Journal of Law, Market & Innovation

ISSUE 1/2025

Journal of Law, Market & Innovation

1/2025

Editors: *Alberto Oddenino – Lorenza Mola – Cristina Poncibò – Riccardo de Caria*

Journal of Law, Market & Innovation
Vol. 4 - Issue 1 - 2025
ISSN 2785-7867
Journal of Law, Market & Innovation

TABLE OF CONTENTS

Foreword to Issue 1/2025 1

Special Section on trade law: Data Strategy & Trade Law

Isabella De Michelis, *INNOVATION LETTER: Monetization as a right: a new-legal economic under FRAND principles* 3

Olesia Shmarakova, *Data strategies and development of trade in data: three policy approaches* 8

Elisabetta Nunziante, *How the EU Data Strategy can foster the growth of Agri-Tech Market* 33

Richa Jain, *Big Data and Competition Law: Navigating Trade Practices in the Digital Age* 63

Arora Pallavi, Jyotsna Manohar, *Ex-Ante Competition Regulation of Digital Markets: Rethinking Regulatory Autonomy under the Gats non-discrimination obligation* 89

General Section

Behrang Kianzad, *Fairness, Digital Markets and Competition Law – Reconciling Fairness Norms in Digital Markets Act, Data Act and AI Act with Competition Law* 133

Alberto Oddenino – Lorenza Mola – Cristina Poncibò - Riccardo de Caria

FOREWORD TO ISSUE 1/2025

The present issue of the *Journal of Law Market & Innovation* covers some strategic topics raising from the interplay of data strategy and trade law. The theme stems from the acknowledgment of the expansion of the digital economy, driven by the extensive exchange, collection and mining of an ever-increasing volume of data, made available through the diffused and ubiquitous presence of technology.

This affects a very wide range of political, societal, economic and legal issues, and among them, global commerce, becoming both a driving force and a challenge for it.

The relationship between trade regulations and the field of big data becomes even more intricate if we consider it not only from the perspective of Data Strategies developed by different states but also from the perspective of transboundary data flow, in the prism of trade law and the related security exceptions. In this respect, the role of EU regulation and policy is pivotal and cannot be underestimated also in its dynamic with the rest of the world.

The conceptual territory covered by the issue is therefore very wide, as well as the potential practical dimension of relevance. It ranges from Digital Strategy and Trade Policy to Data Protection, from Big data in trade logistics and trade facilitation to Antitrust and Competition Law, from E-commerce and Digital Trade to Digital fairness for consumers, from Cybersecurity and Trade to protection of trade infrastructure through cybersecurity standards.

Against this backdrop, all the contributions of the special issue, though covering a wide spectrum, are inspired by the consideration of the international, supranational or transnational legal dimension and attain a considerable level of academic novelty. They build a consistent thread of analysis from general to particular and consist of a coherent proposition of the general topic.

The first contribution by Olesia Shmarakova develops a comparative analysis of the different data strategies along different European Jurisdictions, and in particular EU, UK and Russia. The topic of data governance and policy is indeed a strategic starting point which exerts a strong impact on digital markets and the policy options are related to the balance of interests of at least three categories of subjects, namely states, businesses and individuals.

The second contribution by Elisabetta Nunziante streamlines the issue of data governance in the European Data Strategy, as a factor securing data flows, reducing data

monopolies and fostering the development of new services. The original case study is that of data collected by agricultural technologies, whose secondary use can improve new services and support the green transition, by reducing carbon footprints, optimizing energy consumption and streamlining - among other things - supply chain, pesticides use and water consumption.

The third contribution by Richa Jain introduces the seminal topic of big data and competition law addressing it in a systemic dimension, stemming from the consideration that data accumulation, though a powerful tool for enhancing competitivity of businesses, entails relevant anti-competitive concerns.

The fourth contribution by Arora Pallavi and Jyotsna Manohar again focuses on competition laws, but from the perspective of enforcement. In light of the growing complexities of data-driven digital markets, traditional *ex-post* competition laws are considered as often insufficient, and this prompts many jurisdictions to adopt *ex-ante* regulatory frameworks. For this reason, the compatibility of *ex-ante* competition regulations, such as the European Union's Digital Markets Act (DMA), with the General Agreement on Trade in Services (GATS), is investigated, with a particular focus on the potential violation of national treatment and most-favoured-nation (MFN) obligations.

A.O., L.M., C.P., R.d.C.

Isabella De Michelis[*]

INNOVATION LETTER

MONETIZATION AS A RIGHT: A NEW-LEGAL ECONOMIC PARADIGM UNDER FRAND PRINCIPLES

Abstract

Data is vital to the modern worldwide economy functioning. Data is produced by people and by machines owned by people. Data gets collected and processed, hence used (exploited and monetized) by the industry in a proportion of 100% and above as data is an infinite resource which can be used and reused indefinitely. This property creates a disproportionate advantage for those which are equipped with advanced, integrated powerful processing capabilities, storage space and efficient algorithms to extract information from large dataset.

Against this background, this contribution explores the role that FRAND principle can play to address the information asymmetry arising between businesses and individuals in the gathering of data.

JEL CLASSIFICATION: K0, K11, K20

Data is vital to the modern worldwide economy functioning. Data is produced by people and by machines owned by people. Data gets collected and processed, hence used (exploited and monetized) by the industry in a proportion of 100% and above as data is an infinite resource which can be used and reused indefinitely. This property creates a disproportionate advantage for those which are equipped with advanced, integrated powerful processing capabilities, storage space and efficient algorithms to extract information from large dataset.

Personal data (data which is associated to an individual) is protected by specific laws and regulations almost everywhere in the world and in a stricter way in some regions and countries of the world (e.g. GDPR and privacy in the European Union but also data protection laws in India and privacy and consumer protection laws in California etc). In some regions of the world we also assist to efforts by governments to rule how data gets used by the market and some governments have decided to adopt specific market regulations to this end. In Europe, the Digital Market Act (DMA), the Digital Service Act (DSA), the Data Act (DA) and the Data Governance Act (DGA) entered all into force in the

[*] CEO and founder ERNIEAPP LTD.

 DOI 10.13135/2785-7867/11834

last 2 years. Other countries are gearing similar data market regulations under the view that a monopolistic concentration of data may harm competition, consumers and market proper functioning (e.g. United Kingdom, India etc).

With the rise of Artificial Intelligence (AI) also new sectorial regulation have been considered to apply to data collection, processing and reuse by companies and between companies, especially if personal data is at stake. The AI Act in Europe has paved the way to such an approach.

Since the beginning of Internet, companies have never paid people/users/consumers for their data. Companies do not consider data collected from individuals in need of being paid. Companies collect data (as first party) and or agree to source it from third party suppliers (e.g. data brokers) or exchange it directly like in a barter model with another company (business partners). In these transactions the end users are not participating nor made aware of the value at stake. End users are unlikely given any element of cost benefit analysis to appraise the value of their 'handed out' data. In economic terms users suffer from economic asymmetric information.

Generally speaking, the data assets that companies exploit and monetize is usually made of first party data, collected directly from the end users/customers from different touch points in the digital or physical world and/or second and or third-party data, sourced from third parties that can be partners and or suppliers. Companies have a proven tendency to dilute the data protection level when they exchange data at business-to-business level as they presume the 'personal data consumer protection' component is not at stake under a B2B relationships. This happens in particular for companies which operate business to businesses to consumers services (B2B2C).

End-users/consumers (data subjects as defined by EU GDPR) are not even aware of the rights they can assert under privacy regulation where privacy has been defined as a fundamental right. More notably, end-users are not conscious of the incremental value generated by their data sharing. They ignore the long value chain tail behind their interaction with the devices' screens they engage with 24/24 hrs. They also ignore the stiff competition that exists between companies in quest of good contextual first party data and racing to win user's attention and time to monetize it. Simply put: end users/consumers remain blind on the data economy functioning, their data protection rights, data monetization processes and more broadly how digital value is created, how data is used and exchanged, and which rules apply to the data economy between business stakeholders. They simply ignore that data is what fuels the gig economy wealth. For a very long time, the narrative put into the consumer space was that if the service is offered for free there is a balanced right from the service provider to monetize the data (this was the traditional argument for publishers and social media) but in reality also paid services monetize customer data in a very aggressive way and do not really make a big difference whether the service is paid or free. Spotify and Netflix are two platforms which offer paid services (with Spotify also offering a free service level). Both are also advertisement

platforms. Spotify in particular offers the profiled data extracted from their audience to Facebook which reuses it to target with ads their users. So, the assumption under which if the service is free the user is paying with data and if the service is paid the user is paying for it and he/she is not going to be monetized again through advertisement is a false myth. Companies harvest and monetize data in a continuum – individuals keep ignoring how that is managed and the value that is extracted. The information asymmetry suits well businesses.

If we are to think of web 3.0 and beyond and a full interconnected society, based on AI technology and services adoption, we must think of new models of digital value (wealth) creation and redistribution to include the excluded: end-users/consumers. Hence this redistribution of wealth shall be fair and proportionate as a modern democratic approach to digital. FRAND could be an interesting concept to explore in an evolved consumer-to-business relationship context where the information asymmetry would be balanced by enhanced digital rights management capability on the user's side.

It is a sign of democracy to design such a new model, whereby people do not get considered mere consumers to be exploited but be recognized as key 'contributors and trusted partners' by businesses. In a model like this the recognition to the end-users would not be measured against the upstream data value but the ex post incremental value achieved thank to user' cooperation. An end-user well deserved in-kind or cash back compensation (computed on a FRAND ex post basis) would not be based on the principle that 'data is as raw value input' like if the end-user was to be seen as a commodity supplier but through the lens of his/her cooperation degree (to share data) and the incremental value achieved (and measured) thank to such cooperation.

Even if personal data deserves to fall under a special protection scheme and unless anonymized cannot be commercially exploited and traded (at least under EU GDPR), there is a vast amount of other type of data (non-personal and metadata) which could be traded and exchanged, subject to the fulfilment of certain pre-conditions and which the end-user ignore how commercially it can become an attractive proposition for companies. This notion of 'data use' through digital rights management also resonates well with the broader concept of secondary data reuse and share where the agent determining the re-use time interval and purpose can be the individual rather than the company (service provider).

Establishing by the law a system where the end-users could unilaterally control data rights permission management such as to change how the data get allocated to the market has the potential to significantly impact how wealth is generated in digital and redistributed.

Data subjects have many rights in digital space, especially under EU GDPR. But no explicit right to monetize data until DMA and DA entered into force. This allowed in Europe to do a shift from right to agree to share or to oppose to share, right to view data held by the platform and right to delete such data (e.g. EU GDPR) to right to export and right to

switch service (and carry over the data held by the platform) under EU DMA and also under the EU Data Act.

So we in the European Union now have the legal basis to enable end-users to participate as business partners in the value chain but monetizing someone's personal data remain particularly difficult for players outside the data value chain (like end- users are) as there is no transparent information available to them to help define the 'right' market price or to expose the catalogue of data that could be made available under this scenario.

It is a fact that in current modern societies no business can flourish without data so we can already work under the core assumption that data is always valued more than 0 including for an end user who has no understanding of the data market value nor of the stakeholders on the data demand side which by competing (against another stakeholder) could take that presumed value from zero to higher than zero. And assuming there could be a bidding system the two companies would face, to access the data of the same end user, the price would probably go up if one of the companies would be willing to pay a premium for obtaining exclusive right of use of that individual's data for a longer period of time.

So how can we facilitate a more competitive system between companies when sourcing data and have a pivotal role assigned to the end-user such as to enable him/her to claim a fair compensation and play as a partner in the relationship with businesses? One option is to automate how the end-user can effectively assert his/her 'willingness' to participate in a data sharing 'contract' and prevent companies from opting out from honouring it.

Blurring the difference between personal and non-personal data for monetization purpose is one of the aspects to explore in this paper along with giving some practical examples of why we believe the system could work well.

1. The first key assumption being that there should not be a difference between personal and non-personal data monetization opportunities by the end-user (while there would always be for the service providers if they qualify as data controllers or join controllers);
2. End-users should be left free to allocate the data they generate based on market demand in a dynamic way. To this end a mobile experience is probably more desirable.
3. If the data is generated by a human (through a machine interface eg smartphone, set top boxes laptop, connected cars, EV chargers), the data subject should have full rights to decide on the intended usage and re-usage of such generated data, hence the need to define a common etymology for the 'purposes' that the industry could expose to the users. In such a scenario the user would assert his/her rights under a regime of '*rights of use by purpose'*. Such rights of use would be defined technically through specific attributes (technically readable by machines) e.g. time, geography, purpose and eventually provide for specific limitations of use of

the data, plus include the expected form of compensation (in kind or cash back) and enable the businesses to compete by placing their bids.

How this compensation could be calculated and expressed is also falling in the paper as we assume that it should be FRAND based and paid *ex-post*. This means that no companies could transact with an end user for less than a minimum compensation (in-kind or in cash) and that 3-5% should be based on FRAND terms and should be paid ex-post such as that the 'commitment by the end user to cooperate' (share) would be respected but also verified through the end of the 'time interval'.

As the intended use of data generated by end-users and consumers are multiple and also sometimes not competing with each other it's conceivable that different usages for different time intervals and different geographies would equate to different level of compensation for the end-user. The benefit for the end-user would be significant as the same dataset would be monetized several times, bringing his/her gains to a level of attractiveness.

Examples:

- 6 month committed consent to personal data sharing for programmatic purpose (e.g. targeting) by a social media = user entitled to not less than 3-5% FRAND cashback calculated on incremental advertisement ROI by the social media company;
- 6 months committed consent to personal data sharing for use by an AI agent (for training purpose) = end user entitled to not less than a FRAND 3-5%;
- 6 months committed consent to share devices usage time for use for product enhancement purpose = end user entitled to not less than a FRAND rate (3-5%) for the product improvement only achievable thank to the received data by the manufacturer (can applied to device wholesale price).

Now, at the beginning of AI era and at the sunset of Big Data and Web as we have known it for 20+ years, it's time to think bold to a new digital societal model taking more into account wealth creation and redistribution as we see the AI massive adoption impacting jobs and how human being produce.

We are in the belief that a FRAND based system, incentivizing end-users to allocate more efficiently data through digital rights management, entitling the end users to a fair and proportionate compensation for agreeing to cooperate under pre known and defined variables (time, geography, purpose for example) could benefit the whole ecosystem as companies need data, users would have the option to choose more consciously to which companies sharing it with and the downstream effect could be measurable.

Europe can capitalize on existing laws and regulations to put in place such system, including GDPR and eprivacy, plus the newly adopted specific regulations applying to VLOPS and Gatekeepers under sector specific EU legislations aiming at curbing gatekeepers' dominance and opening to data reuse and reshare paradigms under privacy compliance (e.g. DMA, DSA, DGA, AI Act and Data Act).

Olesia Shmarakova[*]

DATA STRATEGIES AND DEVELOPMENT OF TRADE IN DATA: THREE POLICY APPROACHES

Abstract

The importance of data in the economy is no longer a debatable issue; it is taken for granted. Upon the recognition of this fact, many countries have been solving the problem of improving the quality and availability of data through the development of various models of data sharing for several years. Active academic and business discussions on data policy and governance have finally borne fruit: several jurisdictions have adopted national data strategies (or similar documents).

However, does the existence of a data strategy at the national level indicate that the best conditions for the development of data trade and data markets have been created? How is the strategic approach conducted at the state level related to the actual availability of data to private businesses?

Different jurisdictions define their data governance priorities differently, and the approaches outlined in the strategies are (or are not) reflected in subsequent "direct application" legislation.

This article is devoted to a comparative analysis of strategic documents in the field of data governance of the European Union, United Kingdom, and Russia in the context of their interrelation with the laws that directly regulate the legal regime of various categories of data for commercial turnover.

The first part of the paper will provide a brief overview of the data governance documents of the jurisdictions in question: the European Strategy for Data, the UK National Data Strategy, and the Russian national projects "Digital Economy" and "Data Economy," with a focus on the differences in goal-setting and their potential impact on the further development of both data legislation and digital markets in general.

In the second part of the paper, the EU, the UK, and Russia, respectively, will be analysed in relation to "tactical" legislation that has been adopted or is planned to be adopted in the wake of the said strategic documents. The comparative analysis will focus on those acts that address the regulation of data in commercial circulation, its accessibility for private business, and private business obligations related to data.

In particular, the impact on the data market of the EU Digital Package will be discussed and the recently adopted Data Act will be contraposed with the provisions of a similar initiative of the UK Data Protection and Digital Information Bill 2. Also, this section will touch upon the issue of recognizing data as a legal object under the laws of the relevant jurisdiction and the existence of a general regulation applying as *lex generalis* to any data category.

Finally, the last part of the article will be devoted to comparing the provisions defined at the strategic level with the changes made to regulating data in commerce. Considering this analysis, a policy model for data governance based on the balance of interests of three actors: state, businesses, and individuals, will be described. Based on this approach, an attempt will be made to determine the actual priorities of the

[*] PhD candidate, University of Turin.

DOI 10.13135/2785-7867/11804

legislator for each of the jurisdictions under consideration and their potential impact on the further development of the data markets in these areas.
The article demonstrates that compared jurisdictions differ substantially in terms of the consequences of the chosen regulation path. While Russia may improve state services based on enhancing data availability, it does not aim to create a commercial market for data. Despite increasing data availability, the EU imposes restrictions on data holders. Extensive European regulation may impede data-driven businesses due to high compliance requirements. Conversely, both in the strategic documents and legislative proposal, the UK aims to create a business-friendly environment via precise and unburdensome regulation. Thus, the UK approach is the most effective for enhancing data trade.

JEL CLASSIFICATION: F68; H73; K11; K15; O38.

KEY WORDS: data strategy, data access, data sharing, data policy, trade in data

SUMMARY

1. Introduction – 2. Data strategies and their goals – 2.1 European Strategy for Data – 2.2 UK National Data Strategy – 2.3 Russian strategic documents on data – 3. Legislation in the wake of data strategies – 3.1 European strategy-based acts – 3.2 UK legislative proposals on data – 3.3 Data governance in Russia – 4. Three policy models for data governance – 5. Conclusion.

1 Introduction

With the further development of the digital economy and the rise of Artificial intelligence technologies in particular, data are gaining more and more importance. Data is fuel for AI; data can be used to understand, predict, and even nudge the behaviour of the market incumbents. Thus, the legislation on data, initially developed in most countries from privacy laws, is becoming more complicated and starts to cover issues well outside of the traditional privacy domain.

The recent adoption of the first strategic documents relating specifically to data governance confirms that governments from different jurisdictions acknowledge the importance of data. The EU has adopted the European Data Strategy for data, the UK – the National Data Strategy, and Russia – the federal "Data Economy" project. These documents lay down the basic principles for the further development of state policy and legislation concerning data.

At first sight, the three compared jurisdictions seem to base their data strategies on the same principles, as they declare that economic development requires more data, i.e., data of better quality and more accessible. The other basis is enhancing the functioning of the economy via more extensive use of available data, application of new data analysis technologies, and creation of data-extensive projects in both public and private spheres.

Per the data strategies, the compared jurisdictions plan or adopt particular pieces of legislation dealing with specific data types or particular rights and obligations related to data. These regulations and strategic documents shape the reality of the data market in the relevant jurisdictions and set goals and limits for its further development.

This paper will analyse data's strategic and "tactical" regulation in three jurisdictions: the EU, the UK, and Russia, primarily concentrating on the new legislation adopted or proposed after the relevant strategies. Given the recent adoption of a significant package of substantial new legislation in the European Union, analysing its origins as a policy document on data is interesting. While many states worldwide have adopted or are developing data policies, this paper has chosen to focus on European space and explore how approaches vary within the same European continent. EU policies in this regard are interesting to compare with the UK's approach, as on the one hand, they share common origins, but on the other hand, post-Brexit, the UK has shown a conscious divergence in certain areas. To contrast these two jurisdictions, Russia also borrows a lot from European legislation and approaches but differs significantly in terms of goal-setting and the balance of interests of market participants. A comparative analysis of these three jurisdictions will give an idea of the existing approaches to data governance and trade in data, which are crucial for the market of the European continent.

The paper aims to describe a policy model for data governance in each jurisdiction based on the balance of interests of three actors: state, businesses, and individuals. The literature on the European data strategy and related legal acts is extensive due to the long preceding discussion; Kerber, van Erp, Gallese, and numerous Commission Communications' contributions should be named here. The UK part of the literature is more limited and relates primarily to commenting on particular pieces of legislation without a general analysis of the legal situation (Kemp). The same is true for Russia, as apart from a couple of comprehensive studies (collective monography by the Higher School of Economics and a dissertation of Mefodieva), scholarship is yet scarce on the matter. Moreover, no works performing comparative analysis in the field of data governance were identified concerning these jurisdictions. This contribution opens the topic for further study.

The paper will proceed as follows: the second chapter will be devoted to the analysis of strategic documents on data in each of the three jurisdictions; the third chapter will analyse for the same jurisdictions the particular legislative acts adopted in the wake and on the basis of the strategic documents; finally, the fourth part will define the policy approaches based on the documents above and compare them between the jurisdictions.

This paper's main object of interest is the data in commercial use and how the adoption of strategic documents or further legislation could have changed the situation in the "data market."

2 Data Strategies and their Goals

In recent years, many states, including those belonging to different legal systems and economic formations, have started adopting data governance and access development documents. It is important to emphasize that this is the first time that such documents

have been created at the level of state-wide (and in the case of the EU, even region-wide) strategies, and the relevant documents are, in each jurisdiction where they have emerged, the first of their kind. Although the challenges posed to states by the global world powered by data are the same, states approach them differently. The goals stated in data strategies correlate to a large extent with the state-wide policies and values pursued in the respective jurisdictions.

2.1 European Strategy for Data

Over the last twenty years, the European Union has adopted many acts regulating various aspects of data and information, both of a legislative and political-strategic nature. Of course, many Commission Communications are generally devoted to data, and the most essential document is the European Strategy for Data.[1] Several Commission Communications preceded the adoption of this document on data regulation (2014 - "Towards a data-driven economy"[2]; 2015 - "A Digital Single Market Strategy for Europe"[3]; 2017 - "Building a European data economy"[4]; 2018 - "Towards a common EU data space"[5]), which indicates a long and thorough elaboration of the issue. Further analyses will show that the initial position on specific aspects of data regulation has changed dramatically.

The Strategy sets four pillars as the basis for all future legislation in this field[6]:

(1) Cross-sectoral governance framework for data access and use to avoid internal market sectoral fragmentation.
(2) Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing, and using data interoperability.
(3) Competences: Empowering individuals and investing in skills in SMEs.
(4) Common European data spaces in strategic sectors and domains of public interest.

The European Strategy for Data has identified the problems and devised an action plan to deal with them, including legislative and non-legislative actions.

Among problems, the fragmentation issue between the EU Member States was first on the list due to the EU's unique regulatory situation. Overcoming barriers between Member

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'A European strategy for data' [2020] COM(2020) 66 (European Strategy for data).
[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'Towards a thriving data-driven economy' [2014] COM(2014) 442 (Communication Towards a thriving data-driven economy).
[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'A Digital Single Market Strategy for Europe' [2015] COM(2015) 192 (Communication A Digital Single Market Strategy for Europe).
[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'Building a European data economy' [2017] COM(2017) 9 (Communication Building a European data economy).
[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions 'Towards a common European data space' [2018] COM/2018/232 final (Communication Towards a common European data space).
[6] Art. 5C of the European strategy for data.

States involves not only the harmonization of legislation but also the removal of existing restrictions in national legislation on cross-border data transfers if they occur in another EU country.

However, the second problem, namely the availability of data for innovative reuse, including the development of AI, is common through the compared jurisdictions. The issue of data interoperability and quality is another side of the coin of data availability in general.

Another essential aspect that is specifically noted in the EU Data Strategy is the imbalances in market power. The Commission notes that small numbers of large online platforms "accumulate large amounts of data, gathering important insights and competitive advantages from the richness and variety of the data they hold"[7], and their market power result in “data advantage”. As with any competitive advantage, leveraging data can affect the market's contestability, particularly in a situation where other market incumbents have no legal ways to obtain necessary data from "data monopolies".

The Strategy is a determinant not of the current, but of the future data governance framework in the EU. Based on the Strategy, we expect, on the one hand, a reduction in sectoral data regulation (first pillar) and, on the other hand, the creation of cross-border data pools in specific sectors (fourth pillar).

The focus on specific groups of data users and specific economic sectors makes the European approach the most concrete, even without high-level data regulation at the most general level.

It should be noted that in addition to a wide range of organizational issues, a significant emphasis is placed on the rights of individuals, and the foundations are laid for detailed regulation in the field of private law. One of the planned actions under the strategy is to empower individuals concerning their data and invest in skills and SMEs.

In particular, the Strategy has set up several particular details on how the future regulation in this regard is to be (and was) developed:

1) Providing individuals with more power to enforce their data rights, among other things, via technical tools and standards.
2) Empowering individuals to be in control of their data.
3) Creating means allowing individuals to decide what is done to their data at a granular level.
4) Enhancing data portability rights for individuals.

A special emphasis on the data rights of individuals and particular detail and specificity in this matter, including the granting of new rights, not just better protection of existing ones, distinguishes the European Data Strategy from similar documents in other jurisdictions.

[7] Art. 4 of the European strategy for data.

By now, a significant part of the initiatives provided in the European Strategy for data, at least in the legal domain, has already been realized, the last one is the recently adopted Data Act (DA)[8] along with the Digital Package (to be discussed in detail later).

Therefore, in the coming years, it is likely expected at the European level to take stock of the application of new legislation rather than adopt new strategic documents in this area (with the possible exception of the development of artificial intelligence regulation).

2.2 UK National Data Strategy

Speaking about UK law, it should be noted that the peculiarities of the legal regime of any legal object in comparison with the EU or Russian regulation are related not only to the specific choice of policy concerning this object but also, in general, to the differences between civil and common law. It is commonplace that common law is "less regulative," meaning that common law countries tend to legislate less and give more freedom to the judiciary to decide on what the law should be. However, any general analysis of differences between civil and common law is outside the scope of this paper. Thus, such differences will be presumed without any further comment.

Moreover, the analysis of UK law is further complicated by the fact that EU law was fully applicable when the UK was part of the EU and was phased out after Brexit under the Withdrawal Agreement[9], except 'assimilated law', which is the part of the EU law that was retained upon expiration of the transition period and has now become a new form of domestic UK law. [10] Therefore, for the sake of clarity of comparison, the UK part of this paper will be based on current law. In contrast, the historical analysis of EU law is also applicable to the UK during the period when the UK was part of the EU, and it is not possible to make a valid distinction in this case. This approach limits the scope of the UK part of the analysis to some extent and avoids unnecessary repetition. In addition, it should be noted that the laws of England and Wales will be used for the analysis.

The data governance issue came under the scrutiny of the UK government in the previous decade when the House of Commons discussed a report, "The Big Data Dilemma" (2015).[11] The report addressed different concerns relating to the data economy, emphasizing personal data protection. It is worth noting that even back in 2015, the UK claimed the world-leading data capabilities.

[8] Regulation (EU) 2022/868 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 [2018] OJ N Series L.

[9] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] /C 384 I/01 OJ CI 384/1 (Withdrawal Agreement).

[10] Section 5 of the Retained EU Law (Revocation and Reform) Act 2023.

[11] The House of Commons, Science and Technology Committee, 'The big data dilemma' [2015].

The most important document relating to data of recent years is the National Data Strategy[12], adopted in 2020, which provides a framework for government actions on data. Similarly to the EU approach, the UK Strategy indicates four pillars (Part 2):

1) Data foundations relating to quality and format of data for further use.
2) Data skills relating to ability to exploit data.
3) Data availability relating to access and reuse of data.
4) Responsible data relating to limitations on data use imposed by law, ethics, fairness, sustainability, and accountability.

Missions indicated in the Strategy seem even more critical, as they show particular policy approaches to be taken by the UK government concerning data (Part 3 of the Strategy). It is indicated that the government aims to maintain "a data regime in the UK that is not too burdensome for the average company". Along with a more general goal to enhance the availability of data in general and to share governmental data more efficiently (which are also present in the EU strategic documents), the UK directly underlines that it aims at championing the international flow of data. A more detailed policy framework for the first mission indicated in the Strategy (usability and data availability) is already out.[13] Research carried out supporting this mission states that government intervention may be needed to reduce the present legal barriers to data sharing, particularly in intellectual property, use of data and digital technology, and industry-specific regulation).[14] The other document based on the UK National Data Strategy is the data-sharing governance framework,[15] that along with the Data sharing code of practice prepared by the Information Commission Officer[16] and Freedom of Information Act[17] constitutes the main pillars of the UK framework for public data sharing.

2.3 Russian strategic documents on Data

The development of data regulation in Russia is part of digital transformation, which is declared one of the national goals until 2030.[18]

[12] Department for Digital, Culture, Media & Sport, 'UK National Data Strategy' [2019] <www.gov.uk/government/publications/uk-national-data-strategy> accessed 22 June 2024.
[13] National Data Strategy Mission 1 Policy Framework: 'Unlocking the data value across the economy' [2021] <www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy> accessed 22 June 2024.
[14] Art. 2.1 of the UK Department for Digital, Culture, Media and Sport, 'Increasing access to data across the economy' [2021] <www.gov.uk/government/publications/increasing-access-to-data-held-across-the-economy> accessed 22 June 2024.
[15] UK Central Digital and Data Office, 'Data sharing governance framework' [2022] <www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework> accessed 22 June 2024.
[16] UK Information Commissioner's Office, 'Data sharing code of practice' (May 2021)</ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/> accessed 31 August 2024.
[17] UK Freedom of Information Act 2000.
[18] Decree of the President of Russian Federation 'On national development goals of the Russian Federation for the period until 2030' No. 474 of 21.07.2020.

Working on data regulation framework started even earlier, a strategic document in this area is the Presidential Decree on the Information Society Development,[19] which regulates big data processing, analysis, and data protection.

However, the prominent practical step in digital transformation and data regulation development was made by the federal project "Digital Public Administration," adopted as part of the national "Digital Economy of the Russian Federation" program in 2019. The national data management system was created to increase the efficiency of management decision-making based on the use of State information resources.[20] These regulations deal exclusively with public data and address public management goals.

This project was carried out from 2019 to 2024. It included a wide range of sub-projects and initiatives united by the concept of digitalization of the economy, from IT education for children and the provision of grants for talented students to the creation of numerous new digital public services.

Significant efforts during this period were aimed at digitalizing all spheres related to public administration, developing state information systems, and the online transfer of most interaction mechanisms between the state and citizens and businesses.

The digital sphere, including digital data issues, has received tremendous attention from the government. Among other things, changes concerning IT and the digital sphere have been introduced in the Russian Constitution: in the article concerning the subjects of federal jurisdiction in the system of division of powers between the federal authorities and the regions of the Russian Federation, "information technologies" was added, as well as "ensuring the security of the individual, society and the state in the application of information technologies, circulation of digital data".[21]

Previously, the Constitution did not regulate such issues; moreover, there is no definition of "digital data" in Russian law. However, these amendments and the broader trend towards digitalization, including the development of relevant legislation, have sparked a broad academic debate, from questions of constitutional human rights in the digital age to the digital sovereignty of the state.[22]

However, does a discussion of data turnover mean that there is a specific legal regime for digital data[23] and they become a tradable commodity? Despite the provisions of the Russian Constitution, the "digital data" regime has not yet been further developed in legislation.

[19] Decree of the President of Russian Federation 'On strategy for the information society development in Russian Federation for 2017-2030' No. 203 of 09.05.2017.

[20] Order of the Government of the Russian Federation 'On approval of the Concept of creation and functioning of the national data management system and the action plan ('roadmap') for creating the national data management system for 2019 – 2021' of 03.06.2019 No. 1189-r.

[21] Art.71 of the Constitution of the Russian Federation.

[22] Elena Alferova, 'Digital novels of the Constitution of the Russian Federation: a view of the legal scholars' (2023) 4 Social and humanitarian sciences 106.

[23] MV Yakushev and AA Efremov (ed), *Data Regulation in the Russian Federation: Current status, Problems, Prospects* (Higher School of Economics Publishing House, 2021).

In 2023, work started on a new national project, "Data Economy," until 2030, which will continue the Digital Economy project being finalized. The project will cover all stages of data handling, from data collection (which involves the creation of new sensors) to data transmission and developing communication systems, data storage and security, technical standardization, and data processing and analysis issues. The legislative plan will be created for 2024-2026 in the relevant spheres.

The aim is to create a management system based on big data in the economy and social sphere, whereas the digital infrastructure should be unified for the key industries and spheres.[24] At the same time, according to the president's statement, the Data Economy is necessary due to the threat to national security. Previously, many critical technologies were developed on foreign platforms.[25]

It is noted, though, that this project is, first of all, the state's initiative and not of the market players, and it aims to optimize state governance using big data.[26] For example, one of the project's goals is to build digital platforms in all sectors of the economy.

However, the government should not manage such platforms where there is no need. The project has been criticized for denationalizing the data market and design to create state or near-state monopolies instead of market mechanisms.[27]

Generally, the project includes initiatives aiming to digitalize the work of the government, provision of state services, develop domestic IT equipment, and further strengthen digital sovereignty[28].

Thus, Russia is currently working actively at the strategic state level to create a system of data regulation, including the introduction of new legislation. However, the initiatives are entirely in the area of public law and do not address the issues of private rights concerning data. The discussion of recent years in this area, unlike the European discussion, has never dealt with the development or change of regulation in the area of property or quasi-property rights to data. Since the projects under discussion are primarily concerned with state data or how the state manages data and have not addressed private rights issues, the claim of "state monopolization" of this area seems justified.

From the above comparisons of strategic data management policies and the reflection of the general concept of data or information in the law, all countries under consideration have paid much attention to the issue in recent years and are actively developing policies.

[24] Official communication of the Ministry of Digital Development, Communications, and Mass Media of the Russian Federation of 13 July 2023 [2023].
[25] Julia Tishina and Anna Oris, 'Data go on a national level' (*Kommersant*, 6 December 2023) <www.kommersant.ru/doc/6380045?ysclid=lxanueiplb230066310> accessed 11 June 2024.
[26] Tishina and Oris ibid.
[27] Karen Kazaryan and Irina Levova, 'Numbers for "digital": what is wrong with national project "Data economics"' (*Forbes.ru*, 5 March 2024) <www.forbes.ru/mneniya/507425-cifry-dla-cifry-cto-ne-tak-s-nacproektom-ekonomika-dannyh?ysclid=lxanuj7tjy327964660> accessed 11 June 2024.
[28] 'Data economics and digital transformation of the state' (*TAdviser.ru*, 18 May 2024) <https://www.tadviser.ru/a/745913> accessed 11 June 2024.

At the same time, significant differences are noticeable in target setting and the approach to regulation.

A comparison of strategic approaches to data management shows that all countries under consideration recognize the importance of data in the economy and note the need to develop data availability and reuse. However, significant differences may also be noted. As one of the strategic goals, the EU indicates the creation of common EU data spaces and fighting "internal borders" for data transfer, which is logically taking the possible different approaches and regulations in the Member States. The other policy goal of the EU is empowering individuals. Though the UK and Russia also address the issue of personal data protection in their strategic documents, unlike the EU, they plan to keep the legislation the same to provide any new rights concerning data. In this regard, an essential difference in EU policy is that it is aimed, among other things, to benefit the individuals. The Russian emphasis in data policy is on using data and enhancing government practices via digitalization. At the same time, businesses could reuse the data previously collected by the government. Thus, the state is the primary beneficiary of projects related to big data and the evolution of data governance. As for the UK, a market-oriented approach draws special attention, as the UK government emphasizes that UK companies should benefit from the practical and not too burdensome data regulatory framework. The UK also aims to support its championship in the global arena in this area. Thus, the UK approach is more utilitarian and favoring entrepreneurs.

3 Legislation in the Wake of Data Strategies

3.1 European strategy-based Acts

It should be noted that there is no legislation regulating data/information at the EU level, rather than a specific type. Though the European Strategy for Data operates with the concept of data as such, it does not directly establish a specific legal regime for data that would apply in all Member States. The EU has never discussed or planned to develop such a regulation. Since other regulations dealing with various types of data (such as GDPR[29], Database Directive[30]) are already in place, it would be difficult, if not impossible, to harmonize them for commercial purposes.

Member States, therefore, still have the option to regulate "data or information in general" at the level of national law, for example, in civil codes (provided that such a regime does not conflict with pan-European legislation on a particular type of data).

[29] Regulation of the European Parliament and of the Council No 2016/679 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 [2016] OJ L 119/1 (GDPR).
[30] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77 (EU Database Directive).

Still, in the wake of the European Strategy for Data, several very important legal acts were adopted, dealing with various goals named in the Strategy: Data Governance Act (DGA)[31], Digital Markets Act (DMA)[32], Digital Services Act (DSA)[33], and, finally, the most recent Data Act (DA).

These acts fully or almost completely cover the directions of development of data regulation outlined in the Strategy, including those aimed at increasing data accessibility for private business and commercial turnover.

The DGA is a 'paired' document to the Open Data Directive[34] and regulates, first of all, the conditions for reuse within the EU of specific categories of data held by public sector bodies that the Open Data Directive does not cover. Adopting the DGA will allow the public sector to provide access to protected data (e.g., commercially confidential data) under certain conditions.

In addition, the DGA regulates a significant concept such as data altruism, that is defined as 'data altruism' means the voluntary sharing of data based on the consent of data subjects to process personal data on them or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest".[35]

These are the two most important innovations within the DGA aimed at enhancing data availability for further reuse and deleting the barriers relating to obtaining the data (for example, the need to receive consent to reuse personal data beyond the initial purpose of collection and processing.

Undoubtedly, the adoption of the DGA increases the opportunities for both public bodies and private businesses to access the necessary data. At the same time, the provisions of the DGA are inherently permissive: they impose certain obligations on public bodies, providing counter-opportunities for business.

The other two acts adopted in 2022 in fulfillment of the Strategy are rather opposite in balancing public and private interests concerning data. DSA and DMA primarily regulate obligations and set limits for digital businesses concerning different aspects of their activities, including operating with data. The regulation of data, including the issue of its availability for commercial circulation, is not central to these acts. However, applying their provisions inevitably affects, among other things, the regime of data generated in the provision of digital services.

[31] 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 [2018] OJ L 152/1.
[32] 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 OJ L 265/1.
[33] 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 [2022] OJ L 277/1.
[34] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information (recast) [2019] OJ L 172/56.
[35] Art. 2 (16) DGA.

DMA essentially aims to redistribute the benefits linked to the factual possibility of accessing and using the data between the "gatekeepers" (specifically designated undertakings providing core platform services) and the users of their services, both private and public. Thus, DMA changed the de facto situation by prohibiting the gatekeepers from using certain users' data for certain purposes and granting the users the right to access the data held by the gatekeepers. For example, gatekeepers shall not process personal data of end users using services of third parties that make use of the cope platform services of the gatekeeper in order to provide online advertising services (Art. 5(2)(a) DMA). Though the gatekeeper may continue accessing such personal data, their legal use is banned. Alternatively, the gatekeepers are obliged to provide business users access to data provided for or generated in the context of using relevant core platform services (Art. 6(10) DMA). Thus, on the one hand, DMA expands the possibilities of accessing and reusing data for some persons, and on the other hand, restricts them to the primary addressees of the act - gatekeepers.

Similarly, the DSA sets limitations and obligations concerning data for providers of online platforms, though significantly milder compared to the DMA. Thus, providers of online platforms cannot use users' data for advertisement (even though they have legal access to them) if they are aware and have reasonable certainty that the recipient is a minor (Art. 28(2) DSA). Providers of very large online platforms or very large online search engines are obliged to grant access to necessary data to public bodies (namely Digital Services Coordinator) and vetted researchers (Art. 40 DSA).

The most European relevant act in terms of making data more accessible to market participants is the recently adopted DA. Given the existence of a substantively similar bill in the UK, both of these instruments will be reviewed below in the form of a comparative analysis to highlight better the commonalities and differences in the data policies of these two jurisdictions.

3.2 UK Legislative Proposals on Data

As regards the legal regime of data as such in the UK (in particular in trade and within the horizontal relationships of market participants), the law of England and Wales does not acknowledge any legal (not to say property) rights in data. This approach is further confirmed by the Law Commission, noting that "digital things such as normal digital files that are not (as currently designed) capable of attracting personal property rights as a matter of law."[36]

The laws of England and Wales regulate rights related to data, both in intellectual property and contract law. While intellectual property issues will be discussed separately

[36] Art. 3.19 of the Law Commission's report, 'Digital assets as personal property. Short consultation on draft clauses' [2024] <lawcom.gov.uk/document/digital-assets-as-personal-property-draft-clauses/> accessed 31 August 2024 (UK Digital Assets Draft).

later, it should be noted that data-related contacts are mainly developed under English law, as legal consultants make particular advice for contract drafting.[37] Thus, a precisely defined status of the legal object is necessary for data tradability under contract law, provided the subject matter is defined enough.

It may be added that the laws of England and Wales do not contain any general legal definition of "data" or "information". Concerning data law, the proposal for the Property (Digital Assets) Act 2024 is an important initiative.[38] This proposal covers regulating digital assets such as crypto-assets, NFTs, etc. In its initial stage (2022) is utilized the terminology "data objects", was somehow confusing and was described as *"composed of data represented in an electronic medium, including in the form of computer code, electronic, digital or analog signals", however, further detalization showed that pure information was excluded* from becoming a data object.[39] Later, though the idea evolved to its current status, "data objects" were (more appropriately) renamed into "digital objects", and even the requirement for them to be "composed of data" was deleted as excessive.[40] The actual version of the proposal explicitly excludes information and data (in the form of digital files) as such[41] and implicitly, as the qualifying requirement for the digital asset is vivaciousness. Data, in general, though, is characterized by non-rivalry. Still, the Property (Digital Assets) Act proposal (part of the UK Digital Assets Draft) and previous Law Commission documents are of huge importance for data regulation in the UK, as they introduce completely new doctrinal concepts that can be applied to data, at least to some extent. Digital assets are summed up into the new "third category" of private property apart from things in possession and things in action.[42] Another important concept for data is "control", which is understood by the Law Commission in both factual dimensions ("ability to (1) exclude or to permit access to a third category thing; and (2) put the third category thing to the uses of which it is capable"[43]) and legal. The same concept lies in the basis of any data regulation, for example, personal data (figure of "controller) or trade secret (legal control), and is, to a large extent, applicable to data without any changes.

Thus, although the legislation of England and Wales does not regulate data as such and does not protect under the property rights regime, the regulation of the data-based asset is evolving, which shows the legislator's attention to this area. The approach to the

[37] Richard Kemp, Paul Hinton and Paul Garland, 'Legal rights in data' (Thomson Reuters Practical Law, 25 January 2011) <uk.practicallaw.thomsonreuters.com/5-504-1074?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 21 June 2024.
[38] UK Digital Assets Draft.
[39] Harriet Jones-Fenleigh, Aditya Badami and Jonathan Hawkins, 'The Law Commission's 'data objects': Digital assets as a new property class' (Norton Rose Fulbright, 1 August 2022) <www.nortonrosefulbright.com/en/inside-disputes/blog/202208-the-law-commissions-data-objects-digital-assets-as-a-new-property-class> accessed 22 June 2024.
[40] Law Commission, 'Digital Assets. Summary of final report' [2023] 9 (UK Digital Assets Summary).
[41] Art. 3.31 UK Digital Assets Draft.
[42] Art. 2.2 UK Digital Assets Draft.
[43] UK Digital Assets Summary.

Property (Digital Assets) Act wording reflects the overall common law approach, as the regulation is kept to a minimum despite pervasive preparatory work, and all possible open questions are left to the discretion of the jurisprudence.

The Property (Digital Assets) Act proposal idea is somewhat novel. The legal scholarship also proposes a compromise model of the data law regime, the quasi-property rights, as the traditional concept of possession cannot be applied to data. However, the concept of control used in practice may be introduced instead.[44] Sjef van Erp argues that data already falls within the *numerus clausus* of legal objects. However, some fitting is required in terms of terminology, as about data "ownership and revindication must be replaced by control and access; perhaps – so it might be added – the concept of "transfer" should be replaced by "distribution".[45]

DA specifically regulates the product data and related service data, and, as per the Brussels effect, the regulation in other jurisdictions may also be assessed concerning this specific category of data, as it will have a worldwide effect, similar to the act from the Digital Markets package. Though it is not indicated directly in the DA, the scholars generally agree that the DA primarily covers data from IoT devices[46], i.e., machine-generated, that is also evident from the DA Recitals.

In the UK, there has yet to be any legislation enacted covering a similar scope. However, a legislative proposal has almost made it to the legislation – the Data Protection and Digital Information Bill (DPDI)[47]. DPDI is mainly devoted to data protection regulation, and the differences it plans to introduce in the personal data regime in the UK compared to the EU attract most of the attention of a few commentators. However, the DPDI also contains provisions for sharing customer and business data, which are mainly similar to the DA scope. The DPDI is also essential as a marker of the direction in which the legislation and policies of the UK evolve after Brexit.

