other (economies of scope). An attempt to maximize utility following this logic would ideally lead to the articulation of a robust data market in which companies exchange and share their data, as well as to the creation of consortia or pools[4] where companies share the data they have generated.

However, practice reveals that there are significant obstacles hindering the development of this market. The social utility of data exceeds its private value if it remains under the exclusive control of the company that controls it, does not share it, and/or implements measures to retain it As there are no incentives to overcome these challenges through contracts, it will be necessary to address them by regulating data exchanges and by applying antitrust law to any data-related practices that may result in abuses or illegal agreements. The purpose is not to develop a data market or to promote transactions, but to attain the highest social welfare derived from the combination and sharing of data, avoiding its underutilization (Martens *et al*., 2020, p. 5).

[3] Explanatory Memorandum for the Proposal of Data Act Regulation.

[4] On these, *see* Lundqvist (2018a, pp. 146-154) and Olmedo (2023b; 2023c).

We will identify several market failures that prevent optimizing the utility derived from data.

3.1. Failures Arising from Market Dominance and Data Hoarding by Large Platforms

The capacity of a company to obtain, process, and use data depends to a large extent on its market position. In that regard, larger companies and dominant platforms can access and accumulate vast amounts of data beyond the reach of their competitors. The maximum expression of this market power are digital giants such as Google, Meta, Amazon, Apple, or Microsoft, which constantly obtain huge volumes of data from the combination of multiple businesses. These companies' capacity to obtain data cannot be replicated by their actual or potential competitors. In addition, the power and market presence of these companies that enable these companies to amass such vast amounts of data create a reinforcing cycle: the more data, the more power, which in turn allows to develop mechanisms to capture a higher amount of data. The strategy of these companies is often based on exploiting data that they control for multiple purposes, extending their activity to adjacent markets in which they were not originally present, leveraging their control over data (market leverage). The market power derived from their data resources allows them to break into such markets displacing—and even excluding—pre-existing companies.

Given this market dominance and data-capturing advantage, these companies will not have any incentives to share their data with others, to the extent that the marginal profit they may obtain from the data generated by smaller companies is limited as compared to the benefit of keeping the exclusive control over their own data. In fact, when digital giants are interested in the data generated by a smaller company (due to their specificity, the parameters considered, etc.), it is usually the case that they purchase those companies, absorbing the data generated and coming to control their sources (*data killer acquisitions*). To overcome these problems derived from market dominance, measures have to be promoted to facilitate access to such data, but which at the same time keep the incentives for business investment, allowing the companies which have developed mechanisms for gathering these data to monetize the investment made.

The opposite would introduce negative incentives in the market, discouraging innovation in the sector.

The companies generating data will adopt a decision whether to share them or not analyzing the benefits and costs they expect to get from that sharing. A primary cost consideration is the potential loss of competitiveness resulting from data sharing. The basic market failure in this context appears when the value data may have for the economy as a whole is below its private value for the controlling company. This creates

a data underutilization risk, when comparing the actual use of the data with the potential use maximizing social welfare.

But, at the same time, solution design must also account for incentives. Thus, if data were freely available to the public, incentives to invest in obtaining data will disappear (free-rider problem). This dynamic creates a delicate balance: encouraging data sharing to unlock broader economic value while maintaining the proprietary incentives that drive data generation and innovation.

3.2. Monopolistic Positions in Data Collection

Certain types of data, due to their own features, are only collected by a single company, which thereby acquires a monopolistic position over them. The data collected by these companies lacks direct substitutes, resulting in monopolistic power. As an example, this happens when a company controls a relevant source of data, such as Internet-of-Things (IoT) devices or a widely used operating system (such as iOS for Apple mobile devices or Android for the rest). These companies may also use practices to direct users to use other digital services provided by them or by companies under their control. As an example, this happens when Chrome is the default browser on Android devices or when Internet searches are channeled on Google.

The companies controlling that non-replicable data will be more or less inclined to allow reuse by other actors depending on the intended use. If data is to be reused in a secondary market, we will have to consider whether this secondary use competes with the primary use (i.e., the original company's use of the data). If there is a competition relationship between the two, the data-controlling company will try to block and prevent its use. If the secondary use is not competitive, the company controlling the data may be interested in sharing it (typically in exchange for compensation). Even in the cases in which the dominant company is willing to share data, it may impose anticompetitive conditions, such as setting high prices (monopoly rents) or applying discriminatory pricing to maximize its profit (Martens *et al.*, 2020).

3.3. Transaction Costs

Excepting the cases in which a dominant company gets hold of certain data and excludes their rivals, obstacles persist for companies with an interest in sharing or exchanging with others any data they create. The first of those obstacles has to do with the transaction costs to be incurred to complete the exchanges.

The first component of these costs is relative to the identification of an adequate counterparty, i.e., knowing what company or companies may be generating the data which is relevant to the other party, as well as knowing in general terms what those data are. It is evident that any progress made in this space taking the positions of potential contracting parties closer will have to observe data protection rules.

A second component of the transaction cost is determining an adequate compensation for data. Data exchange can be entirely bilateral and reciprocal (*do ut des*), so that each party compensates others for the access to data by means of granting access to their own data. But this can also be done for a price, so that to access the data generated by a company a compensation must be paid. In this case, the rules which aim to solve market failures stipulate that exchanges should be based on FRAND (fair, reasonable, and non-discriminatory) terms. Finally, in certain cases regulations foster an open or free use of certain types of data, with the purpose of promoting the development of specific markets (as could be the case of data on health care, traffic, etc.).

Legal costs also impact data transactions, as any exchange or business involving data must observe rules on data protection. In that vein, businesses interested in exchanging data will have to adopt specific measures to avoid any data breaches, as well as to face liability in the event that some of the data exchanged have been obtained in violation of the regulations.

As will be analyzed below, one of the most effective ways of overcoming these transaction costs is through data exchange intermediation.

3.4. Technical Obstacles

Data sharing ultimately faces technical problems. And the case is that in many instances the standards and formats used by businesses to code their data do not match those used by other businesses. This makes interoperability and data portability difficult to a large extent, as it prevents that a smooth transfer of data controlled by a business be made so that they be used without impairment and obstacles by others, and so that they may combine those data with their own. To overcome these obstacles, coding standards need to be fixed which allow for the interoperability among the data of most businesses, whether by regulations or by industry self-regulation. The intervention of third parties specializing in portability as intermediaries in data transfers may also be an adequate way to overcome these technical obstacles.

4. European Union Regulation for the Creation of an Effective Data Market

4.1. Objectives to Be Promoted by Regulation

Overcoming these market failures requires adopting regulatory measures. In developing the European Data Strategy, multiple regulations have been adopted to overcome those market failures, promoting a legal framework which is adequate for data exchanges and innovation in the digital space. Such regulation also adopts as a guide the need to promote actual competition among companies, preventing the platforms which occupy—virtually incontestable—positions of super domination in the market from abusing those positions and promoting that rivaling companies may enter the markets these giants dominate.

To frame the European data market, different purposes are sought, including the promotion of possibilities to access higher volumes of data and to combine them to develop better products and services. Likewise, the purpose is to avoid that the digital giants hoard huge volumes of data and use that position of prevalence to exclude from the market any rivals who cannot access the data. To establish a proper competition framework, different ways are recognized so that digital companies which are not considered gatekeepers may access data monopolistically generated by the businesses controlling relevant sources of data or by the gatekeepers. From the substantive point of view, the regulation aims at adopting standards as to data coding and transmission to facilitate interoperability and data portability. Finally, it is about creating European common data spaces in certain economic sectors which are particularly sensitive, so that we can benefit from the usefulness of certain types of data in particular.

In this sense, European regulation covers several levels and its instruments are aimed at several groups. We find regulations especially aimed at digital giants which are defined as gatekeepers due to their offering of core platform services which are a relevant door to access the market. Also, a general regulation governing data exchanges is contained in the Data Act and the Data Governance Act. There is also, ultimately, influence over the control of the conditions established in the contractual relationships among businesses in the digital space, bearing in mind the unbalanced bargaining-power and dependence relationships among them.

4.2. Controlling the Giants: Gatekeepers' Obligations under the DMA

The Digital Markets Act has become the cornerstone of the new regulatory framework in which digital companies operate. Its purpose is to address the virtually incontestable

situation of market domination by the digital giants which are typically known as *gatekeepers.*[5] For that purpose, the Act subjects these platforms to a series of restrictions and duties with the aim of opening such digital markets to competition, overcoming the market failure of incontestable domination positions and lifting insurmountable barriers of entry

[5] The key element in the imposition of duties and restrictions under the DMA is the qualification of an operator as a gatekeeper. The rules have been designed thinking of the digital giants which have more market power (and which may be identified with the so-called GAFAM), but cannot be limited to them. So to offer a definition based on objective criteria, article 3 of the DMA proposal establishes three open and cumulative criteria to be met by the platforms:

(a) That they have a significant repercussion in the domestic market.
(b) That they operate a basic platform service which is an important access door so that business users become end users.
(c) And that they have an entrenched and durable position in their operations or that it be foreseeable that they reach such a position in the near future.

To facilitate the application of this regulation and the assessment over whether these three criteria are met, the presumption is established that the requirements are met when certain thresholds are exceeded. In such a way it is understood that a platform has a significant presence in the market when the company obtains an annual business volume in the European Economic Space equal to or higher than 6.5 billion euros in the last three fiscal years or when its median stock capitalization or equivalent fair market value exceeds 65 billion euros in the latest fiscal year and develops its activity in at least three member States. The requirement of operating a service which is a major access door to reach end users is considered met when the company has more than 45 million end users and more than 10,000 business active users in the Union in the latest fiscal year. Finally, it is considered that an entrenched and durable position, whether actual or potential, is reached in their operations when that number of end and business users is exceeded in each of the latest three fiscal years. Even if the mere overcoming of these thresholds imposes on the platforms the duty to communicate this situation to the Commission, the presumption admits evidence to the contrary. The company operating one or more core platform services overcoming these thresholds may justify before the Commission that it does not meet the requirements under article 3.1 DMA (significant impact on the internal market, being a core gateway for business users to reach end users, and enjoying an entrenched and durable position, now or in the future). For that purpose, the Commission should be presented with sufficient grounds which, in any case, may be discarded by the Commission when it considers that the requirements are met for the company to be considered a gatekeeper.

There are two ways in which a platform may be qualified as a gatekeeper. The first of them takes place at the request of the very company operating the platform—when the company exceeds the quantitative thresholds mentioned, it will communicate that circumstance to the Commission. In such a case, if no sufficient grounds are provided that the company is not a gatekeeper, the platform will be considered a gatekeeper and will be bound as from that moment by the duties and restrictions under the DMA, including the Commission in the list of companies providing core platform services as gatekeepers. The second way takes place at the request of the Commission, which may qualify as gatekeepers those companies which operate core platform services and which it believes should deserve that qualification. For that purpose, it will weigh in multiple criteria, including specifically the platform size, the number of (business and end) users which depend on the platform, the existence of market-entry barriers basically based on the network effects caused and data domination, enjoying important scale and scope effect, the captivity of platform users, or other structural market features.

for actual or potential competitors.[6] In its development, imposing duties and restrictions on the companies designated as gatekeepers, the Act aims at promoting fairness in the operation of these markets as well as their contestability (Krämer and Schnurr, 2021; Schweitzer, 2021).