[44] Sief van Erp, 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects' (2017) European Private Law Institute Working Paper No. 2017/6, 21.
[45] Ibid. 22.
[46] Martina Eckardt and Wolfgang Kerber, 'Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act' (2024) 57 European Journal of Law and Economics 113-143. See Recital 112: "In order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service or other machine-generated data, claim the *sui generis* right under Article 7 of Directive 96/9/EC, and in so doing hinder, in particular, the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation, it should be clarified that the *sui generis* right does not apply to such databases" (emphasis added).
[47] UK DPDI has not yet become legislation: it passed the House of Commons at the end of 2023 and was introduced to the House of Lords; there, it stopped at the report stage when the Parliament was prorogued for dissolution in the run-up to the general elections in the UK. The commentators have noted that if the Labour Party wins (which has eventually happened), it will likely introduce the new version of the Bill (see: David Naylor and Hannah-Mei Grisley, 'What Happened to the UK's Data Protection and Digital Information Bill?' (*Privacyworld Blog*, 2024) <www.privacyworld.blog/2024/06/what-happened-to-the-uks-data-protection-and-digital-information-bil> accessed 06 September 2024). Shortly after this article was finished, the winning Labor Party introduced this new version under the new title Data Use and Access Bill to the Parliament. Thus, this paper still needs to accommodate possible changes in provisions but should be considered in further research. For this reason this paper operates with the name and text of the initial DPDI version.

The scope of the DA covers product data and related service of the connected product or related service, including personal and non-personal data. DPDI, in its turn, deals with the two types of data – "customer data" and "business data", defining them both more widely than DA. Customer data definition, as in the DA, relates to one single customer, while the business data covers the trader's activity concerning all the customers. DA limits the scope of data derived from the connected product or related services. Meanwhile, DPDI covers any product data (connected or not) and data relating to the transaction, such as price and place of conclusion.

DA sets up three main parties of the relations: data holder, user, and third parties authorized by a user. DPDI provides for a wider variety of stakeholders about data: the three similar to DA plus third parties authorized by the data holder, plus "another person of special description" (namely a third party authorized by law), plus the interface bodies. It can be said that the DA reflects the classical contractual structure. At the same time, the DPDI is more oriented towards the market structure as a whole and considers both the direct parties to the interaction and their counterparties and the 'market facility'. Such a comprehensive regulation that considers the multi-stakeholder problem is more optimal if the development of the data market is prioritized. Gallese correctly points out that "Gaining access to the data is a good starting point for Users, but it does not significantly affect the EU market".[48] Given the lack of a clearly defined mechanism for the subsequent use of the data, there is a risk that even if users realize their rights in full, the data will settle with them, and the resulting redistribution of access will not lead to significant changes in the market.

The analysis in this section allows us to conclude that there are many similarities and differences between the legal frameworks of DA and DPDI. Both acts are aimed at solving a radically new task for the state - to create a legal basis for data sharing, first of all, between private parties, and thus overcoming the existing 'technical' monopoly on data that ended up in the hands of manufacturers of goods or providers of services. Currently, the EU legislation is the world's leading legislation in this area, and, of course, the authors of the DPDI cannot fail to take into account the provisions of the DA. The act's adoption was preceded by a very long scientific discussion and several communications of the European Commission, which significantly changed from the initial approach.

Thus, the significant divergences in the DPDI regulatory model were not accidental or deliberate, and DPDI shows the intention of the British legislator to depart from the uniform EU norms. In both the regulation of personal data and approaches to data sharing, the UK legislator demonstrates a more liberal approach to the obligations of businesses. In general, this reflects the overall goal, outlined at the strategic level, of the UK,

[48] Chiara Gallese, 'A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)' (2022) 3 Media Laws 237-270.

achieving (or maintaining) its championship as a jurisdiction that ensures the international flow of data.

Both acts impose an obligation on the de facto data holder to share the data with the user/customer or third parties authorized by the user. Both provide the possibility of charging a fee for the provision of data, at least to cover the costs of the data holder. In other aspects, however, the acts differ to a large extent.

A feature of the DA model is not simply that the user activates sharing - instead, all or most rights to operate with the data are locked on the user. Without the user's consent, data cannot be used by third parties or the data holder. Thus, the EU is changing the *de-facto* model of relations that existed before the act's adoption, in which the data holder operates the data (particularly non-personal data) freely without any specific regulations just because it has a complete technical control over the data. Under the DA model, data are not just shared with the user - most of the legal powers relating to data are officially transferred to the user. The user becomes a central figure whose actions depend on data availability in economics in general.

DPDI does not go that far: it does not touch the de facto situation of data holders having control over the data and operating with them. UK legislative proposal adds an obligation to share these data with the user or other authorized parties – without depriving the data holder of any of its previous powers regarding the data. Unlike the DA, the DPDI does not redistribute data rights by taking actual rights away from one person (data holder) and giving them to another (user); instead, it expands the range of people who can use the data.

In many regards, the model set in the DA is similar to those of the GDPR, as the use of data in both cases is linked to the consent of the "data producer" – user, even though DA covers both data of individual and business users. In a way, DA is also similar to consumer law, as it explicitly empowers the users of connected devices or data-generating services and creates obligations and limitations for manufacturers and service providers. It is customer-centric in most aspects, and the interests and will of the customers prevail over all other market participants.

Moreover, the peculiarity of DA is the contract-based approach to data sharing. Scholars have already called it the "contractualization" of sharing, as in most cases, the provision of data is supposed to be made under the contract. DPDI does not provide for concluding contracts between parties and follows a more public obligation model than a contract.

Overall, following the approval of the data strategies, the EU and the UK have started to actively work on creating new regulations for certain types of data. Moreover, one of the key objectives of the regulation is to define and increase the availability of data specifically for commercialization in the private sector.

3.3 Data Governance in Russia

Scholars note that legal regulation of the tradability of Big Data, including relevant contract rules, is of particular economic importance in Russia.[49] Still, neither the Russian Civil Code nor the sector-specific "digital" legislation provides any particular rules relating to data as such.

A closed list of "tradable" objects is provided in art. 128 of the Russian Civil Code (RU Civil Code I)[50]; before 2007, the list contained the notion of "information", however, it was deleted thereof simultaneously with the adoption of the Fourth Part of the Civil Code (RU Civil Code IV) [51] devoted to intellectual property rights. Amendments of 2019 have introduced to the Russian Civil Code (RU Civil Code III)[52] a particular type of contract for providing information services (art.783.1), but legal norms contain only the general provision that such a contract may require to keep the information secret.

A special law on information[53] covers a large set of issues relating to the information society. Over the last years, it has turned from a highly abstract piece of legislation into a law regulating the Internet and particular types of Internet activities (such as search engines, hosters, marketplaces, etc.) as well as the functioning of the state information systems. This regulation is primarily public, as it defines, to a large extent, the obligations of Internet actors towards the state (such as reporting) or general requirements and prohibitions. This law is similar to the DSA.

The law on information defines information as "messages, data irrespective of the form of its presentation" (art.2) and explicitly states that information may be the object of public, civil, and other legal relations (art.5), though provides a complicated mechanism which is not quite in line with the RU Civil Code I approach. The law states that "the holder of information unless otherwise provided for by federal laws, shall have the right to authorize or restrict access to information, determine the procedure and conditions of such access" (art.6). This norm creates significant difficulties in practice, as it is not clear whether such granting of access is a transaction and how it should be qualified from the point of view of civil law (i.e. special provisions on what types of transactions should be applied to it), as well as what norms of tax legislation are applicable.

Since then, the Russian legal and scientific community has been engaged in a sluggish debate on whether or not information can be considered a tradable object under civil law and whether it should be so.[54] Most scholars agree that information is de facto tradable

[49] Higher School of Economics (n 23).
[50] The Russian Civil Code. Part One. Federal Law of 30.11.1994 N 51-FZ (RU Civil Code I).
[51] The Russian Civil Code. Part Four. Federal Law "of 18.12.2006 N 230-FZ (RU Civil Code IV).
[52] The Russian Civil Code. Part Three. Federal Law of 26.11.2001 N 146-FZ (RU Civil Code III).
[53] Russian Federal law 'On information, information technologies and information security' No. 149-FZ of 27.07.2006 (RU Law on information).
[54] Christina Mefodieva, 'Digital data as an object of civil law regulation in Germany, the USA, and Russia' (Institute of Legislation and Comparative Law under the Government of the Russian Federation Government of the Russian Federation. Dissertation Paper 113 2019).

as any other object under civil law[55], though its tradability is limited by legislative deficiencies, and its exclusion from the Civil Code was a mistake[56]; some insist that information is a sui generis object, "capable of taking the form of other objects of civil rights".[57] The trend of the Russian legal science of recent years is the idea to recognize not information but digital data as a separate object of civil rights, i.e., property in the form of a sui generis right,[58] that shall ensure its tradability on equal footing with other intangible objects.

It is worth noting that despite the general provisions on freedom of contract and the consensus of scientists, transactions related to data turnover in Russia are complicated by the lack of regulation, so in practice, the subject of the transaction is usually clothed in one of the more "understandable" forms - a database or know-how. Thus, legal regulation of data in Russia in recent years has been very active but one-sided, as it mainly affects digitalization and the use of data to improve the efficiency of public administration and vertical relationships but practically does not affect the horizontal relationships of the market participants. The abundant but fragmented regulation without an articulated legal doctrine must be clarified. Given the attention given to the issue of data regime in the economy and public administration, symmetrical work in the field of law is needed to support all initiatives qualitatively.

Thus, the maturity of legal regulation in Russia regarding the product and service-generated data regime lags far behind Europe and the UK, given the need for approved legislation and elaborated legislative initiatives. Attention should also be paid to Russian scientific literature discussing the issue of singling out such data as an object of rights. However, the issue of rights distribution between different persons or access to such data needs to be analyzed. Despite scientific discussions, there are no significant legislative initiatives to regulate this data category in Russia, and there have been none in the past.

Thus, the Russian Federal projects "Digital Public Administration" and "Data Economy", though being by their nature the closes analogy to the Data Strategy, have not resulted in any particular legislation aimed at enhancing the data availability for businesses or developing the regulation (including commercial turnover) of the new types of data. In recent years, there have been different calls from academia to amend the law to accommodate the new digital reality, but they still need to be addressed by the legislature.

[55] D Lebedeva and A Yatsenko, 'Information as an object of civil rights' (2017) 4 Scientific Notes of the V. I. Vernadsky Crimean Federal University 166.
[56] EA Abramova, NN Averchenko and YV Baigusheva et al., *Civil law: textbook* (Prospect, 2013) 387.
[57] AG Tukhvatulina, 'Information as an object of civil rights' (2017) 2 Bulletin of Young Scientists and Specialists of Samara University 249.
[58] Mefodieva (n 54).

4 Three Policy Models for Data Governance

As the above review shows, the data policy documents in all the jurisdictions compared above, to a certain extent, take into account the interests of three groups: the state, business, and individuals. This reflected in the acts that are based on these strategic documents and directly regulate the legal regime of certain categories of data. However, it is important to note that the compared jurisdictions pay attention to the interests of different parties to different degrees and cater to them differently.

In the EU, the further development of data regulation has focused on users' rights, primarily individuals' rights. Back in 2020, the European Strategy for Data proposed to extend the rights of individuals within the framework of Art. 20 GDPR (portability right) by "giving them more control over who can access and use machine-generated data (possibly as part of the Data Act in 2021)".[59]

As the business consultations on the Data Act project demonstrated, the data stemming from professional use of the devices equipped with IoT is interesting for the majority of respondents, who express concerns about these data being exclusively held by the manufacturers.[60]

Thus, the field of attention of the European legislator was not limited only to the interests of individuals but also covered corporate users who could get some value from data. From an economic point of view, if we set aside the value issues of personal data protection, granting business users certain rights to the data they generate is of great value. Because it is business users who are likely to be able to find practical applications for that data and use it to create new value (e.g., by improving their own product) or at least to reduce their costs (e.g., by fixing broken equipment themselves instead of having to go to the manufacturer and pay for their services as necessary). Such data may also be of further economic interest to third parties to whom the user may wish to sell or transfer it (e.g., data on the performance of agricultural machinery for seed producers). As for individuals' data, it will undoubtedly be of personal interest to them. However, it is still difficult to imagine how individuals might subsequently use this data to maximize personal or public welfare.

Besides the explicitly declared goal of user empowerment not declared but self-evident goal of the DA is imposing further limitations on the Big Data monopolies (mostly non-European companies). The omnipresent marker power of a particular set of platforms and data ecosystem and their impact on the data markets has been noted by legal scholars (as well as economists, sociologists, etc.) for a long time now.[61] The current set of particularly

[59] Art. 5C European Strategy for data (n 7).
[60] European Commission, 'Public consultations on the Data Act: Summary report' [2021] <digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 15 April 2024.
[61] See, for example, a 2016 article by Lundqvist: Bjorn Lundqvist, 'Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World' (2016) Faculty of Law, University of Stockholm Research Paper No. 1.

"dangerous" companies exists in the form of the designated gatekeepers[62] under DMA or very large online platforms under DSA. Thus, one can allege that EU DA is the next station in the EU crusade against GAFAM and other Big Tech.

The DGA is generally focused on the interests of businesses and individuals, as it is about greater openness of public data. However, DMA and DSA aim to protect individual users (both business and private persons) and grant them additional data rights at the expense of other businesses. The same is true for the DA, as it gives new rights to data to individuals while limiting the rights of businesses holding the data. The interests of the public sector in acquiring necessary data are also addressed in these acts, though one can hardly allege that they are the cornerstone of the regulation.

Thus, it cannot be said that DSA and DMA aim solely to enhance access to data but rather to redistribute opportunities (including commercial opportunities) for data use between different market participants. Depending on the parties' activity in data use, these acts may either increase or decrease the actual commercial over-use of data. Regarding commercial use of data by private businesses, DMA and DSA regulation is based on the logic of antitrust regulation aimed at balancing the market and ensuring access to a resource (in this case, data) for some persons by restricting this access to others.

Thus, the EU primarily solves the task of rebalancing the data market. The European Strategy for Data raises concerns regarding the vast amounts of data accumulated by Big Tech companies and their high degree of market power.[63] As Bradford notes, the EU, despite the general market orientation, embraces the more state-driven economic policy to assert digital sovereignty[64] (as most of the Big Tech, or gatekeepers, or very large online platforms are not of European origin).

Thus, in choosing between the interests of the three parties mentioned above, in data regulation, the EU puts a stake in protecting the interests of individuals and limiting the interests of businesses (primarily multinationals). This is a striking feature of European regulation that is absent in the other two jurisdictions. Another characteristic feature of the EU model is the detail of regulation and the abundance of extensive legislation. However, this is more a style of European regulation in general than a feature of data regulation specifically.

In its National Data Strategy, the UK has expressed primarily the issues of developing a flourishing data market. Unsurprisingly, further legislative proposals relating to particular data issues are based on enhancing the trade in data and creating more opportunities for data-related businesses within the country. The UK aims to champion itself as a market attracting national and foreign businesses and providing them with opportunities for easier and safer operations. Notably, the UK National Data Strategy, unlike the EU one, does not

[62] European Commission, 'Gatekeepers' <digital-markets-act.ec.europa.eu/gatekeepers_en> accessed 06 September 2024.
[63] Part IV of the European Strategy for Data.
[64] Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology* (Oxford University Press, 2023) 132-133.

emphasize promoting the interests of the individuals or the need to curb the powers of Bit-Tech.

The two most significant legislative proposals concerning data regulation are the Property (Digital Assets) Act 2024 and DPDI, and they are both aimed at simplifying data access and trade rather than limiting it. Property (Digital Assets) Act is made to give more clarity concerning the legal regime of digital assets as tradable commodities and, therefore, enhance their trade. DPDI, in turn, does not define any new type of property but regulates access to existing data for a broader category of users.

The new UK bill - DPDI - develops and extends the Smart Data concept already implemented in all areas of legislation, which is based on slightly different assumptions and values than what has been discussed at EU level.

The DPDI does not use the term Smart Data, instead using the terms 'customer data' and 'business data', however, Smart Data has been used in UK government policy documents, official and unofficial communications, and general business practice and is thus an informal term not so much for the categories of data regulated by Part 3 of the DPDI as for the data exchange model it envisages. Smart Data is officially defined as "secure sharing of customer data, upon the customer's request, with Authorised Third-party Providers (ATPs)" (UK Smart Data Roadmap).

The concept was called Smart Data, and it incorporates both ideas of secure and consented sharing of customer data with third parties. Implementing the project, the UK aims to drive innovation in the financial sector, where it already has an established position as one of the major international financial centers. It also fosters competition, allowing third parties access the needed customer's data. The UK Smart Data Roadmap states that based on the Open Banking success, the government wants to commit to "a Smart Data Big Bang" in the following sectors, including energy, banking, finance, retail, transport, homebuying, and telecommunications (nevertheless, the DPDI is not sector specific).

Thus, even with the imminent adoption of the DPDI, the UK leaves itself room for manoeuvre by being able to introduce the new data-sharing mechanism envisaged by it gradually and piecemeal, assessing the situation in each sector of the economy separately. In this regard, we can agree with the position that "in comparison with the EU developments, the Smart Data proposals appear modest":[65] on the one hand, the project creates positive expectations among its possible beneficiaries (which are rather small and medium-sized businesses than consumers); on the other hand, due to the graded approach, it causes less anxiety among those businesses that will have to incur compliance costs sooner or later.

Though the European and British projects of product and service data regulation are similar in many respects, the UK has considered the experience of discussions. At the same

[65] Kemp, Hinton and Garland (n 37).

time, the UK was part of the European Union, so the background and objectives of the current legislation are different. It is noteworthy that in the EU legislation, it can be called a cornerstone and one of the key goals and values of the project, while in the UK, at all levels of communication it is more about creating business value and developing the data market and asserting the UK's leading role in the world in the field of data trade. The UK project has a decidedly more practical and market-oriented orientation, as seen from the official communications rhetoric. The EU project, in turn, addresses not only the development of the data market and data sharing, but also issues of fair distribution, user's control and protection of user's rights. Undoubtedly, the rights of users who create data have a significant economic component. However, the rhetoric of the DA itself, as well as the previous communications of the European Commission and scientific papers, certainly shows that enhancing transparency, fairness, and protection of the weaker party are no less important in this legislation.

A comparative analysis of the two acts (DA and DPDI) reveals that although both are based on a desire to create a legal framework for data sharing, they come from different value orientations. The DA puts the user and their interests at the center, allowing the user to block further data reuse (at least theoretically). The DPDI creates a framework where data holders would be obliged to share the data under the law without entering into any contracts with the user or third parties. Preliminarily (given that the DPDI is still a bill and does not provide direct application but for the adoption of a delegated law), the model envisaged by the DPDI would be more conducive to data sharing.

This allows to conclude that UK version of strategic development with regard to data is business-oriented, particularly compared to the European one. New legislation proposed does not limit the de facto rights of the businesses they have acquired; however, it gives more opportunity for the other businesses to access this data and, hence, to compete.

Additionally, the UK legislative model is generally characterized by a limited volume of regulation, while many issues are left for the case law. In particular, the Law Commission, while preparing the report, which lies on the basis of the Property (Digital Assets) Act, noted that modern case law also mainly acknowledges digital assets as particular type of property. Thus, the Law Commission has yet to invent the proposed law, but rather, it has systematized the already existing approach. Compared to the European, the UK legislative proposals are generally shorted and less detailed, thus leaving more discretion to the courts.

Unlike other compared jurisdictions, Russia has not yet adopted any legal acts regulating rights to data or access to data concerning the private parties and markets for data in the wake of strategic documents. Neither are there any legislative proposals at a meaningful stage of development that would address these issues. The detailed contents of the new Russian federal project “Data Economy” is yet to be defined, however, judging by its structure, it addressed primarily two types of issues: development of particular

data-related technologies and enhancement of use of data in public administration and provision of state services.

There have been several proposals relating to developing a legal regime of data in the academic literature. However, no unified position was formalized by the scholars, and none of the proposals matured into draft legislation. Despite the high development of various digital services in Russia, the issue of user access to data and its further reuse in the economy must be carefully considered by the legislator or in the scientific literature. From this point of view, the Russian legislation lags behind the EU and UK in terms of maturity, even though at the level of strategic documents on data, the need to improve data accessibility is also indicated.

It should be noted that the lack of development of legislation in commercial data circulation (in particular, regulation of granting access to data to private individuals and private businesses) does not prevent development towards the use of data by public authorities. The rhetoric of several federal projects related to data and the digital economy is primarily aimed at technological development and achieving public goals through data. The new federal project dedicated to data also names 'Digital platforms in public administration' as one of the key directions. Thus, the implementation of Russian strategic documents is primarily aimed at achieving state interests, which differs significantly from the approaches of the EU or the UK.

There is no objective to increase data availability for businesses. However, this could be a side-effect if the state initially accumulates this data and then, if necessary, can provide it to businesses on request. It is not only about the data generated during public activities but also about the data provided by the business. Thus, the state plans to act as an intermediary and, possibly, as a 'trading platform' of business data.

Also, Russia is very technically orientated. The project is primarily aimed at technology development and import substitution. The new project specializes in developing technological solutions in specific areas, for example, artificial intelligence, cloud services, cybersecurity, etc.[66] As the Russian Ministry of Digitisation explains, the new national project “Data economy” “will provide for data collection, including using highly sensitive sensors based on quantum sensors, data transmission, creation of computing and data storage infrastructure using domestic equipment, ensuring data security, including using quantum encryption technology, and obtaining information in real time”.[67]

In general, the policy of the Russian Federation is characterized by a strong focus on public rather than private interests in the field of data use and technologisation, with emphasis on the development of data technologies rather than on the development of the

[66] R Spectr, ‘Structure of the National project “Data Economy” <rspectr.com/novosti/predstavlena-struktura-naczproekta-ekonomika-dannyh?ysclid=m321xb23nz399565880> accessed 09 November 2024.
[67] ‘On the new project “Data Economy”’ (*Portal26km.ru*) <portal26km.ru/articles/obzor/o-novom-natsproekte-ekonomika-dannykh/?ysclid=m321o7m4wj455328312> accessed 09 November 2024.

data market. On the other hand, it is evident that the development of the market in this area requires the development of technologies and can even be mediated by it.

It can be concluded that the EU, having proclaimed empowering individuals as one of its key objectives, continues its trend in the new regulation of machine-generated data to fight international data-driven corporations primarily through breaking their data monopolies and limiting their powers to use the data from EU users. On the other hand, the UK pursues a different policy, focusing on moderate regulation of the data market and creating a regulatory model to ensure the most active circulation of data in the economy without being too burdensome for business. Russia, in turn, focuses on data availability to meet the needs of state bodies and administration. In contrast, legislation concerning the market circulation of data between private individuals has mostly stayed the same since it was initially adopted.

As a matter of policy, though compared jurisdictions have strategic documents on data based more or less on the same level of understanding of the importance of data governance for the economy, further analysis shows significant differences in priorities, which would likely have different impacts on data markets.

5 Conclusion

The existence of strategic documents in the data field in three jurisdictions, the EU, the UK, and Russia, demonstrates that the governments have started acknowledging the critical importance of data governance for future development, irrespective of the political or economic models. This hints that shortly, we may see the adoption of strategic documents on data by many other countries, including developing ones, as they will follow the example.

The high-level goal that can be read out of all the compared strategic documents is to enhance economy and governance by applying the new data-extensive technologies. In turn, it requires an increase in the amount and quality of accessible data and the development of the relevant technologies. This understanding is unified across the compared jurisdictions.

Still, compared jurisdictions differently formulate particular policy goals and emphasize the interests of different interested groups at the strategic level. The EU tends to protect the interests of individuals, in some cases – even at the expense of businesses. The UK is intensely focused on the interests of businesses, including the convenience of operating in the country and the clarity of legal provisions. Conversely, Russia concentrates mainly on the interests of public authorities and better public services.

As for the legislation adopted in the wake of the data strategies, the EU is most active in this area, as it has adopted at least four vast and important acts dealing with various goals set in the strategy: DGA, DMA, DSA, and DA. Though they address various aspects of data governance, their essential feature is rebalancing the "data market". These acts aim

to change the de facto situation on data access and use by authorizing new actors (individuals, users, and partially the governments) to access the data while prohibiting or limiting the use by other actors. The UK, alternatively, opts to legally provide access to data to a broader range of interested parties without limiting the de facto data holders. Though the UK acts on data governance are yet to become legislation, judging by the existing legislative proposals, no new limitations on businesses relating to the data they hold are to be implemented. As for Russia, it has yet to adopt any new laws to amend the existing legal regime for data based on the available strategic documents. However, existing regulations regarding data in the commercial sphere will likely remain the same, as the strategic document is mainly oriented to the public use of data and the development of particular technologies. So far, Russia has not created any new regulations for the relationship between private parties concerning data.

Thus, for Russia, the interests of the state in accessing and using the data prevail in the current policy. As a result of data collection, the state may improve its services and serve as a mediator, or data marketplace, for the businesses. The UK prioritizes business development interests, including attracting data-extensive business to the country by creating unburdensome and effective regulation. The EU in trying to balance the interest of all the three groups of actors, on the one hand, gives more protection to the individuals, but on the other, may hinder data-extensive businesses by too strict requirements and complicated regulatory model.

The EU and the UK approach is based on a similar premise: to increase access to data and grant additional data rights to users. They follow the general trend of protecting the rights of individuals, which continues to evolve across Europe with the development of new technologies and the legislation governing them. However, the UK's approach aims to develop the data market and create optimal conditions for data trading, including for foreign partners. In the European Union, a company operating with data will have to face many requirements and restrictions resulting from the extensive legislation on different data types in recent years. Therefore, in forum shopping, foreign businesses, mutatis mutandis, are likely to prefer the UK due to its more beneficial approach. It will give the UK a competitive advantage by reducing legislative barriers to its business and attracting foreign companies for which European requirements would be too onerous to fulfill. Russia does not impose such onerous restrictions on the use and circulation of data. Still, the lack of regulation and its apparent focus primarily on the interests of the state administration, all other things being equal, make the jurisdiction less attractive as a data market. The significant role of the state in data regulation processes also does not exclude the emergence of burdensome business requirements in data handling and reporting.

The UK has chosen the most favorable and balanced model from the point of view of data market development and trade in data. This model will promote domestic business development and increase the country's attractiveness as a trading partner. The approaches in other comparable jurisdictions are less likely to achieve this goal.

Elisabetta Nunziante[*]

HOW THE EU DATA STRATEGY CAN FOSTER THE GROWTH OF AGRI-TECH MARKET

Abstract

The European Union (EU) has adopted a proactive approach in regulating the data economy, aiming to promote innovation and address competition concerns. The Data Act and the Data Governance Act are two key regulations in this field. The interconnection between the Data Act and the Data Governance Act is particularly significant in the agricultural sector, where data plays an increasingly important role in optimizing production processes and enhancing sustainability. This article examines the potential impacts of the European Union's European Data Strategy, addressing key challenges in the digital transformation of the agricultural sector, with a focus on the interaction between the Data Act and the Data Governance Act. The agricultural sector is increasingly reliant on emerging technologies such as the Internet of Things (IoT), big data, and artificial intelligence (AI), generating vast amounts of "agri-data" with significant potential to enhance productivity, efficiency and sustainability. However, critical issues related to data access, sharing, and trust hinder the sector's progress, including farmer data lock-in, fragmentation of data sets, unmet access needs for key stakeholders, and farmers' reluctance to adopt digital technologies due to trust concerns. The article explores how the Data Act can mitigate farmer lock-in by mandating access to data generated by agricultural machinery and services, while the Data Governance Act fosters trust through rules for data intermediaries, including data cooperatives. Furthermore, it analyses the broader societal benefits of these regulations, such as promoting innovation to address climate change and improve food security through enhanced data access and analysis. Provisions enabling government access to agricultural data are highlighted as a means of improving public policy responses to climate challenges. Furthermore, the article also critically evaluates potential weaknesses of the regulations, including ambiguities in definitions under the Data Act, practical challenges in implementing the Data Governance Act, and the financial and administrative burdens on the agricultural sector. It concludes by emphasizing that the success of these legislative measures depends on their proper implementation and adaptation to the specific needs of the agricultural sector. The discussion closes with recommendations for additional regulatory and legislative refinements to unlock the full potential of digital agriculture

JEL CLASSIFICATION: K1, K2, Q1

SUMMARY

1 Methodology and Scope of analysis – 1.1 Market failures which prevent development of Agri-tech – 1.2 Legal regimes for agricultural data - 2 The impact of Data Act and the Data Governance Act on Agri-tech sector - 2.1 Data Act: Access to the data collected by devices and services of Internet of Things - 2.2 Data

[*] Elisabetta Nunziante is a lawyer qualified in Italy who has specialized in Information technology, media and telecommunication law, data management and data protection. In 2017, she obtained a LLM at King's College London in Intellectual Property and Information law.

 DOI 10.13135/2785-7867/11805

Governance: cooperatives and intermediaries – 3 Can Agri-tech benefit the society at large? – 4 Weaknesses of the EU Digital Strategy acts – 5 Conclusions

1 Methodology and Scope of Analysis

The agricultural sector is undergoing a digital transformation, with the increasing use of technologies such as the Internet of Things (IoT), big data, and artificial intelligence (AI). These technologies generate enormous amounts of data, known as "agricultural data" or "agri-data," which have the potential to improve productivity, efficiency, and sustainability of agricultural practices. However, access to and sharing of this data have become critical issues, leading to discussions on data ownership, privacy, competition, and innovation.

Precision agriculture technologies, such as sensors, drones, and GPS, generate large amounts of data that, when aggregated and analysed, can greatly enhance efficiency and sustainability across the industry. For example, data collected from different stages of agri-food production can inform more precise use of fertilizers, pesticides, and water according to the specific needs of crops and animals.[1] This approach can reduce waste and lower environmental impact by minimizing excessive use of substances that contribute to pollution.[2]

Data sets on climate projections, weather forecasts, water models, and crop-specific information at the individual farm level can be combined to improve and guide investment decisions, as well as to help mitigating the effects of climate change.[3]

Furthermore, real-time data collected through sensors and connected tools can enhance decision-making for farmers and stakeholders across the value chain.[4] When aggregated in pools, agricultural data can reveal and investigate patterns and connections maximising the sector's operational and strategic efficiencies.[5]

[1] Marie Jouanjean, Filippo Casalini, Louise Wiseman and Emily Gray, 'Issues Around Data Governance in the Digital Transformation of Agriculture: The Farmers' Perspective' (2020) OECD Food, Agriculture and Fisheries Papers No 146, OECD Publishing, 6.

[2] Benjamin Kisliuk, Jan Christoph Krause, Hendrik Meemken, Juan Carlos Saborío Morales, Henning Müller and Joachim Hertzberg, 'AI in Current and Future Agriculture: An Introductory Overview' (2024) 37 KI - Künstliche Intelligenz 117.

[3] Ajit Maru, Dan Berne, Jeremy De Beer and others, 'Digital and Data-Driven Agriculture: Harnessing the Power of Data for Smallholders' [2018] F1000Research 7:525 (version 1; not peer reviewed) <https://doi.org/10.7490/f1000research.1115402.1> accessed 2 November 2024.

[4] Maaz Gardezi, Bhavna Joshi, Donna M Rizzo, Mark Ryan, Edward Prutzer, Skye Brugler and Ali Dadkhah, 'Artificial Intelligence in Farming: Challenges and Opportunities for Building Trust' (2023) Agronomy Journal 1217-1228.

[5] Airong Zhang, Richard Heath, Katie McRobert, Rick Llewellyn, Jay Sanderson, Leanne Wiseman and Rohan Rainbow, 'Who Will Benefit from Big Data? Farmers' Perspective on Willingness to Share Farm Data' (2021) 88 Journal of Rural Studies 346; Katrin Martens and Jana Zscheischler, 'The Digital Transformation of the Agricultural Value Chain: Discourses on Opportunities, Challenges and Controversial Perspectives on Governance Approaches' (2022) 14 Sustainability 3905; Andrew Slade, 'Digital Agriculture: Farming in the Digital Age' (2020) A Report for Nuffield Australia Farming Project, <https://www.nuffieldscholar.org/sites/default/files/reports/2018_AU_Andrew-Slade_Digital-Agriculture-Farming-In-The-Digital-Age.pdf> accessed 15 November 2024.

Additionally, improved data utilization enables consumers to track the source and production stages of their food, with beneficial impacts on food safety.[6]

Agri-tech's influence extends to rural economies and community well-being, an area with significant public policy implications particularly impacting the job offer.[7]

The aggregation of data would significantly benefit the numerous small and medium enterprises (SMEs) of the sector, though they have fewer resources to participate effectively in this market. Precision farming and smart agriculture strongly depend on the free circulation of data to achieve high levels of operational efficiency, strategic decision-making and resource optimization.

As mentioned, Agri-tech innovations frequently produce positive externalities, such as environmental positive impacts that benefit society at large. However, the lack of mechanisms to capture these public goods can discourage investments in these technologies.

Conversely, negative externalities, such as dependency on costly proprietary technologies, place financial burdens on farmers, particularly those with limited resources. These externalities create a scenario where the costs and risks associated with Agri-tech adoption are disproportionately borne by individual farmers, reducing incentives for broader adoption across the agricultural sector.

Moreover, data-driven approach in agriculture introduces complex challenges regarding ownership rights and market power dynamics in agribusiness. Indeed, the shift toward data-driven agriculture raises issues that span social, economic, legal, and ethical dimensions.

Addressing these challenges requires robust governance frameworks, such as the EU's Data Act (Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data),[8] to regulate data access and ensure that AI-driven innovations contribute to sustainability goals while fostering trust among stakeholders.

Additionally, AI is poised to redefine agriculture by promoting efficiency and sustainability, but its success depends on the resolution of socio-legal and technical challenges. This necessitates a collaborative approach to data governance and ethical AI deployment in the agricultural sector.

The first part of the article will focus on four fundamental issues identified as obstacles to the development of the Agri-tech sector:

[6] Marilena Gemtou, Blanca Casares Guillén and Evangelos Anastasiou, 'Smart Farming Technologies and Sustainability' in Theo Lynn, Pierangelo Rosati, David Kreps and Kieran Conboy (eds), *Digital Sustainability: Leveraging Digital Technology to Combat Climate Change* (Springer, 2024) 106.

[7] Gardezi and others (n 4).

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

- **Farmer data lock-in:** Farmers have little or no control over farm data after it is collected and face difficulties in changing providers because they cannot take their data with them.
- **Fragmentation of agricultural data sets and exclusive data exchange agreements**: Exclusive data control by first movers also limits the potential for data-driven innovation in emerging digital agriculture markets.
- **Unmet needs for access to agricultural data:** Other actors in the agricultural sector, such as small Agri-tech providers, machinery manufacturers, landowners, and banks, need access to agricultural data and suffer from the lack of a clear path to obtain it.
- **Lack of trust from farmers:** Farmers fear losing control after sharing data, negatively affecting their willingness to adopt digital agriculture technologies.

In its second part, the article aims to analyse how the Data Act and the Data Governance Act can address the identified barriers to the development of digital agriculture. Particularly, the article will analyse how:

- The Data Act addresses concerns related to farmer lock-in with specific technology providers, by ensuring access to data generated by agricultural machinery and related digital services;
- The Data Governance Act contributes to creating a trustworthy environment for sharing agricultural data by defining rules for data intermediaries, including data cooperatives.

In its third part, the article will delve into how the Data Act and the Data Governance Act (Regulation (EU) 2022/868 on European data governance)[9] could have positive effects on the public at large, beyond having an impact on the efficiency of the agricultural sector. Indeed, the Data Act and the Data Governance Act could have a positive impact on climate change and food availability issues, mainly by promoting innovation in the agricultural sector. Particularly, three aspects will be analysed to that respect:

- **Access to and sharing of data:** Access to and sharing of data can lead to the development of more efficient digital agricultural technologies.
- **Analysis of large agricultural data sets**: The analysis of large agricultural data sets can lead to a better understanding of climate change and its impact on food production.
- **Government access provisions in the Data Act:** The Data Act's provisions regarding government access could also enable more efficient public policies to counteract the effects of climate change, such as droughts and floods.

In its fourth part, the article will focus on the potential weaknesses of the Data Act and the Data Governance Act in addressing the challenges of the digital agricultural sector and

[9] 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 [2022] OJ L 152.

the hurdles the latter will have to overcome to benefit from the potential of these regulations. In particular, the article will assess whether definitions such as "product," "related service," and "user" in the Data Act are sufficiently broad to cover all types of agricultural data, including those generated by sensors, machines, and other sources. On the other hand, the analysis will focus on some provisions of the Data Governance Act, such as the notification requirement, which could prove impractical and require further clarification.

In the conclusions, the article will emphasize that the effectiveness of the Data Act and the Data Governance Act will depend on their proper implementation and the ability to address the specificities of the agricultural sector. It will also evaluate possible regulatory and legislative solutions that could overcome the identified obstacles.

1.1 Market failures which prevent development of Agri-Tech

Market failures present a major barrier to Agri-tech development. Such market failures include high initial costs, restricted data accessibility, and the lack of sufficient incentives for technology adoption. These issues create economic obstacles that disproportionately affect SMEs and independent farmers, making it difficult for them to adopt advanced agricultural technologies.

The high costs associated with Agri-tech solutions are among the primary market failures impeding the sector's growth. Advanced technologies like IoT sensors for monitoring soil conditions, drones for precision agriculture, and data processing platforms require significant initial investments. These costs often prevent smaller farms and SMEs from adopting such technologies, leading to an uneven distribution of Agri-tech benefits.[10]

This economic disparity results in a concentration of Agri-tech adoption among larger agribusinesses, leaving smaller entities to rely on less efficient, traditional farming methods. Another factor that discourages adoption is the extended return-on-investment (ROI) period, due to the long payback, which discourage small farms from adopting Agri-tech solutions.[11] For example, while IoT devices and data analytics tools can reduce water and pesticide usage over time, the initial costs are often prohibitive, especially for farmers operating on tight budgets.

One of the main causes of such phenomenon is believed to be the first-mover advantage of tech providers and the lack of a clear framework on data ownership and access for different participants in the sector.[12] According to such opinion, as few big corporations

[10] Beatrice Garske, Antonia Bau, and Felix Ekardt, 'Digitalization and AI in European Agriculture: A Strategy for Achieving Climate and Biodiversity Targets?' (2021) 13 Sustainability 4652.
[11] Evagelos D Lioutas, Chrysanthi Charatsari, Giuseppe La Rocca and Marcello De Rosa, 'Key Questions on the Use of Big Data in Farming: An Activity Theory Approach' (2019) 90-91 NJAS - Wageningen Journal of Life Sciences; Gardezi and others (n 4).
[12] Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector' (2022) TILEC Discussion Paper No DP2022-013, 4.

control the data required to ignite the full power of Agri-tech solutions, small players are cut off the possibility to compete or innovate for the benefit of the whole sector.

The absence of clear frameworks has fuelled widespread concern that unrestricted access to data by manufacturers and agricultural technology companies can stifle competition, ultimately hindering innovation in data-driven agriculture.[13] Indeed, the availability of large data sets has been considered a crucial aspect of competition, as evidenced in the Bayer-Monsanto case.[14]

Furthermore, the lack of interoperability strengthens the position of certain technology operators due to network effects and positive feedback loops, while also hindering data-driven innovation.[15] Proprietary data systems compound this problem by limiting interoperability between platforms, thus restricting data flow across different systems. The lack of interoperability often forces farmers to rely on a single provider's ecosystem, increasing dependency on specific technology providers and reducing flexibility. As a result, proprietary data systems not only inhibit competition but also limit the potential for integrated, cross-platform data solutions essential for comprehensive agricultural management.

Moreover, data sharing in the agricultural sector is also hindered by its fragmented structure. The agricultural sector not only includes farmers, processors, manufacturers, and retailers but also requires interaction with logistics operators, banks, insurance companies, and producers of fertilizers and related products.[16]

Data fragmentation and proprietary control has been a critical bottleneck, preventing farmers from accessing and utilizing data generated by their own machinery and equipment.[17]

However, notwithstanding the value of the causes identified above, the most significant barrier to the development of digital agriculture is the lack of awareness and trust among farmers.[18] Studies have shown that many farmers are unaware of their rights regarding

[13] Michael E Sykuta, 'Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services' (2016) 19 International Food and Agribusiness Management Review 57; Hugh F Williamson and Sabina Leonelli (eds), *Towards Responsible Plant Data Linkage: Data Challenges for Agricultural Research and Development* (Springer 2023).

[14] According to the Commission "*Digital agriculture refers to the collection of data and information about farms with the aim of providing tailored advice or aggregated data to farmers to increase farm productivity. Additionally, the Commission considers that: (iv) digital agriculture, including digitally-enabled prescriptions, is characterised by first mover advantage*". Summary of Commission Decision of 21 March 2018 declaring a concentration compatible with the internal market and the functioning of the EEA Agreement (Case M.8084 — *Bayer/Monsanto*) (notified under document number C (2018) 1709) paragraphs 59 and 129.

[15] Atik (n 12); Leanne Wiseman, Jay Sanderson, Angela Zhang, and Emma Jakku, 'Farmers and Their Data: An Examination of Farmers' Reluctance to Share Their Data Through the Lens of the Laws Impacting Smart Farming' (2019) 90-91 NJAS: Wageningen Journal of Life Sciences 6-7.

[16] Atik (n 12); Imad Antoine Ibrahim and John Mark Truby, 'FarmTech: Regulating the Use of Digital Technologies in the Agricultural Sector' (2023) 12(4) Food and Energy Security <https://onlinelibrary.wiley.com/doi/10.1002/fes3.483> accessed 2 November 2024.

[17] Sykuta (n 13).

[18] Atik (n 12).

data, as well as the extent to which technology providers can access it.[19] Smart Agri-tech devices are largely regulated by standard data licenses unilaterally drafted by tech providers, resulting in bargaining imbalances and information asymmetry.[20]

This knowledge gap leads to a reluctance among farmers to share data, as they fear companies may manipulate it to their detriment, for example, by increasing commodity prices or tech service fees.[21] While farmers recognize the potential of the data they collect, they do not fully understand the value proposition for accessing and using on-farm data. They are also concerned that they may lose control over their data if they share it with multiple recipients.[22] Ultimately, this lack of trust can also be attributed to the absence of business models that provide immediate financial returns to farmers, thereby justifying investments in this field.

1.2 Legal regimes for agricultural Data

The issues that hinder the full development of the digital agriculture sector call for an improved governance framework for data. One of the primary legal challenges in Agri-tech is the ambiguity surrounding data ownership. Data generated by IoT devices, drones, and sensors in agricultural settings often involves multiple stakeholders, including farmers, technology providers, and data processors. This lack of clarity makes it difficult to establish mutually beneficial data-sharing arrangements, as stakeholders are hesitant to invest in data generation and sharing without assurances regarding ownership rights. For example, a farmer using IoT-enabled equipment may lack control over the data produced, as the technology provider could claim ownership under proprietary agreements, creating further disincentives for adoption.

A first attempt to address these issues has been made by industry stakeholders through tools of self-regulation. In 2018, a European Code of Conduct on data sharing though contractual agreement was approved by relevant organizations in the sector.[23] While non-binding, the Code of Conduct highlights the aspects deemed most relevant by concerned stakeholders: data ownership, data access, and portability. This Code marks an important starting point for the development of agricultural technologies, demonstrating that farming companies are willing to share data if a clear framework of rights and obligations is in place. The Code of Conduct advocates for a solution in which farmers retain

[19] Wiseman and others (n 15); Liliana Fadul-Pacheco, Steven R Wangen, Tadeu E da Silva and Victor E Cabrera, 'Addressing Data Bottlenecks in the Dairy Farm Industry' (2022) 12 Animals 721.
[20] Atik (n 12); Ibrahim and Truby (n 16); Gardezi and others (n 4).
[21] Slade (n 5); Atik (n 12); Ibrahim and Truby (n 16).
[22] Emma Jakku, Bruce Taylor, Aysha Fleming, Claire Mason, Simon Fielke, Chris Sounness, and Peter Thorburn, 'If They Don't Tell Us What They Do with It, Why Would We Trust Them? Trust, Transparency and Benefit-Sharing in Smart Farming' (2019) 90-91 NJAS: Wageningen Journal of Life Sciences 1-13.
[23] EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement (CEMA, 2019) <https://www.cema-agri.org/images/publications/brochures/EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_update_2019.pdf> accessed 2 November 2024.

ownership of the (non-personal) data they generate, with the right to share it with third parties and, at the same time, object to its use by providers.