Though originally projected as a new competition tool, the Digital Markets Act is a regulatory measure, aimed at addressing the market failure of excessive power concentration by major platforms and, therefore, directly imposing a series of obligations and prohibitions on gatekeepers. Unlike antitrust laws, it does not prohibit certain behaviors only to later impose remedies and penalties upon verification of their anti-competitive effects. The Act applies *ex ante*, designating gatekeepers and subjecting them to these duties and prohibitions. Non-compliance with these obligations leads to a sanctioning regime, without the need to demonstrate the actual competitive harm caused by the infringing conduct on the market's competitive dynamics.[7]

On September 6, 2023, following the applications submitted by the platforms, the European Commission adopted the first gatekeepers designation decision under the DMA. It identified Alphabet, Amazon, Apple, Bytedance, Meta, and Microsoft as gatekeepers in certain core platform services[8] for the purposes of the DMA and they are, therefore, bound to observe the duties and restrictions established in the regulation. In addition, four market research initiatives have begun to analyze the possibility of excluding 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 operating system iPadOS) even if the thresholds are not met. Instead, the Commission has

[6] It is not the purpose of this article to analyze in detail the regulation, on which there is already in-depth literature. I have referred to it in other studies (Olmedo, 2022; Olmedo, 2023a). In the literature, *see* the detailed analysis developed by Podszun (Podszun, 2024) and Ruiz Peris (2021a; 2021b).

[7] DMA article 29 provides that after starting specific procedures to verify the non-compliance, the Commission will adopt a non-compliance decision when it is verified that an obligation or prohibition have not been complied with. That decision will instruct the gatekeeper to cease and desist with the non-compliance and to provide explanations on how it plans to comply with that decision. In addition, when the non-compliance is verified, the Commission may impose on the gatekeeper sanctions which will not exceed 10% of its total worldwide turnover in the preceding financial year, an amount which may increase up to 20% in the event of recidivism within eight years (article 30, DMA).

[8] In particular, the core platform services affected are the following:

- Social media: TikTok, Facebook, Instagram, and LinkedIn.
- Intermediation: Google Maps, Google Play, Google Shopping, Amazon Marketplace, App Store, Meta Marketplace.
- Advertising: Google, Amazon, Meta.
- Interpersonal communication services regardless of numbering: WhatsApp and Messenger.
- Video sharing: YouTube.
- Search engine: Google Search.
- Web browser: Chrome and Safari.
- Operating system: Google Android, iOS, and Windows PC OS.

decided to exclude the services of Gmail, Outlook.com, and Samsung Internet Browser from being considered core platform services, even if the exceed the thresholds.[9]

Articles 5 and 6 of the DMA establish the obligations and prohibitions to which gatekeepers are bound.[10] For the purposes of these pages, I will only mention that the requirements imposed on platforms designated as gatekeepers expressly include some obligations and prohibitions which are directly related to data control, to wit:

- Not to process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper (article 5.2(a), DMA).
- Not to combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services (art. 5.2(b), DMA).
- Not to cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa (article 5.2(c), DMA).
- Not to sign in end users to other services of the gatekeeper in order to combine personal data (article 5.2(d), DMA).
- Obligation to share data with advertisers and publishers, with the obligation to provide each advertiser or publisher providing online advertising services (or authorized third parties) daily and free information on each advertisement, regarding: (a) the price and fees paid by that advertiser, (b) the remuneration received by the publisher, subject to the publisher's consent; and (c) the metrics on which each of the prices, fees and remunerations are calculated (article 5.9 and 10, DMA).
- Prohibition against using, in competition with business users, any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users (article 6.2, DMA).
- Obligation to provide advertisers and publishers (or any third parties authorized by them) free of charge with access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory (article 6.8, DMA).

[9] As a result, so far, Samsung is escaping its designation as a gatekeeper under the DMA.

[10] Article 5 details a series of pure or unconditional obligations, while article 6 is about obligations "for gatekeepers susceptible of being further specified" by the Commission.

— Obligation to allow end users and third parties authorized by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service (article 6.9, DMA).

— Obligation to provide business users and third parties authorized by a business user, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, which are provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services. With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent (article 6.10, DMA).

— Obligation to provide to any third-party undertaking providing online search engines with access on fair, reasonable and non-discriminatory (FRAND) terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click, and view data that constitutes personal data shall be anonymized (article 6.11, DMA).

Imposing these duties and restrictions on gatekeepers performs a twofold function. From a negative point of view, it aims at curbing the increase in market power of these companies resulting from data combination and concentration (Vezzoso, 2021, p. 400). From a positive point of view, strengthened portability duties are introduced and data access rights are recognized with the purpose of allowing potential rivals to participate in those rights as a requirement to compete against digital giants.[11]

4.3. Designing a Competitive Market in the Data Act

As explained above, the Data Governance Act and, especially, the Data Act are the ways of implementing the European Data Strategy to create an agile market in that respect. The Data Act is aimed at offering the normative basis for businesses not designated as gatekeepers to access any data created by devices, platforms, applications, and software based on the use by their users (Lundqvist, 2023, p. 102). As will be demonstrated, this is one of the main sources of big data nowadays and they are controlled mostly by

[11] As will be seen in the following section, the obligations imposed on gatekeepers in this regard are stricter than what—in a general manner—is established in the Data Act.

gatekeepers. Data generation results directly from these products or devices (including those connected to the Internet of Things or virtual assistants) or they are generated from related services. These related services have to do with every digital service (including software) incorporated into a product or interconnected with software in a way that its absence would prevent the product from performing any of its features. As these products and devices create a large number of data which is essential to compete in this or in secondary markets, measures must be adopted that allow access to them.[12] For that purpose, the regulation makes these data available to its addressees, allowing them to be also accessed by public agencies to attain public purposes when that is required (for example, due to public-interest reasons).

Data is made available by imposing a series of portability obligations and rights aimed at the target companies to access such data in fair, reasonable, non-discriminatory, and transparent terms (which we will call FRAND+ terms). Also, measures are included to promote the re-utilization of the data generated by the public sector, with the purpose of fostering innovation and the development of new products and services.

This normative framework has to be made consistent with the regulation on the protection and privacy of data and their safety, fostering the creation of a framework of trust for the use and transmission of data.

While useful to correct perceived market failures, these measures are not definitive. An actual data market must mature so that data exchange and shared use is promoted. For that purpose, an appropriate regime is needed for the execution of contracts between businesses and the creation of data pools as large (private or public) repositories allowing for the exchange and combination of data.

4.3.1. Portability Duties and Access Rights

The first way to create a competitive market over data is making it easier for the multiple market agents to access data. This access may be granted before the facts, by means of regulation or it may be imposed after the facts, as competition remedies in light of antitrust violations committed by companies with control over data. We will now focus on state intervention imposing measures and granting rights to facilitate the access to data.

The General Data Protection Regulation, as a general regulation in the subject matter, only regulated portability rights in its article 20, recognizing that data subjects had the inalienable right to demand from the data processor the delivery of their data or their transfer to a third party. But such regulation was not promoting third parties to actually exercise that right, promoting the circulation of data.

[12] For a deeper analysis of the purposes and measures in the regulation, *see* Podszun and Offergeld (2022).

That purpose is addressed by the Data Act, whose scope covers business-to-consumer (B2C) and business-to-business (B2B) data exchanges. With that purpose in mind, an obligation is imposed on the manufacturers and designers of related products and services to design any such products and services in a way that allows users to easily access any data resulting from their use, as well as to exercise their right to portability in favor of another company (Picht, 2022).

That is attained, first, by imposing reporting obligations before the end user acquires the product or subscribes to the related service. Afterwards, users are recognized the right to access and use the data generated as a result of these related products or services. And, more importantly from a practical point of view, users are recognized the right to share these data with third parties, allowing the user to transfer them to another user, whether an individual or a business, immediately and free of charge. These third parties undertake to make a fair use of the data received from users, which means processing the data only for the purposes and conditions agreed upon and subject to a series of restrictions.[13] In particular, the party receiving the data shall not:

(a) coerce, deceive, or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user;

(b) use the data it receives for the profiling of natural persons, unless it is necessary to provide the service requested by the user;

(c) make the data it receives available to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;

(d) make the data it receives available to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to the DMA;

(e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose;

(f) prevent the user, including through contractual commitments, from making the data it receives available to other parties.

The Data Act faces, however, significant limitations, as it only covers those personal data which have been directly delivered by the users or observed in their behavior, i.e.,

[13] Under article 6 of the Data Act, they shall process any data made available to them only for the purposes and conditions agreed on with the users.

there is no coverage of the data inferred or derived from the data processing which are not subject to the portability right. Likewise, the actual implementation of the regulation meets major technical obstacles, as it is necessary to standardize the manner in which data are transmitted among businesses in the exercise of those rights and obligations.

The rules in the Data Act must be read together with the DMA, particularly as to the obligations of the platforms designated as gatekeepers to allow the actual portability of the data generated.[14] In addition, the platforms which are designated as gatekeepers cannot benefit from the portability right included in the Data Act, and third parties are not eligible for the transference of data established in the regulation.[15] This prevents platforms from promoting or commercially fostering that a user in any way puts at their disposal the data obtained in the exercise of a user's right to access and portability; from promoting or commercially fostering that a user asks the data owner to make the data available for one of their services; or from receiving any data that a user may have obtained before in the exercise of those rights.

As a general matter, access to such data shall not be free of charge. Given that the collection and initial processing of data demands large investments, the data owner will be entitled to reasonable compensation for making the data available. When determining the amount of such reasonable compensation, a limitation is established when the target is a medium-sized, small or micro enterprise, as in such cases the compensation shall not exceed the costs directly related with making the data available.

4.3.2. The Creation of Common Data Spaces

Imposing portability obligations and rights is not the only way in which data exchanges can be promoted. This purpose may also be reached by intermediating in common data spaces. These are third-party intermediaries—whether public, private, or community in nature—connecting the users interested in data and, by applying the technology, they organize the market, promoting that transactions on data may be carried out, overcoming any market failures existing in each industry. Basically, their contribution will focus on reducing transaction costs, as well as on the mitigation of risks that the transfer of data may entail (as to data protection, secret disclosure, etc.). These intermediaries may contribute to self-regulation among the agents involved, promoting the adoption of standards and technological interoperability.

[14] This portability obligation has to do with any data generated by the end user and is not limited to portability as considered by the General Data Protection Regulation, which deals exclusively with personal data. On this point, *see* Vezzoso (2021, p. 400).

[15] Article 5.2 of the Data Act establishes that "Any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper [under the DMA] shall not be an eligible third party."

The Data Governance Act passed in May 2022 is aimed at creating the appropriate legal framework to promote data access and exchange in the European Union. For that, the purpose is to establish measures fostering the exchange of data among companies, organizations, and public authorities, promoting the collaboration among these agents.

With this purpose, conditions are fixed to reuse certain categories of data produced by public agencies, a framework is established for notification and supervision of providers devoted to data intermediation, a framework is created with voluntary registration in a registry for entities collecting and processing data assigned with altruist purposes and the bases are laid for the creation of a European Innovation Committee on Data.