While farmers are likely to consider the data they generate as their property, applying a traditional ownership model to data is challenging.[24] Identifying the owner of data in the agricultural sector is complex, as the value chain involves multiple players such as the landowner, the farmer, and the machinery producer.[25] Indeed, the debate on fostering digital agriculture has been centred, for long time, around data "ownership" and the allocation of proprietary rights between farmers and machinery producers.[26]

Extending ownership rights over non-personal data has been criticised as an ineffective solution for the market failures identified above, as it does not address negotiation imbalances and, therefore, risks consolidating dominant positions by granting stronger rights to first-mover tech giants.[27] Indeed, the creation of proprietary rights over non-personal agricultural data would not effectively address disparities in negotiation power.

The inability to influence power asymmetry in the agriculture market was, consequently, the main shortcoming of the Code of Conduct, which relied on data-sharing agreements without acknowledging that much of the mistrust in data-sharing mechanisms stems from farmers' difficulties in negotiating data-sharing clauses. Some commentators also proposed that a data commons framework could be established to democratize access to agricultural data, enabling farmers to retain agency over their contributions while also promoting data sharing.[28]

However, focussing on the issue concerning the ownership of data proved to be useless to effectively regulate the market.[29] Data cannot be subject to strictly intended property rights as such approach would result in exclusive rights on information.[30] The European Union has been reluctant to create new exclusive, proprietary-like rights on data due to its non-rivalrous nature, preferring approaches based on data access rights rather than ownership.[31] Even the database rights provided by Directive 96/9/EC on the legal protection of databases is connected to the protection of investments and efforts behind the organisation of database rather than on the protection of data therein contained.

[24] Simon Geiregat, 'The Data Act: Start of a New Era for Data Ownership?' (2022) SSRN <https://ssrn.com/abstract=4214704 or http://dx.doi.org/10.2139/ssrn.4214704> accessed 12 November 2024.
[25] Joan K Archer and Cordero A Delgadillo, 'Key Data Ownership, Privacy and Protection Issues and Strategies for the International Precision Agriculture Industry' (2016) <https://hbfiles.blob.core.windows.net/files/2f53c518-a374-460f-a40e-a82ace4b8605.pdf> accessed 2 November 2024.
[26] Jouanjean and others (n 1).
[27] Can Atik, 'Towards Comprehensive European Agricultural Data Governance: Moving Beyond the "Data Ownership" Debate' (2022) 53 International Review of Intellectual Property and Competition Law 709–714.
[28] Jeremiah Baarbé, Meghan Blom and Jeremy de Beer, 'A Proposed Agricultural Data Commons in Support of Food Security' (2019) 23 The African Journal of Information and Communication 1.
[29] Josef Drexl, Carolina Banda, Begona Gonzalez Otero, Jörg Hoffmann, Daria Kim, Shraddha Kulhari, Valentina Moscon, Heiko Richter and Klaus Wiedemann, 'Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition, Research Paper No 22-05 <https://ssrn.com/abstract=4136484 or http://dx.doi.org/10.2139/ssrn.4136484> accessed 2 November 2024.
[30] Geiregat (n 24).
[31] Drexl and others (n 29).

An additional issue concerning agricultural data regulation is identify a taxonomy which can serve as structured framework for understanding the diverse types of agricultural data while highlighting their interrelatedness and critical role in the digital transformation of agriculture. Agricultural data encompass a broad spectrum of information, making its categorization challenging and inherently non-exhaustive. The EU Code of Conduct on agricultural data sharing identifies five key categories of agricultural data, each reflecting the diverse facets of modern farming practices. These categories include:

1. **Farm Data:** This category includes agronomic data (e.g., soil conditions, crop yields), compliance-related data (e.g., records for regulatory purposes), and livestock data (e.g., health and productivity metrics).
2. **Machine Data:** Generated by system controllers and machine sensors, this includes performance metrics and operational data from agricultural machinery.
3. **Service Data:** Covers information related to maintenance and repair activities of agricultural vehicles and equipment.
4. **Input Data:** Supplied by farmers, this includes data on the types, quantities, and application methods of inputs such as pesticides, fertilizers, and seeds.
5. **Agricultural Service Provider Data**: Includes operational information, such as employee working hours and service logs, collected by external service providers.[32]

From a different perspective, a widely referenced categorization stems from the Bayer-Monsanto case, as outlined by the European Commission:

Farm Data: These are collected either through sensors and machines or directly provided by farmers themselves. Examples include soil moisture levels, crop yields, and livestock health data.

Complementary Data: Supplied by specialized third-party providers, this category includes external information such as maps, soil composition data, and weather forecasts, which complement on-farm data.

Proprietary Data: This refers to data generated by or associated with the products and tools provided by data analysis providers, such as algorithms, proprietary models, or diagnostic outputs specific to their systems.[33]

Another perspective categorizes agricultural data based on the processes underlying their collection. This classification identifies three distinct types of data:

1. **Machine-Generated Data:** Data collected automatically through sensors embedded in machines, drones, or GPS devices. These data sources provide real-time, precise measurements, such as soil moisture, machine performance, or spatial mapping.

[32] Code of Conduct on Agricultural Data Sharing by Contractual Agreement (n 21).
[33] Paolo Guarda, 'Riflessioni in merito alla natura giuridica dei dati nell'agricoltura di precisione: un'interpretazione teleologicamente orientata' (2023) Rivista di Diritto Alimentare, Quaderno n. 1-2023, 20-35.

2. **Process-Mediated Data:** Data generated as a byproduct of business processes on farms, such as purchase records, sales transactions, or order histories, reflecting the operational and commercial aspects of farming.
3. Human-Sourced Data: Data recorded manually by individuals, such as farm logs or field notes, which are later digitized for analysis and integration into digital systems.[34]

These classifications underscore the diverse origins of agricultural data and the collaborative ecosystem in which farmers, technology providers, and external experts interact with varying levels of automation and digitization involved in the process. The fragmented nature of data involved in agritech processes serves a critical function in determining the appropriate regulatory framework to govern its access and sharing.

Most data involved in such processes are categorized as non-personal data.[35] Prior to the adoption of the Data Act, these data sets were not subject to comprehensive regulatory oversight. The Regulation (EU) of 2018/18017, on the free flow of non-personal data, while a step forward, had a limited scope and left many critical aspects to self-regulation by industry stakeholders.[36] Indeed, prior to the approval of the Data Act, self-regulation played a pivotal role in governing (non-personal) data access and sharing. In the agricultural sector, the abovementioned EU Code of Conduct on Agricultural Data Sharing was particularly influential. The Code was rooted in the principle of data ownership based on the origination of the data.[37] According to the Code of Conduct, contractual agreements were required to be transparent and fair. These agreements emphasized the originator's control over the data, granting them the authority to permit access, share data with third parties, and even terminate data processing when deemed necessary. This framework aimed to establish trust among stakeholders while protecting the interests of data originators. However, the EU Code of Conduct on Agricultural Data Sharing was purely voluntary in nature, lacking any binding legal force. In this context, although on a horizontal level, the Data Act addressed a significant gap in the regulatory framework, providing a more robust and structured approach to governing the access and sharing of non-personal data.

While data strictly related to farming activities generally fall outside the scope of personal data—being more closely linked to soil and environmental conditions—connected vehicles, for instance, may collect usage data, GPS and location data that qualify as

[34] Can Atik and Simone van der Burg, 'Report on the Topic of Possible Implications of the EU Data Act on IoT Implementation and Data Practices in Arable Farming' (2023) Tilburg University, <https://edepot.wur.nl/685372> accessed 26 January 2025.
[35] Recital 9 Regulation (EU) of 2018/18017 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 states that "*Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines*".
[36] Leanne Wiseman, Jay Sanderson, Airong Zhang and Emma Jakku, 'Farmers and Their Data: An Examination of Farmers' Reluctance to Share Their Data Through the Lens of the Laws Impacting Smart Farming' (2019) 90-91 NJAS - Wageningen Journal of Life Sciences 100289.
[37] Ibrahim and Truby (n 16).

personal.[38] Other examples of personal data processed by agribusiness include commercial records and camera recordings. Moreover, the aggregation of various data sets, such as those related to production and machine usage, may enable machine service providers to infer insights about the socio-economic conditions of the farmer.[39] Indeed, if technological tools make it possible to turn anonymised/aggregated data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 ("GDPR") is to apply accordingly. While farmers often operate as legal entities and are, thus, their data are outside the scope of the GDPR, it cannot be excluded that some farming activities are carried out at an individual level by solo entrepreneur. In such cases, the data may qualify as personal data, bringing it within the ambit of GDPR protections. Indeed, mixed datasets are typically regarded as subject to the GDPR, due to the stringent criteria applied to determine whether data has been effectively anonymized.

The Data Act and GDPR operate in a complementary manner, with the GDPR providing a robust regulatory framework for the processing, protection, and governance of personal data, while the Data Act establishes harmonized rules for the access, use, and sharing of non-personal data. Together, these instruments create a comprehensive regulatory architecture aimed at addressing the multifaceted challenges of data governance in a rapidly evolving digital landscape.

The collection of data related to agricultural vehicles poses significant challenges, such as identifying a lawful basis for processing, particularly within the context of employment relationships, and ensuring the exercise of data subjects' rights. As a result, data sharing might sometimes require a thorough inventory of personal and non-personal data, a process that can become particularly challenging when dealing with large datasets. This undertaking often demands considerable effort from companies, including those in the agricultural sector.

Moreover, the collection of data from terminal devices is governed by the Directive 2002/58/EC ("e-Privacy Directive"), which requires consent unless the data is necessary for providing an information society service. However, obtaining freely given consent can be problematic. A refusal to consent may compromise the exhaustiveness of the dataset, while, conversely, consent might not be considered freely given in situations involving power imbalances, such as in employer-employee relationships. Furthermore, in employment contexts, the monitoring of employees may invoke additional legal constraints, including prohibitions on certain types of surveillance.

The stringent legal requirements governing personal data impose demands for knowledge and resources that are often beyond the reach of farmers and agricultural enterprises.[40] Farmers and agricultural companies are, often, faced with the obligation,

[38] Guarda (n 33), Wiseman and others (n 36).
[39] Wiseman and others (n 36).
[40] Mosiur Rahaman, Chun-Yuan Lin, Princy Pappachan, Brij B Gupta and Ching-Hsien Hsu, 'Privacy-Centric AI and IoT Solutions for Smart Rural Farm Monitoring and Control' (2024) 24(13) Sensors 4157.

either to comply with the requirements applicable to personal data or to ensure that such data are excluded from their datasets. This often necessitates the use of privacy-enhancing technologies, which are typically costly and complex to evaluate and implement. The lack of capacity exacerbates trust issues and discourages the adoption of new technologies in the agricultural sector.

While the relationship with GDPR remain an issue, the adoption of the Data Act and the Data Governance Act represents a significant step toward addressing these challenges, which are particularly pronounced in the realm of agricultural digital innovation. The Data Act, on one hand, fills the regulatory gap for non-personal data—such as farm data, machinery data, and environmental data—by establishing rights and obligations designed to empower companies contributing to data generation and empowering legal entities on rights over data that they contribute to generate. On the other hand, the Data Governance Act provides a framework for managing such data through collective mechanisms, enabling agricultural companies to address gaps in information, knowledge, and resources as well as to access to anonymization and interoperability tools with lower costs.

However, despite their promising rationales, both acts exhibit gaps and inconsistencies that could hinder their full potential and limit their effective implementation in the agricultural sector, as will be shown in part four of this paper.

2 The impact of Data Act and the Data Governance Act on Agri-Tech sector

The European Digital Strategy seeks to encourage data sharing to maximize its value while safeguarding public interests and fundamental rights.[41]

Common data spaces are at the heart of the EU Digital Strategy. These are structured environments designed to facilitate secure, regulated, and standardized data sharing among multiple stakeholders within specific sectors or domain.[42] The main objective of the European Union's Digital Strategy is to address barriers to the free circulation of data, enabling companies to access and use data easily and safely. Accordingly, the rationale behind the European Digital Strategy is that trustworthy and secure data flows can reduce data monopolies and foster the development of new services.

As explained extensively in paragraph 1, agricultural technology might enhance productivity, sustainability and efficiency in farming by relying on data.

The secondary use of data collected from agricultural technologies can improve service efficiency and support a green transition by reducing carbon footprints, optimizing energy consumption, and streamlining supply chains, water use, and pesticide application.

[41] Geiregat (n 24).
[42] Mark Ryan, Can Atik, Kelly Rijswijk, Marc Jeroen Bogaardt, Eva Maes and Ella Deroo, 'The Future of Agricultural Data-Sharing Policy in Europe: Stakeholder Insights on the EU Code of Conduct' (2024) 11 Humanities and Social Sciences Communications 1197.

The recent Data Act and Data Governance Act introduced by the European Union aim to facilitate data accessibility, portability, and trust among data users and providers—which are key factors to Agri-tech innovation.[43] By regulating access to IoT data and establishing frameworks for data intermediaries and cooperatives, these Acts seek to address the challenges posed by proprietary data silos, unequal bargaining power among stakeholders, and complex legal frameworks.

2.1 Data Act: access to the Data Collected by devices and services of Internet of Things

The Data Act is a key component of the European Digital Strategy, addressing issues of data access, portability, and contractual imbalances, particularly in the realm of IoT (Internet of Things). This regulation seeks to promote data access and control, regulating the sharing of data generated by connected devices and related services to reduce barriers to data flow that hinder innovation and competition. The Data Act, thus, has the potential to tackle lock-in effects, particularly in sectors such as agriculture, where IoT sensors and devices are widely used to monitor soil, crop health, weather, and equipment performance.

The Data Act, in Article 2, introduces a broad definition of "data", which includes both personal and non-personal data, encompassing *"any digital representation of acts, facts, or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*".

The Data Act leverages mechanisms of data access and data portability, allowing data generated within one IoT system to be transferred and used within another. Access and portability rights cover data obtained, generated or collected by a connected product, including information related to its performance, use environment, as well as data reflecting user actions, inactions and events collected during a service linked to a product that influences its functioning.

Article 3 mandates that manufacturers of connected products shall develop and provide their products and services with built-in mechanisms to ensure that data is made easily available to users for free. If direct access is not available, Article 4 requires any natural or legal person with rights to use and share data (known as "data holders") to make this data available without undue delay in a machine-readable format and, when technically feasible, in real-time.

[43] Recital 2 of the Data Governance Act explicitly mentions agricultural among the sector targeted by the European Digital Strategy by stating that *"In its communication of 19 February 2020 on a European strategy for data (the 'European strategy for data'), the Commission described the vision of a common European data space, meaning an internal market for data in which data could be used irrespective of its physical storage location in the Union in compliance with applicable law, which, inter alia, could be pivotal for the rapid development of artificial intelligence technologies […] as proposed in the European strategy for data, […] common European data spaces could cover areas such as health, mobility, manufacturing, financial services, energy or agriculture, or a combination of such areas, for example energy and climate, as well as thematic areas such as the European Green Deal or European data spaces for public administration or skills*".

The Data Act also considers the complexity of IoT device value chains, requiring sellers, renters, and lessors—whether they are the manufacturers or other entities—to provide users with clear and complete information on generated data. The transparency obligations of Article 3 seek to counter users' fear of losing control on data.[44]

This right would allow farmers using connected tools to access all data generated through their use, including metadata that aids in interpreting the data. As explained in recitals 15 and 16, the scope of data access is particularly wide, excluding only information that results from further enrichment or investment by data holders.

In addition to data access, Article 5 significantly extends the rights initially granted by Article 20 of the GDPR for personal data, empowering users to make data and metadata available to third parties and encompassing also data "generated" though the product or services.

The Data Act clearly regulates the obligations that data holders, when transferring data to third parties at the user's request, must follow. In particular, the Data Act establishes that the data sharing between data holder and third recipient shall comply with principles of fair, reasonable and non-discriminatory access (so called "FRAND" principles), a concept rooted in IP and competition law and also found in the Digital Markets Act.[45]

Chapter IV of Data Act also introduces a regulation on unfair clauses in business-to-business relationships concerning access to and use of data, modelled on the framework established for relationships between traders and consumers. The assessment of unfairness will cover all contractual clauses related to data access and use, as well as liability and remedies for breaches or termination of data-related obligations that are inconsistent with the principles of good faith and fairness and that deviate from sound commercial practices. Provisions on unfair B2B data sharing clauses, however, are not limited to relationships involving connected products and related services but apply more broadly to all B2B agreements regulating whose access and use to data. Thus, such provisions will have a wide impact on agricultural sector, covering also the sharing of those data which, as we will analyse in part four of this article, might fall outside the scope of data access and portability rights.

On the other hand, data recipients may use data only for defined purposes and modalities, without the ability to use it for profiling or share it with third parties unless otherwise agreed with the user. Furthermore, they cannot develop a product that competes with the connected product from which the accessed data originate or share the data with another third party for that purpose.

Similarly, data holders are prevented from using readily available data that is non-personal data for reasons other than those included in the contract and cannot share non-

[44] Gordian Konstantin Ebner and Marie Wienroeder, 'SME-Exemption (Art. 7), Product Design, Service Design, and Informational Duties (Art. 3)' in Moritz Hennemann and others (eds), *Data Act: An Introduction* (Nomos 2024).
[45] Benedikt Karsten and Gregor Lienemann, 'Right to Share Data with Third Parties (Art. 5-6) and FRAND Obligations for Data Holders When Providing Access (Art. 8-12)' in Moritz Hennemann and others (eds), *Data Act* (Nomos 2024).

personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user.

Conversely, data holder may refuse to share data to protect trade secrets. The nature of the new right established by the Data Act is still debated. While it has been argued that the limits imposed to data holders and third parties are such to create a type of ownership for the benefit of the user, other have argued that the rights of the data holder to refuse sharing data is strengthening its position of ownership on data.[46]

However, it can be argued that the Regulation does not aim to regulate data as a proprietary asset but as an essential resource that underpins competitive markets, social welfare, and technological innovation, thus equally balancing the positions of the different subjects involved.[47]

The rights of access and portability are especially relevant in the agricultural sector, as they allow farmers to access data produced by machinery, sensors, soil monitoring equipment, drones, and weather stations, enabling them to decide how and with whom their data is shared.[48] In this way, farmers and agricultural companies can make more informed decisions. Furthermore, portability rights allow them to exploit accumulated data and transfer it to other platforms without losing years of historical data, preserving the continuity and utility of valuable records.[49]

This is a transformative intervention, as it reduces dependency for small businesses and allows them to choose from a variety of services based on cost and quality.[50]

However, interoperability, defined as the ability of different systems, applications, and services to exchange, interpret, and process data, is essential to break down data silos both within and across sectors.[51] Data from a variety of sources—such as soil sensors and weather satellites—can have discrepancies in data formats, measurement units and standards. For instance, a farmer may use data from soil moisture sensors, weather forecasts, and crop growth models to determine optimal irrigation and fertilization schedules. Without interoperable systems, such data remains siloed within specific applications, limiting its usefulness and making it more difficult for farmers to make

[46] Geiregat (n 24).
[47] Karsten and Lienemann (n 45).
[48] Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector'(2022) Tillburg Law School Research paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144737>; Christopher John Rawlings and Robert P Davey, '*From Farm to FAIR: The Trials of Linking and Sharing Wheat Research Data' in* Hugh F Williamson and Sabina Leonelli, *Towards Responsible Plant Data Linkage: Data Challenges for Agricultural Research and Development (Springer, 2022) 107-123.*
[49] Josef Drexl, 'Data Access and Control in the Era of Connected Devices: Study on Behalf of the European Consumer Organisation BEUC' (2018) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 2 November 2024.
[50] EIP-AGRI Workshop, 'Data Sharing: Ensuring Fair Sharing of Digitisation Benefits in Agriculture', Final Report (2017) 7 <https://ec.europa.eu/eip/agriculture/sites/default/files/eip-agri_workshop_data_sharing_final_report_2017_en.pdf> accessed 2 November 2024.
[51] Can Atik, 'Understanding the Role of Agricultural Data on Market Power in the Emerging Digital Agriculture Sector: A Critical Analysis of the Bayer Monsanto Decision' in David Bosco and Michal S Gal (eds), *Challenges to Assumptions in Competition Law* (Edward Elgar Publishing, 2021) 41-78.

informed decisions.[52] Recital 103 acknowledges the importance of addressing issues of standardization and semantic interoperability to facilitate common data spaces, assigning the Commission a role in prioritizing these aspects and issuing common specifications when needed.

Article 33 of the Data Act emphasizes transparency and data accessibility, requiring detailed descriptions of data formats, structures, and access methodologies to facilitate dataset exchange and usage across various sectors and entities.[53]

Moreover, the Data Act also introduces provisions which may help to create a trustworthy environment, addressing farmers' concerns. Indeed, data holders cannot use such data to derive insights about the economic situation, assets and production methods of, or the use by, the user or the third party in any other manner that could undermine the commercial position of that user or third party on the markets in which they are active. Similarly, third party recipients are prevented from carrying out such activities to the detriment of data holders

In so far, the Data Act limits the way data are processed to create an environment in which data are used transparently and fairly, with a multifaceted approach which considers every involved subject. Such approach may thus be able to address the lock of trust on data flows and data sharing which, as argued above, is one of the main barriers for a wider recourse to such technologies.

2.2 Data Governance: cooperatives and intermediaries

The Data Governance Act complements the Data Act by introducing a new regulation of data intermediaries: trusted entities that facilitate data-sharing between parties while ensuring security, compliance and data quality.

In Agri-tech, where data sharing among farmers, suppliers and researchers is essential, the Data Governance Act may help overcome the lack of trust in data transactions, especially from smaller actors in the agricultural sector.

A "data intermediation service", as defined, in Article 2 paragraph 11 of the Data Governance act, refers to a service designed to facilitate commercial relationships for data sharing between an undefined number of data subjects and data holders, on one side, and data users, on the other. This facilitation can involve technical, legal, or other mechanisms, including supporting data subjects in exercising their rights related to personal data.

Intermediaries help ensure that data exchanges meet regulatory requirements, thereby increasing the reliability and accessibility of shared data for various stakeholders. In

[52] Baarbé and others (n 26).
[53] AgriDataSpace Consortium, 'Building a European Framework for the Secure and Trusted Data Space for Agriculture: D2.1 Multi-stakeholder Governance Scheme and Business Models for Agricultural Data Spaces' (2024) <https://agridataspace-csa.eu/wp-content/uploads/2024/07/AgriDataSpace_D2.1_FinalVersion.pdf> accessed 2 November 2024.

practice, data intermediaries act as gatekeepers, managing consent frameworks, anonymization protocols, and data quality checks. For instance, an intermediary might collect and anonymize data on crop yields from multiple farms before allowing its sharing, protecting the confidentiality and proprietary interests of individual farms.

The Data Governance Act regulation of data intermediation focuses on ensuring that such entities operate "neutrally" under "FRAND" (Fair, Reasonable, and Non-Discriminatory) conditions and with adequate security measures. Specifically, the Act mandates that data intermediaries must ensure structural separation and unbundling of services. Data intermediation services must be provided through a dedicated legal entity, and the data collected cannot be used for purposes other than making it available to data users. In this context, agricultural companies could be encouraged to share data with intermediaries, as these entities are legally bound to act as neutral parties with respect to the data.

The Data Governance Act is regulating different kind of data intermediation services: services that facilitate interactions between data holders and potential data users (such as data marketplaces or data pools), services that connect data subjects who wish to share their personal data or individuals wishing to share non-personal data with potential data users and data cooperative services.

Data cooperative services, are organizational frameworks composed of data subjects, individual entrepreneurs, or SMEs whose primary goal is supporting members in exercising their rights regarding data, facilitate discussions about data processing purposes and conditions that align with members' interests, negotiate terms for data processing, whether it involves non-personal or personal data, on behalf of members. Data cooperatives play a key role as they pursue the objective of a community management of data, leveraging relational value and increasing negotiation power of its participants.[54] For instance, this model enables farmers to seek advice from independent experts rather than being limited to those affiliated with the equipment used to collect the data or to negotiate with providers which have greater bargaining power.[55] Such framework can foster farmers' trust especially if they adopt bylaws designed to address trust issues and to prioritize collaboration and equitable access.[56]

However, to achieve the full potential of the Data Governance Act, cooperatives shall also support collective data-sharing among individuals and entities with shared interests, that is allowing farmers to aggregate their data resources and giving them access to a

[54] Marina Micheli, Eimear Farrell, Bruno Carballa Smichowski, Monica Posada Sanchez, Serena Signorelli and Michele Vespe, *Mapping the Landscape of Data Intermediaries* (Publications Office of the European Union 2023) <https://publications.jrc.ec.europa.eu/repository/handle/JRC133988> accessed 26 January 2025.
[55] Jouanjean and others (n 1); Elettra Bietti, Ander Etxeberria, Morshed Mannan and Janis Wong, 'Data Cooperatives in Europe: A Legal and Empirical Investigation' (2021) Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society, <https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf> accessed 2 November 2024.
[56] Maria Francesca De Tullio, 'Intelligenza artificiale, sovranità alimentare e data governance' (2024) 1S BioLaw Journal - Rivista di BioDiritto 192-220.

larger dataset. Cooperatives aiming to promote the growth of digital technology should function as common pool resources, independent from the vertical integration with agricultural machinery or input supply systems. Cooperatives should be able to assist their member farms in adopting best practices and ensuring compliance with GDPR requirements, particularly in the anonymization and secure management of datasets. Moreover, cooperatives shall play a critical role in addressing interoperability challenges by developing solutions that enable the integration of data from diverse sources and providers.[57] These cooperatives can leverage pooled data to optimize collective practices, reduce redundancy and improve regional planning efforts.[58] For instance, the establishment of regional farming cooperatives that collect anonymized data on crop health and soil conditions might enable participants to benefit from aggregated insights into regional trends.

By offering these resources, cooperatives can help their members navigate the complexities of data governance and leverage digital technologies more effectively. This shared data model can help small-scale farms gain competitive insights that are typically accessible only to larger agricultural corporations and help address concerns about fair value distribution, granting farmers greater control over their data. This approach, furthermore, fosters greater flexibility and collaboration, empowering members to adopt innovative technologies and optimize their operations without being constrained by proprietary systems.[59]

Examples of data cooperatives in agriculture include the Grower's Information Service Cooperative (GISC) in the United States, which enables farmers to collect, store, and manage data to enhance their business activities, and the Scottish Agricultural Organisation Society (SAOS) in Scotland, which has implemented a shared database to ensure traceability in the food chain and prevent outbreaks.[60]

By addressing challenges faced by individual farmers, cooperatives might incentivise the rise of a more inclusive agricultural ecosystem where data becomes both accessible and impactful. In other words, cooperatives are well-positioned to fulfil a pivotal role in data governance, as defined by the OECD.[61]

Reliance on data cooperatives can help uphold the principle of data sovereignty which entails control by an organization over the access, use, storage, and sharing of their data. However, it is crucial that the role of data cooperatives extends beyond merely

[57] AgriDataSpace Consortium, 'Roadmap for Deployment and Operation of the Data Space for Agriculture', Deliverables D4.1 and D4.2 (31 March 2024) <https://pureportal.ilvo.be/files/43149075/D4.1_4.2_ADS_Roadmap-towards-CEADS.pdf> accessed 26 January 2025.

[58] Bietti and others (n 53); Paul Bodenham, 'Data Cooperatives in Agriculture: An Opportunity for Farmers?' https://www.academia.edu/102692993/Data_cooperatives_in_agriculture_An_opportunity_for_farmers accessed 26 January 2025.

[59] Bodenham (n 58).

[60] Micheli and others (n 54).

[61] OECD, 'Data Flows and Governance' (OECD) <https://www.oecd.org/en/topics/policy-issues/data-flows-and-governance.html> accessed 26 January 2025.

safeguarding data sovereignty. They shall actively drive the collective advancement of digital technology by assuming an orchestrating role—facilitating interaction among stakeholders, fostering collaboration, and ultimately creating value through these interactions.[62] Facilitating data sharing is a critical component in ensuring the sustained growth of digital agriculture. In this regard, cooperatives can adopt various forms of collaboration, including[63]:

1. **Cooperative to Members**: Where cooperatives provide services of advocacy, consultancy and assistance to their members.
2. **Member-to-Cooperative:** Members provide their data to the cooperative, which then leverages this collective resource to maximize its potential.
3. **Member-to-Member:** The cooperative acts as an intermediary, facilitating data sharing and collaboration among its members.
4. **Federated Cooperation**: Cooperatives enable collaboration between multiple organizations, fostering synergies across different entities.
5. **Third-Party Connections:** Cooperatives establish links with external parties, creating opportunities for broader cooperation and innovation.

However, as we will further analyse in part four, the definitions of the Data Governance Act might hinder such developments, supporting only the model "Cooperative to Members" rather than the other standards.

In addition to data cooperatives, purely intermediation services can also play a pivotal role, particularly as they serve to bridge the gap between data holders and potential data users, enabling both bilateral and multilateral data exchanges. Such services are especially valuable in fostering inclusive data governance, which facilitates horizontal cooperation among stakeholders.

This category includes, for example, data marketplaces and data-sharing pools:[64]

- **Data marketplaces** function as intermediaries that match data supply with demand, simplifying and facilitating data exchanges between parties.
- **Data-sharing pools**, on the other hand, leverage synergies by combining complementary datasets from multiple stakeholders, creating added value and unlocking insights that individual datasets alone could not achieve.

By enabling seamless cooperation and unlocking the potential of shared data, cooperatives and intermediaries can become catalysts for innovation and progress in the digital agricultural ecosystem. However, it remains unclear whether the Data Governance Act serves as an effective instrument to achieve these objectives or if it acts as a barrier to the full development of such organizations. This issue will be further analysed in part four of this paper.

[62] Micheli and others (n 54).
[63] Fabio Bravo, 'Data Cooperatives' in Fabio Bravo (ed), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo* (Giappichelli, 2024); Bodenham (n 58).
[64] Micheli and others (n 54).

3 Can Agri-Tech benefit the society at large?

The Agri-tech sector offers transformative potential to address pressing societal challenges, including food security, economic sustainability, and environmental health. The deployment of technologies such as IoT devices, machine learning algorithms, and advanced data analytics in agriculture enables precision farming, resource optimization, and scalable innovations.

One of the foremost societal benefits of Agri-tech is its potential to improve global food security. The integration of IoT and data analytics in agriculture enables farmers to make data-driven decisions that optimize crop yield, reduce waste, and conserve water resources particularly helping the challenge to face climate change.[65] By allowing for tailored crop management, precision agriculture helps address food insecurity while reducing the environmental footprint of farming. With access to real-time data, farmers can manage their resources more efficiently, a critical step in addressing food shortages exacerbated by climate change and population growth. The Data Act supports this by mandating data accessibility and interoperability, which empowers farmers to integrate diverse datasets from IoT devices across different platforms.

By standardizing access to agricultural data, the Data Act enables governments to aggregate data at a regional or national level, providing valuable insights for public policy.[66] Policy-makers might be able to track environmental indicators, assess the impact of agricultural practices on biodiversity, and adjust regulations as needed to minimize environmental harm.

Aggregated data can also assist in early-warning systems for crop failures, droughts, and other climate-related risks, allowing governments to implement preemptive policies that stabilize food supply chains. The Data Act enables public bodies to request access to data held by private entities under certain conditions, particularly when the data serves a public interest. This includes situations where data is essential for responding to public emergencies, such as natural disasters or health crises, or for implementing policies aimed at improving public welfare. For example, in the agricultural sector, if a region faces an imminent threat of crop failure due to extreme weather, the Data Act allows public authorities to request and use data on crop conditions, water availability, and weather forecasts.

The Data Governance Act significantly enhances public access to data by establishing a framework for the use of public sector data and creating data-sharing mechanisms that promote transparency and accountability. One of the Act's key provisions is its support for public sector bodies in making data available to third parties, particularly when the data has substantial societal benefits, such as in Agri-tech. This structured approach facilitates

[65] Garske and others (n 10); Michèle Finck and Marie-Sophie Mueller, 'Access to Data for Environmental Purposes: Setting the Scene and Evaluating Recent Changes in EU Data Law' (2023) 35(1) Journal of Environmental Law 109-131.
[66] Jouanjean and other (n 1).

the use of public sector data in innovative applications, allowing entities to leverage information that supports public welfare while respecting existing regulation on data protection and confidentiality.

The Data Governance Act also introduces the concept of data altruism—encouraging individuals and organizations to voluntarily share data for the common good.

Data altruism is a central concept in the Data Governance Act, designed to encourage individuals, companies, and other organizations to voluntarily share data for the common good. This framework allows data to be donated for altruistic purposes, such as scientific research, public health, environmental protection, and sustainable agricultural practices. By promoting data altruism, the Act opens new opportunities for researchers, policymakers, and public institutions to access diverse datasets that might otherwise remain private, thus enabling more comprehensive studies and informed policy decisions. For example, in Agri-tech, data altruism could involve farmers and agricultural firms voluntarily sharing anonymized data on soil health, crop performance, or water usage to support environmental conservation efforts or food security initiatives. Data altruism enables communities and stakeholders to support societal objective, defining a framework which safeguards existing regulations on data.

4 Weaknesses of the EU Digital Strategy Acts

Despite the EU Digital Strategy Acts' ambitious goals of fostering data accessibility and trust, several weaknesses limit their effectiveness, particularly in rapidly evolving sectors like Agri-tech. One significant concern is the complexity of compliance. The Acts impose detailed requirements around data-sharing, interoperability and privacy which can be challenging for small and medium-sized enterprises (SMEs) to implement. The regulatory burden posed by the Digital Strategy Acts could place smaller firms at a disadvantage, as they often lack the resources to meet complex compliance standards. This issue is especially relevant in Agri-tech, where data-sharing between diverse stakeholders—such as farmers, researchers, and technology providers—is essential for innovation. Yet, the stringent regulatory framework could discourage smaller players from participating fully, thereby consolidating the market power of larger entities that can afford to navigate these legal demands. The Acts may inadvertently stifle innovation by imposing strict controls on data usage and access, which could deter novel data applications or experimentation. By focusing on control and regulation, the Digital Strategy may create barriers to flexible, adaptive data practices that could otherwise benefit sectors like Agri-tech, where innovation depends on cross-functional data access and agile responses to technological advancements.

Another notable weakness is the lack of clear technical standards to support interoperability across sectors. Despite legislative support, achieving full interoperability in the agritech sector remains challenging. One major issue is the lack of universal

standards across diverse agricultural systems and data sources. Each piece of equipment or software may have proprietary data formats and protocols, making it difficult to create standardized formats that work universally. For instance, machinery from different manufacturers often use unique data systems that may not communicate with each other, complicating data integration across platforms. Critics argue that while the Data Act establishes the legal groundwork, the absence of specific technical standards may hinder its effectiveness in practice.[67]

Another major concern is the potential for increased compliance costs and burdens on small and medium-sized enterprises (SMEs). The Data Act places significant obligations on data holders to provide users with access to IoT-generated data, a requirement that can be both technically challenging and financially burdensome for smaller entities with limited resources. The compliance demands of the Data Act may disproportionately affect SMEs, placing them at a disadvantage relative to larger corporations that can better afford legal and technical adaptations.[68] The risk of vendor lock-in, thus, remains. Despite the Act's attempts to reduce data monopolies, larger firms may continue to dominate by offering proprietary systems that smaller players find challenging to integrate, reducing the competitive openness intended by the legislation.

Moreover, there are concerns that the definitions included in the Data Act are too narrow to unlock the value of agricultural data. Firstly, it has been argued that the concept of "product and related service" is not adequately tailored to meet the needs of farmers. While it may encompass machinery generated data, it does not include camera and drone recordings, and there are significant uncertainties as to whether it extends to sensor-generated data.[69] Additionally, the extent to which the notion of "related service" encompasses data sent to technology providers at the farmer's input remains unclear. If "related service" is interpreted narrowly to cover only the functionality of IoT solutions, a substantial volume of data risks being excluded from the framework. Moreover, the exclusion of data inferred through processing poses a significant challenge to achieving comprehensive data portability.[70] For example, prescription recommendations and tailored data-driven solutions, which are critical outputs for precision agriculture, would fall outside the scope of portability, thus, favouring the lock-in with first-comer providers. This limitation could undermine the ability of farmers to fully leverage the benefits of data sharing and digital innovation in agriculture. Indeed, the rights of access and portability set up by the Data Act only address cases in which farmers own, rent or lease machines and do not impact on proprietary datasets, thus being ineffective to foster the

[67] Finck and Mueller (n 65); Can Atik, 'Horizontal Intervention, Sectoral Challenges: Evaluating the Data Act's Impact on Agricultural Data Access Puzzle in the Emerging Digital Agriculture Sector' (2023) <https://www.x-mol.com/paper/1697102708941279232> accessed 15 November 2024.
[68] Ibid.
[69] Atik and van der Burg (n 34).
[70] Guarda (n 33).

growth of alternative technologies providers or to encourage players in the downstream markets.[71]

It has also been argued that the definitions of the Data Act are excessively user-centring. The user-centric rights established under the Data Act provisions present several drawbacks. The Data Act does not consider the specific business models in agricultural sector as, frequently farmers would fall outside the definition of "users" as the machinery is used through cooperatives or shared machines or even by third parties to which the specific functions are outsourced, thus not only excluding them from the right to access and portability but also allowing third parties to use and exploit such data.[72] In this context, the European Code of Conduct was arguably better suited to address the sector's unique needs. By associating ownership with data origination, the Code underscored the principle that those who generate data through their activities should benefit from it and participate in the value it creates. Furthermore, the user-centric approach risks rendering these rights underutilized, as has already been observed with data portability provisions under the GDPR, thus failing to reach the goals for which they have been created.

The Data Act imposes several limitations on the ability of recipients and data holders to further reuse data, particularly by making such reuse contingent on obtaining consent.[73] However, it remains unclear what specific characteristics this consent must meet. It appears that the required consent may align more closely with contractual consensus than GDPR-style opt-in, which raises further questions about whether multiple layers of consent will be necessary. The framework designed in the Data Act is explicitly inspired by the data portability and access rights enshrined in the GDPR. While such a structure is justified in the GDPR due to the personal nature of the data and the fundamental right to control one's own information, the same rationale does not apply to non-personal data generated in the context of commercial activities, such as farming.

In addition, the Data Act addresses data sharing through provisions aimed at prohibiting consumer-like unfair contractual clauses, designed to rebalance unilateral terms and conditions. While these measures are intended to foster a trustworthy environment for data sharing, their effectiveness is questionable. The enforcement mechanism primarily relies on the judicial invalidation of unfair clauses, which requires parties to engage in resource-intensive litigation.

As a result, on the one hand the strict user-centric provisions risk being ineffective in creating a trustworthy environment capable of promoting data flows. On the other hand, by narrowly focusing on individual rights without adequately addressing collective or sector-specific needs, the Data Act may inadvertently undermine its broader objectives,

[71] Can Atik, 'Addressing Data Access Problems in the Emerging Digital Agriculture Sector: Potential of the Refusal to Deal Case Law to Complement Ex-Ante Regulation' (2023) 19(3) European Competition Journal 380.
[72] Ryan and others (n 42).
[73] Atik and van der Burg (n 34).

particularly in the agricultural data ecosystem, where collaborative and sectoral approaches are vital for fostering innovation and sustainable growth.

In this context, the Data Governance Act could provide opportunities to mitigate and address the shortcomings of the Data Act by supporting the development of shared data ecosystems. By fostering collaboration and enabling collective approaches to data management, the Data Governance Act has the potential to enhance data sharing and create a more integrated and cooperative framework that meets the diverse needs of stakeholders, particularly in sectors like agriculture.

However, one of the primary criticisms is that the Data Governance Act's regulatory structure for data intermediaries is both complex and costly, which may deter organizations from adopting these roles, especially in less profitable or resourceless sectors like Agri-tech. While the Data Governance Act offers new opportunities for collective data use, several challenges remain in implementing these frameworks. For one, establishing and maintaining data cooperatives requires robust governance structures that balance the interests of diverse stakeholders.[74] Additionally, creating a legal infrastructure for data intermediaries involves complex considerations, such as compliance with GDPR and network security.[75] The operational requirements for data intermediaries, including strict compliance with data privacy standards and security measures, create significant barriers to entry for smaller entities.[76] For smaller or non-profit organizations that might serve as intermediaries for community-oriented data-sharing initiatives, these regulations can become prohibitive, reducing the effectiveness of the data-sharing goals and potentially limiting data availability in public-interest sectors. Administrative overhead required to maintain compliance with rigorous data governance standards can create delays and bottlenecks in data flows, particularly in fields requiring real-time data analysis, such as precision farming.[77] Critics of the Data Governance Act also argue that without clear guidelines on data monetization and profit-sharing, data cooperatives may face challenges in sustaining operations over time.[78] In many industries, including agriculture, data collection, management, and storage represent significant investments in both time and resources.

Another significant issue in the regulation of data intermediaries, which could limit their ability to address the gaps in the Data Act within the agricultural sector, is the strict purpose limitation introduced by the Data Governance Act. The Act restricts data

[74] AgriDataSpace Consortium (n 57).
[75] Atik (n 27); Freyja van den Boom, 'Driven by digital innovations: Regulating Connected Car Data Access and Use for Telematics Insurance in Europe' (2022) <https://eprints.bournemouth.ac.uk/36956/> accessed 15 November 2024.
[76] AgriDataSpace Consortium (n 57); Atik (n 27); Raffaele Giaffreda and others, 'Building a European Framework for the Secure and Trusted Data Space for Agriculture: D3.1 Definition of Requirements for Agriculture Data Space Building Blocks' (2024) <https://agridataspace-csa.eu/wp-content/uploads/2024/07/AgriDataSpaceDeliverable_D3.1_Reviewed_V1.pdf> accessed 15 November 2024.
[77] Ali Basharat, Michael Bewong, Branka Krivokapic-skoko, Ryan HL Ip, Clifford Lewis, Yeslam Al-Saggaf and Md Zahidul Islam, 'The Role of Data Governance in Addressing Potential Risks Associated with Agricultural Data Exchanges: A Systematic Literature Review' (2024) <https://ssrn.com/abstract=4863615> accessed 15 November 2024.
[78] AgriDataSpace Consortium (n 57); Ryan and others (n 42).

intermediation services from providing added-value functions such as aggregation, enrichment, or transformation of data. While this limitation may encourage farmers and other users to share data by ensuring their control over its use, it risks hindering the broader development of the sector by curtailing innovation.[79] Under the framework of the Data Governance Act, the role of data intermediation services is confined to facilitating data exchange, including transforming data formats to ensure interoperability. Additionally, intermediaries may offer services such as temporary storage, data curation, conversion, anonymization, pseudonymization, and ensuring the security and reliability of their platforms. While these functions are important, the inability to add significant value through data aggregation or enrichment could stifle opportunities for innovation and collaboration, which are essential for advancing the agricultural sector's digital ecosystem. Similarly, to what has been argued regarding the Data Act, it appears that European lawmakers have sought to replicate the framework of the GDPR without adequately distinguishing cases where datasets are predominantly, if not entirely, composed of non-personal data. This lack of differentiation risks imposing inappropriate regulatory requirements on non-personal data, potentially creating inefficiencies and hindering the effective utilization of such datasets in sectors like agriculture.

Such limitations become even more apparent when considering the scope of data cooperatives. According to the definition, data cooperatives are described as "*data intermediation services offered by an organizational structure constituted by data subjects, one-person undertakings, or SMEs who are members of that structure*. Their main objectives include supporting members in exercising their rights regarding data, making informed choices before consenting to data processing, exchanging views on data processing purposes and conditions, representing members' interests regarding their data, and negotiating terms and conditions for data processing on behalf of their members, whether for non-personal or personal data. If interpreted narrowly, this definition would restrict the role of data cooperatives to advocacy functions rather than empowering them to provide tangible support in unlocking the value of the data their members generate. Such a limited interpretation risks overlooking the critical role cooperatives could play in fostering innovation, value creation, and more equitable data-sharing practices. If this were the case, cooperatives would need to rely on distinct intermediation services—either through third-party providers or by establishing a separate legal entity—designed to pool data and facilitate its sharing with third parties. However, value-added services would need to be provided separately, through a distinct third-party provider or entity. This separation complicates the ability of such an entity to generate value through platform network effects and hinders the development of a sustainable revenue structure to support its operations.

[79] Bodenham (n 58); Atik (n 11); Bravo (n 63).

Moreover, limiting data cooperatives to representing the interests of sole undertakings or SMEs appears to be a flawed strategy. While most participants in these networks will indeed be small enterprises, the definition fails to address a key issue: power asymmetries in relationships with product and service providers are not inherently linked to the size of the undertaking. Additionally, small and medium-sized enterprises could benefit significantly from opportunities to share data and best practices with larger companies, creating synergies and fostering innovation. By restricting the scope of data cooperatives in this manner, the framework risks undermining their potential to address structural imbalances and drive collective advancements across the data economy.