As to private business-to-business relationships, the most interesting point of the regulation is, precisely, the creation of a notification and supervision framework to provide data intermediation services,[16] with the purpose of giving legal certainty and a regulatory framework for the entities whose purpose is to connect data owners with their addressees who may be interested, promoting the creation of data spaces, data pools, or data cooperative services. This is how the creation of data marketplaces and the intervention of data brokers are promoted.

The providers of data intermediation services shall not use the data for purposes other than making them available to end users. To avoid the imposition of abusive commercial practices, tying clauses are not allowed, as the regulation requires that commercial contractual conditions, including those relative to prices, for the provision of data intermediation services to a data holder or a data user shall not depend on the fact that the holder or user uses other services provided by the same intermediation service provider or a related entity.

In addition, in providing intermediation services obligations are created as to confidentiality, data interoperability—guaranteeing that they are not in a format that is easily exportable

[16] These are defined (article 2.11 of Regulation EU 2022/868) as follows: "a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:

(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;
(b) services that focus on the intermediation of copyright-protected content;
(c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;
(d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships."

and usable by multiple addressees—, and the provision of service in fair, transparent, and non-discriminatory terms.[17]

4.3.3. Control of Fairness in B2B and P2B Data Exchanges

A. Control Instruments in the Data Act

The Data Act also introduces some measures to promote fairness in data exchanges among businesses, avoiding unfair practices or preventing that the dependence situation that some of them may experience be exploited. As in many cases there are instances of power imbalance in data exchanges, the Act introduces measures to avoid that companies with higher bargaining power use such power to impose unfair conditions against other weaker companies that depend on them.

For that purpose, there is a list of contractual clauses which are understood to be abusive when they have been unilaterally imposed on medium-sized, small, or micro enterprises. The scope of this provision is reduced, as it only protects smaller companies. If the situations of bargaining-power imbalance occurred affecting larger companies (large company versus digital platform which is a gatekeeper, for example), control for abuse would be subject to the general regulation of unfair commercial practices, as well as—if applicable—to the Platform 2 Business Regulation, which I will discuss in the next section.

Just like with the Spanish Unfair Competition Act[18] after the transposition of Directive 2005/29/CE[19], the Data Act is based on a general restricting clause which considers abusive any contractual clause which, due to its nature, entails that its application deviates from good business practices in terms of data access and its use in violation of the principles of good faith and fair trade. Then, a double list of black clauses[20]—clauses which will always be considered abusive—and gray clauses[21]—clauses which are presumed to be abusive except evidence to the contrary—is introduced.

[17] *See* article 12, Data Governance Act.

[18] Article 4.

[19] Especially article 5.

[20] 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.

[21] 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

B. Fairness Control in the P2B Regulation

If we consider the relative position of the companies which interact at the digital level, it will be seen that there is a significant situation of financial dependence among companies providing products or services (whether digital or not) and the platforms distributing them massively in the digital sector. These relationships between platforms and businesspersons requiring their intermediation (*Platform to Business*, P2B) demand a special regulation supplementing the specific obligations contained in the Digital Market Act for the gatekeepers (as not all platforms will be considered as such) and the Data Act (Graux *et al.*, 2022). This regulation, also, supplements the protection mechanisms in the regulation on unfair competition, whether at the community or national levels, generally or specifically for certain industries.

All in all, the objective scope of this Regulation is wider than mere data practices. Its purpose is to ensure transparency, fairness, and the possibilities to claim in commercial relationships among business users requiring the online intermediation services provided by intermediation platforms for the development of their activities, as well as the users of corporate web pages as to online search engines (which would also act as intermediary platforms).[22]

These platforms' pillar to act is the imposition of transparency and information obligations in the general terms that the intermediary platforms impose on their business users. Considering the relationship of financial dependence in this environment (Estevan, 2022, pp. 57-80), special rules are detailed for the restriction, suspension, and termination of commercial relationships, so that platforms have to notify their intent to walk away from relationships with adequate advance notice and always for cause. The regulation is completed with a regulation of the way in which business users are classified in search

party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;

(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.

[22] An express exclusion from its scope of application are online payment services, online advertising tools, and online advertising exchange platforms, which are not aimed at facilitating the beginning of direct transaction or to enter into contractual relations with consumers.

results,[23] stating the general terms of the parameters to be used for priority and the reasons for choosing and prioritizing them.

There are also specific rules for the differentiated treatment of own products or services,[24] which is much more limited (due to obvious reasons) than the one imposed by the Digital Market Act on gatekeepers. This way, the non-gatekeeper providers of intermediation services will simply have to describe in their general terms the differentiated treatment they may give to their own products or services or to those of other business users, only justifying which are the financial, commercial, or legal reasons for that differentiated treatment. In the frequent case that the intermediary be designated as a gatekeeper—the case of Amazon, Google or, if designated as such, non-GAFAM intermediary platforms such as Booking.com—those obligations shall apply in addition to those in the DMA, such as the prohibition against self-preferencing.[25]

The specific rules governing contractual agreements between platforms and business users are of special interest for these reflections in connection with the data generated with the use of the platform or search engine.[26] The P2B Regulation imposes on the platform or search engine a duty to communicate in their general terms a description of the technical and contractual access they have of personal or other data provided by business users or consumers in using the services provided, identifying in a specific manner certain aspects on which advertising will be made (treatment of personal data, definition of which data derived from the use of the platform can be accessed, etc.).[27]

[23] *See* article 5, P2B Regulations.

[24] *See* article 7, P2B Regulations.

[25] Article 6.5, DMA: "The gatekeeper shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking."

[26] *See* article 9, P2B Regulation.

[27] In particular, under article 9(2), the providers of intermediation services shall inform users on:

(a) whether the provider of online intermediation services has access to personal data or other data, or both, which business users or consumers provide for the use of those services or which are generated through the provision of those services, and if so, to which categories of such data and under what conditions;

(b) whether a business user has access to personal data or other data, or both, provided by that business user in connection to the business user's use of the online intermediation services concerned or generated through the provision of those services to that business user and the consumers of the business user's goods or services, and if so, to which categories of such data and under what conditions;

(c) in addition to point (b), whether a business user has access to personal data or other data, or both, including in aggregated form, provided by or generated through the provision of the online intermediation services to all of the business users and consumers thereof, and if so, to which categories of such data and under what conditions; and

(d) whether any data under point (a) is provided to third parties, along with, where the provision of such data to third parties is not necessary for the proper functioning of the online intermediation services, information specifying the purpose of such data sharing, as well as possibilities for

The scope of this Regulation covers other specific contractual terms, a regulation of obligations of exclusivity, of establishing internal dispute settlement mechanisms, the submission to mediation of any conflicts between platforms and their business users, the filing of court actions by representative organizations or associations and public agencies and the preparation of conduct codes by the providers of online intermediation services.

4.3.4. Contractual Solution: Data Pool Intermediation

Like common data spaces, some of the failures in this market may be overcome thanks to the creation of data pools or consortiums. In this case, we are faced with forms of sharing B2B data among closed groups, unlike what happens with common data spaces, which are set as open-access platforms which can be accessed by any interested party to get and share data on a given industry.

A data pool contract is that whereby two or more parties (pool partners) agree to share their data in a consortium. Such sharing may be done by transferring one's own data to a means under the joint control of partners or of a third-party intermediary (trustee, escrowee, or administrator) acting on behalf of the partners; or, in a more decentralized manner, allowing each of the partners that the other may access certain data under their control, or giving them the possibility of exploiting certain data sources, with or without the intervention of a third party.[28]

In particular, to solve market failures and reduce risks derived from making data available, the pool's intermediation is used, so that each party preserves the same control over their primary data obtaining at the same time access to the data resulting from the pooling. Normally, this happens by means of industrial data platforms or data trusts acting in a neutral manner toward the participants.

For data exchanges to take place effectively, it is necessary to also eliminate technical obstacles, promoting the creation of standards and facilitating the creation of protocols assumed by the industry which allow for data mobility. For that purpose, the activity of intermediaries and of cloud and marginal data processing services becomes essential. The ultimate goal of the regulation in this regard is to eliminate the material obstacles which may hinder the effective exercise of this right to mobility.

These intermediaries also contribute to reducing transaction costs attached to the need to agree on the contractual terms of the exchange. This way, they facilitate that parties may reach agreements on the distribution of benefits derived from data sharing.

business users to opt out from that data sharing.

[28] European Commission, Joint Research Centre, 2023, pp. 59-61; ALI-ELI, *Principles for a Data Economy – Data Transactions and Data Rights*; the last draft was proposed by ELI in 2021.

Data intermediaries must determine a redistribution mechanism, managing the benefits and costs of creating the pool.

5. Preventing and Repressing Anticompetitive Practices in the Data Market with Antitrust Law

Antitrust law addresses problems in market operation after the conducts limiting, restricting, or falsifying competition have taken place. The same happens with the data market. Antitrust law will only apply in this industry when the companies which are active in the data market perform conducts which are an abuse of dominant position, enter into anticompetition agreements, or plan to develop concentration activities which result in a significant hindering of competition in the affected market. In the event of antitrust violations, the competition authority shall verify the existence, if any, of a prohibited conduct and shall impose sanctions and order remedies to dissuade that conduct and reestablish the competition situation altered. In the case of concentrations, the authority will make a prospective and counterfactual analysis of how the market would be after the transaction projected and communicated takes place. Based on the results of such study, the antitrust authority will decide whether to authorize or not the execution of concentration.

As can be seen, the intervention of antitrust authorities after the fact in light of violations may not always be appropriate. That is because the authority only acts when the violation has been committed and, therefore, the damage to the market has already been caused. In particularly dynamic markets such as digital markets, anticompetition conducts or agreements are particularly harmful and may give rise to situations which, once completed, cannot be reverted. As to data specifically, these conducts may give rise to abusive hoarding practices used to strengthen—even more—the dominant position of companies, giving them an uncontested position. Therefore, in the most serious cases, an appropriate regulation of the market will be proper, whether general (as is the case of the Data Act or the P2B Regulation) or specific in nature for the platforms considered gatekeepers (as is the case of the Digital Markets Act).

All in all, these ways of acting—regulation and competition—do not exclude each other; instead, they supplement each other. Even if regulatory measures are adopted to try to solve some of the most serious failures in the data market, antitrust law will have to continue going after any corporate practices restricting competition in this regard. Those conducts include the fixation of monopolistic prices to grant access to the data or price discrimination practices. Likewise, specific control must be made of vertical concentration transactions with the purpose of introducing a second market related to data within the corporate structure of the purchaser. Killer acquisitions are of special interest in this regard.

Some authors have said that not granting access to data may be understood as a conduct of abuse of dominant position by exclusion and, therefore, be within the scope of application of the prohibition under article 102, TFEU. However, for that qualification to be possible—applying the doctrine of essential facilities (Graef, 2016; Colangelo and Maggiolino, 2017)—it is necessary that data be considered essential, to the extent that it is materially or financially impossible in another manner to obtain them and that they are essential to compete in the secondary market (other than that in which they are marketed). As these conditions are not met in a general way,[29] it will be extremely complex to apply this prohibition to the refusal to license data itself. In addition, doing so may disincentive companies' investments in new ways of obtaining data from which they derive value for their business.