5 Conclusions

The EU Digital Strategy Acts, including the Data Act and the Data Governance Act, represent significant steps toward building a more accessible, interoperable, and transparent data-sharing environment within the European Union. Designed to unlock the societal and economic potential of data, these Acts aim to balance the needs of private innovation with public interests, providing frameworks that empower various sectors—including agriculture—to leverage data for sustainable development and technological advancement. While the Acts offer promising frameworks, this analysis highlights several key areas where their practical impact may be constrained by regulatory complexity, operational barriers, and insufficient incentives.

The Data Act makes important strides in improving data accessibility and interoperability, particularly for sectors like Agri-tech that depend on integrated data from IoT devices for precision farming and environmental monitoring. By establishing rights to data portability and reducing data monopolies, the Data Act supports a more open and competitive data ecosystem. However, its lack of detailed technical standards on interoperability and the potential compliance burden it places on small and medium-sized enterprises may limit its accessibility and impact. For the Data Act, clearer technical guidelines and scaled compliance requirements for SMEs would enhance its usability and inclusivity, particularly in resource-intensive fields such as agriculture.

Data Governance Act aspires to create a more open and cooperative data ecosystem, several inherent weaknesses limit its effectiveness. The complexity and high compliance costs associated with data intermediaries, challenges in managing and verifying data altruism contributions, and a lack of incentives for data-sharing all pose significant barriers to the Act's goals. For sectors like Agri-tech, where data accessibility and interoperability are essential for sustainable development and innovation, these limitations may restrict the positive impact of the Data Governance Act. To enhance its effectiveness, further refinement of the Act, including clearer standards for data quality, simplified compliance frameworks, and practical incentives for participation, would be beneficial in encouraging a robust, inclusive, and trustworthy data-sharing environment.

Implementing more sector-specific legislation, or sectorial acts, within the EU's digital regulatory framework offers both clear advantages and notable drawbacks. One significant advantage is that sectoral acts allow for tailored regulations that can address the unique needs, challenges, and standards of specific industries, such as Agri-tech, healthcare, or finance. For example, an Agri-tech-specific data act could establish interoperability standards and data-sharing requirements suited to agricultural IoT devices, soil monitoring systems, and climate data. According to some commentators a targeted approach would likely improve regulatory clarity and help smaller entities to adopt practices that align with sector-specific goals and standards.[80] Furthermore, sectorial acts can enhance public policy effectiveness by ensuring that regulations reflect the unique environmental, economic and social impacts of each sector, supporting more targeted responses to issues such as food security or climate adaptation.[81] However, sectoral acts also introduce challenges, particularly around regulatory fragmentation. A sector-specific approach can create inconsistent regulations across industries, complicating data-sharing between sectors and potentially hampering cross-industry innovation. Sectorial regulations may also block data flows by imposing standards that are incompatible with those in related sectors. In Agri-tech, where data-sharing intersects with fields such as environmental monitoring, logistics and finance, sector-specific standards might restrict seamless data integration and cooperation. Additionally, maintaining multiple sectoral acts requires greater administrative oversight, increasing the regulatory burden on the EU and on organizations that operate across multiple sectors. The difficulties of navigating multiple regulatory frameworks can place a disproportionate burden on SMEs that lack resources for comprehensive compliance, potentially excluding smaller players from a robust data economy. Consequently, while sectoral acts offer the benefit of specialized, relevant regulation, they may also impede broader data integration and add complexity to the EU's digital regulatory landscape. Moreover, sector-based legislation can also create uncertainty, also consider the need to integrate it with several other legislations (such as the data protection, IP and trade secret laws).

Overall, the EU Digital Strategy Acts provide a foundational framework that aligns with the Union's goals of creating a secure, transparent and innovation-friendly digital economy. However, the limitations identified in this analysis underscore the need for further refinement to maximize the Acts' positive impact. By addressing the technical, operational, and legal challenges within these frameworks, the EU can foster a more robust, inclusive data ecosystem that empowers not only large entities but also SMEs, non-profits, and individual contributors.

[80] Ryan and others (n 42).
[81] Mark Ryan and Melchior Bizot-Espiard, 'Design Principles and Guidelines for Agricultural Data Spaces Based on Legislation and Ethical Principles' (AgriDataspace, 2024) <https://agridataspace-csa.eu/wp-content/uploads/2024/07/D2.2_AgriDataSpace_Updated-V2.pdf> accessed 15 November 2024; Atik (n 27).

A significant step forward could be achieved by leveraging the delegation under Article 41 of the Data Act, which empowers the European Commission to "*develop non-binding model contractual terms on data access and use, including terms on reasonable compensation and the protection of trade secrets.*" In this regard, the Commission could opt to develop sector-specific contractual terms tailored to the unique characteristics of individual sectors, considering their specific market conditions and competition challenges.[82] The importance of this approach is accentuated by the experience with the EU Code of Conduct, which has demonstrated that the contractual framework is a fundamental element in shaping relationships between parties in the value chain. However, contractual terms alone may not be sufficient. Effective incentives are necessary to encourage parties to renegotiate or adapt their existing agreements to align with the model terms. At the national level, one potential mechanism to achieve this could involve imposing fines for the use of unfair contractual terms, following the established principles of consumer protection law. Such sanctions could motivate stakeholders to adopt the model contractual terms voluntarily while also addressing persistent power asymmetries that risk being perpetuated, despite the progressive steps introduced by the Data Act and Data Governance Act. This dual approach—binding model terms at the EU level and enforcement mechanisms at the national level—could ensure a more balanced and equitable data-sharing ecosystem.

As with regard the Data Governance act, to realize these objectives, it is essential to define and encourage specific revenue models that sustain these platforms and provide clear incentives for stakeholders to participate. A combination of economic, technical, and collaborative incentives will be key to ensuring widespread adoption and effective integration of data spaces in the agricultural sector.

Moreover, is essential that the interpretation of Data Act and Data Governance Act allows a smooth communication across all the subjects, particularly allowing intermediaries to be recipients of IoT data, acting on behalf of and to allow access to several data users on the basis of FRAND agreement.[83] Indeed, Recital 26 of the Data Act suggest that data intermediaries can act on behalf of users. A transparent and interlinked process may indeed create a data ecosystem that works not only for business but for the society at large. With continued adjustments to these regulatory frameworks, the EU can lead the way in creating a data-driven society that balances innovation with public responsibility, supporting sustainable growth and societal resilience in the digital age. A more holistic approach which combines the general framework of the Data Act and Data Governance Act, with existing code of conducts and Commission approved model contractual clauses appears to be the most effective strategy to bridge the gap between the regulations and the specific needs of the market.

[82] Atik (n 12).
[83] Gabriele Carovano and Michèle Finck, 'Regulating Data Intermediaries: The Impact of the Data Governance Act on the EU's Data Economy' (2023) 50 Computer Law & Security Review 105830; Geiregat (n 24).

Indeed, the complex and multifaceted structure of agricultural supply chain requires a multi stakeholder approach which acknowledges diversity and interconnectedness of actors (farmers, tech providers, researchers, financial companies, real estate owners) and which is able to allow every subject in the supply chain to gain value from its participation, in a balanced manner.[84] The goal of the efforts shall be obtaining consensus among all this subjects.

In order to achieve such goal, it is necessary to include incentives for all different participants to the supply chain. For instance, farmers and agricultural producers could be incentivised to make their data available with monetary service compensation or with other utilities such as reduced fees for the use of machinery, similarly to what happened with insurance black box in Italy.[85] Also, technology providers can build business model which are based on data exchange with farmers and cooperatives whereas data intermediaries can request monetary compensation based on license fees or commission to data exchange.[86] Also, cooperatives can incentivise the creation of common licensing of data, to third parties providing value added services. For this purpose, European common space which encourages collaborative frameworks shall be explored and monitored.

For instance, the Common European Agricultural Data Space (CEADS), aims to enable secure, transparent, and responsible data sharing, processing, and analysis within the agricultural sector. The preceding AgriDataSpace project played a crucial role in preparing for CEADS by mapping existing data-sharing initiatives, defining necessary components, and developing a multi-stakeholder governance framework. This approach ensures inclusivity, involving farmers, technology providers, public entities, and associations.[87] The project also examined evolving legislative frameworks to balance data openness, innovation, and privacy, and identified the technical solutions required for a secure, interoperable, and autonomous data-sharing environment. CEADS shall operate as a decentralized federation of data spaces, grounded on four key pillars: a legal and ethical framework, robust data governance, technical architecture, and sustainable management and funding.[88] Challenges, such as standardization across diverse systems, shall be carefully evaluated, with trust and transparency serving as critical foundations for stakeholder collaboration and participation. Such platforms should enable seamless data

[84] Jouanjean and others (n 1).
[85] Giaffreda and others (n 76); See also Art. 132-ter of Italian Legislative Decree n. 209 of 7 September 2005, n. 209 according to which "*in the presence of at least one of the following conditions, to be verified before or at the same time as the conclusion of the contract or its renewals, insurance companies shall apply a discount determined by the company […] in the event that electronic mechanisms that record the vehicle's activity, called "black box" or equivalent, or additional devices are installed, at the proposal of the insurance company, or are already present and portable, identified, for the sole minimum functional requirements necessary to ensure the use of the data collected, in particular, for tariff purposes and the determination of liability at the time of accidents*".
[86] Giaffreda and others (n 76).
[87] Giaffreda and others (n 76).
[88] Ibid.

sharing across various stakeholders, unlocking the full potential of subsidiarity and data centralization envisioned under the Digital Strategy.

On the one hand, it is essential to enhance the participation of vertically integrated operators by recognizing the diverse needs of different agricultural sectors, such as harvesting, crop cultivation, and animal husbandry, while also valuing the role of regional intermediary services, given the critical importance of location in agriculture. On the other hand, these platforms should facilitate data sharing with third parties such as insurers to enable premiums that accurately reflect the specific risks and characteristics of agricultural businesses, logistic providers to enhance the farm-to-fork chain as well researchers to promote sustainability initiatives. An enhanced shared environment could further drive innovation by creating new business opportunities, such as the emergence of specialized warranty providers and maintenance services, while also fostering competition and encouraging manufacturers to develop improved products and services. To fully realize the potential of data spaces, it is vital to establish an interconnected ecosystem where centralized platforms achieve interoperability and address market fragmentation. This requires clear guidance on how the Data Act and Data Governance Act should be interpreted and harmonized, with issues being addressed either at the national level or through directives and guidance from the European Commission.

The Regulation (EU) 2024/1689 ("AI Act") also adds an essential layer to the EU's digital strategy by specifically addressing the use of artificial intelligence in sectors like agriculture, where AI technologies play a pivotal role in driving innovation and sustainability. With specific regard to Regulation (EU) No 167/2013 on the approval and market surveillance of agricultural and forestry vehicles Art. 103 of the AI Act provides that when adopting delegated acts, the Commission shall ensure that artificial intelligence systems which are safety components of such vehicles meet the requirements for high-risk AI. This sector-specific approach not only mitigates risks associated with the misuse of AI, such as biased algorithms or opaque decision-making processes, but also promotes trust in AI systems. Furthermore, the AI Act emphasizes the importance of harmonized standards and certifications, which can enhance interoperability and foster collaboration across stakeholders in agriculture, from farmers to technology providers. However, its successful integration with the Data Act and Data Governance Act will be critical to create a cohesive regulatory environment that facilitates innovation while safeguarding ethical and social considerations in the agricultural sector. This interplay among the Acts is vital for achieving the EU's vision of a sustainable, data-driven, and technologically advanced agricultural economy.

*Richa Jain**

BIG DATA AND COMPETITION LAW:
NAVIGATING TRADE PRACTICES IN THE DIGITAL AGE

Abstract

According to International Data Cooperation, it is expected that the world data will grow at a compound annual rate of 61% that is from 33 Zettabytes in 2018 to 175 Zettabytes by 2025[1].

It is prudent to say that data, more specifically consumer data, can be termed as the new raw material for digital businesses. By skilfully leveraging big data (which is the collection of large and complex data sets), e-commerce companies are able to understand the current market trends and consumer purchasing behaviour. This gives them the potential to make near-accurate forecasts and enhance the user shopping experience by providing personalised products, implementing targeted advertising, optimising prices, and elevating customer services. Although the accumulation of big data gives companies a substantial competitive advantage yet, it's use is not free from anti-competitive concerns.

This paper aims to shed light on present and potential anti-competitive practices that data-driven businesses indulge in that can lead to market distortion. The author brings forth both sides of the discussion, one that argues how big data can lead to anti-competitive practices and the other that tries to disprove this notion. The debate around big data and its impact on competition law usually circles around three questions that shall be addressed in this paper. Firstly, could accumulating data could contribute to market power and anti-competitive actions? Secondly, what are the effects of big data on market transparency? Thirdly, could data be used as an instrument to do anti-competitive conduct and abuse of dominant position?

Apart from trying to find answers to these questions, this paper also examines some key elements of competition law, such as delineating 'relevant market' and assessing 'dominance', that are regarded as prerequisites in any antitrust inquiry across the globe. The author discusses these elements via an international comparative study of big data-related cases. This article concludes by arguing whether or not reliance on traditional antitrust tools makes the regulator's work difficult in assessing trade practices that involve big data. This study further proposes a few recommendations that may be of benefit to competition regulatory authorities in inquiries related to anti-competitive investigation by digital commerce companies using big data.

JEL CLASSIFICATION: K21; L41; L42; L44

SUMMARY

1. Introduction – 2. Defining Big Data – 3. Role of Data in Competitive Analysis - 3.1 Data as a Source of Market Power - 3.2 Effects of Big Data on Market Transparency - 3.3 Anti-Competitive Practices Associated with Data – 3.3.1 Refusal to Grant Access – 3.3.2 Data and Price Discrimination – 3.3.3 Data-Driven Mergers

* Advocate, Telangana; Ph.D. Research Scholar, Rajiv Gandhi National University of Law, Punjab, India.

[1] Andy Patrizio, 'IDC: Expect 175 Zettabytes of Data Worldwide by 2025' (*Network World*, 2018) <https://www.networkworld.com/article/966746/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html> accessed 10 June 2024.

DOI 10.13135/2785-7867/11805

– 3.3.4 Use of Data for Tie-In Arrangements - 3.3.5 Concerted Actions – 3.3.6 Data and its Effects on Privacy – 4. Pro-Competition Effects of Big Data: Counter-Argument – 4.1 Free Availability of Data – 4.2 Fluidity of Data-Driven Market Power – 4.3 Data Privacy Concerns are Outside the Jurisdiction of Competition Regulators – 5. Is Competition Law Ready for Big Data? – 5.1 Delineating 'Relevant Market' – 5.2 Assessing Dominance – 5.3 Data-Sharing to Aid Competition – 5.4 Merger Thresholds – 6. Conclusion

1 Introduction

Digitisation has completely overhauled the way businesses are done today. It has allowed a large number of companies to achieve huge profits hinged around business models that primarily focus upon the collection and commercial use of data. The role of data in developing business strategies has become a universally debated topic. Companies are now able to collect and analyse enormous amounts of customer data and achieve systematic conclusions from them in real-time.[2] The chairperson of America's Federal Trade Commission commented that "*data is today's currency*".[3] Data is viewed as an element so essential for trade practices in the digital age that it is being referred to as the "new oil".[4] Although the profits that are generated from data collection are dependent upon how it is used, yet clearly, the collection of data in itself has become a crucial intangible asset.[5]

Appropriate utilisation of data has become so crucial for the viability of a few digital markets, such as social networks, online advertising, search engine markets, and e-commerce, that they are now being referred to as 'data-driven markets'. Google, for instance, has become a prominent illustration of a data-driven business in the domain of online search engine markets. As one may be well aware, consumers can use Google and its services freely without any cost as a zero-priced product. However, the hidden reality is that these services are not free, and in fact, Google's business model primarily relies upon the aggregation of user data and its exploitation through sophisticated online advertising methodologies.[6] The data that any social media website, e-commerce company or search engine like Google generates "can be worth up to $5000 per person

[2] Bruno Lasserre and Andreas Mundt, 'Competition Law and Big Data: The Enforcer's View' (2017) 1 Italian Antitrust Review 87.

[3] Edward Wyatt, 'Edith Ramirez is raising the F.T.C.'s voice' (*New York Times*, December 2014) <https://www.nytimes.com/2014/12/22/business/federal-trade-commissionraises-its-voice-under-its-soft-spoken-chairwoman.html> accessed 10 June 2024.

[4] 'The World's Most Valuable Resource is No Longer Oil, but Data' (*The Economist*, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 10 June 2024.

[5] TP Priyadarsini, 'Big Data Analytics: A Cause of Concern for Competition?' (2020) 9(1) NLIU Law Review 65.

[6] The Competition and Markets Authority, 'Online Platforms and Digital Advertising Market Study' (2020) <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 10 Jan 2025.

per year to advertisers"[7], highlighting how data has become the new raw material for businesses.

Utilising data for businesses has a significant economic impact. Collecting and analysing data can increase the allocative, dynamic and static efficiencies by reducing the cost of production, improving the quality of goods and resources, and increasing transparency.[8] It also puts pressure on the new and existing entrants to innovate and develop new products.[9] E-commerce represents a major chunk of the digital universe that accumulates data in the form of customer's digital activity. Although traditional brick-and-mortar stores also possess information about consumer preferences and buying patterns yet, their knowledge is limited by geography and the volume of consumers that approach them.

By skilfully utilising big data, e-commerce companies are able to predict trends and enhance the user shopping experience by providing targeted advertising, personalised products, optimising selling prices and customer services. Consequently, data becomes an asset that has a crucial competitive benefit for the companies; however, the implications of accumulating big data on digital trade warrant further examinations and discussions.

This paper aims to contribute to the discourse by identifying key issues and variables relevant to assessing the interplay between big data collection, market power, and competitive practices. To execute this aim, the paper has been divided into six parts. In the first part, the impact of digitalisation on modern business practices has been introduced. The second part gives a brief overview of big data, its collection and analysis methodologies. Subsequently, the third part discusses the role of big data in competitive analysis. Various theories of harm that are typically associated with data collection and its exploitation within the digital markets that affect trade and competition are also discussed. The fourth part presents a balanced examination of the discussion surrounding big data, articulating one perspective that contends such data can foster anti-competitive practices while the opposing viewpoint that seeks to negate this assertion. The fifth part highlights the unique challenges and implications presented by big data in the digital trade to the regulatory authorities. The paper concludes by detailing several domains in which competition regulatory authorities face challenges and opines several recommendations for potential rectification.

[7] Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) 40(2) William Mitchell Law Review 849.

[8] Organisation for Economic Cooperation and Development, *Data Driven Innovation: Big Data for Growth and Well Being* (OECD Publishing, 2015) <https://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en> accessed 10 June 2024.

[9] Organisation for Economic Cooperation and Development, *Protecting and Promoting Competition in Response to "Disruptive" Innovations in Legal Services* (OECD Publishing, 2016) <https://www.oecd-ilibrary.org/finance-and-investment/protecting-and-promoting-competition-in-response-to-disruptive-innovations-in-legal-services_ca47c852-en> accessed 10 June 2024.

2 Defining Big Data

To propound the debate around the interface of competition law and big data, it is pertinent to first understand what constitutes big data and how it is collected, analysed and used by companies in the digital marketplace. Although there is no specific definition of the term 'data', it, in a wider sense, refers to any information or its representation that is being stored in a computer. Personal data such as geo-locations, online shopping patterns, social media activity, as well as web browser histories can be categorised as data. The buzzword of discussion in this debate concerning anti-competitive practices in the digital age is not merely data but big data- which is not a well-defined concept.[10] The term 'big data' can be traced back to the 1980s wherein it was referred to as the variety of customer data lists used to increase the efficiency of advertisements.[11] At present, common aspects of big data are said to include large amounts of various kinds of data that are produced at a rapid speed from multiple sources, whose operation, management and analysis require powerful processors, latest algorithms and new storage and data transportation techniques.[12] The collection and management of big data sets present inherent complexities due to which they cannot be effectively dealt with using traditional database processing techniques.

It is often characterised by four "V Factors, i.e., velocity, volume, variety and value".[13] Wherein velocity refers to the speed at which new data can be generated, distributed and analysed even without the necessity to store it. For instance, it only takes milliseconds for a trading system to gather social media signals that trigger their responses to buy or sell shares.[14] Volume refers to the staggering amount of data that is continuously getting generated on the internet. The factor variety is connotated to the different types of data that are being generated, including social media posts, Google searches or even e-retail purchases. Value refers to the limit to which this inescapable and extensive data can be used to generate profits. For instance, e-commerce companies can gather customer search and preference data to do predictive analytics, which involves estimating demand, forecasting price changes, assessing risks, and predicting consumer preferences and behaviour. This can be extremely valuable to the company as it can help them do targeted advertising, reduce risks, improve performance and increase profits.

As far as collecting big data is concerned, there are various methods through which companies gather data. Customers typically disclose their private information in exchange

[10] Han Hu and Yonhhang Wen, 'Toward Scalable Systems for Big Data Analytics: A Technology Tutorial' (2014) 2 IEEE Access 652.
[11] Erik Larson, 'What Sort of Car-rt-sort Am I? Junk Mail and the Search of Self' (*Harper's Magazine*, July 1989) <https://harpers.org/archive/1989/07/what-sort-of-car-rt-sort-am-i-junk-mail-and-the-search-for-self/> accessed 10 Jan 2025.
[12] OECD-2015 (n 8).
[13] Organisation for Economic Cooperation and Development, *Supporting Investment in Knowledge Capital, Growth and Innovation* (OECD Publishing, 2013) <https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en> accessed 10 June 2024.
[14] Priyadarsini (n 5).

for products and services that are often offered at no cost and are financed through advertising.[15] For instance, personal data is often furnished by consumers when creating social media accounts. As a result, organisations acquire not only essential details such as addresses, email contacts, date of birth, and payment information but also gather insights into shopping preferences or, in some cases, access to photos and videos of consumers. By tracking consumer web history and analysing cookies, digital companies can gain a deeper insight into consumer's interests and preferences. Digital companies have the capacity to deduce new information using pre-existing data, such as inferring gender or age, by evaluating consumer shopping behaviours. Big data collected through these methods are commonly referred to as 'first-party data' as they involve companies directly engaging in data collection related to their own consumers. Additionally, companies may utilise the services of external entities that share or sell data to gather 'third-party data'. Such third-party data may include big data sets that are stitched together after being collected from various non-private sources such as public, academic, or government sources.

Organisations across the globe have made observations signifying the important role data plays in competition between enterprises. The Organisation for Economic Cooperation and Development ('OECD') categorised big data as a core economic asset that could create significant competitive benefits for firms.[16] Data was metaphorized as "the new oil" at the World Economic Forum.[17] In the *Matrimony.com Case,* the Competition Commission of India also recognised the increasing value of data for business and reinforced the metaphor by stating, "It would not be out of place to equate data in this century to what oil was to the last one."[18] Furthermore, the European Commission, in the *Google (Shopping) Case,* emphasised how the ability to collect and process large amounts of data bestows a competitive advantage on a firm, having the potential to create an exclusionary effect on rivals.[19] The Competition and Markets Authority of the UK also highlighted how the ability to control and analyse user data entrenches a company's market position.[20] Furthermore, in a consultation paper, even the Competition Bureau of Canada highlighted how enterprises' competitive performance, especially in the digital age, is increasingly driven by their ability to harness and use data.[21] Data undoubtedly has

[15] OECD-2015 (n 8).
[16] OECD-2013 (n 13).
[17] K Schwab, A Marcus and JR Oyola, 'Personal Data: The Emergence of a New Asset Class' (*World Economic Forum*, 2011) <https://www.mdpi.com/1999-5903/15/2/71#B1-futureinternet-15-00071>accessed 10 Jan 2025.
[18] Case COMP 7/30, *Matrimony.com limited v Google LLC* [2012].
[19] Case COMP/AT. 39740, *Google Search (Shopping)* [2017] OJ L 248/1.
[20] Competition and Markets Authority (n 6).
[21] Competition Bureau Canada, 'Big Data and Innovation: Implications for Competition Policy in Canada' (2024) <https://competition-bureau.canada.ca/how-we-foster-competition/consultations/big-data-and-innovation-implications-competition-policy-canada> accessed 10 June 2024.

competitive significance in the digital age. However, whether it raises competition concerns is dependent upon who controls the data and how it is used.

3 Role of Data in Competitive Analysis

The digital economy's technological advancements have revolutionised how businesses gather, analyse, and apply data in almost every sector. This gives firms crucial economic benefits and creates pro-competitive effects. However, in some situations, the method of collection and analysis of data can also contribute to raising antitrust concerns. The debate around big data and its impact on competition law usually revolves around three questions.[22] Firstly, whether accumulating data could contribute to market power? Secondly, what are the effects of big data on market transparency? Thirdly, could data be used as an instrument to do anti-competitive conduct and abuse of dominant position?

3.1 Data as a Source of Market Power

The first question that arises is whether accumulating data could contribute to market power. According to the OECD, the economics of big data favour market dominance.[23] To enunciate, digital enterprises that have a significantly higher market share also tend to have access to larger big data sets, holding key information of their customers. According to the first argument, holding a larger quantity of data allows digital companies to provide qualitative, tailor-made services to the consumers, which in turn attracts more consumers and, consequently- more data (snowball effect). Furthermore, higher revenues generated by larger companies fuel higher investments that allow them to use better algorithms, new functionalities, and entry into other markets, accumulating even more data.

According to the counter-argument, this trend of gathering vast amounts of big data harms the competition by "*converging towards a monopolisation of data-related markets.*"[24] In markets where data is a prerequisite to business, access to data is particularly important for new entrants to compete effectively. In such situations, 'data monopolisation' creates challenges for new entrants to access or collect the same volume of data, creating significant barriers to entry. For instance, Google in the online search engine market and Amazon in the e-commerce market have such a vast consumer base that they can collect huge amounts of big data sets by analysing user activity and transactions. They can also buy or receive data from third-party companies. This phenomenon, coupled with network effects, which represent demand-side economies of

[22] Lasserre and Mundt (n 2).
[23] Organisation for Economic Cooperation and Development, *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report* (OECD Publishing, 2014) <https://doi.org/10.1787/9789264229358-en> accessed 10 June 2024.
[24] Lasserre and Mundt (n 2).

scale, can impact the value of the platform, service or product based upon the users who leverage it and may limit the vigour of competition.[25]

To enunciate further, network effects can be generally categorised into two types: direct and indirect. Direct network effects occur when the value of a product or service increases with the number of users or buyers, as evident from social media platforms like LinkedIn or Instagram.[26] Indirect network effects occur when a platform is dependent upon two distinct groups of users, such as producers and consumers or developers and users. As more participants from one group join and engage on the platform, the value amount for the other group increases, as illustrated by the operations of the e-commerce companies and taxi services.[27] The impact of network effects on competition may manifest in multiple ways. They may enhance competition by encouraging platforms to invest and compete better to acquire more consumers.[28] Conversely, they can also impede competition as the new entrants or smaller existing competitors might not be able to gather data to a similar extent due to fewer transactions or limited users.[29] Furthermore, even the third-party companies may refuse to share or sell data to the smaller competitors.[30] This could contribute to widening the gap in market share between larger dominant entities and newer market entrants.[31]

3.2 Effects of Big Data on Market Transparency

The second question that arises is whether data has an impact on market transparency. On one hand, it can be argued that data has the potential to significantly increase market transparency between the supplier and the customer, which can foster healthy competition.[32] Increasing transparency can also benefit the consumer by reducing information asymmetry and enabling them to compare prices and ratings of two products on two different forums. For instance, a customer can review and compare prices of similar goods on Amazon and eBay, which empowers them to make a well-informed decision. This, as a consequence, leads to more healthy and intensive competition in the market, encouraging digital businesses to innovate and improve their prices and quality

[25] G7 Competition Authorities, 'Compendium of Approaches to Improving Competition in Digital Markets', (*Hiroshima Summit*, 2023) <https://assets.publishing.service.gov.uk/media/654b7439b9068c000d0e7554/2023_updated_compendium_of_approaches_to_improving_competition_in_digital_markets_1.pdf> accessed 10 January 2025.

[26] Tim Stobierski, 'What are network effects' (*Harvard Business School Online*, 2020) <https://online.hbs.edu/blog/post/what-are-network-effects> accessed 10 June 2024.

[27] Ibid.

[28] G7 Competition Authorities (n 25).

[29] Ibid.

[30] Lasserre and Mundt (n 2).

[31] Lina M Khan, 'Amazon's Antitrust Paradox' (2016) 126 Yale Law Journal 710.

[32] Timothy Morey, Theodore Forbath and Allison Schoop, 'Customer Data: Designing for Transparency and Trust', (*Harvard Business Review*, May 2015) <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust> accessed 10 January 2025.

of goods. Additionally, market transparency allows new entrants to know about customer requirements and the sale offers of their competitors, thereby lowering the cost of entry in the digital market.

However, on the flip side, it is argued that increased transparency due to data collection between suppliers could also hinder competition and harm consumers.[33] Especially in cases where market concentration is high, transparency among suppliers can even lead to explicit or even implicit collusion via the use of algorithms.[34] For instance, it can be noticed how some competing players in the same industry, such as airlines, hotel booking, and cab/transportation booking companies, apply dynamic pricing algorithms to increase or decrease their prices in consonance with their rivals. Due to the industry's dynamic nature, continuous change in supply and demand necessitates continuous data collection and price adjustments. This makes it difficult to implement explicit cartel agreements in these markets, so the enterprises opt for collusion via algorithms and create an illusion of conscious parallelism, which is difficult to detect.[35] Coordinated parallel behaviour can also happen by programming the algorithm to follow data being released by a particular leader (also referred to as the hub and spoke model), buying the same data or data analysing algorithm from the same third party.[36] Increased transparency may lead to a decrease in price competition between competing firms, resulting in their reluctance to lower prices.

3.3 Anti-competitive Practices Associated with Data

The third question that arises is whether data could be used as an instrument to engage in anti-competitive conduct and abuse of dominant position. This question can be answered by analysing six practices that shall be dealt with in this section.

3.3.1 Refusal to Grant Access

As discussed earlier, big data can become an instrument for market power and even anti-competitive conduct if its access is restricted by a dominant company. This is especially noticeable in situations where data is considered an 'essential facility' by the company requesting access.[37] Companies generally incur substantial costs when they gather and analyse data, which incentivises them to create anti-competitive business strategies to limit their competitor's ability to access the same data. This often leads to

[33] Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016) 368.
[34] Ariel Ezrachi and Maurice E Stucke, 'Two Artificial Neural Networks Meet in an Online Hub and Change the Future (of Competition, Market Dynamics and Society)' (2017) Oxford Legal Studies Research Paper 24.
[35] Ibid.
[36] Suzanne Rab, 'Artificial Intelligence, Algorithms and Antitrust' (2020) Competition Law Journal, 141,150.
[37] Priyadarsini (n 5).

the formation of exclusive agreements with third-party data providers, leading to the denial of access to data, creating entry barriers, and foreclosure of competitors.[38]

The Court of Justice of the European Union, in the '*Microsoft Case'*[39] discussed whether withholding 'interoperability information' from competitors would constitute as an abuse of dominant position. In a relatively strict manner, the Court held that to categorise any information as 'essential facility', the parties would have to showcase that (i) the dominant company's data is unique, and the competitor does not have the possibility to obtain the data necessary for the performance of its services; (ii) refusal to grant access to data would prevent the introduction of a new product; (iii) the refusal is devoid of any reasonable justification; (iv) the refusal shall wipe out the competitor from the market.[40]

As emphasised by the French Competition Authority in the *Cegedim Case,* refusal to grant access to data could be categorised as anti-competitive in cases of 'discriminatory action', whereby (i) access to data is provided to certain competitors while it is denied to other competitors or, (ii) where data of certain consumers is given to down-stream competitors, while data of other consumers is restricted.[41] In this particular case, 'Cegedim', a prominent company that provided medical databases in France, sold its primary database called 'OneKey' to certain pharmaceutical laboratories (primary consumers of the product) but refused to sell it to other consumers that used Cegedim's competing software 'Euris' in the relevant market of 'customer relationship management' within the health sector. The French Competition Authority ruled such action to be discriminatory and on the grounds that Cegedim was a dominant player in the market, such discrimination was held to be restrictive of competition between Euris and Cegedim during 2008-12.[42]

Refusal to allow access to data could be discriminatory even in cases where self-preferencing principles are violated.[43] For instance, in some cases, online enterprises may perform the dual role of providing the platform (being the aggregator or marketplace) as well as acting as a competitor on the same platform, giving them disproportionate competitive leverage.[44] It is expected that the platform should not be biased towards any particular goods or services, even those owned by them. In such cases, they may be able

[38] AP Grunes and ME Stucke, 'No Mistake about it: the Important Role of Antitrust in the Era of Big Data' (2015) 3 University of Tennessee Legal Studies Research Paper 269.

[39] Case T-201/04, *Microsoft Corp v Commission* [2007] ECR II-3601, paras 320-336.

[40] Damian Geradin and Monika Kuschewsky, 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue' (*Concurrences*, 2013).

[41] 'Cegedim' (*French Competition Authority Decision No 14-D-06*, 8 July 2014) <https://www.autoritedelaconcurrence.fr/en/decision/decision-14-d-06-8-july-2014-practices-implemented-company-cegedim-sector-medical> accessed 10 June 2024.

[42] Ibid.

[43] *Google Search (Shopping)* (n 19).

[44] Bipasha Kundu, 'Too Deferential: Critiquing CCI's Approach in the Amazon Private label Brands Case' (*NLSIU Law School Policy Review,* 22 January 2023) <https://lawschoolpolicyreview.com/2023/01/22/too-deferential-critiquing-ccis-approach-in-the-amazon-private-label-brands-case/> accessed 21 September 2024.

to gather not only information about consumer behaviour but also details about the products that their competitors are selling on their marketplace. Through data analysis, they have the potential to identify the most sought-after products and adjust the pricing and visibility of those products for their benefit. To aggravate the situation even further, they can restrict the competitors from accessing the information about their transactions with the consumers. Search limitations on information transfers could violate the ethos of platform neutrality and hamper fair play in the e-commerce market.

Additionally, the dominant entities could enter into exclusive dealing agreements with third-party data providers, making it difficult for the competitors to access the data. The European Commission fined Google €1.49 billion for breaching the European Union Antitrust Rules and abusing its market dominance by entering into restrictive agreements with third-party websites, preventing Google's competitors from placing their advertisements on these websites.[45] Although Google appealed against the order, the Commission held that Google, through these actions, violated Article 102 of the Treaty of the Functioning of the European Union (TFEU) and Article 54 of the European Economic Area (EEA) Agreement, which prohibits the abuse of dominant position.[46]

Another classic example to highlight this issue is the *Amazon Buy Box Case*[47], wherein the European Commission found that Amazon used non-public data regarding online retailers that competed with it as a seller on its marketplace. Through this, Amazon was able to aggregate and analyse business data from hundreds of individual sellers in the European Union to gather valuable insights that allowed it to favour its own retail products and products by its associated companies. Cases like these highlight the growing enforcement against companies that create barriers to access or indulge in self-preferencing leading to violation of competition laws.

However, according to the counter-argument, the dominant company that has collected the data is in a fiduciary relationship with consumers.[48] This relationship necessitates that the company that has gathered the data must enforce careful measures to safeguard the privacy of individuals and protect their sensitive information from potential breaches, misuse, or exploitation.[49]

[45] Case AT 39740 *Google (AdSense)* [2019] OJ L151/1.

[46] Ibid; European External Action Service, 'Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising' (*Press Release of European Commission*, 20 March 2019) <https://ec.europa.eu/commission/presscorner/detail/en/ip_19_1770> accessed 14 August 2024; *See* also, Case C-816/19 *CJEU Appeal* [2021] ECLI:EU:C:2021:894.

[47] Joined *Amazon Marketplace* (Case COMP/AT.40462) and *Amazon Buy Box* (Case COMP/AT. 40703) Commission Decision 2022/9442 EU [2022].

[48] Ariel Dobkin, 'Information Fiduciaries in Practice: Data Privacy and User Expectations', (2018) 33(1) Berkeley Technology Law Journal 1,7.

[49] Ibid.

3.3.2 Data and Price Discrimination

Through big data analytics, a company can identify and classify consumers based on their search history, purchasing habits, and willingness to pay higher amounts for luxury goods and facilitate price discrimination.[50] To enunciate, if a company knows about a consumer's preferences and general price range, it can adapt to the prices of the individual customer group.

On the one hand, it can be argued that price discrimination is beneficial for consumers and is a key element of competition because it allows consumers to buy products at a lower price, which they would not have been able to afford at a higher price.[51] However, according to the counter-argument, price discrimination also has its own negative impacts and can be categorised (in the words of the French Competition Authority) as "an unfair breach of consumer equality."[52] Price discrimination can heighten the information asymmetry between the supplier and the consumer and can lead to higher search costs for the consumer.[53] Price discrimination adapts and lowers prices for a particular set of consumers; similarly, it can adapt to give higher prices for the same products to another set of consumers,[54] which is unfair. However, to regard it as an anti-competitive practice, the presence of abuse of dominant position or vertical restraint is necessary.

3.3.3 Data-Driven Mergers

Accumulation of big data also raises concerns regarding the assessment of merger cases. A company can stitch a strategy to obtain access to new data by combining with a company that possesses a large amount of relevant data. Acquisition of data-rich firms (even with lower revenue) can grant significant data control, enabling the acquiring firm to enhance targeted, personalised advertisement and increase network effects. According to the OECD, 'big data related' mergers have more than doubled between 2008 and 2015.[55]

For instance, in the case of the *Facebook/WhatsApp* merger, the European Commission examined the impact of this merger on the possibility of data access and subsequent

[50] Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2013) 40(2) William Mitchell Law Review 849, 864.

[51] Organisation for Economic Cooperation and Development, *Executive Summary of the Roundtable on Price Discrimination* (*OECD Publishing*, 2018) <https://one.oecd.org/document/DAF/COMP/M(2016)2/ANN5/ FINAL/en> accessed 14 August 2024.

[52] French Competition Authority and Bundeskartellamt, 'Joint Study on Competition Law and Data' (10 May 2016) <https://www.autoritedelaconcurrence.fr/en/publications/joint-study-competition-law-and-data> accessed 30 January 2025.

[53] Lasserre and Mundt (n 2).

[54] Ezrachi and Stucke (n 34).

[55] European Data Protection Supervisor, 'Report of Workshop on Privacy, Consumers, Competition and Big Data', (*Council of European Union*, 2014) <https://www.edps.europa.eu/sites/default/files/ publication /14-07-11_edps_report_workshop_big_data_en.pdf> accessed 14 August 2024.

utilisation for advertising in the market.[56] The merger was eventually approved without competitive concerns as the European Commission found the data collection by Facebook would not be a problem after the merger as many other companies were also collecting extensive data. However, the question remains whether emerging data-driven markets can give rise to 'vertical or conglomerate' effects if the merger allows the larger company to do data concentration and restrict upstream or downstream competitors' access to data.

The European Commission has discussed vertical mergers in the *Microsoft/LinkedIn Case*[57], highlighting how a merger between two dominant companies in different markets can lead to the foreclosure of the competitors. To ascertain whether the merger is anti-competitive, the European Commission examined (i) the ability of the merged entity to foreclose its potential or existing competitors, (ii) the presence of any economic incentive to do foreclosure of competitors, (iii) the significant adverse effect of the foreclosure strategy on the competition.

Another merger that raised antitrust concerns was in 2022 when Amazon acquired 'One Medical', a membership-based primary-care provider with extensive access to patient's healthcare records. This merger raised red flags regarding Amazon's ability to use consumer's healthcare data for unrelated purposes, such as influencing consumer behaviour, improving their advertisement, and extending dominance in the e-commerce market. Although the merger was approved, the United States Federal Trade Commission (FTC) has put the merger under further scrutiny to monitor how Amazon protects sensitive consumer healthcare information to initiate enforcement actions, if needed.[58]

Additionally, data-driven markets can also promote horizontal mergers between two entities in different positions within the upstream and downstream markets. This can decrease the competition, especially in cases where markets are concentrated, and data is the primary input without any effective substitute. For instance, a merger between a prominent or dominant player and a new entrant may result in an alteration of access to data and shall increase the concentration of data if the new entrant has access to big data sets collected in different markets. Through this, companies can use data-driven market power to attain prominence in the adjacent market.[59]

A similar issue occurred in the *Google/Fitbit*[60] merger, wherein the European Commission examined the concerns regarding the potential foreclosure of competing

[56] *Facebook/WhatsApp* (Case COMP/M.7217) Commission Decision 2014/7239 EU [2014] OJ L2985 1 para 164.
[57] *Microsoft/LinkedIn* (Case COMP/M.8124) Commission Decision 2016/8404 [2016].
[58] US Federal Trade Commission, 'Joint Statement of Chair Khan and others, Regarding Amazon.com, Inc's Acquisition of 1Life Healthcare, Inc.' (2023) <https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalkhanslaughterwilsonbedoya.pdf> accessed 14 August 2024.
[59] German Monopolies Commission, 'Competition Policy: The Challenges of Digital Markets: Special Report' (Law Com No 68, 2015).
[60] *Google/Fitbit* (Case COMP/M.9960) Commission Decision 2004/139 [2020] 1.

wristwear suppliers from accessing Google Play. The Commission investigated the possibility of Google treating the competing wearable devices within the app store in a biased manner by lowering the ratings or delaying the approval process for updates. The app store represents an upstream market; therefore, if app developers responsible for competitive wearable devices are treated unfavourably, it could result in the foreclosure of competing vendors in the downstream market.[61] It also raised vertical concerns and was viewed as containing conglomerate characteristics as it centred on deteriorating the interoperability between smartphones operating on Android OS and competing wearable devices. The Commission eventually permitted the combination based upon Google's commitment that it would not use Fitbit's health and fitness data for advertising and would license certain Android APIs free of cost to allow interoperability between competitors.

3.3.4 Use of Data for Tie-in Arrangements

Tie-in arrangements or tie-in sales include an agreement wherein the purchaser of a particular good or service is required as a precondition to either make a purchase of another good or service from the seller or agree not to buy the tied goods from any other supplier. The basic premise behind these arrangements is to finish the inventory and to make profits via clubbed sales. In the data-driven market, enterprises may leverage data obtained from one market to establish or enhance their market dominance or power in another market through tied sales that could be deemed as anti-competitive, having the potential to cause adverse effects on competition. To enunciate further, the Competition and Markets Authority of the UK has highlighted that when a company collects and sells data for a long period of time, it would be easier for it to enter into the data analytics markets owing to its market power compared to its competitors.[62] In such situations, it may be tempted to tie its data analytics services with access to its acquired data, which is anti-competitive.[63] Similarly, the French Competition Authority opined that "cross usage of data" by acquiring data in one market to gain market power in another can have anticompetitive effects.[64]

In India, WhatsApp and Facebook were accused of tie-in sales. It was alleged that "*WhatsApp's proposed business model of integrating its payment app called 'WhatsApp*

[61] Akihilo Nakagawa and Noriaki Matsushima, 'A Note on Conglomerate Mergers: The Google/Fitbit Case' (2023) 67(6) Japan and the World Economy Journal 101203.

[62] Competition and Markets Authority, 'Commercial Use of Consumer Data' (2016) 38, 90 <https://assets.publishing.service.gov.uk/media/5a7f2a8840f0b6230268dd76/The_commercial_use_of_consumer_data.pdf> accessed 14 August 2024.

[63] Ibid.

[64] French Competition Authority, 'Relatif à L'utilisation Croisée des Bases de Clientèle, No. 10-A-13' (2010) <https://www.autoritedelaconcurrence.fr/fr/avis/relatif-lutilisation-croisee-des-bases-de-clientele> accessed 10 January 2025.

Pay' within its messaging app is anti-competitive."[65] Furthermore, WhatsApp used customer data to attract customers and provide customised advertisements, which was monetised by Facebook to generate revenue and to distort the market. Allegations for the violation of Section 4(2)(e) of the Indian Competition Act, 2002 were levied on the parties. However, the Competition Commission of India dismissed the case, stating that there was a lack of *prima facie* contravention of the Act.

The European Commission, in the *Google Android Case*[66], found that Google had violated its dominant position by tying the Google Search app to its Play Store app. Also, Google's arrangements with device manufacturers to mandate pre-installation of Google's app to limit competition in the market created ecosystem lock-in, giving Google a unique competitive advantage that its competitors could not offset. The commission fined Google €4.125 billion, highlighting the strict enforcement of competition law to tackle the abuse of dominant position by tie-in arrangements.[67]

However, according to the counter-argument, tie-in arrangements cannot be categorised as anti-competitive *per se* as they have their own set of economic benefits.[68] It is argued that after utilising and analysing user data, companies can increase sales by offering goods as a single combined package along with additional discounts, attractive prices, or complementary products by virtue of tying or bundling. Amazon, for instance, recommends 'frequently brought together products', giving customers appealing options to purchase different categories of products. So, if a customer buys a phone, recommendations of phone cases and screen guards are given for consumers' benefit. Therefore, it is imperative that in a data-driven economy, the competition authorities assess tie-in arrangements based on whether they are likely to promote or restrict competition, balancing both pro-competitive justifications and potential anti-competitive risks.

3.3.5 Concerted Actions

As discussed earlier, data collection can increase transparency between suppliers, limit competition and, in cases where market concentration is high, could even lead to cartelisation via the use of artificial intelligence.[69] Competition laws generally look down upon the existence of cartels as they can cause adverse effects on the competition in the market. With the insurgence of data-based algorithms to execute collusive agreements

[65] *Harshita Chawla v WhatsApp and Facebook* [2020] COMP 15/2020.
[66] Case AT. 40099, *Google Android* [2018] OJ C402/19.
[67] European Commission, 'Antitrust: Commission Fines Google €4.125 Billion For Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google Search Engine' (18 July 2018) <https://ec.europa.eu/commission/presscorner/detail/en/ip_18_4581> accessed 10 January 2025.
[68] Michael A Salinger, 'Tying and Bundling in a Nearly Contestable Market' (2011) SSRN Electronic Journal <DOI:10.2139/ssrn.1857551> accessed 10 January 2025.
[69] Ezrachi and Stucke (n 34).

and fix concerted prices, it has become increasingly difficult for competition regulatory authorities across the world to establish the existence of cartels that are more than mere conscious price parallelism.

The Canadian Competition Bureau also recognised that companies may use big data and artificial intelligence to innovate novel ways to implement cartel agreements.[70] A member of the Competition Commission of India stated that finding methods to prevent collusion between self-learning algorithms could be one of the biggest challenges that competition law enforcers have ever faced.[71] To combat this issue, the (then) European Commissioner issued a strict warning to companies that use pricing algorithms to facilitate tacit collusion.[72] Competition and Market Authority of the UK published research on 'Pricing Algorithms, Collusion, and Personalised Pricing', which states that some algorithmic decisions should be presumed to be anti-competitive.

3.3.6 Data and its Effects on Privacy

A significant concern regarding the collection of big data by dominant enterprises pertains to its impact on data privacy. Although most governments have executed specific statutes to look after data protection yet, they cannot exist in silos, especially in cases where the eligible violation of data privacy has been done by a dominant enterprise whose business model is predominantly based upon the collection and analysis of data. According to the OECD, data plays a pivotal role in platform markets' power and in situations where consumers and users become data subjects, "data privacy has the possibility of becoming a relevant non-price parameter of competition whether as a dimension of quality or of choice".[73]

For instance, the German Competition Authority issued an order against Meta (then Facebook) for excessive collection of user data through third-party websites and other services owned by Facebook without user consent.[74] Meta's actions were held to be an

[70] Canada Competition Bureau, 'Big Data and Innovation: Key Themes for Competition Policy in Canada' (2018) <https://competition-bureau.canada.ca/en/big-data-and-innovation-key-themes-competition-policy-canada> accessed 10 January 2025.

[71] Augustine Peter, 'Speech at the ASSOCHAM 5th International Conference on Competition Law and Tech Sector' (*Competition Commission of India*,19 January 2018) <http://164.100.58.95/node/3707> accessed 10 June 2024.

[72] Organisation for Economic Cooperation and Development, *Algorithms and Collusion - Note from the European Union* (OECD Publishing, 2017) <https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf> accessed 10 January 2025; Margrethe Vestager, 'Algorithms and Competition-Speech at the Bundeskartellamt 18th Conference on Competition' (*European Commission*, 17 March 2017) <https://ec.europa.eu/newsroom/comp/newsletter-archives/2831> accessed 10 June 2024.

[73] Organisation for Economic Cooperation and Development, *The Intersection Between Competition and Data Privacy-Background Note* (OECD Publishing, 2024) <https://one.oecd.org/document/DAF/COMP(2024)4/en/pdf> accessed 10 June 2024.

[74] Bundeskartellamt, 'Facebook Inc. Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing' (6 February 2019) Ref B6-22/16

abuse of its dominant position in the market for online social networks in Germany and a violation of Section 19(1) of the German Competition Act.[75] Meta, however, challenged this German ruling, leading to a preliminary reference at the Court of Justice of the European Union (CJEU).[76] The CJEU ruled that competition authorities can assess the compliance of the General Data Protection Regulation when examining abusive actions under the competition law.[77] Further, unfair data processing conditions imposed by a dominant enterprise could be categorized as an 'abuse' under Section 102(a) of TFEU. This case highlights the stern view being taken against data-driven companies with strong market power, primarily relying on collecting and analysing user data that may get incentivised to reduce the level of privacy and further increase data collection to a level that may become unfair, abusive, and detrimental to the consumers and competitors.

In India as well, a similar approach was observed when the Competition Commission of India started an investigation into WhatsApp's Privacy Policy for abusing its dominant position and violating Section 4 of the Indian Competition Act 2002. WhatsApp was accused of imposing unfair conditions upon users through its privacy policy and data-sharing terms.[78] WhatsApp and Facebook appealed against this investigation in the Supreme Court of India, citing that this investigation fell within the jurisdiction of the information technology law framework and not competition law. Interestingly, their appeal was rejected, and the Competition Commission of India was asked to further investigate the competition concerns around WhatsApp's data collection and usage.[79]

4 Pro-Competition Effects of Big Data: Counter-Argument

The discussion around the implications of big data on competition is incomplete without highlighting the benefits consumers can get through data analytics. Through appropriate collection, utilisation, and application of data, consumers can get personalised services from dominant companies such as Google, Amazon, and YouTube. Research has showcased that few customers believe that a data-driven company can (i) provide a better experience by using customer's personal information, (ii) decrease the prices or provide free services due to the use of their customer data. In many cases, the value of these tailored services may surpass the consumer's concern regarding their data privacy.[80] It has been contended that monetisation of big data should be viewed as "economically rational profit-

<https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=> accessed 30 January 2025.

[75] Ibid.

[76] Treaty of the Functioning of the European Union [2008] OJ C115/47, Article 267.

[77] Case C-252/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537.

[78] *Updated Terms of Service and Privacy Policy for WhatsApp Users* [2021] (COMP/01/2021).

[79] *Meta Platforms Inc. v Competition Commission of India* [2022] (SLP (C) No. 17121).

[80] Morey, Forbath and Schoop (n 32).

maximising behaviour that results in obvious consumer benefits."[81] The following part outlines a few arguments that highlight the pro-competitive effects of big data in the digital markets.

4.1 Free Availability of Data

According to one argument, big data can create entry barriers owing to the difficulty of collection and replication of unique data; however, according to the counter-argument, citing big data as an entry barrier is a myth as data is omnipresent and freely available.[82] When considering the competitive impact of data ownership by one enterprise, the primary issue is whether similar big data in terms of size and relevance is available to another efficient enterprise. Three factors may contribute to the high accessibility of data between competitors. Firstly, data is considered non-rival goods, which means that the collection and use of one type of big data does not hinder other enterprises or companies from using the same data. Secondly, data acquired by one company is available for other companies to purchase (provided they can access it in both previous cases).[83] Thirdly, consumers can also provide similar data to different companies, whether they are competitors or not (multi-homing), making data availability seamless.

However, the non-rivalrous nature of data does not mean that it is equally accessible to all companies. As discussed earlier, companies may gain a competitive advantage due to the uniqueness of the data, which may not be easy to get, incentivising companies not to share them with their competitors.[84] This is coupled with the fact that access to data may also require some underlying costs and investments, like the development of data centres, building a significant customer base, innovation costs, research and development expenses, acquisition costs, and costs to develop highly technical algorithms for data analysis.[85] It makes it very difficult for a new entrant to amass a large number of consumers, collect data, and the consequential market power to become a significant rival.

Furthermore, data collected and sold by third-party intermediaries can also be used by new entrants. These third-party intermediaries use various data-collecting technologies such as tracking by cookies, picking up data from public authorities, or simply gathering data from alternative or unfair means. However, buying this data may be more expensive

[81] D Daniel Sokol and Roisin Comerford, 'Antitrust and Regulating Big Data' (2016) 23 Geo Mason Law Review 1129.
[82] Geoffrey A Manne and Ben Sperry, '*Debunking the Myth of a Data Barrier to Entry for Online Services*' (*International Center for Law and Economics*, 26 March 2015) <https://laweconcenter.org/images/articles/icle-tf_nomi_comments_20150526.pdf> accessed 10 June 2024.
[83] Nils-Peter Schepp and Achim Wambach, 'Big Data and its Relevance for Market Power Assessment' (2016) 7(2) Journal of European Competition Law and Practice 120.
[84] Priyadarsini (n 5).
[85] Lasserre and Mundt (n 2).

and less valuable for the new entrant than the data collected by continuous consumer interaction.

4.2 Fluidity of Data-driven Market Power

Another characteristic of the digital market is the potential of consumers to multi-home, whereby the consumer can utilise the services of different providers and share similar data within the same horizontal market.[86] For instance, in the e-commerce market, a consumer may share their relevant information (such as their name, phone number, and address) with multiple players like Amazon, Flipkart or eBay. Multihoming can reduce the possibility of the formation of a data monopoly and may even reduce market power.[87] In such situations, mere possession of data cannot confer a high competitive leverage. For instance, 'X' (formally Twitter) in the social networking market or 'Tinder' within the online dating platform market were successfully able to disrupt the market and supersede the older players that may have gathered ample data before them, showcasing higher importance of innovation and lesser of data as far as granting competitive benefits are concerned.[88]

The value of data is frequently perceived as temporary.[89] There exists a perpetual demand for new and differentiated data; therefore, even when a company possesses a substantial volume of data, competitors may undermine its competitive prowess by acquiring more relevant information.[90] In the case concerning the merger between *Microsoft and Skype*, the European Commission recognised that Microsoft's substantial market share, estimated to be between 80 to 90 per cent in the video communication sector, did not necessarily indicate the presence of dominant market power.[91] This conclusion was grounded in the rapidly evolving and innovative characteristics inherent within the technology sector. The General Court affirmed this rationale, highlighting that elevated market shares in dynamic, technology-centric markets often lack sustainability and that consumers are presented with numerous alternatives, which help to maintain competitive pressure.[92] This perspective was subsequently reaffirmed in the *Facebook/WhatsApp* case in 2014, where it was established that a high market share does

[86] David S Evans and Richard Schmalensee, 'The Industrial Organisation of Markets with Two-Sided Platforms' (2007) 3(1) Competition Policy International 151.
[87] Ibid.
[88] DS Tucker and HB Wellford, 'Big Mistakes Regarding Big Data' *(The American Bar Association*, December 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549044> accessed 30 January 2025.
[89] Sokol (n 81).
[90] Ibid.
[91] *Microsoft/Skype* (Case COMP/M. 6281) Commission Decision 2011/7279 [2011] OJ L 268/1.
[92] Sangin Park, 'Market Power in Competition for The Market' (2009) 5(3*) Journal of Competition Law and Economics* 571.

not equate to enduring competitive harm, particularly considering the relative ease with which new competitors can enter the communications market.[93]

4.3 Data Privacy Concerns are Outside the Jurisdiction of Competition Regulators

According to the OECD, although data protection and competition authorities operate under distinct conceptual frameworks and pursue different public policy objectives, yet, there is an increasing focus on the simultaneous application of these two legal regimes within digital markets.[94] On the one hand, the anonymised nature of big data poses no threat to consumer privacy; on the other hand, it has been acknowledged that big data analytics has the potential to challenge the fundamental principles of privacy laws.[95]

As per research, utilisation of big data undermines the effectiveness of informed consent in three significant ways: (i) it is impossible for firms that possess the data to provide adequate notice, as it is unpredictable when a particular conclusion might be derived; (ii) users are unable to provide meaningful consent for the use of their data in big data analyses at every juncture; and (iii) the applicability of concepts such as consent, portability, and access to knowledge obtained through data analysis is ambiguous, particularly when such data has been anonymised, as there may not be a breach of any individual obligation.[96]

For instance, in the *Google/Nestlab*[97] and the *Facebook/WhatsApp*[98] transactions in the early 2000s, the United States regulators iterated that data privacy and misuse of data by platforms are issues exclusively within the jurisdiction of consumer protection authorities and are outside the scope of antitrust regulations.[99] Even in the *Microsoft/LinkedIn Case*[100], the European Commission reminded that "the risks associated with data combination strategies would be mitigated and addressed by the applicable data privacy rules". In the recent past, the Competition Bureau of Canada also shared the 'separatist perspective' like its US and EU counterparts observing, that its jurisdiction is not inclusive of data privacy concerns that are unrelated to competition, as competition and data privacy laws are "associated with different rights and focus on different harms".[101]

[93] Facebook (n 56).
[94] OECD-2024 (n 73).
[95] Priyadarsini (n 5).
[96] Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) *International Data Privacy Law* 74.
[97] US Federal Trade Commission, 'Early Termination Notices 200140457: Nest Labs Inc. and Google Inc.' (February 2014) <https://www.ftc.gov/legal-library/browse/early-termination-notices/20140457> accessed 14 August 2024.
[98] US Federal Trade, 'FTC Notifies Facebook, Whatsapp of Privacy Obligations in Light of Proposed Acquisition' (2014) <https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed-acquisition> accessed 14 August 2024.
[99] Pinar Akman and Martin Christen, 'International Perspectives on Privacy and Competition law' (*American Bar Association*, 2022) <https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-february/international-perspectives-on-privacy-and-competition-law/> accessed 14 August 2024.
[100] *Microsoft/LinkedIn* (n 57).
[101] OECD-2024 (n 73).

Historically, competition law and data privacy were viewed as distinct areas of regulation. However, as discussed in the earlier parts, many jurisdictions are now beginning to recognise that collection and access to consumer data pose significant implications for competition policy and enforcement. For instance, Articles 101 and 102 of TFEU prohibit the abuse of a dominant position in the market through data collection, control, or privacy, which impacts competition.[102] Therefore, it is prudent to say that data privacy is now being regarded not merely as an independent variable but also as a potential component of quality, which can serve as a basis for fair competition amongst companies.

5 Is Competition Law Ready for Big Data?

The above discussion showcases how there are arguments for and against the issue regarding the potential of big data to affect competition in the long run. Proving foreclosure of competitors or adverse effects on competition in the market due to data ownership presents significant challenges, specifically due to the inherent characteristics of the digital market, such as its multi-sided nature, prevalence of multi-homing, and dynamic conditions of the digital trade. The following part outlines a few arenas where the competition regulatory authorities encounter challenges while addressing this issue along with suggestions for rectification.

5.1 Delineating 'Relevant Market'

The first step in identifying anti-competitive behaviour is identifying the relevant market. A market where businesses are powerless to regulate the prices of the goods they sell is said to be perfectly competitive.[103] This is because the market for the specific good in question has many buyers and sellers, each of whom is small in comparison to the market's size, and when the products sold are the same, there are no obstacles preventing new businesses from entering the market.[104] A poorly defined market can impact the assessment of market power and anti-competitive practices; therefore, it is a challenge for competition authorities across the world to define a 'relevant market' in the digital marketplace. Traditionally, two factors are taken into consideration to define the relevant market: (i) the relevant product market, which includes goods and services; (ii) the

[102] *Meta Case* (n 77).
[103] Competition Commission of India, *Competition Law Module for Administrative and Judicial Academies* (1st edition, Government of India, 2019).
[104] Ibid.

relevant geographical market, which connotes the geographical location where the competition takes place.[105]

However, in the context of big data, delineating relevant markets becomes a complex task due to the presence of factors such as the intangible nature of data, consumer multi-homing, network effects, and the multi-sided nature of platforms -as they cater to many types of different groups of users like buyers, sellers, consumers or advertisers concurrently and possibly in different jurisdictions.[106] For instance, online platforms like Google or Instagram do not monetarily charge consumers for their 'services' but collect vast amounts of personal data.[107] The challenge in such situations lies in determining relevant markets for data-driven businesses that may not conform to traditional market boundaries. While data is a crucial contributor to market power, it is not always clear whether it should be treated as a separate product or simply part of a broader service offering, as the market power may not manifest on all sides simultaneously.

Furthermore, in antitrust cases, the definition of 'relevant market' is established through the application of the 'substitutability test', which identifies the relevant market as the collection of goods and services that are interchangeable or substitutable with each other from the perspective of the consumer.[108] A vital tool for determining substitutability is the "Small but Significant, Non-Transitory Increase in Price (SSNIP) test or Hypothetical Monopolist Test, which evaluates whether, for a small, yet significant price rise (of about 5% to 10%), the consumers of a particular product would shift their choices to another product."[109] If so, then the two products can be considered to be part of the same market.

In the case of big data, the SSNIP or Hypothetical Monopolist Test may become ineffective. Big data does not fit within the pigeon-hole of being either a product or service, making the SSNIP test ineffective for two reasons. Firstly, unlike tangible goods, big datasets can be reused multiple times simultaneously by many firms, making it difficult to define them within the norms of a single market based on substitution. Secondly, many platforms gather data in return for free of cost services.[110] In such situations, determining

[105] Vicente Bagnoli, 'The Big Data Relevant Market as a Tool for a Case-by-Case Analysis at the Digital Economy: Could the EU Decision at Facebook/WhatsApp Merger Have Been Different?' (12th Ascola Conference, 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064795#> accessed 14 August 2024.

[106] Organization for Economic Cooperation and Development, *The Digital Economy, New Business Models and Key Features in Addressing the Tax Challenges of the Digital Economy* (OECD Publishing, 2014).

[107] *Google Search (Shopping) Case* (n 43); European Commission, 'Antitrust: Commission Fines Google €2.42 Billion For Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service' (27 July 2017) <https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1784> accessed 14 August 2024.

[108] Tilottama Raychaudhuri, 'Abuse of Dominance in Digital Platforms: An Analysis of Indian Competition Jurisprudence' (2020) 1 Competition Commission of India Journal on Competition Law and Policy 1.

[109] Ibid.

[110] European Commission (n 107).

substitutability in terms of 'small yet significant price rise' makes the whole concept redundant.[111]

Therefore, instead of viewing data as a product to define the relevant market, other ancillary factors, such as consumer preference or a company's ability to analyse and act on data, may be considered by the regulators while investigating cases. In the case of multi-sided platforms, the regulators can define a relevant product market for the products being offered by the overall platform or the products offered on each side of the platform as a distinct relevant market. The European Commission's case against *Google*[112] also provides insight into assessing market dominance. The Commission highlighted that Google's actions of accumulating users' big data created high entry barriers even though, in this case, data itself was not the sole focus of market definition. Further, the Commission identified four separate but interrelated product markets that were affected by Google without explicitly distinguishing between a single market approach and multiple separate markets but focusing on the source for competitive constraints.

5.2 Assessing Dominance

The increasing reliance on data for trade and innovation within digital markets presents challenges to traditional analysis of dominance under competition regulation, as the competition between digital enterprises is no longer solely centred around monetary pricing. The primary challenge associated with assessing dominance in cases related to data is the manner in which data is utilised along with its uncertain value, which complicates the application of price-based analytical tools as data itself does not possess a fixed value.[113] Its potential value is derived from the application of data analytics in the digital trade. Merely acquiring or holding data sets big datasets is inefficient in the long run for two reasons: firstly, the organisation must be capable of unlocking its potential value in conjunction with employing sophisticated algorithms that can extract valuable insights from the information; secondly, the organisation must be engaged in continuous data collection and maintaining access to relevant datasets.[114]

Due to the dynamic nature of data-driven digital markets, companies that have accumulated large amounts of big data sets that contribute to their market power may become temporarily dominant but may eventually be replaced by companies with better products, advanced algorithms, personalised recommendations (like Netflix)[115], higher

[111] Howard A Shelanski, 'Information Innovation and Competition Policy for the Internet' (2013) 161 University of Pennsylvania Law Review 1663.
[112] *Google Android* (n 66).
[113] Tone Knapstad, 'Digital Dominance Assessing Market Definition and Market Power for Online Platforms Under Article 102 TFEU' (2023) 20(2) European Competition Journal 412.
[114] Ibid.
[115] Andrei Hagiu and Julian Wright, 'When Data Creates Competitive Advantage' (*Harvard Business Review*, January 2020) <https://hbr.org/2020/01/when-data-creates-competitive-advantage> accessed 28 January 2025.

search accuracy, better technology or novel ideas (like the replacement of Yahoo! and Bing by Google or Myspace and Orkut by Facebook). In such circumstances, enforcing strict regulations that hinder the ability of these companies to achieve such market power or temporary dominance may not only impede innovation but may even be detrimental to overall economic growth and consumer welfare.[116]

Furthermore, the term 'dominance' is the key term here because one of the primary challenges in enforcing competition regulation is the lack of finding a company to be dominant in the relevant market. An entity is said to be dominant when it possesses the ability to behave independently of market forces.[117] Many digital platforms collecting consumer big data cannot be termed 'dominant' due to the presence of other significant competitors who are also collecting similar data (for instance, due to consumers' multi-homing), which renders them unable to operate independently of market forces.

It is pertinent to mention that dominance in itself is also not a sign of anti-competitive action. In the *Google case*, the Competition Commission of India noted that if an enterprise accumulates big data to wield substantial market power, it is not the core cause of concern; the cause of concern shall arise when the enterprise abuses this dominant position to stifle competition and innovation, create entry barriers, and exploit the market adversely impacting the consumer.[118] Only by holding the big data of consumers, digital companies do not exclude new entrants.[119]

This means that in such circumstances, case-to-case evaluation by the regulatory authority is necessary to assess dominance. Assessment can be based upon various parameters such as size and resource of the enterprise, number of end users and their dependence on the company, economic power of the company, network effects, barriers to entry, cost of substitutable goods, data-driven advantages or data leveraging techniques.

5.3 Data-sharing to Aid Competition

As discussed in the earlier parts, prominent digital companies in a data-driven market can hold and restrict access to large amounts of big data, hindering fair play. Data sharing among computers can facilitate the realisation of 'data value transfer' and its co-creation, enhancing product innovation.[120] Additionally, such data sharing can augment the attractiveness of the product and intensify competition within the market. Access to

[116] Shelanski (n 111).
[117] Knapstad (n 113).
[118] *Matrimony.com* (n 18).
[119] US Federal Trade Commission, 'Generative AI Raises Competition Concerns' (29 June 2023) <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns> accessed 28 January 2025.
[120] Haifei Yu, Yanbin Gao and Yuanyuan Lu, 'Company Data Sharing, Product Innovation and Competitive Strategies' 234 (2023) Expert Systems with Applications 121083.

relevant data can enable new market entrants to anticipate evolving market needs, deliver targeted products and services, and triumph over data-rated barriers to entry.[121] Furthermore, data sharing by those with exclusive access to valuable information or essential data with new entrants can reduce consumer welfare concerns and increase overall market efficiency.

The concentration of data with a single player (data monopoly) has the potential to cause market failure and loss of efficiency that could otherwise be achieved by leveraging that data.[122] To promote fair competition, it may become imperative to mandate the sharing of essential data on a case-to-case basis, specifically in markets where the ability of new entrants to compete effectively is hindered without access to data possessed by the dominant enterprises.[123] To justify the collection of data, fair, reasonable, and non-discriminatory (FRAND) pricing could be determined to compensate the data-sharing digital company.[124] The concept of FRAND is frequently discussed in relation to Standard Essential Patents can be effectively utilised to attain a balance between fostering competition and minimising the intrusion into databases of major technological companies.[125]

The 'Citymapper' case study is a great example of how data sharing fosters innovation and enhances consumer welfare. Following 'Transport for London's' provision of free, real-time data in 2009 in an open format, a business called Citymapper generated economic benefits of approximately GBP 130 million annually within the United Kingdom, showcasing how an appropriate data-sharing strategy can be established without unfairly harming the original owner of data.[126] Furthermore, the UK's "Online Platforms and Digital Advertising Market Strategy, 2019" and EU's "Regulation on Contestable and Fair Markets in the Digital Sector Act, 2022 (DMA)" are noteworthy regulations that have established explicit and proposed data-sharing obligations. According to these laws, dominant search engine service providers must share click and query data with competing search engines. The Act also requires gatekeepers to provide "effective, high-quality, continuous and real-time access and use of aggregated and non-aggregated data"[127], showcasing the growing regulations to promote data-sharing between competitors.

[121] Priyanka Vinayak Bhat, 'Data Sharing for Contestability in Data-Driven Digital Markets: An Analysis' (2023) 4 Competition Commission of India Journal of Competition Law and Policy 1,1.
[122] Jan Kramer and Daniel Schnurr, 'Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies' (2022) 18(2) Journal of Competition Law and Economics 255.
[123] Vikar Kathuria, 'Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy' (2020) 8(3) Journal of Antitrust Enforcement 511.
[124] Mathew Heim and Ignor Nikolic, 'A FRAND Regime for Dominant Digital Platforms' (2019) 10(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 38, 55.
[125] Ibid.
[126] Bhat (n 121).
[127] Regulation (EU) 2022/1925 of the European Parliament and of the Fair Markets in the Digital Sector (Digital Markets Act) [2022], Art 6(10).

5.4 Merger Thresholds

As discussed in the earlier parts, competition authorities are recognising that control over data can enhance market power. In a data-driven market, a merger like this could increase the concentration of relevant data and could restrict the entry and expansion of new companies. Although it is difficult to find a 'one-size-fits-all' merger control policy that can be applied in all merger matters cutting across all jurisdictions as competition policy across the goal is dependent upon various factors such as personal laws, available resources, the experience of regulators and policymakers, and the overall economic status of the country.[128]

Yet, the policymakers must widen the ambit of review to scrutinise mergers by large digital companies even if they do not meet the traditional threshold criteria based upon monetary value. Regulators must pay attention to 'killer acquisitions' in the data-driven markets where large firms buy smaller firms to pre-emptively eliminate future competition. Many jurisdictions have already improved or are in the process of improving their merger control standards to incorporate data-driven combinations. For instance, competition regulatory authorities of Germany[129] and Austria[130] have recognised the lacunas and have introduced the 'value of transaction threshold', through which an acquisition exceeding a value limit can be reviewed even if the turnover or threshold criteria are not met. The Digital Markets Act (DMA) of the European Union also scrutinises data-based mergers. The DMA specifically targets large digital platforms (or 'gatekeepers'), mandating them to notify any merger that they plan to undertake in advance if it involves the collection of large data sets or could adversely impact the competition in the market. Furthermore, through its "Digital Markets, Competition and Consumers Act, 2024", the UK has introduced acquirer-focused merger control thresholds to strengthen the Competition and Market Authorities' investigations and enforcement powers. The Australia Competition and Consumer Commission recommended lowering thresholds for tech mergers, arguing that high thresholds often overlook data-centric acquisitions. Interestingly, unlike its European counterpart, the Australian Commission denied the *Google/Fitbit merger*[131] due to its potential anti-competitive impacts, highlighting the uncertainty in this arena.

Each merger control regime possesses its own criteria for assessing whether a specific transaction will receive approval; polar verdicts in the Google/Fitbit cases, as discussed

[128] United Nations Trade and Development, Intergovernmental Group of Experts on Competition Law and Policy, 'Round Table on Recent Developments in Merger Control Standards' (2024) <https://unctad.org/system/files/information-document/ccpb_IGECOMP2024_PROG_RT_developments_ merger_control_standards_en_0.pdf> accessed 14 August 2024.

[129] German Competition Act 2017 (9th Amendment) (GWB), s. 35 (1a).

[130] Cartel and Competition Law Amendment Act 2017, s. 9(4).

[131] Australian Competition and Consumer Commission, 'ACCC Rejects Google Behavioural Undertaking for FitBit Acquisitions' (2020) <https://www.accc.gov.au/media-release/accc-rejects-google-behavioural-undertakings-for-fitbit-acquisition>accessed 14 August 2024.

above, are a classic example of this. While the overarching ideology may exhibit similarities across many jurisdictions, it is essential to have a global collaboration. Collaboration on an international and regional level is crucial for creating a comprehensive consensus on merger standards, given that business mergers of multinational digital entities significantly affect markets in various jurisdictions.[132]

6 Conclusion

Based upon the above discussion, and after analysing both sets of arguments for and against big data, it can be inferred that big data is fundamentally neither good nor evil. Yet its insurgence and utilisation in trade practices in the digital age cannot be overlooked. The potential of big data to enhance services and products is significant. The effective enforcement of competition regulations can ensure that stakeholders maximise this potential. The practice of collecting, analysing, and utilising data, especially customer data, is a practice that has been in use for a long time. However, recent developments, driven by rapid technological advancements, increased digitalisation, and enhanced connectivity, have dramatically expanded the velocity, variety, volume and value of data and its sources. Consequently, the economic significance of data has escalated rapidly.

The potential adverse effects on competition in a data-driven market have also increased substantially and should not be overlooked. Competition authorities must update their strategies to maintain their effectiveness as regulators. Failure to do so may result in them becoming detached from market realities and reliant on outdated investigative techniques. Therefore, the competition regulating authorities must consider technical, data-related variables when evaluating market power and company behaviour. Due to the diverse and even ambiguous effects of data utilisation, it is pertinent that the regulators assess market situations on a case-by-case basis. In this context, the dynamic characteristics of digital markets- such as network effects, multi-homing, and use of advanced algorithms, must be taken into account.

It is evident that competition regulatory authorities across the world are still in a nascent stage of addressing this new challenge. Therefore, it is essential for them to and hence their strategy to continue being effective regulators. Furthermore, increased collaboration amongst regulatory authorities worldwide, along with the cooperation of data protection agencies, will yield mutual benefits. By fostering such collaborations, authorities will be better equipped to tackle the challenges that big data presents for trade in the digital economy.

[132] United Nations Trade and Development (n 128).

Pallavi Arora[*] *and Jyotsna Manohar*[**]

EX-ANTE COMPETITION REGULATION OF DIGITAL MARKETS: RETHINKING REGULATORY AUTONOMY UNDER THE GATS NON-DISCRIMINATION OBLIGATION

Abstract

In light of the growing complexities of data-driven digital markets, traditional *ex-post* competition laws are often insufficient, prompting many jurisdictions to adopt *ex-ante* regulatory frameworks. This paper examines the compatibility of *ex-ante* competition regulations, such as the European Union's Digital Markets Act (DMA), with the General Agreement on Trade in Services (GATS), focusing on the potential violation of national treatment and most-favoured-nation obligations. The paper critiques the Appellate Body's narrow approach in *Argentina-Financial Services*, which limits the consideration of regulatory intent in the GATS non-discrimination analysis. It advocates for a broader approach that integrates regulatory purpose in assessing 'likeness' and 'less favourable treatment'. The paper concludes that such a perspective would ensure that *ex-ante* competition regulations, like the DMA, can be justified under GATS without undermining fair competition, while allowing states to regulate digital markets effectively.

JEL Classification: F13; K21.

SUMMARY

1. Introduction – 2. Rationale for *Ex-Ante* Competition Regulation of Data-Driven Digital Markets – 2.1 Data Dynamics: Traditional Markets versus Digital Markets – 2.2 Limitations of *Ex-Post* Competition Law in Data-Driven Digital Markets – 2.3 Emergence of *Ex-Ante* Competition Regulation Across Jurisdictions – 2.3.1 Overview of EU's DMA – 2.3.1.1 Scope of Application and Designation of Gatekeepers Under DMA – 2.3.1.2 *Ex-Ante* Obligations Under DMA – 2.3.2 Overview of *Ex-Ante* Competition Regulation in Other Jurisdictions – 3. *Ex-Ante* Regulation and the US Big Tech Lobby: Concerns over Potential Violation of the WTO's Non-Discrimination Obligation: An Overview – 4. Approach to Assessing the Consistency of *Ex-Ante* Competition Regulations with the Non-Discrimination Obligation under GATS – 4.1 The Non-Discrimination Obligation and General Exceptions Clause under GATS: An Overview – 4.2 *De facto* discrimination and the DMA - 4.3 Justifying *Ex Ante* Competition Regulations under the GATS General Exceptions Clause – 5. *Ex-Ante* Competition Regulation and the GATS Non-Discrimination Obligation: Is the Regulatory Context Relevant? – 5.1 The 'Likeness' Analysis under GATS: Exploring Pathways to Accommodate Regulatory Autonomy – 5.1.1 Combined Reference to 'Service and Service Supplier' under the GATS 'Likeness' Analysis – 5.1.2 The Aim

[*] Legal Consultant (at the level of Assistant Professor) at the Centre for WTO Studies, Indian Institute of Foreign Trade, New Delhi, India. E-mail: pallavi@iift.edu.
[**] Young Professional at the Centre for WTO Studies, Indian Institute of Foreign Trade, New Delhi, India.

 DOI 10.13135/2785-7867/11806

and Effects Test under the GATS 'Likeness' Analysis – 5.1.3 Nature and Extent of Competitive Relationship: Can the Regulatory Context Play a Role? – 5.1.4 Exploring Approaches to Integrate the Regulatory Purpose under the 'Competitive Likeness' Test - 5.2 The 'Less Favourable Treatment' Test under GATS: How Relevant is the Regulatory Context? – 5.2.1 Resurgence of the Aim and Effects Test under the 'Less Favourable Treatment' Analysis? – 5.2.2 The AB Ruling in *Argentina-Financial Services*: A Shift Toward Formalism – 6. Conclusion.

1 Introduction

Regulating data-driven digital markets has presented significant challenges for competition authorities, highlighting the need for *ex-ante* regulation alongside traditional *ex-post* competition law enforcement. Digital markets differ from traditional ones due to their reliance on user data, network effects, and economies of scale, which allow dominant firms to strengthen their market position and suppress competition. The traditional *ex-post* competition law framework, which addresses anti-competitive behaviour only after it occurs, is often too slow and insufficient to address the fast-paced dynamics of digital markets. This has led to a shift toward *ex-ante* regulation, where preemptive measures are taken to prevent anti-competitive practices and ensure fair competition before harm occurs. Various jurisdictions are adopting or considering such regulations to address these complexities effectively.

A frontrunner in *ex-ante* competition regulation is the European Union's (EU) Digital Markets Act (DMA). Introduced in 2022, the DMA targets large digital platforms identified as Gatekeepers and imposes *ex-ante* obligations to prevent anti-competitive behaviour before it occurs. By establishing these preemptive obligations, the DMA seeks to promote fair competition in digital markets, addressing concerns about market dominance and the slow response of traditional *ex-post* competition laws. Meanwhile, other jurisdictions are also experimenting with the *ex-ante* competition regulation of digital markets. Countries like Germany, South Korea, Australia, Canada, Japan, and the United Kingdom have already implemented such laws, while China, India, and the United States (US), among others, are exploring similar initiatives.

However, large US tech corporations, particularly the Big Tech companies, have voiced strong opposition to the adoption of *ex-ante* competition regulations, both within the US and in other jurisdictions. They have criticised regulations like the DMA as potential violations of the World Trade Organisation's (WTO) non-discrimination obligation, contending that its provisions unfairly target US-based digital firms. According to these corporations, the DMA's qualitative and quantitative thresholds for designating Gatekeepers disproportionately capture major US tech companies, while largely excluding digital firms from the EU and other countries. This, they argue, places US firms at a competitive disadvantage by subjecting them to strict *ex-ante* obligations, while competitors from the EU and other WTO Members remain regulated under the comparatively lenient *ex-post* competition framework.

Given this background, this paper examines whether *ex-ante* competition regulations constitute *de facto* discrimination under the General Agreement on Trade in Services (GATS). Specifically, it analyses the consistency of these regulations with the national treatment (NT) and most-favoured-nation (MFN) obligations under GATS. Using the DMA as a case study, the paper revisits the central debate on whether and to what extent the regulatory context of a measure should be considered in assessing 'likeness' and 'less favourable treatment' under Articles II and XVII of GATS. This analysis is particularly relevant when such measures cannot be justified under the closed list of regulatory justifications under the GATS general exceptions clause, which do not account for the complexities of digital markets.

This issue has gained renewed attention following the Appellate Body's (AB) decision in *Argentina-Financial Services*, the most recent case addressing regulatory autonomy under the GATS non-discrimination obligation. In this ruling, the AB significantly limited the consideration of regulatory intent in GATS non-discrimination analysis. This marks a departure from both prevailing scholarly perspectives and the WTO's evolving jurisprudence, which had been moving towards recognising the regulatory purpose behind measures under the non-discrimination analysis. It has far-reaching implications for modern regulatory frameworks, particularly *ex-ante* competition laws.

This paper critiques the AB's position, arguing for the inclusion of regulatory intent either in the 'likeness' assessment or the evaluation of 'less favourable treatment'. Accordingly, we examine other interpretive approaches to the 'likeness' and 'less favourable treatment' analyses that provide greater deference to regulatory objectives. Such approaches, we contend, would preserve the policy space states require to implement measures addressing the intricate challenges of the digital economy.

The paper is organised as follows. Section 2 explores the rationale for *ex-ante* competition regulations in data-driven digital markets, emphasising the inadequacy of traditional *ex-post* competition law in addressing the unique challenges of these markets. Section 3 examines the criticisms by the US big tech lobby against *ex-ante* regulations on the grounds that they amount to *de facto* discrimination under the GATS framework. Section 4 outlines the legal framework for assessing whether *ex-ante* regulations, like the DMA, comply with MFN and NT obligations under GATS. It also highlights the greater role of regulatory context in GATS compared to the General Agreement on Tariffs and Trade (GATT). Section 5 investigates whether the regulatory intent behind *ex-ante* measures can shape the interpretation of 'likeness' and 'less favourable treatment' under the GATS non-discrimination provisions, particularly for *de facto* discrimination, by revisiting WTO jurisprudence on the aim and effects test and reflecting on the AB's reasoning in *Argentina-Financial Services*. Finally, Section 6 concludes.

2 Rationale for *Ex-Ante* Competition Regulation of Data-Driven Digital Markets

Regulating data-driven digital markets has presented substantial challenges for competition authorities worldwide, sparking an active debate on the potential role of *ex-ante* regulation in complementing *ex-post* enforcement of competition law.[1]

This section explores the rationale behind adopting *ex-ante* regulation for digital markets and examines the legislative developments in various jurisdictions to address these challenges.

2.1 Data Dynamics: Traditional Markets versus Digital Markets

In the context of digital markets, data has emerged as a critical strategic asset.[2] Digital firms collect vast amounts of user data through interactions on their platforms, which they leverage to gain valuable insights.[3] This results in a complex reality where services that appear 'free' entail an implicit price where users effectively pay with their personal data. This is markedly different from traditional markets where monetary transactions dominate.[4]

Dominant firms use the data under their control to enhance their services, leverage targeted advertising, and deliver personalised user experiences, which creates substantial competitive advantages for them over new entrants.[5] Such strategies not only suppress competition, but also reinforce market dominance.[6] The following discussion explores how the interplay of data-driven feedback loops, network effects, and lock-in effects creates a self-reinforcing or virtuous cycle that solidifies platform dominance in the digital economy.

A key factor in this self-reinforcing cycle is the ability of data-rich firms to continuously improve their services based on data-driven feedback loops.[7] The **user feedback loop enables firms to leverage** a large user base to gather more data, improve service quality,

---

[1] OECD, '*Ex Ante* Regulation in Digital Markets – Background Note by the Secretariat' (2021) <https://one.oecd.org/document/DAF/COMP(2021)15/en/pdf> accessed 12 January 2025.

[2] Damien Geradin and Dimitrios Katsifis, 'Strengthening Effective Antitrust Enforcement in Digital Platform Markets' (2021) 18(2) European Competition Journal 365-66.

[3] Ibid.

[4] Laura Veldkamp, 'Valuing Data as an Asset' (2023) 27(5) *Review of Finance* 1545-1562; Dan Ciuriak, 'The Economics of Data: Implications for a Data-Driven Economy' (*Centre for International Governance Innovation*, 2020) <https://www.cigionline.org/articles/economics-data-implications-data-driven-economy/> accessed 16 November 2024.

[5] Markus Spiekermann, 'Data Marketplaces: Trends and Monetisation of Data Goods' (2019) 54(4) Intereconomics - Review of European Economic Policy 208-216.

[6] Andres V Lerner, 'The Role of 'Big Data' in Online Platform Competition' (*SSRN*, 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780#:~:text=Lerner-,Andres,Lerner&text=At%20issue%20is%20whether%20the,and%20more%20aggressive%20antitrust%20intervention.> accessed 15 January 2025.

[7] Andrei Hagiu and Julian Wright, 'Data-Enabled Learning, Network Effects and Competitive Advantage' (2023) 54(4) The RAND Journal of Economics 1.

and attract even more users.[8] The **monetisation feedback loop** allows intermediaries to profit from aggregated user data for targeted advertising, generating additional revenue to reinvest in service quality, which in turn attracts further users.[9] These self-reinforcing feedback mechanisms create a strong competitive advantage, making it increasingly difficult for new entrants to challenge incumbents, especially when combined with network effects and lock-in effects, as discussed below.

N**etwork effects** refer to the greater value a user gains from a service as more people use it.[10] For example, in the context of digital markets, the value of an e-marketplace to a consumer grows as the number of sellers on the platform increases, and *vice versa*. These dynamics create significant barriers to market entry, as newcomers must not only replicate existing service quality, but also counteract the entrenched network advantages of their more established counterparts.[11]

While network effects draw users to large platforms, lock-in effects make it difficult for them to leave incumbent platforms in favour of new entrants. Lock-in arises from high switching costs that discourage users from migrating to competing platforms.[12] These costs stem from both data-based and non-data-based mechanisms. For instance, Google Chrome enhances convenience by collecting browsing data to personalize content, storing recommended passwords, and offering autofill functionalities. Additionally, its interface design, including tab management and synchronisation features, foster user familiarity and efficiency, further discouraging switching.[13] These elements reinforce the competitive advantage of the incumbent by locking users into a single ecosystem.

In sum, the self-reinforcing nature of data-driven feedback loops, network effects and lock-in effects create a virtuous cycle of platform entrenchment. This is exacerbated by the vital role played by economies of scale in digital markets.[14] Economies of scale refer to decreased per-unit production costs as the quantity of goods or services produced increases.[15] While economies of scale are common across industries, the effect is more pronounced in digital services.[16] In the latter, the cost of serving an additional user or increasing usage by existing users is minimal.[17] A digital enterprise can generate revenue

[8] Lerner (n 6) 3-19; D Daniel Sokol and Roisin Comerford 'Antitrust and Regulating Big Data' (2016) 23 (1129) George Mason Law Review 1147-48.
[9] Ibid.; OECD, 'Big Data: Bringing Competition Policy to the Digital Era' (2016) <https://web-archive.oecd.org/temp/2022-02-21/414870-big-data-bringing-competition-policy-to-the-digital-era.htm> accessed 18 November 2024.
[10] Geradin and Katsifis (n 2) 363-64.
[11] Andrei Hagiu and Julian Wright, 'When Data Creates Competitive Advantage' (*Harvard Business Review*, 2020) <https://hbr.org/2020/01/when-data-creates-competitive-advantage> accessed 18 November 2024.
[12] Emanuele Giovannetti and Paolo Siciliani, 'Platform Competition and Incumbency Advantage under Heterogenous Lock-in Effects' (2023) 63(1) Information Economics and Policy 1-2.
[13] Jiawei Zhang, 'The Paradox of Data Portability and Lock-In Effects' (2023) 36(2) Harvard Journal of Law & Technology 667-668.
[14] Geradin and Katsifis (n 2) 363.
[15] George J Stigler, 'The Economies of Scale' (1958) 1 The Journal of Law & Economics 54-71.
[16] Sten Thore, 'Economies of Scale in the Digital Industry' in Pedro Conceição and others (eds), *Knowledge for Inclusive Development* (Greenwood Publishing Group 2002).
[17] Geradin and Katsifis (n 2) 363.

through subscriptions, usage fees, or commissions without significantly increasing costs. Even if the service is free, the enterprise still gains valuable user data, which can be monetised or used to enhance the service.[18]

The intersection of these elements leads to the phenomenon described as 'winner-takes-most' markets.[19] Here, competition stretches beyond mere product features or pricing. Instead, the competition centres on establishing dominance within the market.[20] Such dynamics often culminate in market concentration, with one or a few firms overshadowing the landscape. Even when a digital firm does not meet legal definitions of dominance, its influence can be so profound that it behaves like a dominant player.[21]

2.2 Limitations of *Ex Post* Competition Law in Data-Driven Digital Markets

Competition law traditionally operates on an *ex-post* framework, where interventions occur only after anti-competitive behaviour has been identified.[22] This approach, designed in a pre-digital era, struggles to keep pace with the unique complexities of digital markets.