Another problem posed by the application of antitrust law to solve some of the failures in the data market is the design of appropriate remedies, i.e., the delimitation of measures that may be imposed on violating companies to overcome the competition problems generated as a result of their conducts. In that regard, the applicable regulations[30] establish that remedies imposed against violators must be necessary and proportionate to the relevant ends. In light of violations made in the data market, in many cases it will be very complex to design adequate and proportionate measures to put an end to the violation and restore competition conditions. Because of that, it is especially appropriate to resort to measures such as fragmentation of data which may be accessed by the companies, by means of erecting Chinese walls or the creation of data silos, preventing dominant companies from combining data stemming from different sources. Likewise, depending on the cases, access remedies may be adequate, offering the interested companies and competitors in the market access to certain data sources to eliminate the competitive advantage.[31]

[29] It should be remembered that data are a non-rivalrous, non-appropriable, and generally accessible resource.

[30] At the community level, article 7 of Regulation (EC) No. 1/2003, of 16 December 2002, on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty provides that the Commission may impose on businesses "any behavioural or structural remedies which are proportionate to the infringement committed and necessary to bring the infringement effectively to an end. Structural remedies can only be imposed either where there is no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the undertaking concerned than the structural remedy." At the level of Spanish domestic legislation, article 53.2(b) of Law No. 15/2007, of July 3, on Antitrust, establishes that the resolutions of the Council of the National Commission of Markets and Competition on violations may contain "the imposition of determined conditions or obligations, whether structural or behavioral. In the option between structural or behavioral problems of equivalent effectiveness, the option will be the one which is less harmful for the company in question."

[31] Scholars offer multiple proposals which are extremely interesting to overcome competition problems in digital markets, *see* (Gal and Petit, 2021; Lancieri and Pereira, 2021).

However, the design of remedies is directly faced with the problems of determining their need and proportionality. Likewise, in many cases these remedies will entail structural measures (release of essential assets, fragmentation of companies or business branches…). Such measures do not fit easily within the current regulatory framework of Regulation 1/2003.

The design and control with the observance of these access remedies is very complex. Therefore, in many cases it is believed that the most appropriate solution is to address the issue from a regulatory and data governance perspective. That approach means choosing a regulation before the facts instead of imposing measures in antitrust files.

Another way which has been explored is by means of what has come to be known as *experimentalist antitrust*. It entails that the businesses which have violated antitrust regulations try to reach a conventional termination with the authority, proposing measures—commitments—to overcome the competition issues which cropped up. In some cases, the use of these measures may be appropriate. As an example, we may mention the case heard by the Italian *Autoritá Garante della Concorrenza e del Mercato* against Google for the imposition of obstacles to data portability. By means of the commitments offered to *Weople,* measures are implemented to overcome the technical obstacles derived from data portability, promoting the action of third-party intermediaries who contribute to portability effectiveness connecting data export and import formats.

About the article

Notes on conflict of interest. The author declares not to have any conflict of interest as to the publication of this article.

Contribution in the article. The author assumed all the roles established in *Contributor Roles Taxonomy* (CRediT).

Funding. This publication is part of the project *Legal framework for dynamic competition in digital markets and for innovation by means of Artificial Intelligence* (CODIG-IA), ref. PID2021-122536OB-I00 (Eugenio Olmedo Peralta, PI), funded by MCIN/ AEI/10.13039/501100011033 and by the European Union "NextGenerationEU"/PRTR; as well as of the project *Consumers and small professionals in contracts in Digital Markets: anticompetition and unfair practices and exploitation of financial dependence* (CoMeDi), Ref. ProyExcel_00665. Excellence Projects, Program of Assistance to I+D+i, on competitive concurrence, Andalusian Plan of Research, Development, and Innovation (PAIDI 2020) (PIs: Olmedo Peralta/Benavides Velasco).

References

Cattaneo, G., Micheletti, G., Glennon, M., La Croce, and C. Mitta, C. (2020). *The European Data Market Monitoring Tool*. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/72084

Cohen, N. and Wendehorst, C. (2021). *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights.* https://www.principlesforadataeconomy.org

Colangelo, G. and Maggiolino, M. (2017). Big Data as Misleading Facilities. *European Competition Journal, 13*(2-3), 249-281. https://dx.doi.org/10.2139/ssrn.2978465

European Commission (2017). *La construcción de una economía de los datos europea.* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM 9 final.

European Commission (2020). *Una Estrategia Europea de Datos.* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM 66 final.

Crémer, J., De Montjoye, Y., and Schweitzer, H. (2019). *Competition Policy for the Digital Era, Final Report for the European Commission*. Publications Office. https://data.europa.eu/doi/10.2763/407537

Estevan, C. (2022). Desequilibrios de poder en los mercados digitales: plataformas y dependencia. *Actas de Derecho Industrial y Derecho de Autor*, (42) 57-80. https://doi.org/10.2307/j.ctv37xg23w

Franck, J. and Peitz, M. (2019). *Market Definition and Market Power in the Platform Economy*. Centre on Regulation in Europe. https://cerre.eu/publications/market-definition-and-market-power-platform-economy/

Furman, J., Diane, C., Fletcher A., McAuley D., and Marsden, P. (2019). *Unlocking Digital Competition*. *Report of the Digital Competition Expert Panel*. HM Treasury. https://doi.org/10.17639/wjcs-jc14

Gal, M. and Petit, N. (2021), Radical Restorative Remedies for Digital Markets, *Berkeley Technology Law Journal, 37*(1) 617-674. https://ssrn.com/abstract=3687604

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

Graux, H. Somers, G. Van Camp, S., Morel, S., Herrera, F., Maridis, G., Di Giacomo, D., and Vassot, S. (2022). *Study on model contract terms and fairness control in data sharing and in cloud contracts on data access rights.* Publications Office of the European Union. https://data.europa.eu/doi/10.2838/174720

IDC and Open Evidence. (2017). European Data Market SMART 2013/0063.