As mentioned, digital markets diverge significantly from traditional markets. They are characterised by features such as multi-sided platforms,[23] lock-in effects, network effects, zero-price services, and significant access to consumer data.[24] These characteristics complicate the delineation of relevant markets and the assessment of dominance among digital entities. As a result, incumbents can consolidate their market positions, allowing even non-dominant digital enterprises to exert considerable market influence and evade regulatory scrutiny.[25]

Second, the complexity of delineating the 'relevant market' and assessing the dominance of digital enterprises in the said market adds substantially to the time taken to redress complaints against such enterprises.[26] The present *ex-post* framework of competition law is not designed to facilitate timely and speedy redressal of anti-

[18] Richard A Posner, 'Antitrust in the New Economy' (2000) John M. Olin Program in Law and Economics Working Paper No. 106.
[19] Cyrille Schwellnus and others, 'Labour Share Developments Over the Past Two Decades: The Role of Technological Progress, Globalisation and "Winner-Takes-Most" Dynamics' (2018) OECD Economics Department Working Paper No. 1503; OECD, 'The Evolving Concept of Market Power in the Digital Economy – Note by Brazil' (2022) <https://one.oecd.org/document/DAF/COMP/WD(2022)31/en/pdf> accessed 15 January 2025.
[20] International Monetary Fund, 'World Economic Outlook: Growth Slowdown, Precarious Recovery' (*IMF Report*, 2019) 55-57.
[21] Lina Khan, 'Amazon's Antitrust Paradox' (2018) 126(3) Yale Law Journal 710-805.
[22] Michael G Jacobides and Ioannis Lianos, 'Ecosystems and Competition Law in Theory and Practice' (2021) 30(5) Industrial and Corporate Change 119-1229.
[23] Michael A Cusumano, 'The Evolution of Research on Industry Platforms' (2022) 8(1) Academy of Management Discoveries 7-14.
[24] OECD (n 9).
[25] Alok Prasanna Kumar and Manjushree RM, 'Data, Democracy and Dominance: Exploring a New Antitrust Framework for Digital Platforms' in Centre for Communication Governance (ed), *The Future of Democracy in the Shadow of Big and Emerging Tech* (National Law University Delhi Press 2021) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-future-of-democracy-in-the-shadow-of-big-and-emerging-tech-ccg-248.pdf> accessed 20 November 2024.
[26] Geradin and Katsifis (n 2) 372.

competitive conduct by digital enterprises, given the extensive fact-finding and a tiered adjudicatory process involved in *ex-post* enforcement proceedings. Moreover, *ex-post* enforcement does not always lead to optimal restoration of competition in evolving and fast-paced markets. Investigations into incumbent players under *ex-post* competition law, which begin *after a* contravention has occurred, are resource-intensive and time-consuming.[27] Meanwhile, the market may irreversibly tip in favour of the incumbent and consequently drive out competitors.[28] The harm thus caused is irremediable *ex post facto*. Moreover, *ex-post* competition investigations are limited to the narrow claims made in each specific case.[29] As such, they may not effectively address repeated conduct by the same digital enterprise or similar conduct by different enterprises.

Given these considerations, regulators across several jurisdictions have come to the conclusion that the powers of competition authorities under the *ex-post* model may fall short in facilitating the early detection and intervention necessary to prevent irreparable harm in digital markets.[30] As a response, many jurisdictions have either adopted or are contemplating introducing *ex-ante* regulations to complement *ex-post* competition enforcement.[31] The rationale driving this shift is that the benefits associated with proactive monitoring and intervention in digital markets will likely outweigh the risks of over-regulation inherent in the *ex-ante* approach.[32]

2.3 Emergence of *Ex Ante* Competition Regulations across Jurisdictions

Ex-ante regulation of digital markets entails a framework that preemptively addresses potential anti-competitive behaviours and structural inefficiencies before they manifest. In contrast to *ex-post* enforcement—which responds after a violation has occurred—*ex-ante* regulation imposes specific obligations and prohibitions on dominant digital platforms. It seeks to complement the *ex-post* enforcement of competition law by effectively setting the groundwork to mitigate risks associated with monopolistic practices and market distortions in advance.

The EU's DMA represents a pioneering effort in *ex-ante* competition regulation. Similarly, other jurisdictions have either implemented or are in the process of introducing

[27] Congressional Research Service, 'Regulating Big Tech: CRS Legal Products for the 118th Congress' (2024) <https://crsreports.congress.gov/product/pdf/LSB/LSB10889> accessed 20 November 2024.
[28] Nicolas Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' (2021) 12(7) Journal of European Competition Law & Practice 529-541.
[29] Geradin and Katsifis (n 2) 372-73.
[30] UNCTAD, 'Global Competition Law and Policy Approaches to Digital Markets' (Report of the United Nations Conference on Trade and Development, 2024) <https://unctad.org/system/files/official-document/ditcclp2023d7_en.pdf> accessed 15 January 2025.
[31] See, for example, the European Union's Digital Markets Act (2022); the United Kingdom's Digital Markets, Competition and Consumers Act (2024); South Korea's App Store Act (2021); Australia's News Media and Digital Platforms Mandatory Bargaining Code (2021); and Canada's Online News Act (2023).
[32] Congressional Research Service (n 27).

such legislation. Germany,[33] South Korea,[34] Australia,[35] Canada,[36] Japan,[37] United Kingdom,[38] have already enacted ex-ante competition laws, while countries like China,[39] India,[40] and the US,[41] among others, are considering similar measures.

In what follows, Section 2.3.1 delves into the substantive features of the EU *ex-ante* regulation, the DMA, to understand its overall design and architecture for *ex-ante* regulation, followed by Section 2.3.2, which presents a summary overview of *ex-ante* regulations that have been implemented or are under consideration in other jurisdictions.

2.3.1 Overview of the EU's DMA

In 2022, the EU enacted the DMA, establishing itself as the first jurisdiction to implement a framework of *ex-ante* regulation for digital markets, designed to work alongside its existing *ex-post* competition law under Articles 101 and 102 of the Treaty on the Functioning of the European Union. The adoption of the DMA was motivated by several factors, notably the protracted timelines associated with *ex-post* investigations and the tendency of digital markets to inherently favour large incumbents, leading to a risk of irreversible market tipping.[42]

2.3.1.1 Scope of Application and Designation of Gatekeepers under the DMA

The DMA applies exclusively to large entities identified as 'Gatekeepers'.[43] To qualify for Gatekeeper status, an entity must offer at least one of the eight specified 'core platform services' outlined in the DMA. These services include online intermediation, online search engines, video-sharing platforms, virtual assistants, social networking, communication platforms, advertising services, operating systems and cloud services.[44] Furthermore, the European Commission (EC) retains the authority to integrate emerging digital services into this framework following a market investigation.[45]

[33] The Competition Act (*Gesetz gegen Wettbewerbsbeschränkungen* - GWB) (2021).
[34] The Telecommunications Business Act (2021).
[35] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act (2021).
[36] Online News Act (2023).
[37] Act on Promotion of Competition for Specified Smartphone Software (2024); and Act on Improving Transparency and Fairness of Digital Platforms (2021).
[38] Digital Markets, Competition and Consumers Act (2024).
[39] The Draft Classification Guidelines (2021); and Draft Responsibility Guidelines (2021).
[40] Digital Competition Bill (2024).
[41] American Innovation and Choice Online Act (2022); Open App Markets Act (2022); and Ending Platform Monopolies Act (2021).
[42] Petit (n 28) 529.
[43] See, Article 3(1) of Digital Markets Act (2022) (DMA). For an overview of the DMA, see, Nicolas Petit (n 28); and Jorg Hoffmann, Liza Hermann, and Lukas Kestler, 'Gatekeeper's Potential Privilege – The Need to Limit DMA Centralization' (2024) 12(1) Journal of Antitrust Enforcement 126-147.
[44] Article 2(2) DMA.
[45] Article 19(1) DMA.

The DMA establishes two pathways for designating an entity as a 'Gatekeeper': the first involves meeting specific quantitative thresholds outlined in the regulation,[46] while the second allows for designation via the EC's residual authority.[47] To determine Gatekeeper status, a comprehensive assessment of both qualitative and quantitative criteria as outlined in the DMA is necessary.

For an entity to qualify as a Gatekeeper under the DMA, it must meet three specific qualitative criteria:

i. It must exert a significant influence on the internal market of the EU,
ii. It must operate a core platform service that acts as a critical gateway for business users to reach end users, and
iii. It must maintain an entrenched and durable position competitive position in its operations, or it must be likely to attain such a position in the near future.[48]

For greater clarity, the DMA specifies that the qualitative thresholds above are deemed satisfied if the quantitative thresholds below are met.

i. An entity is presumed to have a significant impact if it operates the same core platform service (e.g., search engines, social networking, or online marketplaces) in at least three EU member states and has an annual turnover of at least **€7.5 billion** in the European Economic Area in the last three financial years, or a market capitalisation of at least **€75 billion** in the last financial year.[49]
ii. A service qualifies as a critical gateway between business users and end users if it serves at least 45 million monthly active end users (approximately 10% of the EU population) and 10,000 yearly active business users in the EU.[50]
iii. An entity is presumed to have an entrenched and durable position in the market if it consistently meets the above thresholds for active users and business users over the past three financial years.[51]

2.3.1.2 *Ex-Ante* Obligations under the DMA

The DMA imposes *ex-ante* obligations on Gatekeepers, including both prohibitions and mandatory requirements, concerning the core platform services specified in the designation decision.[52]

The DMA prohibits Gatekeepers from *i)* bundling or tying core platform services,[53] *ii)* restricting users from switching[54] or changing preinstalled default services,[55] *iii)* imposing

[46] Article 3(3) DMA.
[47] Article 3(8) DMA.
[48] Article 3(1) DMA.
[49] Article 3(2)(a) DMA.
[50] Article 3(2)(b) DMA.
[51] Article 3(2)(c) DMA.
[52] Article 5 DMA.
[53] Articles 5(7) and 5(8) DMA.
[54] Article 6(6) DMA.
[55] Article 6(4) DMA.

platform parity clauses,[56] and *iv)* engaging in self-preferencing practices.[57] Further, Gatekeepers are restricted from processing or cross-using data obtained through their core platform unless they meet notice and consent requirements under the EU's General Data Protection Regulation.[58] The DMA also prohibits Gatekeepers from using non-publicly available data generated by or provided by business users while using their core platform services.[59]

In addition to the prohibited conduct above, the DMA mandates Gatekeepers to ensure third-party software interoperability with their operating systems (OS) and provide free, effective interoperability for third-party hardware and software providers using core platform services.[60] This includes parity in how third-party and Gatekeeper features interact with the OS or virtual assistants. Further, Gatekeepers are required to adopt transparent, fair, and non-discriminatory practices in relation to self-preferencing.[61] They must also allow users to uninstall default software easily, except when such services are essential to the OS or device functionality.[62]

The DMA also requires Gatekeepers to provide end users with free technical tools to port data generated through core platform services.[63] Business users must also receive free, continuous, real-time, and high-quality access to all data generated using the Gatekeeper's core platform service.[64] Further, to reduce data concentration in online search markets, Gatekeepers' search engines must offer third-party search engines anonymised access to ranking, query, click, and view data on fair, reasonable, and non-discriminatory terms.[65]

Finally, the DMA establishes obligations for Gatekeepers who offer number-independent interpersonal communication services (NIICS).[66] Gatekeepers must ensure the interoperability of basic NIICS functionalities with EU third-party providers by providing the required technical interface free of charge. Additionally, the DMA specifies a phased timeline for implementing interoperability across different NIICS features.[67]

2.3.2 Overview of *Ex-Ante* Competition Regulation in Other Jurisdictions

The adoption of the DMA positions the EU as a leader in *ex-ante* competition regulation for digital markets. However, other jurisdictions are also adopting or exploring similar

[56] Article 5(3) DMA.
[57] Article 6(5) DMA.
[58] Article 5(2) DMA.
[59] Article 6(2) DMA.
[60] Article 6(4) DMA.
[61] Article 6(7) DMA.
[62] Article 6(5) DMA.
[63] Article 6(9) DMA.
[64] Article 6(10) DMA.
[65] Article 6(11) DMA.
[66] Article 7 DMA.
[67] Article 7(2) DMA.

regulations. Table 1 outlines countries that have implemented *ex-ante* regulations, while Table 2 highlights the key features of legislative proposals in countries considering such measures.

Table 1: Overview of *Ex Ante* Competition Regulations Adopted in Various Countries

Country	Scope of Application	Nature of *Ex-Ante* Obligations
Germany	Name of Legislation: The 10th Amendment to the German Competition Act, also known as the *Gesetz gegen Wettbewerbsbeschränkungen* (GWB) Act (2021). Digital Firms covered by the Legislation: Companies which *i)* have no competitors, *ii)* are not exposed any substantial competition; or *iii)* have a 'paramount market position in relation to its competitors' (Section 18(1)). This determination may be based on a non-exhaustive set of criteria, including the entity's relative market power, financial strength, access to competitively sensitive data, and its influence on the business activities of third parties (Section 18(3)).	Prohibited Conduct: The German competition authority may prevent companies from engaging in certain anticompetitive behaviours, including abuse of dominant position (Section 19(1)), self-preferencing (Section 19a(2)(1)), hindering competitors' market access through exclusive pre-installation, integration, or advertising restrictions (Section 19a(2)(2)), expanding the dominant position to a new market (Section 19a(2)(3)), using competitively sensitive data in a way that raises barriers to market entry (Section 19a(2)(4)), impeding interoperability (Section 19a(2)(5)), providing insufficient information about their services (Section 19a(2)(6)), or demanding benefits for handling the offers of another undertaking which are disproportionate to the reasons (Section 19a(2)(7)) (See also Sections 20 and 21).

South Korea	Name of Legislation: Amendment to the Telecommunications Business Act, also known as the 'App-Store Act', 2021. Digital Firms covered by the Legislation: The Act aims to promote increased competition in the app market by regulating the conduct of app market business operators as defined in Article 2(13).	Prohibited Conduct: This legislation prohibits app market business operators from abusing their dominant position in the market by *i)* forcing app developers to use the firms' own payment systems (Article 50(9)), *ii)* unfairly delaying the review of mobile content (Article 50(10)), and *iii)* unfairly deleting mobile content from the app market (Article 50(11)). Obligatory Conduct: An app market business operator must prevent damage to users and protect their rights by implementing measures like specifying settlement of payment and refund for mobile contacts in the app's terms of use (Section 22-9(1)).
Australia	Name of Legislation: Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021. Digital Firms covered by the Legislation: The Act aims to ensure fair remuneration by 'designated' digital platforms to news businesses for their content. The designation of digital platforms is determined based on *i)* whether there is a significant bargaining power imbalance between Australian news businesses and the digital platform or service, and *ii)*	Obligatory Conduct: In case voluntary agreement regarding remuneration cannot be reached with designated digital platforms, registered news businesses have the right to proceed under the Act for bargaining and mediation (Division 6, Section 52ZD to Section 52ZJ) followed by arbitration (Division 7, Section 52ZK to Section ZZE). Designated digital platforms also have a general obligation to *i)* notify news businesses in advance regarding algorithmic

	whether the digital platform has made a significant contribution to the sustainability of the Australian news industry through, *inter alia,* voluntary agreements to remunerate news businesses for their content (Section 52E(3)).	changes (Division 4, Section 52S), *ii)* share information with the entity generating news content relating to user interactions (Division 4, Section 52R), and *iii)* refrain from differentiation between news organisations due to their participation or non-participation under the Act (Division 5, Section 52ZC).
Canada	Name of Legislation: The Online News Act, 2023. Digital Firms covered by the Legislation: This Act applies to 'digital news intermediaries', or companies that operate social media platforms or search engines in Canada where there is a 'significant bargaining power imbalance' between its operator and news business. Factors considered in making this determination include: *i)* the size of the intermediary or operator; *ii)* whether the market for the intermediary gives the operator a strategic advantage over new businesses; and *iii)* whether the intermediary occupies a prominent market position (Section 6).	Prohibited Conduct: A digital news intermediary must not discriminate, show undue preference, or disadvantage eligible Canadian news businesses (Section 51). Obligatory Conduct: The Act aims to ensure that digital news intermediaries designated under the Act fairly compensate news businesses when their content is made available on their services. Platforms must first attempt to reach voluntary commercial agreements with news businesses. If negotiations fail, the parties must follow the bargaining process provided under the Act (Section 18-44).
Japan	Name of Legislation: The Act on Improving Transparency and Fairness of Digital Platforms, 2021.	Obligatory Conduct: Specified digital platforms are required to disclose certain information to both user providers and general users. For user

	Digital Firms covered by the Legislation: This Act designates 'specified digital platforms' whose transparency and fairness must be significantly improved, based on thresholds such as total revenue from sale of goods and services, number of users, or other indicators (Article 4(1)).	providers, platforms must provide details on, among other things, fees charged for goods or services and disclose the criteria used for ranking displayed information, including any sponsored rankings (Article 5(2)(i)). For general users, platforms must, among other things, outline the criteria for ranked results, clearly indicate sponsored rankings, and disclose the terms and conditions related to acquiring or using data on user searches, views, and purchases (Article 5(2)(ii)).
United Kingdom	Name of Legislation: Digital Markets, Competition and Consumers Act, 2024. Digital Firms covered by the Legislation: The Competition and Markets Authority (CMA) may designate an undertaking as having 'strategic market status' (SMS) if it is *i)* linked to the United Kingdom (Section 4), *ii)* has substantial and entrenched market power (Section 5), and *iii)* has a position of strategic significance in respect of the digital activity (Section 6). There is also a turnover threshold for a business to be designated as an SMS, and this must exceed £25 billion in global turnover in the relevant period,	Prohibited Conduct: The CMA has the power to impose conduct requirements on SMS entities under Chapter 3 of the Act. These include the prohibition of discriminatory terms, conditions, or policies against certain users (Section 20(3)(a)), self-preferencing (20(3)(b)), behaviour that enhances its market power or reinforces its strategic significance (Section 20(3)(c)), bundling and tying (Section 20(3)(d)), restricting interoperability (Section 20(3)(e)), limiting how users or potential users engage in relevant digital activities (Section 20(3)(f)),using data unfairly (Section 20(3)(g)), and restricting the ability to use

	or £1 billion of UK turnover in the relevant period (Section 7).	products from other undertakings (Section 20(3)(h)). Obligatory Conduct: SMS entities are required to adhere to specific conduct requirements, including engaging in fair trade on reasonable terms (Section 20(2)(a)), establishing effective procedures for handling complaints and disputes with users or potential users (Section 20(2)(b)), and providing clear, accurate, and easily accessible information about relevant digital activities (Section 20(2)(c)). Additionally, SMS entities must give users or potential users explanations and reasonable notice before implementing changes to a digital activity, particularly those with a material impact (Section 20(2)(d)). Furthermore, they must present users with options or default settings in a way that enables informed and effective decision-making (Section 20(2)(e)).

Table 2: Overview of Countries Contemplating the Adoption of *Ex-Ante* Competition Regulation

Country	Scope of Application	Nature of *Ex-Ante* Obligations
China	Name of Proposal: The Draft Classification Guidelines and Draft Responsibilities Guidelines, 2021. Digital Firms covered by the Proposal: The Draft Classification Guidelines categorise platforms based on number of users, businesses offered, market valuation, and ability to affect sellers' ability to reach their consumers. On the basis of this classification system super platforms are subject to the special obligations detailed in the Draft Responsibilities Guidelines. The criteria for designating a super platform include: *i)* at least 500 million annual active users in China in the preceding year; *ii)* engagement in at least two types of platform business; *iii)* a market value of at least RMB 1 trillion at the end of the previous year; and *iv)* a strong ability to restrict merchants from contacting users (Article 3.3).	Prohibited Conduct: Super platforms are prohibited from using non-public data in the absence of legitimate reasons (Article 1(1)), using tied-in services of a related platform (Article 1(2)), and self-preferencing (Article 2). Obligatory Conduct: Super platforms to promote interoperability of services among other platform operators (Article 3), adhere to principles of fairness (Article 2), ensure strong data protection (Article 4), implement compliance mechanisms (Article 5), conduct risk-assessments (Article 6 and 7), be subject to an independent audit (Article 8), use their resources to promote innovation (Article 9) and prevent crime and illegal activity on their platform (Article 10-14).
India	Name of Proposal: Digital Competition Bill, 2024. Digital Firms covered by the Proposal: The proposal	Prohibited Conduct: The draft proposal prohibits SSDEs from engaging in practices like unfair, discriminatory and non-

	proposes the *ex-ante* regulation of entities susceptible to market concentration, called Systemically Significant Digital Enterprises (SSDEs), like search engines, social networking services, operating systems and web browsers. The committee recommends using quantitative and qualitative thresholds to identify SSDEs. The quantitative criteria include an entity's significant financial strength based on factors like turnover, gross merchandise value, and market capitalisation, as well as significant spread based on the number of businesses and end users in India. The qualitative criteria include an entity's resources and volume of aggregated data (Section 3).	transparent dealing (Section 10), self-preferencing (Section 11), using non-public data of business users to compete with them (Section 12(1)), using or sharing users' personal data across services or with third parties without their consent (Section 12(2)), restricting users from using third-party applications (Section 13), preventing business users from contacting customers, promoting offers, or directing them to other services, unless such restrictions are essential to its core services (Section 14), and tying and bundling (Section 15).
United States of America	Name of Proposal: The American Innovation and Choice Online Act, 2022 Digital Firms covered by the Proposal: This proposal, if enacted, would cover online platforms with *i)* at least 50 million monthly active US-based users, or 100,000 US-based monthly active business users at any point during the 12 preceding months; *ii)* owned or controlled by an entity with annual sales exceeding $550 billion, or average market capitalization exceeding $550	Prohibited Conduct: The proposed legislation prohibits 10 categories of conduct, including self-preferencing (Section 3(a)(1)) and Section 3(a)(9)), limiting a competitor's products, services, or business from competing on the platform in a way that significantly harms competition (Section 3(a)(2)), discriminating in the application of their terms of service among similarly situated business users, harming competition (Section 3(a)(3)), restricting

	billion, or at least 1 billion worldwide monthly active users in the preceding 12 months; and *iii)* is a "critical trading partner" for the sale or provision of any product or service offered on or directly related to the platform (Section 2(a)(5)(B)).	interoperability (Section 3(a)(4)), tying and bundling (Section 3(a)(5)), using non-public data generated by users (Section 3(a)(6)), restricting a business user from accessing data it generates on such platforms or data that platform users generate by interacting with a business user's products or services (Section 3(a)(7)), app pre-installation and steering (Section 3(a)(8)), and retaliation against users for raising good faith concerns (Section 3(a)(10)).
	Name of Proposal: The Open App Markets Act, 2022 Digital Firms covered by the Proposal: The proposal aims to prevent prominent app-store operators from engaging in anti-competitive practices in app markets. This legislation would apply to a 'covered company', which is defined as any person that owns or controls an app store for which users in the United States exceed 50,000,000 (Section 2(3)).	Prohibited Conduct: The proposed legislation aims to protect a competitive app market by prohibiting covered companies from certain types of conduct, including self-preferencing (Section 3(e)), exclusivity and tying with respect to in-app payment systems (Section 3(a)), interference with legitimate business communications (Section 3(b)), use of non-public business information derived from a third-party app for the purpose of competing with that app (Section 3(c), impeding interoperability (Section 3(d)), and self-preferencing in search (Section 3(e)).

		Obligatory Conduct: Covered Companies shall provide developers timely, equivalent access to OS interfaces, development information, and hardware/software features (Section 3(f)).

3 *Ex-Ante* Competition Regulations and Concerns over Potential Violation of the GATS Non-Discrimination Obligation: An Overview

The National Foreign Trade Council (NFTC), a prominent US business association advocating for open international trade and tax policies, has raised concerns with the US Trade Representative (USTR) regarding the potential violation of the WTO's non-discrimination obligation by *ex-ante* competition regulations.[68] Representing a broad spectrum of industries engaged in global commerce, the NFTC includes influential players

[68] National Foreign Trade Council, 'Comments Regarding the Compilation of the National Trade Estimate Report on Foreign Trade Barriers' (2024) USTR-2024-0015 8 ('NFTC Report 2024'); King & Spalding, 'The EU Digital Markets Act: Targets Discrimination Against U.S. Companies in Violation of WTO Commitments and Threatens the Re-Set of Trade Multilateralism and Trans-Atlantic Relations' (*KS Law*, 8 June 2021) <https://www.kslaw.com/attachments/000/008/860/original/EU_Digital_Markets_Act_-_Trade_law_and_systemic_implications_8_June_2021.pdf?1624300896> accessed 17 January 2025; Meredith Broadbent, 'The Digital Services Act, the Digital Markets Act, and the New Competition Tool: European Initiatives to Hobble U.S. Tech Companies' (*The Centre for Strategic and International Studies*, 10 November 2020) <https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool> accessed 17 January 2025; Daniel Rangel and others, '"Digital Trade" Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies' (*Rethink Trade, American Economic Liberties Project*, November 2022) <https://rethinktrade.org/wp-content/uploads/2022/11/20221101-AELP-DocLayout-v7.pdf> accessed 17 January 2025.

in the US tech industry. Notably, Big Tech companies such as Amazon, Google, Meta, and Microsoft serve on the NFTC's board of directors.[69] With their substantial financial and organisational resources, Big Tech exerts significant influence over the NFTC's advocacy priorities, often steering them toward defending their commercial interests.[70]

This influence is evident in the NFTC's approach to *ex-ante* competition regulations. Despite the US contemplating similar regulations domestically, Big Tech has successfully lobbied the NFTC to frame such regulations in other jurisdictions as potential violations of the WTO non-discrimination obligation.[71] At the same time, Big Tech continues to oppose the introduction of *ex-ante* competition regulations within the US itself.[72] The NFTC report highlights concerns about *ex-ante* regulations in countries such as India, Turkey, and Brazil, with particular emphasis on the EU's DMA.[73] The report argues that the DMA disproportionately targets US-based digital firms, violating the EU's WTO obligations by imposing stricter requirements on them compared to their non-US counterparts.

Ex-ante competition regulations, as previously discussed, aim to address potential distortions in digital markets by preemptively regulating certain platforms and digital service providers. The DMA, for instance, identifies Gatekeepers based on specific qualitative and quantitative thresholds, including their size, economic influence, intermediary role, and entrenched market position.[74] Once designated, Gatekeepers are subject to obligations designed to prevent anti-competitive practices, such as bundling services, enforcing platform parity clauses, or engaging in self-preferencing. They must also ensure fair access to data, enhance interoperability, and reduce data concentration.[75] In contrast, companies not classified as Gatekeepers are regulated under an *ex-post* framework, which applies enforcement measures only after anti-competitive conduct has been identified. This dual framework subjects Gatekeepers to more stringent,

[69] National Foreign Trade Council, 'Board of Directors' <https://www.nftc.org/about/board-of-directors/> accessed 17 January 2025.
[70] Rangel and others (n 68) 1; Tony Romm, 'Amazon, Facebook, Other Tech Giants Spent Roughly $65 Million to Lobby Washington Last Year' (*The Washington Post*, 22 January 2021) <https://www.washingtonpost.com/technology/2021/01/22/amazon-facebook-google-lobbying-2020/?itid=lk_inline_manual_10> accessed 17 January 2025; Tony Romm, 'Tech Giants Led By Amazon, Facebook and Google Spent Nearly Half a Billion on Lobbying over the Past Decade, New Data Shows' (*The Washington Post*, 22 January 2020) <https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/?itid=lk_interstitial_manual_17> accessed 17 January 2025.
[71] Rangel and others (n 68).
[71] National Foreign Trade Council (n 69).
[72] Anna Edgerton and Emily Birnbaum, 'Big Tech Spent $95 million trying to kill Congress' Most Aggressive Oversight Bill in Years. It's Looking Like It Worked' (*Fortune*, 6 September 2022) <https://fortune.com/2022/09/06/big-tech-spent-95-million-congress-oversight-bill/> accessed 17 January 2025; Kent Walker, 'The Harmful Consequences of Congress's Anti-Tech Bills' (*Google Blog*, 18 January 2022) <https://blog.google/outreach-initiatives/public-policy/the-harmful-consequences-of-congresss-anti-tech-bills/> accessed 17 January 2025.
[73] NFTC Report 2024 (n 68).
[74] See, Section 2.3.1.
[75] See, Section 2.3.1.

preemptive obligations while other firms remain subject to less intrusive, case-by-case enforcement.

The NFTC report asserts that these thresholds disproportionately affect US companies while exempting many EU and other non-US platforms from similar obligations.[76] Although the DMA appears origin-neutral, commentators note that its criteria for Gatekeeper designation result in *de facto* discrimination.[77] In this view, US-based firms are far more likely to be subjected to the DMA's onerous *ex-ante* obligations, while EU and other foreign platforms largely fall under the more lenient *ex-post* competition framework.

Commentators supporting the NFTC's position argue that *ex-ante* competition regulations violate the GATS.[78] To be covered by the GATS, a measure must be adopted by a WTO Member that impacts trade in services.[79] *Ex-ante* regulations are legal instruments adopted by governments, making them 'measures by Members' under Article I.1(3)(a) and Article XXVIII(a) of the GATS. The next step is to determine whether these measures fall under any of the modes of supply specified in Article I:2. The AB report in *US-Gambling*[80] and academic literature[81] suggest that digital services fall under Mode 1 (cross-border supply) and Mode 2 (consumption abroad). Thus, since *ex-ante* regulations affect the competitive conditions for digital services under Modes 1 and 2, they qualify as measures *affecting* trade in services under Article I:1 of the GATS.

The USTR has acknowledged the above concerns in the National Trade Estimate (NTE) Report, which assesses significant obstacles to US exports of goods and services. In both the 2022[82] and 2023[83] NTE Reports, the USTR recognised the DMA as a potential barrier to digital trade. However, the 2024 NTE Report marked a notable shift by excluding the DMA from its list of potential trade barriers. This change reflects a broader policy shift under the Biden administration, which has placed more emphasis on respecting the regulatory priorities of US trade partners rather than solely focusing on defending the interests of US-based companies.[84]

---

[76] NFTC Report 2024 (n 68) 8. See also, Coalition of Services Industries, 'Comments for the National Trade Estimate Report on Foreign Trade Barriers Docket Number USTR-2021-0016' (2021) 21.
[77] King & Spalding (n 68); Broadbent (n 68); Rangel and others (n 68).
[78] Ibid.
[79] General Agreement on Trade in Services [1995] (GATS), Article I:1.
[80] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Report of the Appellate Body (7 April 2005) WT/DS285/AB/R.
[81] Arvin Kristopher Razon, 'Liberalising Blockchain: An Application of the GATS Digital Trade Framework' (2019) 20 Melbourne Journal of International Law 13-15; Usman Ahmed, Brian Bieron and Gary Horlick 'Mode 1, Mode 2, or Mode 10: How Should Internet Services Be Classified in the Global Agreement on Trade in Service?' (*BU School of Law International Law Journal*, 24 November 2015) <https://www.bu.edu/ilj/2015/11/24/mode-1-mode-2-or-mode-10-how-should-internet-services-be-classified-in-the-global-agreement-on-trade-in-service/#_ftn1> accessed 19 November 2024.
[82] United States Trade Representative, '2022 National Trade Estimate Report on Foreign Trade Barriers' (2022) 217 ('NTE Report 2022').
[83] United States Trade Representative, '2023 National Trade Estimate Report on Foreign Trade Barriers' (2023) 173-74 ('NTE Report 2023').
[84] United States Trade Representative, '2024 National Trade Estimate Report on Foreign Trade Barriers' (2024) 1; Simon Lester, 'Katherine Tai on Online Business Models and Digital Regulation' (*International Economic Law and Policy Blog*, 18 March 2024) <https://ielp.worldtradelaw.net/2024/03/katherine-tai-on-online-business-models-and-digital-

The exclusion of the DMA from the 2024 report has drawn significant criticism from the NFTC, which contends that the USTR has not fulfilled its statutory obligation to identify and analyse all major trade barriers affecting US digital firms, regardless of the policy justifications put forth by other countries.[85] Accordingly, the NFTC has submitted comments urging the USTR to include the DMA in the 2025 NTE Report as a potential barrier to digital trade for US firms.[86]

In addition to the DMA, the USTR also identified *ex-ante* competition regulations in other jurisdictions, such as South Korea's App Stores Law[87], Australia's News Media Bargaining Code[88] and Germany's GWB Digitisation Act[89] under the NTE Reports during the period 2021 to 2023, to finally drop these claims under the 2024 NTE Report. As the USTR begins drafting the 2025 NTE report, it remains to be seen whether the Trump administration will reconsider its position on *ex-ante* regulations like the DMA and reinstate it as a potential trade barrier in the digital economy. Recent developments indicate a more confrontational approach, with President Trump signing a memorandum directing scrutiny of the EU's DMA, warning that such regulations dictate how American companies operate within the EU.[90]

4 Approach to Assessing the Consistency of *Ex-Ante* Competition Regulations with the Non-Discrimination Obligation under GATS

As countries explore various forms of *ex-ante* competition regulations to address the abuse of market dominance by large digital platforms, it is crucial that the GATS does not unduly constrain this policy space. The primary objective of such regulations in digital markets is to tackle the unique challenges posed by data-driven platforms and to overcome the limitations of traditional *ex-post* competition enforcement. Countries must retain the flexibility to experiment with regulatory frameworks to ensure fair competition in their digital markets, provided such measures are not protectionist. This aligns with the principle of embedded liberalism, which underpins the WTO framework.

Accordingly, our analysis of the GATS compatibility of *ex-ante* competition regulations focuses on the extent to which countries can justify the regulatory intent behind these

regulation.html> accessed 20 November 2024; Thibault Denamiel, John Strezewski and William Alan Reinsch, 'The Trade Winds are Turning: Insights into the 2024 National Trade Estimate' (*Centre for Strategic and International Studies,* 5 April 2024) <https://www.csis.org/analysis/trade-winds-are-turning-insights-2024-national-trade-estimate#:~:text=It%20instructs%20USTR%20to%20identify,Organization%20Joint%20Statement%20Initiative%20negotiations> accessed 20 November 2024.

[85] NFTC Report (2024) (n 68).

[86] Ibid.

[87] United States Trade Representative, '2021 National Trade Estimate Report on Foreign Trade Barriers' (2021) 333; NTE Report 2022 (n 82) 327.

[88] NTE Report 2022 (n 82) 37; NTE Report 2023 (n 83) 27.

[89] NTE Report 2023 (n 83) 173-4.

[90] Foo Yun Chee, 'US Demands EU Antitrust Chief Clarify Rules Reining in Big Tech' (*Reuters,* 24 February 2025) <https://www.reuters.com/technology/us-demands-eu-antitrust-chief-clarify-rules-reining-big-tech-2025-02-23/?utm_source=chatgpt.com> accessed 25 February 2025.

measures as aimed at fostering fair competition in domestic digital markets, so long as they remain non-protectionist. To explore this further, our analysis focuses specifically on the DMA as a case study. The DMA is widely regarded as a frontrunner in the *ex-ante* regulation of digital markets and has influenced similar initiatives globally.[91] By using the DMA as the focal point, we examine how its regulatory objective of curbing anti-competitive practices by Gatekeepers interacts with the GATS non-discrimination obligation.

As we explore subsequently in this paper, the integration of regulatory intent within the framework of the GATS non-discrimination obligation has long been a subject of debate among trade scholars. Many argue that the unique characteristics of trade in services necessitate greater deference to regulatory autonomy when interpreting the GATS non-discrimination obligation. However, the AB's last ruling on this issue in *Argentina – Financial Services* significantly narrowed the policy space for justifying regulatory intent under the GATS non-discrimination obligation. By adopting an overly formalistic approach, the AB has made it more challenging for countries to defend measures like the DMA under the non-discrimination obligation. While critical of this AB report, we explore alternative approaches from scholarly literature to incorporate regulatory context into the interpretation of the GATS non-discrimination obligation. Doing so would enable countries to better justify legislations like the DMA aimed at regulating the digital economy.

To this end, Section 4 begins by outlining the broad framework of the GATS non-discrimination obligation, focusing on the MFN and NT principles. It then examines whether the DMA would amount to *de facto* discrimination under the GATS. Following this, we address the challenges of defending the DMA under the GATS general exceptions clause. Finally, we argue for integrating the regulatory context into the analysis of either the 'likeness' test or the 'less favourable treatment' test under the GATS MFN and NT obligations. This approach would allow countries pursuing *ex-ante* competition regulations like the DMA to justify their measures aimed at fostering a level-playing-field in the digital economy.

4.1 The Non-Discrimination Obligation and General Exceptions Clause under GATS: An Overview

The GATS non-discrimination obligation is rooted in the principles of MFN and NT under the GATT, 1947. These principles ensure fairness in international trade by requiring Members to provide equal treatment to all trading partners (under MFN treatment) and avoid discrimination between domestic and foreign services and service suppliers (under

[91] Lilla Nóra Kiss, 'The Brussels Effect: How the EU's Digital Markets Act Projects European Influence' (*Information Technology & Innovation Foundation*, 7 March 2024) <https://itif.org/publications/2024/03/07/the-brussels-effect-how-the-digital-markets-act-projects-european-influence/?utm_source=chatgpt.com> accessed 17 January 2025.

NT). These obligations include both *de jure* and *de facto* forms of discrimination and are subject to the general exceptions under Article XIV, which allow Members to justify measures taken in pursuit of legitimate regulatory objectives.

The MFN obligation is covered under Article II of the GATS. It requires WTO Members to provide services and service suppliers from any Member with 'treatment that is no less favourable' than the treatment given to 'like' services and service suppliers from any other country. This obligation applies immediately and unconditionally, ensuring that no Member is disadvantaged in comparison to others in terms of market access or regulatory treatment.

Under the GATS, MFN treatment generally applies across all service sectors. However, pursuant to Article II:2 of the GATS and the 'Annex on Article II Exemptions', Members were permitted to exempt specific measures or service sectors from MFN obligations when the agreement was concluded. Another carve out of the GATS MFN obligation is the waiver for least developed countries (LDCs), adopted during the 2001 Ministerial Conference.[92] This is similar to the enabling clause under the GATT in that it allows preferential treatment, but only for LDC services and service suppliers.[93]

The NT obligation is covered under Article XVII of the GATS. It requires WTO Members to treat services and service suppliers of other Members no less favourably than their own like services and service suppliers. In contrast to the MFN obligation, the NT obligation under GATS applies only to service sectors and modes of supply explicitly included in a Member's Schedule of Specific Commitments.[94] This scheduling framework introduces a flexible and progressive approach to trade liberalisation within the WTO. Using a positive-list approach, Members can individually specify the sectors and modes of supply for which they undertake NT commitments, allowing them to tailor their obligations to align with their domestic policy objectives and developmental priorities.[95] This implies that in the context of *ex-ante* competition regulations, the NT obligation would only extend to those sectors and modes of supply that Members have included in their Schedule of Specific Commitments.

Another issue relevant from the perspective of *ex-ante* competition regulations is whether a commitment made by a WTO Member in a traditional sector can extend to similar services delivered digitally. The AB in *China - Publications and Audiovisual Products* addressed this by adopting an evolutionary interpretation of GATS Schedules, holding that generic terms in a Member's Schedule can evolve with technological

[92] The Fourth WTO Ministerial Conference (Doha, 9-14 November 2001).

[93] As a side note, other exceptions to the GATS MFN obligation include Article III:3 concerning frontier towns, Article VII concerning mutual recognition agreements and Article V concerning economic integration agreements like regional and preferential trade agreements.

[94] WTO, 'Schedules of Specific Commitments and Lists of Article II Exemptions' <https://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm> accessed 17 January 2025; Peter Van den Bossche and Werner Zdouc, *The Law and Policy of the World Trade Organisation* (Cambridge University Press, 2017) 525 ff.

[95] Van den Bossche and Zdouc (n 94).

developments.[96] It ruled that China's NT commitment for sound recording also applied to digital sound recording.[97] While the broader principle of technological neutrality under GATS remains debated,[98] the AB clarified that sufficiently generic terms in a Member's Schedule can extend to digital services.

This reasoning is equally applicable to distribution services.[99] If a Member's Schedule includes a generic commitment for 'distribution services', it could extend to e-commerce platforms like Amazon. The core function of distribution services—facilitating the movement of goods to consumers—remains consistent across traditional and digital modes. Thus, commitments that are not explicitly limited to physical methods could be interpreted to include digital channels. This would require Members to treat foreign e-commerce platforms like Amazon no less favourably than 'like' domestic competitors, ensuring that WTO rules adapt to the realities of the digital economy.

Furthermore, the GATS non-discrimination obligation encompasses both *de jure* (or 'in law') discrimination and *de facto* (or 'in fact') discrimination.[100] To elaborate, a measure is considered *de jure* discriminatory when the text of the law, regulation, or policy clearly treats the service or service provider from one WTO Member less favourably than that from another. On the other hand, a measure may still constitute *de facto* discrimination if, despite appearing origin-neutral, its application in practice results in unequal treatment between the services or service providers of different WTO Members, thereby favouring one over the other.[101]

Finally, the MFN and NT obligations are subject to the general exceptions under Article XIV of the GATS. This provision allows Members to justify violations of the MFN and NT obligations in pursuit of a narrowly defined and exhaustive list of legitimate regulatory objectives.[102] These exceptions are subject to the *chapeau* to Article XIV, which guards against protectionist regulatory measures that 'constitute a means of arbitrary or unjustifiable discrimination' or 'a disguised restriction on trade in services'.

---

[96] WTO, *China-Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Report of the Appellate Body (21 December 2009) WT/DS363/AB/R, 396.
[97] Ibid., 364.
[98] Ines Willemyns, *Digital Services in International Trade Law* (Cambridge University Press 2021) chapter 4.
[99] WTO, 'Distribution Services' <https://www.wto.org/english/tratop_e/serv_e/distribution_e/distribution_e.htm> accessed 17 January 2025.
[100] WTO, *European Communities – Regime for the Importation, Sale, and Distribution of Bananas*, Report of the Appellate Body (9 September 1997) WT/DS27/AB/R, 234. See also, WTO, *Argentina-Measures Relating to Trade in Goods and Services*, Report of the Appellate Body (14 April 2016) WT/DS453/AB/R, 6.105. Notably, paragraphs 2 and 3 of Article XVII of the GATS explicitly include *de facto* discrimination under the NT obligation by clarifying that both 'formally identical' or 'formally different' treatment could modify the conditions of competition, resulting in 'less favourable treatment'. Natens explains that the clarification contained under these paragraphs is a codification of the GATT 1994 jurisprudence on 'less favourable treatment' and the same interpretation extends to Article II of the GATS in relation to MFN. See, Bregt Natens, *Regulatory Autonomy and International Trade in Services: The EU Under GATS and RTAs* (Edward Elgar Publishing, 2016) 125-127.
[101] For a difference between *de jure* and *de facto* discrimination see, Van den Bossche and Zdouc (n 94) 309.
[102] Van den Bossche and Zdouc (n 94) 325-388 and 339-411.

Based on the above discussion, the legal elements of the MFN and NT obligations under the GATS can be outlined as follows. *First*, it is essential to determine whether the measure in question constitutes *de jure* or *de facto* discrimination. *Second*, the 'likeness' of the services and service suppliers has to be examined, with GATS jurisprudence indicating a presumption of 'likeness' in cases of *de jure* discrimination, i.e., in instances where distinction between services and service suppliers is based exclusively on origin.[103] The *third* element requires an assessment of whether there is 'less favourable treatment' by comparing the treatment accorded to like services and service suppliers. Finally, the MFN and NT obligations are subject to the general exceptions under Article XIV of the GATS. Together, these elements provide the framework for evaluating the compatibility of a measure with the MFN and NT obligations under the GATS.

Against this backdrop, the subsequent analysis uses the DMA as a case study to evaluate the GATS compatibility of *ex-ante* competition regulations.

4.2 *De facto* discrimination and the DMA

The first step in assessing the GATS compatibility of the DMA is to determine whether it constitutes a *de facto* or *de jure* form of discrimination. As outlined earlier, the NFTC argues that *ex-ante* regulations, like the DMA, are facially origin-neutral, as they do not explicitly target US firms. For example, the DMA does not exclusively designate core platform service suppliers from the US as Gatekeepers. Hence, the DMA does not result in *de jure* discrimination. However, the NFTC holds that the thresholds for designating Gatekeepers under the Act disproportionately impact US firms while excluding digital platforms from the EU and other jurisdictions.[104] This creates *de facto* discrimination, with US firms facing more stringent *ex-ante* obligations under the DMA, while non-US firms are subject to less rigorous *ex-post* competition law.

It is worth noting that in 2023, the EC designated six tech giants—Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft—as Gatekeepers under the DMA.[105] In 2024, Apple's iPadOS and Booking were also designated as Gatekeepers.[106] This brings the total number of core platform services subject to the DMA's regulations to 24. Strikingly, five of these companies are of US origin—Alphabet, Amazon, Apple, Meta, and Microsoft—while ByteDance is based in China and Booking is of Dutch origin. The question that follows is whether such a designation can amount to *de facto* discrimination under the GATS.