Jean, S. Perrot, A., and Philippon, T. (2019). Competition and Trade: Which Policies for Europe? *Notes du conseil d'analyse économique, 51*(3), 1-12. https://shs.cairn.info/journal-notes-du-conseil-d-analyse-economique-2019-3-page-1?lang=en

Krämer, J. and Schnurr, D. (2021). Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies. *JCL&E, 18*(2), 255-322. https://dx.doi.org/10.2139/ssrn.3789510

Lancieri, F. and Pereira, C. (2021), Designing Remedies for Digital Markets: The Interplay Between Antitrust and Regulation. *Journal of Competition Law and Economics*, 613-669. https://dx.doi.org/10.2139/ssrn.3704763

Lundqvist, B. (2018a). Competition and Data Pools. *Journal of European Consumer and Market Law, 7*(4), 146-154. https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/7.4/EuCML2018031

Lundqvist, B. (2018b), Data Collaboration, Pooling and Hoarding under Competition Law. *Stockholm Faculty of Law Research Paper Series*, (61), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278578.

Lundqvist, B. (2023). *Regulating Access and Transfer of Data*. Cambridge UP.

Martens, B., De Streel, A., Graef, I., Tombal, T., and Duch, N. (2020). *Business-to-Business data sharing: An economic and legal analysis*. JRC Digital Economy Working Paper 2020-05. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf

Micheli, M., Farrell, E., Carballa, B., Posada, M., Signorelli, S., and Vespe, M. (2023). *Mapping the landscape of data intermediaries*. Publications Office of the European Union. https://doi.org/10.2760/8943

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

Olmedo, E. (2023a). La construcción de un régimen jurídico para el sector digital más allá del Reglamento de Mercados Digitales. In J. I. Ruiz Peris, F. González Castilla,

F. González and C. Estevan (Eds.), *Mercados digitales y competencia*. Tirant lo Blanch.

Olmedo, E. (2023b). Los contratos de pools de datos (data pools): Aproximación a su régimen jurídico y función económica. In L. Miranda and J. Pagador (Eds.), *Contratación mercantil: digitalización y protección del cliente/consumidor*. Marcial Pons.

Olmedo, E. (2023c). Colaboración en la generación, intercambio y procesamiento de datos (Big Data): entre la cooperación lícita y las conductas antitrust. In J. I. Ruiz Peris (Ed.) *Cooperación y Mercados Digitales*. Atelier.

Picht, P. (2022). Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law. *Max Planck Institute for Innovation and Competition Research Paper,* (22-12). https://dx.doi.org/10.2139/ssrn.4076842

Podszun, R. and Offergeld, P. (2022). The EU Data Act and the Access to Secondary Markets. *Study for the Ludwif-Fröhler-Institut für Handwerkswissenshaften.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4256882

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

Ruiz Peris, J.I. (2021a). Gatekeepers, discriminación autopreferente exclusionaria y reforzamiento de la posición de dominio: La nueva propuesta europea de Digital Markets Act. In J. Martí (Ed.), *Competencia en mercados digitales y sectores regulados*. Tirant lo Blanch.

Ruiz Peris, J. I. (2021b). La nueva Digital Markets Act, una respuesta híbrida de la Unión Europea a los gatekeepers GAFA. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, (57).

Schweitzer, H. (2021). The Art to Make Gatekeeper Positions Contestable and the Challenge to Know what is Fair: A Discussion of the Digital Markets Act Proposal. *Zeitschrift für Europäisches Privatrecht*, (3) 503-544. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3837341

Scott Morton, F., Bouvier, P., Ezrachi, A., Jullien, B., Katz, R., Kimmelman, G., Melamed A., Morgenstern, J. (2019). *Committee for the study of digital platforms: Market structure and antitrust subcommittee report*. Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business.

Vezzoso, S. (2021). The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU. *European Competition Journal, 17*(2), 391-406. https://dx.doi.org/10.2139/ssrn.3772724

Regulations

Law No. 3/1991, of January 10, of Unfair Competition.

Directive 2005/29/CE relative to unfair commercial practices of companies in their relationships with consumers.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Platform 2 Business, P2B Regulation).

Regulation (EU) 2022/868, of the European Parliament and of the Council, of 30 May 2022, on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act, DMA).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

Documents

Explanatory Memorandum to COM(2020)767 - European data governance (Data Governance Act). https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vle2l9jb8hw2

Cases

STJUE (Gran Sala) of 9 November 2004, in the matter of C-338/02, “Fixtures Marketing Ltd. v. Svenska Spel AB”.

STJUE (Gran Sala) of 9 November 2004, in the matters C-46/02, “Fixtures Marketing Ltd v. Oy Veikkaus AB”

STJUE (Gran Sala) of 9 November 2004, in the matters C-203/02, “British Horseracing Board Ltd v. William Hill”

STJUE (Gran Sala) of 9 November 2004, in the matters C-444/02, “Fixtures Marketing Ltd v. OPAP”.

Autoritá Garante della Concorrenza e del Mercato, provvedimento n. 30736, A552, of May 22, 2023, “Google-Ostacoli alla portabilità dei dati”.

Abbreviations

B2B:	Business-to-business.
B2G:	Business-to-government.
DMA:	Digital Markets Act.
FRAND:	Fair, reasonable and non-discriminatory.
G2B:	Government-to-business.
G2G:	government-to-government.
GDPR:	General Data Protection Regulation.
P2B:	Platform-to-business.
STJUE:	Sentencia del Tribunal de Justicia.