[103] WTO, *Argentina – Financial Services* (n 100) 6.38-6.41.
[104] NFTC Report (2024) (n 68) 8.
[105] European Commission, 'Gatekeepers' <https://digital-markets-act.ec.europa.eu/gatekeepers_en#:~:text=On%206%20September%202023%20the,those%20gatekeepers%20have%20been%20designated.&text=Alphabet%20Inc.,Apple%20Inc.&text=ByteDance%20Ltd.,Meta%20Platforms%2C%20Inc> accessed 20 November 2024.
[106] Ibid.

Notably, WTO jurisprudence confirms that both the MFN and NT obligations under the GATS include *de facto* discrimination within their scope.[107] Thus, the key issue is determining if a measure results in *de facto* discrimination. So far, scholars have distinguished two approaches to determining *de facto* discrimination under WTO law: *i)* the asymmetric impact test, and *ii)* the diagonal test.[108] Under the asymmetric impact test, *de facto* discrimination occurs when a measure affects a greater proportion or number of imports from a specific group more negatively than it impacts 'like' domestic services and service suppliers (under NT) or services and service suppliers from another Member (under MFN treatment). On the other hand, under the diagonal test, *de facto* discrimination is considered to exist if even a small number—potentially just a few (or even one)—of the imported services and service suppliers are treated less favourably than any of the services and service suppliers from the domestic industry (under NT) or any other Member (under MFN treatment).

Building on Ehring's example, assume, for instance, a hypothetical situation where 100 domestic services/ service suppliers stand vis-à-vis 100 imported 'like' services/ service suppliers.[109] Under the asymmetric impact test, *de facto* discrimination in the context of NT occurs if more or a higher percentage of imported services/ service suppliers are negatively affected compared to domestic services/ service suppliers. For example, if 6 (=6%) digital firms from the US providing a certain core platform service (eg. social networking services) listed under the DMA are designated as Gatekeepers compared to 3 (=3%) EU digital firms providing the same service, it would result in *de facto* discrimination. On the other hand, under a more stringent interpretation of the diagonal test, a measure will qualify as *de facto* discriminatory if it treats even one imported service/ service supplier less favourably in comparison to one domestic service/ service supplier, regardless of how the other 99 domestic and 99 imported services/ service suppliers are affected by the measure. So, under the diagonal test, there could be *de facto* discrimination in the context of NT if even one US digital firm providing a certain core platform service gets designated as a Gatekeeper under the DMA compared to one EU digital firm providing the same service that is not designated as a Gatekeeper.

The WTO adjudicatory bodies have not been entirely consistent in their findings on whether the diagonal test or the asymmetric impact test should be the basis for assessing *de facto* discrimination.[110] However, the most recent intervention on this point was by

[107] With regard to Art. II GATS, see, WTO, *EC-Bananas III* (n 100) 233. With regard to Art. XVII GATS, see, WTO, *European Communities – Regime for the Importation, Sale and Distribution of Bananas – Recourse to Article 21.5 by Ecuador*, Report of the Panel (12 April 1999) WT/DS27/RW/ECU, 6.149.

[108] Lothar Ehring, '*De Facto* Discrimination in WTO Law: National and Most-Favoured-Nation Treatment – or Equal Treatment?' (*The Jean Monnet Centre for International and Regional Economic Justice*, 2001) <https://jeanmonnetprogram.org/archive/papers/01/013201-04.html> accessed 20 November 2024.

[109] Ibid.

[110] Nicolas F Diebold, *Non-Discrimination in International Trade in* Services (Cambridge University Press, 2010) 43; Ehring (n 108).

the AB in *EC-Asbestos*,[111] which rejected the diagonal test used by the panel and noted in its *obiter dictum* that discriminatory effects must specifically disadvantage the group of imported goods as a whole, requiring evidence of asymmetric impact.[112] Similar to AB's position in *EC-Asbestos*, there is greater support for the asymmetric impact test among scholars and commentators.[113]

In view of the foregoing, based on the asymmetric impact test, to establish *de facto* discrimination under the GATS NT and MFN obligations, the US would need to demonstrate that the DMA disproportionately affects US-based digital platforms offering certain core platform services compared to their counterparts from the EU or other Members providing the same services. Specifically, the US must show that a higher proportion of US platforms are designated as Gatekeepers under the DMA compared to platforms from the EU (for NT) or any other Member (for MFN treatment), creating a higher regulatory burden for US digital firms. This argument aligns with the approach of the AB in *EC-Asbestos*, which emphasises the need to assess the discriminatory effects on imports as a whole rather than focusing on isolated cases of disadvantage under the diagonal test.

Given the likelihood of the US challenging *ex-ante* competition regulations like the DMA on grounds of *de facto* discrimination under the asymmetric impact test, an important question arises: can countries implementing such legislation successfully defend the regulatory intent behind these measures—namely, curbing Gatekeepers from distorting digital markets—within the GATS framework? The most apparent recourse for justifying legitimate regulatory objectives under GATS is the general exceptions clause in Article XIV. However, as the following subsection demonstrates, the grounds for exception under Article XIV are narrowly defined and inadequate to address the regulatory needs of the digital economy. This analysis serves as a segue into the longstanding debates over the extent to which the regulatory context can and should be considered within the 'likeness' and 'less favourable treatment' analysis of GATS' non-discrimination obligation. The following subsection delves into these issues, laying the foundation for a more detailed examination of incorporating regulatory context into the 'likeness' and 'less favourable treatment' analysis under Section 5.

4.3 Justifying *Ex Ante* Competition Regulations under the GATS General Exceptions Clause

Based on the structure of the GATS non-discrimination obligation discussed in Section 4.1, it is clear that when *de facto* discrimination stemming from *ex-ante* competition regulation is established, the most straightforward defense for states implementing such regulations would be to justify the regulatory intent under the general exceptions

[111] WTO, *European Communities - Measures Affecting Asbestos and Products Containing Asbestos*, Report of the Appellate Body (12 March 2001) WT/DS135/AB/R.
[112] Ibid., 100.
[113] Diebold (n 110) 44; Ehring (n 108).

provided in Article XIV of the GATS. However, Article XIV provides an exhaustive and narrowly defined list of grounds for justifying potentially GATS-inconsistent measures.[114] Modelled on Article XX of the GATT 1947,[115] these grounds are limited in scope and were drafted at a time when the regulatory challenges posed by the dominance of mega-digital platforms could not have been anticipated. Consequently, it would be difficult to justify *ex-ante* competition regulations under existing grounds, namely *(a)* public morals and public order;[116] *(b)* human, animal or plant life or health;[117] *(c)* the securing of compliance with GATS-consistent laws or regulations;[118] *(d)* the imposition or collection of direct taxes;[119] and *(e)* agreements of double taxation.[120] In sum, the restrictive nature of Article XIV's justifications makes it challenging to align such measures with the evolving need to address competition distortions caused by dominant digital platforms.

Since the general exceptions clause does not cover all legitimate policy objectives that may necessitate distinctions between services and service suppliers, Natens, among others, emphasises the importance of considering the regulatory intent behind a measure under the GATS MFN and NT analysis in order to avoid 'objectionable constraints on regulatory autonomy'.[121] The basis for reading the regulatory context in the non-discrimination obligation stems from the preamble to the GATS, which recognises 'the right of Members to regulate … the supply of services within their territories in order to meet national policy objectives'. Unlike the GATS, the GATT preamble does not explicitly emphasise preserving Members' regulatory policy space. According to Cossy, this reflects the greater political sensitivity of services trade, which is more heavily regulated and inherently complex due to factors like intangibility of services, varied modes of supply, and the inseparability of services from their suppliers.[122] Scholars argue that these dynamics, coupled with the GATS more intrusive impact on regulatory autonomy, warrant greater consideration of the regulatory context in assessing non-discrimination obligation, particularly in cases of *de facto* discrimination.[123] They support a subjective approach to

[114] Van den Bossche and Zduoc (n 94).
[115] Notably, the grounds for exceptions under Article XX of the GATT are broader than those under Article XIV of the GATS. For a comparison of the GATT and GATS general exceptions clauses see, Nicolas F Diebold, 'The Morals and Order Exceptions in WTO Law: Balancing the Toothless Tiger and the Undermining Mole' (2008) 11(1) Journal of International Economic Law 44 ff.
[116] Article XIV (a) GATS.
[117] Article XIV (b) GATS.
[118] Article XIV (c) GATS.
[119] Article XIV (d) GATS.
[120] Article XIV (e) GATS.
[121] Natens (n 100) 105. See also, Diebold (n 110) 79-80; Robert E Hudec, 'GATT/WTO Constraints on National Regulation: Requiem for an Aim and Effects Test' (1998) 32(3) Int'l Lawyer 626 ff; Frieder Roessler, 'Increasing Market Access Under Regulatory Heterogeneity: The Strategies of the World Trade Organisation' in OECD (ed), *Regulatory Reform and International Market Openness* (OECD 1996) 121–122.
[122] Mireille Cossy, 'Some Thoughts on the Concept of 'Likeness' in the GATS' in Marion Panizzon, Nicole Pohl and Pierre Sauve (eds), *GATS and the Regulation of International Trade in Services* (Cambridge University Press 2008) 339-341.
[123] Ibid. Similarly, Zdouc argues that 'overtly strict interpretations of the GATS non-discrimination clauses – irrespective of possibly *legitimate policies* pursued by national legislators – could in effect undermine sovereign regulatory powers of WTO Member governments to a larger degree than similarly strict interpretations of corresponding GATT provisions'. See, Werner Zdouc, 'WTO Dispute Settlement Practice Relating to the GATS' (1999) 2(2) Journal of International

the non-discrimination obligation and reject overly formalist or positivist interpretations of the NT and MFN obligations that fail to safeguard *bona fide* domestic regulations while targeting protectionist measures.[124]

While there is broad scholarly support for incorporating the regulatory context into the GATS non-discrimination obligation, scholars diverge on how this could be analytically achieved. Natens, Cossy, and Hudec advocate for considering regulatory intent under the 'likeness' test,[125] while Pauwelyn and Trachtman suggest doing so under the 'less favourable treatment' test.[126] WTO jurisprudence has shown signs of evolving toward accommodating regulatory context within the 'less favourable treatment' analysis.[127] However, the AB's most recent ruling on this issue, in *Argentina-Financial Services*, reversed this trend by endorsing a formalist interpretation of the GATS MFN and NT obligations, significantly limiting the scope for considering the regulatory purpose under these provisions.

The AB's turn to formalism in interpreting the non-discrimination obligation in *Argentina-Financial Services* poses significant challenges to the legitimacy of measures like *ex-ante* competition laws, which fall outside the narrowly defined exceptions under Article XIV GATS. Given this context, Section 5 examines the evolution of WTO jurisprudence and scholarly perspectives on incorporating regulatory purpose within the 'likeness' and 'less favourable treatment' tests of the non-discrimination obligation. Building on this analysis, we critique the shortcomings of the AB's ruling in *Argentina-Financial Services* as regards its implications for regulatory interventions to govern the digital economy like the DMA and advocate for the inclusion of regulatory purpose under either the 'likeness' or 'less favourable treatment' test, as suggested by scholars.

5 *Ex-Ante* Competition Regulation and the GATS Non-Discrimination Obligation: Is the Regulatory Context Relevant?

This Section examines the potential for incorporating the regulatory context into the GATS non-discrimination obligation. Section 5.1 focuses on the 'likeness' analysis, while

Economic Law 342. In contrast, Pauwelyn argues that regulatory intent should be interpreted consistently within the non-discrimination obligation of both GATT and GATS. See, Joost Pauwelyn, 'Comment: The Unbearable Lightness of Likeness' in Marion Panizzon, Nicole Pohl and Pierre Sauve (eds), *GATS and the Regulation of International Trade in Services* (Cambridge University Press 2008) 358-396.

[124] Amelia Porges and Joel P Trachtman, 'Robert Hudec and Domestic Regulation: Resurrection of Aim and Effects' (2003) 37(4), Journal of World Trade 784; Hudec (n 121) 633; Aditya Mattoo and Arvind Subramanian, 'Regulatory Autonomy and Multilateral Disciplines: The Dilemma and a Possible Resolution' (1998) 1(2) Journal of International Economic Law 305.

[125] Natens (n 100) 105-138; Cossy (n 123) 327-357; Hudec (n 121) 626 ff.

[126] Joel P Trachtman, 'Lessons for GATS Article VI from the SPS, TBT, and GATT Treatment of Domestic Regulation' (*SSRN*, 2002) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=298760> accessed 17 January 2025 64; Pauwelyn (n 123) 358-369; Diebold also explores the possibility of treating regulatory purpose as an independent and substantive element of the non-discrimination obligation, while acknowledging the legal challenges associated with justifying this approach. See, Diebold (n 110) 83 ff.

[127] Porges and Trachtman (n 124) 788-797; Cossy (n 122) 345-346; Pauwelyn (n 123) 362-367.

Section 5.2 shifts attention to the 'less favourable treatment' test. It also discusses how the AB's conservative ruling in *Argentina-Financial Services* has made it increasingly difficult for states to justify regulatory interventions like the DMA. Furthermore, the Section investigates scholarly proposals to integrate regulatory context into the 'likeness' and 'less favourable treatment' tests, evaluating whether these approaches provide more effective solutions than the AB's ruling in *Argentina-Financial Services*, especially in the context of modern regulatory interventions in the digital economy.

5.1 The 'Likeness' Analysis under GATS: Exploring Pathways to Accommodate Regulatory Autonomy

Greater deference to regulatory autonomy in the 'likeness' analysis would allow countries implementing regulations like the DMA to argue that platforms designated as digital Gatekeepers under the Act are not 'like' other platforms outside its scope. This argument rests on the premise that Gatekeepers, due to their size, access to data, network effects, etc., hold a greater potential to distort digital markets. Therefore, accommodating the regulatory distinctions that define Gatekeepers under the 'likeness' test could justify their separate treatment within the GATS framework. On this basis, Gatekeepers, subject to *ex-ante* competition obligations, would be distinguished from non-Gatekeepers, who remain governed by traditional competition law applied on a case-by-case and *ex-post* basis. Given this context, the following analysis explores the extent to which the 'likeness' test can incorporate regulatory considerations, enabling a more nuanced interpretation of the differential treatment of various service suppliers.

5.1.1 Combined Reference to 'Service and Service Supplier' under the GATS 'Likeness' Analysis

A key distinction in the 'likeness' analysis under the GATS compared to the GATT lies in the scope of comparison. The GATS explicitly references both 'services and service suppliers', whereas the GATT limits its analysis to products, excluding any consideration of the producers.[128] In other words, the GATS extends the 'likeness' assessment beyond the service itself to include the attributes of the entities providing those services.

This understanding aligns with GATS jurisprudence, which has progressively established that the 'likeness' analysis must account for both services and service suppliers. In *EC-Bananas III*, the panel adopted a simplistic approach, stating that 'to the extent that entities provide these like services, they are like service suppliers'.[129] Similarly, in *Canada-Autos*, the panel applied this reasoning to GATS Article II, treating service

[128] Natens (n 100) 106-109.
[129] WTO, *European Communities-Regime for the Importation, Sale and Distribution of Bananas,* Report of the Panel (22 May 1997) WT/DS27/R/USA, 7.322.

suppliers as 'like' if they provide 'like' services.[130] However, it highlighted the case-specific nature of its decision, leaving open the possibility for future panels to develop a more nuanced analysis. Subsequent cases introduced greater nuance. In *China – Publications and Audiovisual Products*, the panel held that if origin alone drives differential treatment, the 'like service suppliers' requirement is met, but a more detailed analysis is needed when other factors are involved.[131] Similarly, *China-Electronic Payment Services* recognised that while 'like' services may imply 'like' suppliers, this presumption is not absolute and requires a case-by-case analysis.[132] Finally, in *Argentina-Financial Services*, the AB clarified the integrated nature of the 'likeness' analysis under Articles II and XVII of the GATS.[133] According to the AB, the 'likeness' test requires considering both the services and the service suppliers in a holistic manner, with the relative weight of each factor depending on the competitive relationship in the specific case.[134] This marked a shift towards a more comprehensive and balanced approach, recognising the interdependence of services and suppliers in assessing 'likeness'.

Building on GATS jurisprudence, commentators argue that the joint reference to services and service suppliers in Articles II and XVII of the GATS necessitates greater consideration of the regulatory context in the 'likeness' analysis compared to the GATT.[135] They contend that without such consideration, the explicit inclusion of 'service suppliers' in the GATS would be rendered meaningless.[136] The inclusion of service suppliers under the GATS, they argue, indicates an intention to allow for a more detailed assessment of the regulatory factors influencing trade in services, distinguishing it from the GATT's narrower focus on products.[137] In essence, commentators suggest that requiring 'likeness' to be assessed for both the service and its supplier under the GATS should allow for differentiation among service suppliers based on the regulatory context.[138]

In the context of *ex-ante* regulatory frameworks like the DMA, this distinction becomes critical. The DMA targets market distortions caused by dominant digital firms, designated as Gatekeepers, by imposing regulatory obligations tailored to their unique market power. Under the GATS 'likeness' analysis, services are assessed for their competitive relationship based on four key factors: *i)* the nature and characteristics of the services, *ii)* their end-use, *iii)* consumer preferences, and *iv)* service classification.[139] Applying these criteria,

[130] WTO, *Canada-Certain Measures Affecting the Automotive Industry*, Report of the Panel (11 February 2000) WT/DS139/R, 8.46.
[131] WTO, *China-Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Report of the Panel (12 August 2009) WT/DS363/R, 7.975.
[132] WTO, *China-Certain Measures Affecting Electronic Payment Services*, Report of the Panel (16 July 2012) WT/DS413/R, 7.701, 7.705.
[133] WTO, *Argentina – Financial Services* (n 100) 6.29.
[134] Ibid.
[135] Cossy (n 122) 327; Natens (n 100) 106-109; Zdouc (n 123) 295–346; WTO, 'Negotiations on Emergency Safeguard Measures' (Report by the Chairperson of the Working Party on GATS Rules, 2003 S/WPGR/9) 3.
[136] Cossy (n 122) 329-331; Natens (n 100) 106 ff.
[137] Cossy (n 122) 329.
[138] Cossy (n 122) 327-357; Natens (n 100) 105-138; and Hudec (n 121) 626 ff.
[139] WTO, *Argentina-Financial Services* (n 100) 6.32.

services like Google's online search or Meta's messaging platforms could be considered 'like' the same services offered by smaller competitors within the EU or any other Member. However, the explicit reference to service suppliers in the GATS provides an opportunity to incorporate regulatory context into the 'likeness' analysis. Gatekeepers like Google and Meta possess disproportionate market power and a unique ability to influence market dynamics, distinguishing them from other service suppliers even if their services may be 'like'. This distinction—rooted in the dominant market position of the service suppliers rather than the intrinsic characteristics of the services they provide—forms the basis of their classification as Gatekeepers under the DMA. Therefore, their 'unlikeness' arises not from the nature of the services they provide but from their dominant position as service suppliers and its regulatory implications.

Building on the discussion above, a key question emerges: to what extent does WTO jurisprudence permit the consideration of the regulatory context in assessing the 'likeness' of service suppliers under Articles II and XVII of the GATS? The following sub-section delves into this issue, examining the interplay between regulatory autonomy and the interpretation of 'likeness' in the context of GATS.

5.1.2 The Aim and Effects Test under the GATS 'Likeness' Analysis

The aim and effects test, developed under the GATT framework, sought to expand the traditional 'likeness' analysis by incorporating considerations of a measure's regulatory purpose and its market impact.[140] Introduced in the *US – Malt Beverages*[141] case and elaborated in the unadopted *US – Taxes on Automobiles* panel report,[142] this approach was grounded in GATT Article III:1, which prohibits internal measures that aim to 'afford protection to domestic production'.[143] The test was particularly useful in cases of *de facto* discrimination, where measures did not explicitly distinguish products based on origin.[144]

Under the aim and effects test, a panel would assess whether regulatory distinctions had a legitimate aim and whether they produced a protectionist effect favouring domestic products. If a measure's purpose and effect were unrelated to protectionism, regulators could differentiate between products without breaching GATT obligations. As an advocate of the approach, Hudec argued that it provided greater deference to regulatory autonomy while addressing both trade effects and the *bona fides* of regulatory purposes.[145]

[140] Porges and Trachtman (n 124) 784.
[141] WTO, *United States-Measures Affecting Alcoholic and Malt Beverages*, Report of the Panel (7 February 1992) DS23/R.
[142] WTO, *United States-Taxes on Automobiles*, Report of the Panel (11 October 1994) DS31/R, 5.10; Notably, the Panel Report on *US – Taxes on Automobiles* was not adopted by the GATT Contracting Parties, primarily due to the EU's opposition to the aim and effects test. See, Diebold (n 110) 79.
[143] Ibid., 5.7-5.9.
[144] Hudec (n 121) 626-628.
[145] Ibid.

However, the aim and effects test was ultimately rejected by the AB in *Japan – Alcoholic Beverages II* for the following reasons.[146] *First*, the first sentence of Article III:2 of the GATT on 'like products' does not reference the broader policy goals under Article III:1 of not 'afford[ing] protection to domestic production', which was the basis for justifying the aims and effects test.[147] *Second*, allowing aim and effects considerations could undermine the balance struck under Article XX exceptions, which specifically address justifications for trade-restrictive measures.[148] *Third*, the test could introduce undue subjectivity in evaluating regulatory motives, requiring panels to second-guess a regulator's intent.[149]

The rejection of the aim and effects test extended to the GATS in *EC – Bananas III*. The AB explicitly stated that neither Article II nor Article XVII of the GATS provided a basis for considering a measure's aims and effects.[150] It highlighted that, unlike Article III:1 of the GATT, which contains the phrase 'afford protection to domestic production' that formed the basis for introducing the aim and effects test, the MFN and NT obligations under the GATS do not include such a reference. Instead, under the GATS, the AB noted, regulatory considerations are addressed primarily through the general exceptions clause in Article XIV.[151]

Scholars have also expressed concerns about the aim and effects test, criticising it for introducing a subjective theory of 'likeness' that inherently involves making value judgments between economic considerations and other policy objectives as well as places an undue burden on WTO adjudicatory bodies to determine which regulatory purposes are legitimate.[152] Furthermore, identifying the true regulatory purpose of a trade-restrictive measure is particularly challenging, as many measures are designed to pursue multiple policy objectives simultaneously.[153] This inherent complexity, critics argue, undermines the test's practicality and consistency in application.

In sum, the AB in *EC – Bananas III* effectively closed the door to considering the regulatory context in the GATS 'likeness' analysis by invoking the aim and effects test. However, this raises the subsequent question: to what extent can the regulatory context

[146] WTO, *Japan – Taxes on Alcoholic Beverages*, Report of the Appellate Body (4 October 1996) WT/DS8/AB/R, WT/DS10/AB/R, WT/DS11/AB/R 18.
[147] Ibid., 4.
[148] Ibid.
[149] Ibid., 27-28.
[150] WTO, *EC-Bananas III* (n 100) 241.
[151] Ibid.
[152] William J Davey and Joost Pauwelyn, 'MFN Unconditionality: A Legal Analysis of the Concept in View of its Evolution in the GATT/WTO Jurisprudence with Particular Reference to the Issue of "Like Product"' in Thomas Cottier, Petros C Mavrodis and Patrick Blatter (eds), *Regulatory Barriers and the Principle of Non-Discrimination in World Trade Law* (University of Michigan Press 2000) 38.
[153] Thomas Cottier and Matthias Oesch, *International Trade Regulation – Law and Policy in the WTO, the European Union and Switzerland* (London: Cameron May & Staempfli Publishers 2005) 407; Petros Constantinos Mavrodis 'Regulatory Barriers and the Principle of Non-Discrimination' in World Trade Law: Past, Present, and Future' in Thomas Cottier, Petros C Mavrodis and Patrick Blatter (eds), *Regulatory Barriers and the Principle of Non-Discrimination in World Trade Law* (University of Michigan Press 2000) 130.

still be considered when assessing the 'nature and extent of the competitive relationship' between services and service suppliers under the GATS 'likeness' analysis?

5.1.3 Nature and Extent of Competitive Relationship: Can the Regulatory Context Play a Role?

Having rejected the aim and effects test for determining 'likeness', WTO adjudicatory bodies have endorsed a GATS 'likeness' analysis focusing on the 'nature and extent of the competitive relationship'.[154] Based on the GATT jurisprudence, this approach emphasises that services and service suppliers are considered 'like' if they are in a competitive relationship with each other. For instance, in *China – Electronic Payment Services*, the panel highlighted that Article XVII aims to ensure equal competitive opportunities for like services and service suppliers and that the determination of 'likeness' must be made on a case-by-case basis.[155] This involves examining the specific circumstances of each case and relying on arguments and evidence to assess whether services and service suppliers are 'essentially or generally the same in competitive terms'.[156]

More recently, the AB in *Argentina – Financial Services* further clarified that the criteria traditionally used to assess 'likeness' for goods under GATT could inform the analysis of 'likeness' in relation to services and service suppliers under GATS.[157] Accordingly, the AB ruled that *i)* the nature and characteristics of the services and service suppliers, *ii)* end-use, *iii)* consumer tastes and preferences, and *iv)* classification of services are the key elements of the 'likeness' analysis under GATS.[158] Further, the AB noted that these criteria must be adapted to account for the specific context of services trade, particularly as, unlike GATT, GATS explicitly considers both services and service suppliers.[159] Another significant distinction from the GATT framework is the existence of multiple modes of supply under GATS Article I:2, which adds a unique layer of complexity to the analysis of 'likeness' under GATS.[160] Nevertheless, the AB emphasised that the fundamental objective of the 'likeness' analysis remains consistent with the GATT approach: to determine whether services and service suppliers are in a competitive relationship. Thus, the AB seemed to make room for considering the regulatory context in the 'likeness' analysis but within the framework of assessing the 'nature and extent of competitive relationship' between the services and service suppliers, rather than treating the regulatory context as a self-standing factor in the 'likeness' analysis.[161]

[154] WTO (n 132) 7.697.
[155] Ibid., 7.701.
[156] Ibid., 7.702.
[157] WTO, *Argentina – Financial Services* (n 100) 6.31.
[158] Ibid.
[159] Ibid., 6.34.
[160] Ibid., 6.33-6.34.
[161] Ibid.

The AB's approach in *Argentina-Financial Services* opens the door to considering how the regulatory context may influence the nature and extent of such competitive relationship, particularly in relation to service suppliers. Cossy and Natens note that the regulatory intent may play a role in determining 'likeness' based on the competitive relationship between service suppliers when assessing *i)* the characteristics of service suppliers and *ii)* consumer tastes and preferences.[162] However, how far the regulatory context can be considered when assessing the characteristics of service suppliers and consumer tastes and preferences is moot.

Under the GATS framework, various supplier-related characteristics, such as company size, skills, technological capabilities, and experience, have been proposed as relevant in determining 'likeness'.[163] While the parties in *EC – Bananas III*, *Canada – Autos* and *US-Gambling* invoked these criteria, panels have generally not made them central to the analysis.[164] Cossy argues that such criteria are difficult to apply consistently, as they may not always reflect the competitive relationship between suppliers.[165] For example, why should company size matter if both large and small firms provide competing services? This issue is especially pertinent in the context of the DMA, where dominant platforms like Google and Meta may offer services that are 'like' those of smaller competitors despite their market dominance. In such cases, relying on supplier-related criteria like annual turnover, market capitalisation, and entrenched market position could potentially result in artificially differentiating core platform service providers that offer essentially 'like' services. Although such criteria might hold relevance in an *aim and effects* test—where the regulatory intent behind a measure is integral to the 'likeness' analysis—they appear less pertinent when assessing the competitive relationship between service suppliers based solely on their inherent characteristics.

Similar concerns arise when incorporating regulatory context into the assessment of service suppliers' 'likeness' based on consumer perceptions. In the case of the DMA, it is unclear whether consumers differentiate between services provided by Gatekeepers like Google, Amazon, and Meta and those of non-Gatekeepers due to the dominant market position of the former. In digital markets, consumer choices do not sufficiently reflect such regulatory distinctions. Instead, consumers tend to prefer services like Google for online search, Amazon for e-commerce, and Meta for social networking, driven by factors such as network effects, low price points, and convenience. These preferences are shaped more by the functional attributes of the services than by concerns about the vast consumer data held by these platforms or their significant influence on shaping consumer choice through algorithmic targeting. Natens also highlights that emphasising consumer preferences places an undue burden on consumers, a responsibility that may be

[162] Cossy (n 122) 336-339; Natens (n 100) 121.
[163] Zdouc (n 123) 333; Markus Krajewski, *National Regulation and Trade Liberalization in Services* (Kluwer Law International, 2005) 105.
[164] Cossy (n 122) 336-338.
[165] Ibid.

unreasonably heavy.[166] Moreover, WTO dispute settlement bodies have not relied on consumer preferences when assessing 'likeness' under GATS.[167] This suggests that integrating consumer perceptions into the 'likeness' analysis remains underexplored in GATS practice and it is difficult to conclude that the market dominance of Gatekeepers has a direct bearing on consumer perceptions.

5.1.4 Exploring Approaches to Integrate the Regulatory Purpose under the 'Competitive Likeness' Test

The AB's rejection of the aim and effects test within the 'likeness' analysis underscores the WTO adjudicatory bodies' reluctance to recognise 'regulatory likeness' as a separate criterion beyond 'competitive likeness'. At the same time, justifying regulatory purpose within the 'competitive likeness' framework remains challenging, as discussed in Section 5.1.3, particularly for *ex-ante* competition regulations like the DMA. This prompts Cossy to question whether there is a need for 'something different' under the GATS.[168] In this context, we believe Natens' proposal to integrate regulatory purpose within the 'competitive likeness' test merits closer consideration.

According to Natens, '[c]ombining an assessment of consumer tastes and habits, and the characteristics of the service supplier, in so far as they are relevant to the supply of the service, appears to be the most suitable way to determine the 'likeness' of two service suppliers'.[169] Applying this approach to *ex-ante* competition regulations, such as the DMA, offers a basis to differentiate between Gatekeepers and non-Gatekeepers under the 'competitive likeness' analysis. Gatekeepers are defined by inherent characteristics such as substantial annual turnover, dominant market capitalisation, and entrenched market positions. These attributes grant Gatekeepers unparalleled control over consumer data, which significantly shape the services they supply and set them apart from non-Gatekeepers.

As discussed in Section 2.1, Gatekeepers leverage their control over data to secure major competitive advantages. By using consumer data to improve services, personalise experiences, and optimise targeted advertising, Gatekeepers generate advantages like network effects and customer lock-in.[170] This allows Gatekeepers to establish market dominance and outperform smaller competitors. In contrast, non-Gatekeepers, lacking comparable access to data, cannot replicate these advantages in the services they supply. They are unable to match the same levels of personalisation, operational efficiency, or consumer retention achieved by Gatekeepers. This disparity underscores the critical

[166] Natens (n 100) 118.
[167] Cossy (n 122) 339.
[168] Ibid.
[169] Natens (n 100) 119 ff.
[170] See, Section 2.1.

influence of Gatekeepers' inherent characteristics on the services they supply, highlighting the importance of factoring these elements into the assessment of 'likeness'.

This approach aligns with the AB's acknowledgment in *Argentina-Financial Services* that the 'likeness' analysis under GATS must adapt to the specific context of services trade, including the characteristics of service suppliers. By emphasising the relevance of regulatory purpose within the 'competitive likeness' analysis, WTO adjudicatory bodies can better address modern regulatory initiatives, such *ex-ante* competition regulations. However, it remains to be seen whether future panels will adopt a more expansive interpretation of the 'competitive likeness' test under GATS, as suggested by Natens.

Next, we turn to explore the extent to which the regulatory context can be incorporated into the 'less favourable treatment' test.

5.2 The 'Less Favourable Treatment' Test under GATS: How Relevant is the Regulatory Context?

Similar to the GATT, a measure is considered to result in 'less favourable treatment' under Articles II and XVII of the GATS if it modifies the conditions of competition in favour of domestic services and service suppliers (under NT) or services and service suppliers from another Member (under MFN treatment).[171] A critical question for our analysis is the extent to which the regulatory context could be considered when assessing 'less favourable treatment' under GATS.

Ex-ante regulations, such as the DMA, can be considered to result in 'less favourable treatment' for platforms designated as Gatekeepers because they modify the conditions of competition to their detriment. The DMA imposes pre-emptive obligations on Gatekeepers, meaning these platforms are required to comply with stringent obligations even before any anti-competitive behaviour is identified. This contrasts with traditional competition law, which generally operates on an *ex-post* basis, intervening only after anti-competitive conduct has been detected. This results in additional compliance costs for Gatekeepers.[172] Moreover, under traditional competition law, the relevant market must be defined, and dominance in the said market established before applying competition rules, followed by a case-by-case analysis of whether the conduct harms competition, typically using an effects-based approach that considers the impact on consumer welfare.[173] The DMA, however, sidesteps the requirement of establishing the relevant market and dominance therein. Instead, it applies predefined qualitative and quantitative criteria to designate Gatekeepers regardless of the market context. Additionally, the DMA

[171] Van den Bossche and Zdouc (n 94) 335-338 and 408-412.
[172] European Commission, *Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)* COM (2020) 84.
[173] OECD, 'Ex-Ante Regulation and Competition in Digital Markets'*(OECD*, 2021) < https://www.oecd.org/en/publications/ex-ante-regulation-and-competition-in-digital-markets_c83e178d-en.html> accessed 16 March 2025.

imposes strict prohibitory and mandatory obligations on Gatekeepers without considering whether the conduct in question benefits consumers. In sum, the *ex-ante* nature of the DMA, along with its broad, non-case-specific obligations, makes it significantly more onerous than traditional competition law, thereby modifying the competitive conditions to the detriment of the designated Gatekeepers.

In light of the above arguments, it becomes crucial to consider whether the regulatory context can be integrated into the assessment of 'less favourable treatment' under Articles II and XVII of the GATS. Taking into account the regulatory intent behind *ex-ante* competition legislations such as the DMA within the 'less favourable treatment' analysis would mean that such measures would not be deemed to modify the conditions of competition to the detriment of Gatekeepers, as their primary objective is to level the playing field in the digital market. This consideration, however, would depend on the absence of any protectionist intent behind these measures.

5.2.1 Resurgence of the Aim and Effects Test under the 'Less Favourable Treatment' Analysis?

To recap, the aim and effects test—allowing for consideration of the regulatory context behind a non-protectionist measure—was introduced as part of the 'likeness' analysis in *US – Malt Beverages*[174] case and elaborated in the unadopted *US – Taxes on Automobiles*.[175] The basis for its introduction was the phrase 'afford protection to domestic production' under Article III:1 of the GATT. One of the significant points of opposition to its application to the GATS non-discrimination obligation was the absence of the phrase 'afford protection to domestic production' under Articles II and XVII of the GATS.[176]

However, scholars have observed a resurgence of the aim and effects test in WTO jurisprudence, albeit under the 'less favourable treatment' analysis, rather than the 'likeness' analysis as previously applied.[177] In its ruling under Article III:4 of the GATT, the AB in *EC – Asbestos* held that 'the term "less favourable treatment" expresses the general principle, in Article III:1, that internal regulations "should not be applied … so as to afford protection to domestic production"'.[178] Some commentators have interpreted this statement as supporting the aims and effects approach.[179] Subsequently, in *Dominican Republic – Import and Sale of Cigarettes*, the AB found that a measure's detrimental effect on imports could be attributed to factors other than origin, thereby allowing consideration

[174] WTO, *United States-Measures Affecting Alcoholic and Malt Beverages*, Report of the Panel (7 February 1992) DS23/R.
[175] WTO, *United States-Taxes on Automobiles*, Report of the Panel (11 October 1994) DS31/R, 5.10.
[176] WTO, *EC-Bananas III* (n 100) 241.
[177] Porges and Trachtman (n 124) 788-797; Cossy (n 122) 345-346; Pauwelyn (n 123) 362-367.
[178] WTO (n 111) 100.
[179] Rob Howse and Elisabeth Türk, 'The WTO Impact on Internal Regulation – A Case Study of the Canada – EC Asbestos Dispute' in Gráinne de Búrca and Joanne Scott (eds), *The EU and the WTO: Legal and Constitutional Aspects* (Hart Publishing 2001) 299.

of the regulatory context.[180] However, in this case, the factors other than origin were not linked to the measure's aim or purpose but were instead tied to economic factors, such as market share.[181] Finally, in the context of *EC – Approval and Marketing of Biotech Products*, Diebold observes that the Panel required the complainant to provide evidence demonstrating that the differential treatment is attributable to origin rather than to a permissible regulatory objective, such as safety.[182] In conclusion, while WTO jurisprudence has neither explicitly endorsed nor rejected the subjective theory of 'less favourable treatment', there are indications that WTO adjudicatory bodies are inclined to move in this direction.[183]

Recognising the jurisprudential shift towards incorporating regulatory purpose within the 'less favourable treatment' test, Pauwelyn identifies several factors that WTO adjudicatory bodies must consider to ensure that only non-protectionist measures withstand scrutiny under this approach. These include the structure, design, and architecture of the regulation; the manner in which the regulation is applied; the impact of the regulation on the group of imported products compared to the group of like domestic products; evidence of a protectionist purpose, which must be objectively established rather than based on subjective intent; and evidence of alternative non-protectionist purposes that justify the regulation and its differential treatment of like products.[184] According to Pauwelyn, fulfilling just one of these criteria is unlikely to suffice; instead, adjudicators must evaluate and balance these factors collectively.[185] Pauwelyn further notes that there should be some link between the regulation and the non-protectionist objective it aims for; however, this connection does not need to meet the strict standard of a 'necessity' test.[186]

In our view, Pauwelyn's proposed framework for ensuring that only non-protectionist regulatory measures pass scrutiny under the 'less favourable treatment' analysis offers a viable model for integrating regulatory purpose within this analysis. In the context of measures such as the DMA, this framework would ensure that only measures aimed at leveling the playing field in digital markets are justified. Specifically, it would ensure that such measures do not modify the conditions of competition to the detriment of Gatekeepers under the pretext of promoting fairness in digital markets.

[180] WTO, *Dominican Republic – Measures Affecting the Importation and Internal Sale of Cigarettes*, Report of the Appellate Body (25 April 2005) WT/DS302/AB/R, 96.
[181] Diebold (n 110) 82.
[182] WTO, *European Communities – Measures Affecting the Approval and Marketing of Biotech Products*, Report of the Appellate Body (29 September 2006) WT/DS291/R, 7.2514; Diebold (n 110) 82-83. See also, Pauwelyn (n 123) 366.
[183] Diebold (n 110) 83.
[184] Pauwelyn (n 123) 366.
[185] Pauwelyn (n 123) 366-367.
[186] Pauwelyn (n 123) 367-369.

5.2.2 The AB Ruling in *Argentina-Financial Services:* A Shift Toward Formalism

The last AB ruling on the issue of integrating the regulatory context under the 'less favourable treatment' analysis was *Argentina – Financial Services*, where the panel and the AB adopted contrasting positions. The panel's approach allowed for consideration of the regulatory context within the 'less favourable treatment' analysis, while the AB reversed the panel's finding, emphasising a stricter interpretation that focused on whether a measure modified the conditions of competition to the detriment of imported services and service suppliers, with little room to accommodate broader regulatory considerations.

The panel in *Argentina-Financial Services* noted that the GATS preamble highlights the importance of the right to regulate while promoting progressive liberalisation in the trade of services.[187] Further, under Article II:1 of the GATS, the concept of 'treatment no less favourable' applies not only to services but also to service suppliers, introducing additional complexities. In light of these factors, the panel concluded that the potential for regulatory distinctions is consistent with GATS obligations.[188] According to the panel, measures that differentiate between service suppliers may not constitute 'less favourable treatment' if they align with legitimate regulatory objectives. This interpretation reflects the dual objectives outlined in the GATS preamble: fostering transparency and liberalisation while respecting the Members' right to regulate service suppliers to meet national policy goals. In sum, the panel supported a nuanced balance for integrating regulatory considerations into the interpretation of 'less favourable treatment' under GATS.[189]

In contrast, the AB in *Argentina – Financial Services* reversed the panel's interpretation of 'treatment no less favourable' under Articles II:1 and XVII of the GATS, clarifying that this legal standard focuses primarily on whether a measure modifies the conditions of competition, rather than requiring an additional inquiry into the regulatory objectives underlying the measure.[190] The AB emphasised that the GATS structure allows Members to retain flexibilities in their commitments, such as through specific market access and NT commitments, as well as exceptions for national policy objectives under Articles XIV of the GATS.[191]

The AB's reasoning underlined that the non-discrimination provisions of the GATS should focus on whether the measure in question modifies the conditions of competition to the detriment of like services or service suppliers of other Members.[192] The regulatory objectives that might justify such a measure should be addressed instead through the

[187] WTO, *Argentina-Measures Relating to Trade in Goods and Services,* Report of the Panel (30 September 2015) WT/DS453/R, 7.232.
[188] Ibid., 7.233.
[189] Ibid., 7.232-7.233.
[190] WTO, *Argentina-Financial Services* (n 100) 6.106.
[191] Ibid., 6.112, 6.114.
[192] Ibid., 6.126.

general exceptions clause. The AB further clarified that while the regulatory context may not directly influence the 'less favourable treatment' analysis, it can still be relevant depending on whether or not the measure in question modifies the conditions of competition.[193] The AB noted in this regard that,

> [S]uch assessment must begin with a careful scrutiny of the measure, including consideration of the design, structure and expected operation of the measure at issue. In such assessment, to the extent that evidence relating to the regulatory aspects has a bearing on conditions of competition, it might be taken into account, subject to the particular circumstances of a case, and as an integral part of a panel's analysis of whether the measure at issue modifies the conditions of competition to the detriment of like services or service suppliers of any other Member.[194]

The AB's interpretation in *Argentina-Financial Services* imposes a narrow view on the role of the regulatory context in the analysis of 'less favourable treatment' under GATS. According to the AB, the regulatory context can only be considered when the measure in question does not modify the competitive conditions to the detriment of imported services or service suppliers. Practically, this scenario would only apply when there is no 'genuine relationship' between the measure and the adverse impact.[195] However, in cases where such a genuine relationship exists—i.e., where the measure directly affects the competitive opportunities of imported services or service suppliers—the regulatory intent would not be considered in determining whether there has been 'less favourable treatment'. Additionally, the AB emphasised that any regulatory objectives must be justified under the general exceptions clause of Article XIV of the GATS.[196] However, as discussed previously, applying this justification to modern *ex-ante* regulations like the DMA is problematic, as the narrow exceptions outlined in Article XIV do not allow Members to adequately address the dynamic and complex realities of the digital economy. Moreover, as argued by Diebold and Pauwelyn, a subjective interpretation of the non-discrimination obligation does not render the general exceptions clause inutile, as it remains applicable in cases of *de jure* discrimination.[197]

---

[193] Ibid., 6.127.
[194] Ibid.
[195] Natens (n 100), 129. See, *United States – Certain Country of Origin Labelling (COOL) Requirements*, Report of the Appellate Body (23 July 2012) WT/DS384/AB/R, WT/DS386/AB/R, 270. This principle is also reflected in footnote 10 to Article XVII of the GATS, which clarifies that when the conditions of competition are affected by the inherent competitive disadvantages of the foreign service provider, such treatment does not constitute less favourable treatment.
[196] WTO, *Argentina-Financial Services* (n 100) 6.113-14.
[197] Diebold (n 110) 80; Pauwelyn (n 123) 367-68; Robert L Howse and Donald H Regan, 'The Product/Process Distinction – An Illusory Basis for Disciplining 'Unilateralism' in Trade Policy' (2000) 11(2) European Journal of International Law 266; Donald H Regan, 'Regulatory Purpose and 'Like Products' in Article III:4 of the GATT (With Additional Remarks on Article III:2)' in George A Berman and Petros C Mavrodis, *Trade and Human Health and Safety* (Cambridge University Press 2006) 454–55.

In light of the above, we argue that the AB's formalist approach in *Argentina-Financial Services*, which excludes regulatory objectives from the 'less favourable treament' analysis, may not be fully equipped to address the realities of modern regulatory measures, such as the DMA, which seek to regulate digital markets. Unlike the AB's rigid interpretation, Pauwelyn's approach provides a more nuanced framework to integrate regulatory purpose within the 'less favourable treatment' analysis. By considering factors such as the structure and application of the regulation, its impact on competition, and evidence of non-protectionist objectives, Pauwelyn's proposed approach enables the justification of non-protectionist regulatory measures within the framework of the 'less favourable treatment' analysis. This approach is particularly relevant for justifying measures like the DMA, which aim to level the playing field in digital markets without altering competitive conditions to the detriment of Gatekeepers. In contrast, the AB's narrow focus in *Argentina – Financial Services* fails to adequately account for such legitimate regulatory objectives, prioritising formal criteria over subjective considerations. As a result, it risks undermining the ability of governments to justify important regulatory measures designed to address complex challenges of the digital economy.

6 Conclusion

As more countries experiment with *ex-ante* regulations to govern competition in their digital markets, it is essential that the GATS does not constrain states' ability to adopt such measures, in keeping with the embedded liberalism principle central to the WTO system. This issue necessitates revisiting longstanding debates about the extent to which the GATS permits deference to the regulatory purpose behind measures that may conflict with the non-discrimination obligation.

The GATS preamble acknowledges Members' right to regulate in pursuit of legitimate national policy objectives, a provision that takes on particular significance in the context of services trade. Services, by nature, present complexities—such as intangibility, varying modes of supply, and the challenge of separating services from their suppliers—that distinguish them from goods. However, the GATS general exceptions clause is narrow in scope, offering only an exhaustive list of justifications for potential violations, which fails to address modern regulatory challenges, particularly in the digital sphere. These factors have prompted scholars to call for a broader consideration of the regulatory context when assessing the GATS non-discrimination obligation, particularly in cases of *de facto* discrimination.

However, in its most recent ruling on this issue in *Argentina-Financial Services*, the AB adopted a rigid formalist approach, concentrating solely on the competitive relationship between services and service suppliers while overlooking the regulatory purpose behind such measures. This approach creates challenges for justifying *ex-ante* competition

regulations, which aim to level the playing field in digital markets by pre-emptively regulating dominant platforms.

In contrast, we advocate for reading the regulatory context through the 'likeness' test, as proposed by Natens, or the 'less favourable treatment' test, as suggested by Pauwelyn. According to Natens, factors such as service supplier characteristics or consumer preferences should influence the determination of 'likeness', provided they have a bearing on the nature of the services supplied. Under Natens' approach, Gatekeepers can be distinguished from non-Gatekeepers based on characteristics such as market dominance and control over consumer data. These elements shape the services Gatekeepers offer, enabling them to leverage advantages like personalised services and network effects—advantages that smaller competitors cannot replicate—making Gatekeepers not 'like' non-Gatekeepers.

Pauwelyn's approach, in turn, allows for the integration of regulatory purpose within the 'less favourable treatment' test, evaluating factors such as the regulation's design alongside objective evidence of a protectionist intent. This framework ensures that only non-protectionist regulatory measures pass scrutiny. In the context of regulations like the DMA, it would ensure that measures designed to foster fairness in digital markets are justified provided they do not unduly alter the competitive conditions to the detriment of Gatekeepers.

In conclusion, compared to the AB's approach in *Argentina-Financial Services*, Natens' and Pauwelyn's approaches offer more compelling frameworks for evaluating the regulatory context, ensuring that *ex-ante* competition measures like the DMA can be justified under the GATS without undermining fair competition in digital markets.

*Behrang Kianzad**

FAIRNESS, DIGITAL MARKETS AND COMPETITION LAW – RECONCILING FAIRNESS NORMS IN DIGITAL MARKETS ACT, DATA ACT AND AI ACT WITH COMPETITION LAW

Abstract
The present article explores the implication of fairness as a regulatory and competition law concept applied to digital and Artificial Intelligence markets, in light of recent law and policy developments targeting the interaction between data, market power and competition law.
Much of the policy discussions, legislative proposals as well some emerging case law elevate the matter of "fairness" in the context of digital markets and AI, creating both a novel regulatory framework as well as encouraging competition law to curb "unfairness" of said markets and related "unfair practices".
The interface between intellectual property rights and competition law is of utmost importance in this context, where we might find similar analogous insights as we can find regarding the matter of fairness within traditional EU competition law. Further, the question remains whether the "fairness norm" expressed in regulatory acts such Digital Markets Act, EU AI Act and the EU Data Act are akin to the "fairness" norms found in Union competition law, mainly under Article 102 Treaty on the Functioning of the European Union (TFEU).

JEL CLASSIFICATION: K2; K21;K23;K24;L4;L5;B5

SUMMARY

1. Fairness as a regulatory concept in digital markets – 2. Fairness as a concept in law and economics - 3. Fairness as a goal for EU Competition law and policy – 4. The interface between competition law and intellectual property law – 5. The interaction between ex ante regulation and ex post competition law enforcement in digital markets – 6. Conclusions

1 Fairness as a regulatory concept in digital markets

Much of the policy discussions, legislative proposals as well some emerging case law elevate the matter of "fairness" in the context of digital markets and encourage competition law to curb "unfairness" of said markets and related "unfair practices".

* LLM / PhD, School of Economics and Management, Lund University. This research has been supported by a grant by Johan and Jakob Söderberg Foundation.

 DOI 10.13135/2785-7867/11807

[1] Paraphrasing the Danish legal scholar Alf Ross, the problem with the above is that "Fairness, like a harlot, is at disposal of anyone",[2] meaning that the intuitive, subjective element invariably entailed in the concept of fairness - if not defined consistently, objectively and practically - will make the concept rather void.

Although there are several EU directives and regulations to be found which deal with "fairness / unfairness" in various sectors,[3] and although Union competition law elevates fairness literally in Article 102 Treaty on the Functioning of the European Union[4] (henceforth TFEU), the matter of "fairness" is much more elevated in the recently introduced legal acts targeting digital, data- and AI-driven markets.

Therefore, the present article will by way of delimitation focus on Digital Markets Act,[5] the EU AI Act[6] as well as the EU Data Act,[7] which all elevate fairness to a high-degree in those sectors, and do indeed seem to align with each other regarding the ontological definition of fairness as "equitable exchange" per the literal wording of those said acts as will be demonstrated.

One such prime example is the recently introduced Digital Markets Act, as the final legislative act elevates the concept of "unfair" in no less than 43 instances while "fairness" is mentioned in 18 instances. Nowhere in the document is fairness / unfair legally or economically defined beyond the mere contours of what would constitute "unfairness" and the desired outcome of "fair markets", which has become a point of criticism already.[8]

A definition is given at the point 33 in the preamble of the act, defining unfairness for the purposes of the regulation as "unfairness should relate to an imbalance between the

[1] Margarethe Vesterager, 'Fair Markets in a Digital World' (Danish Competition and Consumer Authority, Copenhagen, March 9, 2018); Johannes Laitenberger, 'EU Competition Law in Innovation and Digital Markets: Fairness and the Consumer Welfare Perspective' (Brussels, October 10, 2017).

[2] Alf Ross, 'Analysis and Critique of the Philosophy of Natural Law', in Alf Ross (ed), *On Law and Justice* (Oxford University Press, 2019), 350.

[3] See Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain [2019] OJ L 111; Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; 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 [2019] *OJ L 186*; Regulation (EU) 2021/2117 of the European Parliament and of the Council of 2 December 2021 amending Regulation (EU) No 1308/2013 establishing a common organization of the markets in agricultural products [2021] *OJ L 435*.

[4] Consolidated Version of the Treaty on the Functioning of the European Union [2012] *OJ C 326*, Article 102.

[5] 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 [2022] *OJ L 265*.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts [2024] *OJ L 2024/1689* (Artificial Intelligence Act).

[7] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] *OJ L, 2023/2854* (Data Act).

[8] See Wolfgang Kerber, 'Taming Tech Giants with a Per Se Rules Approach? The Digital Markets Act from the "Rules vs Standard" Perspective' (2021) 3 Concurrences 28.

rights and obligations of business users where the gatekeeper obtains a disproportionate advantage".

Students of economics would argue that any successful business deal does display some "disproportionality", and already we arrive at the grand debates on whether markets should strive to produce optimal, efficient results, or socially and morally desirable results, and whether there exists a trade-off between these two, or if there is possible to overcome the dichotomy.

The present article will not attempt to grapple itself with these matters as this has been done at some length in other works[9] and would lead the focus astray, but the next section will delve briefly into the contours of the grand debates sketched above.

Moving on to the next regulatory act elevating fairness, the EU AI Act mentions "fair" in 17 instances, also referring to the seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental well-being and accountability, framed in 2019 Ethics guidelines for trustworthy AI developed by the independent AI HLEG appointed by the Commission.[10]

Fairness in turn in the AI Act is merely defined as "Diversity, non-discrimination and fairness means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law."[11] This writing does not expand our knowledge at all, since it merely references rather general non-discrimination and non-bias ideals, and refers to other bodies of Union law prohibiting "unfair biases", but also "unfair behaviours", one would presume.

Indeed, as seen from point 45 in the preamble of the EU AI Act, it is prescribed that "practices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation."[12]

Finally, the Regulation (EU) 2023/2854,[13] also known as the " EU Data Act," which establishes rules for fair access to and the use of data within the EU, the term **"fair"** appears prominently as the regulation focuses on ensuring equitable data-sharing among various stakeholders. The EU Data Act mentions the word **"fair" 28 times,** where the

[9] Behrang Kianzad, 'Beyond Justice versus Efficiency – Reconciling Law and Economics Approaches to Fairness' in Klaus Mathis and Avishalom Tor (eds), *Law and Economics of Justice: Efficiency, Reciprocity, Meritocracy* (Springer 2024), 91-130.

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act) [2024] OJ L168/1, p. 27.

[11] Ibid.

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act) [2024] OJ L168/1, point 45, preamble.

[13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L, 22.12.2023.

regulation primarily focuses on establishing fair access and sharing of data to foster balanced opportunities within the EU's data economy.

However, while the document is oriented around promoting fair and balanced data sharing, specific terms like **"unfair"** and **"unfairness"** do not appear frequently as key legal terms in the regulation itself. Instead, "unfair" may appear in relation to consumer protection or unfair contractual practices, defined partly by way of reference to various other directives on unfair commercial practices.[14]

The EU Data Act nevertheless in para 62 defines certain terms relating to data as being ex ante "unfair" and others presumed to be such, which mimics the so-called hardcore restrictions and block exemptions under Article 101 TFEU,[15] making it even more relevant to draw insights from EU competition law debates on the matter of fairness for the purposes of interpretation and enforcement of the EU Data act.

The above can be compared to the Unfair Commercial Practices Directive,[16] which mentions "unfair" in 32 instances but gives a clear-cut definition of what constitutes such "unfair" practices in Article 5.2, defining such practices as a) those contrary to the requirements of professional diligence, and (b) materially distorting or likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.

Although such *ex ante* regulations relating to Digital Market actors (gate keepers, core platform providers, Tech giants), Data and AI all elevate fairness, when this is done in relation to "fair" markets, or fairness towards consumers, the interaction with Union competition law regime is self-evident. Nevertheless, as indicated in the DMA, "existing Union law does not address, or does not address effectively, the challenges to the effective functioning of the internal market posed by the conduct of gatekeepers that are not necessarily dominant in competition-law terms… At the same time, since this Regulation aims to complement the enforcement of competition law, it should apply without prejudice to Articles 101 and 102 TFEU".[17]

[14] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29; Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22.

[15] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L, 22.12.2023, para 62: 'In order to ensure legal certainty, this Regulation establishes a list of clauses that are always considered unfair and a list of clauses that are presumed to be unfair."

[16] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005] OJ L149/22.

[17] 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) [2022] OJ L265/1, preamble, points 5 and 10, respectively.

As fairness has long been a controversial competition law concept[18] seen from the perspective of welfare economics[19] (which puts the analytical and normative emphasis on economic efficiency, not fairness), there is manifest risk for a hampered and non-harmonious enforcement. Although welfare economics are not the only economic school affecting competition law, and there is indeed a shift away from those theories to other economic theories[20] being better suited to deal with the legal matter of fairness, the impact of the welfare economics on European competition law is still considerable.[21]

Interestingly, a range of competition law cases have seen the light of the day[22] targeting exactly the type of data-driven, often-times algorithmic, abusive behaviour, a trend that will only continue as further scrutiny, ex ante regulation but also ex post competition law enforcement is levied against such data & AI-driven markets.

Concluding on the matter of fairness as a concept pertaining to laws governing behaviours, markets and economics, at the outset, we can note that the doctrine is torn between Neoclassical and welfarist approaches casting efficiency as the be-all goal and rationale of competition law, on the one hand;[23] and New Brandesian / Neo-Kantian approaches, on the other hand;[24] emphasizing a host of issues to be addressed by competition law, ranging from fairness to inequality.

Thus, it is necessary to investigate, compare and lay bare the ontological and epistemological similarities and differences between the *ex ante* approach chosen in DMA, EU AI Act and EU Data Act with the ex post approach in Union competition law. This would in turn enable a more in-depth analysis of the implications of centring regulatory instruments as well as competition law and enforcement policy around the concept of fairness in this area from a law and economics perspective.

Following the introduction, the second section discusses the concept of fairness from a law and economics perspective and offers an overview of the contentious debates surrounding the concept of fairness. Thereafter, the third section moves on to the matter of fairness within EU competition law as an object but also its practical applicability. The fourth section discusses the interaction between competition law and intellectual property law in general, while the fifth section delves more deeply into comparing the ex ante approach to fairness in regulation of data-driven markets with the ex post approach

[18] Damien Gerard, 'Fairness in EU Competition Policy: Significance and Implications' (2018) 9 Journal of European Competition Law & Practice 211.
[19] Louis Kaplow and Steven Shavell, 'Fairness versus Welfare' (2001) 114 Harvard Law Review 961.
[20] Behrang Kianzad, 'A Neo-Kantian Approach to Competition Law? – The Re-Emergence of Fairness in Antitrust Law & Policy' in Ramsi Woodcock (ed), *Toward an Inframarginal Revolution -Redistributing the Gains from Trade* (forthcoming, Cambridge University Press, May 2025).
[21] Dzmitry Bartalevich, 'The Influence of the Chicago School on the Commission's Guidelines, Notices and Block Exemption Regulations in EU Competition Policy: The Influence of the Chicago School' (2016) 54 JCMS: Journal of Common Market Studies 267.
[22] See e.g. US District Court for the Middle District of North Carolina, RealPage, Case No. 1:24- cv-00710, Complaint, 23 August 2024; Amazon v District of Columbia (DC Court of Appeals, Case No 22-CV-0657, 22 August 2024); Case T-334/19 *Google and Alphabet v Commission (Google AdSense for Search)* [2024] ECLI:EU:T:2024:634.
[23] Kaplow and Shavell (n 19).
[24] Kianzad (n 9).

of competition law. The sixth section concludes that the approach in DMA, EU Data Act and EU AI Act regarding what constitutes "equitable exchange" as well as "fair and contestable" versus what constitutes "unfair behaviour" should be firmly grounded and inspired by the long-standing approach to those matters within European competition law, as well as insights from behavioural economics regarding fairness preferences, in order to offer legal certainty and harmonious application throughout the Union.

2 Fairness as a concept in law and economics

Rebutting the criticism by Alf Ross cited in the introduction, one could argue that as relative, subjective and abstract as the concept of fairness might present itself, the entirety of human history and experience is filled with in-depth inquiries on the matter of fairness and justice, alongside philosophical, legal, economic, psychological and even neurological studies in search of what constitutes fair and unfair, respectively.

The question of what constitutes fairness and justice, its conditions and conditionality, and its volition and volatility, has been a defining character of the legal, philosophical, ethical debates since time immemorial. According to various Natural Law schools, fairness and justice are the departing notion, and final outcome, of the legal discipline, having its roots in religious texts via imperial decrees and later, the first legal texts and treaties. Other schools, such as legal realists and legal positivists, rather emphasise the procedural fairness and the process of codification as the main element of the legal discipline.[25]

The division of the Justice and Fairness concept along the lines of reciprocity, equality and conformity to social and moral norms or laws have dominated much of the Western discourse on Justice and Fairness. As such, concepts such as consequentialism, deontology and virtue ethics have subsequently been developed. Consequentialists put the emphasis on maximisation of beneficial outcomes, aligning the theory with utilitarianism, focusing on both individual and societal maximisation of "utility", counting Jeremy Bentham among others as important figures.

Deontological discourse ("deon" from Greek word for duty and "logos" meaning science) denotes the diametrical opposition of utilitarianism, in that the discourse put the emphasis on the moral value and volition inherent in actions, and not, the outcome and consequences. The outcome, even if not beneficial from a strict utilitarian viewpoint, is secondary to the moral good inherent in the action. Immanuel Kant can be said to have formulated the greatest treatise on the matter, complete with his formulation of the Categorical Imperative, a "moral law" to be determined by reasoned experience, denoting that all actions should be such that they could be elevated to a universal law.[26]

The economic research has mainly taken the form of behavioural and experimental research, beyond traditional political economy, with Kahneman et alia. laying some of the

[25] Hans Kelsen, *Pure Theory of Law* (Lawbook Exchange Ltd, 2009).
[26] Immanuel Kant, *Grundlegung zur Metaphysik der Sitten* (Felix Meiner Verlag, 2016).

groundwork of this field of research in mid 1980´s. In behavioural science, fairness oftentimes denotes the social preference for equitable outcomes, largely alongside the views of fairness.[27]

Such preference for equitable outcomes can also manifest itself as “inequity aversion”, denoting people’s tendency to dislike unequal payoffs in their own or someone else’s favour, a matter which has been investigated by way of experimental games, such as the ultimatum, dictator, and trust games.[28]

Briefly explained, the Ultimatum Game consist of a setting where one player, called the proposer, is endowed with a set amount, such as $100. The proposer will then share this amount with another player, called the responder, by way of a proposal regarding division of the total sum in question. After the proposition is made, the responder has the choice to accept or reject the offer made by the proposer. If the responder accepts the offer, both players get to keep the proposed sum. However, if the responder rejects the offer, neither party gets to keep any of the proposed division. The players are aware of the rules of the game in advance, thus characterising the game as an "ultimatum game."[29]

According to traditional game theory, which assumes rational decision-making and strict utility maximization, the proposer should offer the smallest possible sum. This is because the responder faces a choice between accepting this minimal amount or receiving nothing. Accepting even a very small sum would increase the responder's utility compared to receiving nothing at all. This outcome constitutes a Nash Equilibrium, named after American Economist John Nash (1928-2015) which describes a solution to a non-cooperative game where players, knowing the playing strategies of their opponents, have no incentive to change their strategy, as having reached Nash equilibrium, a player will be worse off by changing their strategy.

Given this logic, proposers initially have no incentive to make "fair" offers. Surprisingly, experimental evidence shows proposers frequently do offer relatively fair shares, and responders often reject offers they perceive as unfair. Research indicates that most proposers offer between 40% and 50% of the total amount, and responders almost always accept these offers. However, when the offered share decreases to around 20%, responders reject the proposal about half the time. Rejection rates further increase as offers drop to 10% or below."[30]

---

[27] Daniel Kahneman, Jack L Knetsch and Richard H Thaler, ‘Fairness as a Constraint on Profit Seeking: Entitlements in the Market’ (1986) 76 The American Economic Review 728; Daniel Kahneman, Jack L Knetsch and Richard H Thaler, ‘Fairness and the Assumptions of Economics’ (1986) 59 The Journal of Business S285.

[28] Ernst Fehr and Klaus M Schmidt, ‘A Theory of Fairness, Competition, and Cooperation’ (1999) 114 The Quarterly Journal of Economics 817.

[29] Mascha van ‘t Wout and Johannes Leder, ‘Ultimatum Game’ in Virgil Zeigler-Hill and Todd K Shackelford (eds), *Encyclopedia of Personality and Individual Differences* (Springer International Publishing, 2018).

[30] Daniel Houser and Kevin McCabe, ‘Experimental Economics and Experimental Game Theory’ in *Neuroeconomics* (Elsevier, 2014) 19–34; see also Stéphane Debove, Nicolas Baumard, and Jean-Baptiste André, 'Models of the Evolution of Fairness in the Ultimatum Game: A Review and Classification' (2016) 37(3) Evolution and Human Behavior, 245–54; MA Nowak, ‘Fairness Versus Reason in the Ultimatum Game’ (2000) 289 Science 1773.

The fair allocation can be seen as evidence regarding fairness as constraint on pecuniary gaining, where people engage in fair sharing "in order to avoid large deviations from what they consider a fair solution. This type of behaviour has been extensively documented in laboratory experiments with games such as the ultimatum game and the dictator game".[31]

The implication of Fairness concerns for Game Theory and Equilibrium was already highlighted by Rabin in 1993, noting "People like to help those who are helping them, and to hurt those who are hurting them...one should care not solely about how concerns for fairness support or interfere with material efficiency, but also about how these concerns affect people's overall welfare."[32]

Earlier still, the seminal work by Kahneman, Knetsch and Thaler in 1986,[33] of great importance for the context of the present work on excessive pricing, demonstrated that people are wary of pricing unfairness, where prior prices of the undertaking served as one benchmark for such fairness considerations.

Just a year earlier in 1985, the non-maximising tendencies (framed around non-rationality) and its implications for rationality and overall Economic Equilibrium was also investigated by Akerlof and Yellen.[34] Building on prior work by Artur Okun in 1981,[35] who had also observed that firms do not maximise prices despite facing excess demand (such as new models of automobiles or tickets for events which ex ante are known to generate excess demand), Kahneman et alia. investigated the fairness perceptions regarding (unfair)pricing.

The observed behaviour in the experimental games and the asserted human bias towards fairness and equity was by some labelled as altruism, however, the work by Fehr and Schmidt showed that this was not the case, as noted "Altruism is consistent with voluntary giving in dictator and public good games. It is, however, inconsistent with the rejection of offers in the ultimatum game, and it cannot explain the huge behavioural differences between public good games with and without punishment. It also seems difficult to reconcile the extreme outcomes in market games with altruism."[36]

The above does indeed hold immense theoretical and practical implications when e.g. AI driven algorithmic pricing substitute the human price determination dynamics about which we have amassed considerable knowledge in the past. AI, lacking any “moral” or “legal” constrictions and considerations, is thus able to engage in a truly profit-maximising

[31] Alexander W Cappelen and others, 'The Pluralism of Fairness Ideals: An Experimental Approach' (2007) 97(3) American Economic Review, 818–27; John von Neumann and Oskar Morgenstern, *Theory of Games and Economic Behavior* (Princeton University Press, 60th Anniversary Commemorative Edition, 2007).
[32] Matthew Rabin, ‘Incorporating Fairness into Game Theory and Economics’ (1993) 83 The American Economic Review 1281.
[33] Kahneman, Knetsch and Thaler (n 27).
[34] George A Akerlof and Janet L Yellen, ‘Can Small Deviations from Rationality Make Significant Differences to Economic Equilibria?’ (1985) 75 The American Economic Review 708.
[35] Arthur Okun, *Prices and Quantities: A Macroeconomic Analysis* (Brookings Institution 1981).
[36] Fehr and Schmidt (n 28).

behaviour without risk of losing reputation, sales or encountering competition law scrutiny, left unchecked.

As indicated the concept of fairness is in law and economics is indeed surrounded by controversies, with some schools rejecting fairness to be an economic concept at all. There are three main problems with the line of reasoning which rejects "any conceptual basis in economics"[37] regarding fairness as a legal-economic concept (where in European law we find a clear prohibition against unfair pricing), on both normative and empirical lines. Firstly, total welfare is not the object of European competition law, and never has been, as seen from the legal-history and jurisprudence of CJEU, which is geared towards consumer welfare.[38]

Secondly, the definition of "economists" or "economics" in a monolithic sense is not a correct framing of the discipline and its practitioners, rather, enforcement against undue rent transfer and profiteering can indeed be seen as the prima facie function of competition law, in preventing undue wealth transfer, creation of market power and preventing in-efficiencies.

The conceptual basis of human aversion against unfair pricing is rather solid from both behavioural and neuro-economics studies. In comparison, empirical and neurological evidence for utilitarianism, rational choice and Homo Oeconomicus are yet to be substantiated. Fairness is further able to be aggregated and modelled in a strict economic sense.[39]

Thirdly, the assertion of "serious economic harm" being a risk associated with vigorous enforcement against excessive pricing must be qualified on a case-by-case approach, in the light of an empirical reality demonstrating the opposite, i.e., the absence of a causal relationship between excessive profits and innovation as the evidence examined rather points to less innovation and wealth and not being able to create "welfare", if this latter is defined on a societal and not individual level.[40]

The re-emergence of the concept of fairness in competition policy[41] which have long been dominated by technocratic, econometric, marginalist approach forwarding efficiency as the only rationale and end-goal can thus be seen as a re-affirmation of the

[37] Frédéric Jenny, 'Abuse of Dominance by Firms Charging Excessive or Unfair Prices: An Assessment' in Yannis Katsoulacos and Frédéric Jenny (eds), *Excessive Pricing and Competition Law Enforcement* (Springer International Publishing 2018).
[38] Doris Hildebrand, 'The Equality and Social Fairness Objective in EU Competition Law: The European School of Thought' (2017) 1 Concurrences 1; Ioannis Lianos, 'Some Reflections on the Question of the Goals of EU Competition Law', in Ioannis Lianos and Damien Geradin (eds), *Handbook on European Competition Law*, (Edward Elgar Publishing, 2013), 1–84.
[39] Stefan Wintein and Conrad Heilmann, 'Theories of Fairness and Aggregation' (2020) 85 Erkenntnis 3; Jan Boone, 'Pricing above Value: Selling to an Adverse Selection Market' (2020) CentER Discussion Paper 2020-023; Marcel Canoy and Jan Tichem, 'Lower Drug Prices Can Improve Innovation' (2020) 14(2–3) European Competition Journal, 278-304.
[40] General Secretariat OECD, 'Beyond Growth: Towards a New Economic Approach - Report of the Secretary General's Advisory Group on a New Growth Narrative' (12 September 2019).
[41] Sandra Sandra, Marco Colino, 'The Antitrust F Word: Fairness Considerations in Competition Law' [2019] Journal of Business Law 329.

social policy rationales underpinning competition law[42] (but also intellectual property law to a great extent) and can serve as a clarification of the multitudes of rationales and benchmarks, fairness being one.

Having discussed the overall contours of the debate in law and economics of laws relating to economic activity in the above, it becomes clear that the re-emergence of the concept of fairness in competition policy[43] is rather eye-catching. Competition law and policy has long been dominated by technocratic, econometric, marginalist approach forwarding efficiency as the only rationale and end-goal. The next section moves on to discuss the matter of fairness as a goal for EU competition law, economics and policy, using Article 102 TFEU as proxy.

The next section moves on to the matter of fairness within EU competition law as an object but also its practical applicability.

3 Fairness as a goal for EU Competition law and policy

The inherent tension between the legal discipline (concerned primary with delivering justice and fairness) and the economic discipline (concerned primary with ensuring equilibria and allocative efficiency) is probably most evident in the case of "fairness" rules such as Article 102a TFEU ban on "unfair pricing", but also in the areas such as essential facilities and FRAND licensing, highly relevant to the digital markets.

As per the literal wording of Article 102a, to be applied by the Commission and the NCAs, the undertaking in question must a) hold a dominant position in the relevant market b) engage in a conduct capable of having an effect on trade within the internal market and c) allegedly have abused its dominant position and market power in some ways foreseen by the Article 102a - such as imposing unfair pricing.

The article in question is "law of the land" across all Member States, and it has been subject to an ever-increasing harmonization efforts within European competition law, where the latest step consist of the Directive 2019/1 of 11 December 2018, accords more powers to NCAs.[44]

In regard to the object and function of Article 102 TFEU, as established by settled jurisprudence of the CJEU, the main function of EU competition law rules, including Article 102a TFEU is to “prevent competition from being distorted to the detriment of the public interest, individual undertakings and consumers, thereby ensuring the well-being of the European Union… Accordingly, Article 102 TFEU must be interpreted as referring

[42] Ioannis Lianos, ‘Polycentric Competition Law’ (2018) 71 Current Legal Problems 161.
[43] Sandra Marco Colino, 'The Antitrust F Word: Fairness Considerations in Competition Law' (2019) Journal of Business Law 329.
[44] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market [2019] OJ L11/3.

not only to practices which may cause damage to consumers directly…but also to those which are detrimental to them through their impact on competition"[45]

Fairness can thus be said to constitute a guiding principle behind Union competition law in general and Article 102 TFEU specifically, which been routinely applied by the EU case law to both exclusionary and exploitative cases, and fairness has indeed been cited as a goal for EU competition law.[46]

Traditionally, competition law can be said to have been seen as a tool to ensure "fair and contestable markets",[47] which is the parlance of the Digital Markets Act. While the Court of Justice of the European Union (CJEU) plays a crucial role in interpreting and enforcing EU laws, including the DMA, there is no specific reference to the exact phrase "fair and contestable markets" in its rulings. However, the CJEU has addressed concepts related to market fairness and contestability in various cases concerning competition law and digital markets.

For instance, in the Courage v. Crehan decision, the CJEU emphasized the importance of private enforcement in competition law, aligning with the DMA's objective of ensuring fair and contestable markets.[48]

Additionally, the CJEU has been involved in cases related to the DMA's enforcement. For example, in July 2024, the General Court upheld[49] the European Commission's designation of ByteDance, the owner of TikTok, as a gatekeeper under the DMA, reinforcing the regulation's aim to maintain fair and contestable digital markets

The CJEU has rather used tin recent years, "competition on the merits"[50] but already in Consten and Grundig in 1966 the court emphasized that the Union competition rules intended to ensure a "fair share" to consumers, and recently in its Interflora decision the CJEU referred to the matter of "fair competition".[51]

Furthermore, regarding the interaction between data and competition, the CJEU in its Lindenapotheke judgement held that:

"it is important to recall that access to and use of personal data are of great importance in the context of the digital economy. Access to personal data and the ability to process

[45] Case C-52/09 *Konkurrensverket v TeliaSonera AB* (Preliminary ruling, Judgment of the Court (First Chamber) [2011] *OJ C 103*, paras 22 and 24 and case law cited therein.
[46] Konstantinos Stylianou and Marios Iacovides, 'The Goals of EU Competition Law - A Comprehensive Empirical Investigation' [2020] SSRN Electronic Journal.
[47] Einer Elhauge and Damien Geradin, *Global Competition Law and Economics* (Hart Publishing, 2011) 1; see also William J Baumol, John C Panzar and Robert D Willig, *Contestable Markets and the Theory of Industry Structure* (Harcourt Brace and Jovanovich, 1982).
[48] Case C-453/99 *Courage Ltd v Bernard Crehan and Bernard Crehan v Courage Ltd and Others. Reference for a preliminary ruling: Court of Appeal (England and Wales) (Civil Division) - United Kingdom* [2020] ECLI:EU:C:2001:465. See Jörg Hoffmann, Liza Herrmann and Lukas Kestler, 'Gatekeeper's Potential Privilege—The Need to Limit DMA Centralization' (2024) 12(1) Journal of Antitrust Enforcement 126–147.
[49] Case T-1077/23 *Bytedance v Commission* [2024] ECLI:EU:T:2024:478.
[50] See e.g. Case C-413/14 P *Intel Corp. Inc. v. European Commission* [2017] ECLI:EU:C:2017:632 , Case C-48/22 P *Google v Commission* [2024] ECLI:EU:C:2024:67; *Servizio Elettrico Nazionale and Others v Autorità Garante della Concorrenza e del Mercato* (Case C-377/20) [2021] ECLI:EU:C:2021:710; *Deutsche Telekom AG v European Commission* (Case C-280/08 P) [2010] ECLI:EU:C:2010:603; *France Télécom SA v European Commission* (Case C-202/07 P) [2009] ECLI:EU:C:2009:214.
[51] Case C-323/09 *Interflora Inc. v Marks & Spencer plc* [2011] ECLI:EU:C:2011:604, para 64.

such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, in order to take account of the reality of this economic development and to ensure fair competition, it may be necessary to take into account the rules on the protection of personal data in the context of the application of competition law and the rules on unfair commercial practices".[52]

Adding to this dimension the interaction between sector regulation and competition law, and the dichotomy depicted above in parts of law and economics doctrine on the nature of competition law, one is faced with an emerging law and economics field where insights from both consumer protection, non-discrimination and competition law are intertwined in ensuring "fair and contestable markets".

But can fairness be said to have acted as an independent goal of European competition law? As a departing point, a comprehensive empirical data study[53] of the decisions by the Commission, judgements by Court of Justice of European Union and Advocate General Opinions as well as Commissioner for Competition Speeches, might be a helpful tool laying bare *de lege lata*, before embarking on the normative discussion which invariably has more a *de lege ferenda* character.

The data study investigated 1082 Commission decisions, 2267 CJEU and General Court judgements and AG opinions, spanning a timeline between 1960´s and 2020. The study shows that seven overarching goals are found in the references in the documents examined, these goals being integration, freedom to compete, structure, competition, welfare, efficiency and fairness.

Looking at the Protocol No 27, annexed to the Treaty of Lisbon, the goals of EU competition Law are described as "...the internal market as set out in Article 3 of the Treaty on European Union includes a system ensuring that competition is not distorted."[54]

The object of European competition law has nevertheless ever since its conception been the target of fierce scholarly (and political) debate on whether it should concern protection of consumer welfare or the competitive process as such, beyond the European Economic Integration and harmonisation of inner market. Albeit, as formulated by Ioannis Lianos "the quest for the goals of competition law may prove in the end a meaningless exercise. Indeed, social goals affecting the interpretation and implementation of EU competition law are evolving and are highly dependent on the institutional and political context."[55]

Evidently, the matter of fairness is "at the heart of the matter" and cannot be ignored. As noted by Johannes Laitenberger, then director of DG Competition in 2017 "Fairness" is as old as competition law itself. Standing on the floor of the U.S. Senate in 1890, Senator Sherman explained that his bill was about ensuring "free and fair competition"...Likewise,

[52] Case C-21/23 *ND & DR v European Commission* [2024] ECLI:EU:C:2024:846.
[53] Stylianou and Iacovides (n 46).
[54] Consolidated Version of the Treaty on European Union - Protocol (No 27) on the Internal Market and Competition [2008] OJ C115/309.
[55] Lianos (n 42).

the Spaak Report of 1956 – when the EU competition rules were first discussed – stressed the importance of "fair" competition."[56]

Moving on to distinguish "competition law" from "unfair trading" laws as per the German legal tradition, Laitenberger points to the fact that although competition law is primarily more concerned with restriction of competition, than unequitable behaviour among competitors, the matter of fairness belongs firmly to the realm of competition law, as well. Laitenberger noted that "the term "fair" appears in Article 101(3) TFEU, while the term "unfair" appears in Article 102 TFEU. The preamble of the TFEU calls for concerted action in order to guarantee "fair" competition. It is a rationale that underpins the EU competition rules."[57]

Margarethe Vesterager, European Commissioner for Competition, revisited the theme of fairness in yet another speech in 2018, this time at a conference titled "Fairness and Competition", noting the long-roots of fairness from the Codes of Hammurabi to modern day refined tools and answers to what constitute "fairness" in a market setting, with competition law rules being one example.[58]

In regard to the matter of exploitative, unfair and excessive pricing by dominant undertakings and detailing the latest actions by the Commission in regard to exploitative pricing practices, the recent years have seen a marked focus on fairness and protecting consumers from abuse of dominant companies.[59]

This particular legal-policy focus on fairness towards consumers as a central tenet of European competition law is also self-evident in a range of other activities and statements from the Commission, Council and the Parliament in regard to fairness, but also a string of enforcement of the most important EU competition law rules on fairness, such as the prohibition against unfair pricing.

As also noted by Damien Gerard, also at the Member State level, fairness seems to be used "as a convenient unifying concept to capture and convey the overarching objective of competition policy, thereby also accommodating different conceptions of the defining principles of justice governing social institutions, including the role and scope of government intervention".[60]

Indeed, European competition law has designated "unfair pricing" as inherently evil and harmful to consumers warranting enforcement beyond market dynamics and even the reach of sector regulators. This is evident in cases such as the case of excessive mobile roaming surcharges or excessive pharmaceutical pricing. The latter received immense

[56] Johannes Laitenberger, 'EU Competition Law in Innovation and Digital Markets: Fairness and the Consumer Welfare Perspective' (Brussels, October 10, 2017).
[57] Johannes Laitenberger, 'EU Competition Law in Innovation and Digital Markets: Fairness and the Consumer Welfare Perspective' (Brussels, October 10, 2017).
[58] Margarethe Vesterager, 'Fairness and Competition - Speech at GCLC Annual Conference' (Brussels, January 25, 2018).
[59] Margarethe Vesterager, 'Protecting Consumers from Exploitation' (Chillin' Competition Conference, Brussels, November 21, 2016); Neelie Kroes, 'Preliminary Thoughts on Review of Article 82' (Fordham Corporate Law Institute, September 23, 2005).
[60] Gerard (n 18).

attention on both Commission and member state levels from 2016 onwards, resulting in a range of decisions against unfair and excessive pharmaceutical pricing across the EU.[61]

Regarding roaming charges, this was a legislative saga[62] that began in 2002 and ended about15 years later with the abolition of all roaming charges within European Union whereas as of 15 June 2017, European consumers have been able to use their mobile devices while travelling within a the EU, paying the same prices as they would do at home, under the so called "Roam like at Home" principle.[63]

Directive (EU) 2018/1972 on European Electronic Communications Code[64] thus target excessive pricing and conditions thereof within the telecommunication sector and enables national regulatory agencies to intervene in the market in order to prevent excessively high prices if the competition in the market is not able to function properly.

Another example is the Unfair Commercial Practices Directive of 2005, having a strict consumer protection characteristic, albeit offering some insights into the focus on fairness towards consumers. Unfair Commercial practices are defined in Article 5 of the Directive as being a practice that "…is contrary to the requirements of professional diligence" and "materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed or of the average number of the group when a commercial practice is directed to a particular group of consumers".[65]

Although the Directives cited above target areas of law other than competition law and cannot be thus are not able of being directly invoked or applied by analogy in a competition law context, the reasoning of the Commission in regard to unfairness, markets and consumers are is closely related to matters routinely addressed by competition authorities and courts when dealing with market behaviour and market power.[66]

---

[61] Behrang Kianzad, 'Towards Fair Pricing of Medicines?' (2022) 6(1) European Health & Pharmaceutical Law Review, 2-23.

[62] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33; Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC [2007] OJ L171/32, repealed and replaced by Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union [2012] OJ L172/10.

[63] Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC [2007] OJ L171/32; Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union [2012] OJ L172/10.

[64] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321/36.

[65] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L149/22.

[66] For a comparison between fairness elements in Article 102 TFEU and other bodies of law such as contract law and unfair commercial practices, see Pinar Akman, *The Concept of Abuse in EU Competition Law: Law and Economic Approaches* (Hart Publishing, 2015).

The focus of Article 102 TFEU in regard to direct, exploitative abuses and prevention of harm to consumers is also affirmed by the settled case law of CJEU, why e.g. Digital Markets Act (DMA) refers to the Union competition law by way of references to articles 101 and 102 TFEU.[67]

DMA was also inspired by Union competition law as evidenced by the preparatory works and annexes surrounding the document, mainly elevating article 102 TFEU.[68] Nevertheless, as DMA clearly states, the aims and purposes pursued by DMA differ slightly from objectives pursued under Union competition law, framed as:

"This Regulation pursues an objective that is complementary to, but different from that of protecting undistorted competition on any given market, as defined in competition-law terms, which is to ensure that markets where gatekeepers are present are and remain contestable and fair, independently from the actual, potential or presumed effects of the conduct of a given gatekeeper covered by this Regulation on competition on a given market. This Regulation therefore aims to protect a different legal interest from that protected by those rules and it should apply without prejudice to their application."[69]

One could argue that the prohibition against "unfair, excessive pricing" in European competition law is construed alongside equality and equity in exchange per the Aristotelian and Just Price tradition informing the ratio legis of the prohibition, but also its *ratio oeconomica*.[70]

This is an important insight when attempting to understand and compare the "fair and contestable" and "equitable exchange" notions of fairness entailed in DMA with fairness norms in European competition law on e.g. unfair pricing.

Aristotle devoted an entire book in his Ethics to the matter of Justum Pretium, or Just Price, noting "But the justice in transactions between man and man is a sort of equality need, and the injustice a sort of inequality…according to arithmetical proportion. Therefore, this kind of injustice being an inequality, the judge tries to equalize it…therefore the equal is the intermediate between the greater and the less…therefore the corrective justice is the intermediate between loss and gain."[71]

[67] Joined Cases 6 and 7-73 *Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission of the European Communities* [1974] ECLI:EU:C:1974:18; Joined Cases C-468/06 to C-478/06 *Sot. Lélos kai Sia and Others* [2008] ECR I-7139, para 68; Case C-280/08 P, *Deutsche Telekom v Commission*, Judgment of the Court (Second Chamber) [2010], ECLI:EU:C:2010:603, para 176.

[68] See e.g. Commission Staff Working Document SWD(2020) 363 final, Impact Assessment Report – Annexes, Brussels, 15.12.2020, Annex 5.6; European Commission, Digital Markets Act - Impact Assessment Support Study, Annexes, December 2020, Annex 4 "case studies".

[69] Digital Markets Act, para 11, preamble.

[70] Behrang Kianzad, *What Makes A Price (Un)Fair)? Excessive Pharmaceutical Pricing in European Competition Law* (Det Juridiske Fakultet, København 2022).

[71] Aristotle, *Nicomachean Ethics, Book VII* (Batoche Books, translated by WD Ross, 1999).

This interpretation of "Just Price" thus re-connects with the Aristotelian position on "equality in exchange".[72] This approach to "just price"[73] was further developed in Roman Law and the concept of laesio enormis[74], and later during the Medieval times by Albert the Great and Thomas Aquinas[75] et alia, in part re-connecting with the biblical concept of "usury", and thus came to impact the European competition law prohibition against unfair pricing.[76]

Further economic research has targeted fairness in pricing and the notions of customers related to increase in pricing, demonstrating that consumers are generally less accepting of price increases as result of a short term growth in demand than rise in costs.[77]

Regarding unfairness in pricing, if defined as per article 102 TFEU, the reliance on past prices when judging appropriateness of current prices and use of current prices to predict future prices has also been demonstrated by other researchers,[78] however past prices are not the sole determinant regarding fair pricing perceptions, where prevailing competitive prices are also of importance.[79]

However, it appears that people do not spontaneously or fully appreciate retailer costs when judging fair prices. Profit is viewed as constituting a large proportion of the selling price.[80] Interestingly, comparison with past prices, or prices charged for the same product in other markets, are two of the central assessment methods related to unfair and excessive pricing in European jurisprudence related to Article 102a TFEU.[81]

Indeed, the reference to "fairness" is also found in Article 101(3) in relation to pro-competitive effects of an agreement which might make Article 101 incompatible in cases "which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit" and does not unduly restrict competitors and competition.

What constitutes a "fair share" is probably on pair regarding complexity as finding what would constitute a "fair price", if not yet more complex, as defining a fair share must invariably involve a more subjective and discretionary measures, similar to how a competitive price is determined using of the Cost Plus approach and other benchmarking approaches developed in the jurisprudence.

---

[72] Aristotle, *Nicomachean Ethics*, 1132b, lines 31–33 as cited in Michal S Gal, 'Abuse of Dominance – Exploitative Abuses' in Lianos and Geradin (n 39).
[73] Oswald von Nell-Breuning, 'The Concept of Just Price' (1950) 8(2) Review of Social Economy, 111–22.
[74] Michal S Gal, 'Abuse of Dominance – Exploitative Abuses' in Lianos and Geradin (n 39) 385–422.
[75] Daryl Koehn and Barry Wilbratte, 'A Defense of a Thomistic Concept of the Just Price' (2012) 22 Business Ethics Quarterly 501.
[76] For an in-depth inquiry on the roots of the prohibition, see: Kianzad (n 70).
[77] Daniel Kahneman, Jack L Knetsch, and Richard H Thaler, 'Fairness as a Constraint on Profit Seeking: Entitlements in the Market' (1986) 76(4) The American Economic Review 728 – 774.
[78] Richard A Briesch and others, 'A Comparative Analysis of Reference Price Models' (1997) 24 Journal of Consumer Research 202.
[79] Kahneman, Knetsch and Thaler (n 27).
[80] Lisa E Bolton, L Warlop and JB Alba, 'Explorations in Price (Un)Fairness - Oepartement Toegepaste Economische Wetenschappen -Research Report 0145' [2001].
[81] Jenny (n 37).

A further example of the emphasis on fairness, direct harm to consumers, and artificially high prices is the 2019 EU Directive on competition law, which empowers the competition authorities of the Member States to be more effective enforcers and ensures the proper functioning of the internal market, noting that "effective enforcement of Articles 101 and 102 TFEU is necessary to ensure fairer and more open competitive markets in the Union".[82]

A final example demonstrating the increased Fairness-trend is the New Competition Tool by the European Commission, which was designed to combat tech-giants, when hindering emergence of new competitors by their sheer size and market power, thus aiming towards structural remedies, a clear U-turn to Big-Is-Bad and per se illegality, one might argue.[83] An effort that was outshone by the enactment of Digital Markets Act and the AI Act, providing the ex ante investigate powers to the Commission and relevant authorities and creating per se liability rules for e.g. designated gatekeepers or developers of high-risk AI systems.

Narrowing down the discussion of fairness to e.g. "fairness in pricing" for the purpose of comparing Union competition law with the notions of fair markets and equitable exchange in DMA, there exist a substantial body of economic research on the matter of fairness notions related to pricing which can guide and inform enforcement and legal certainty. In regard to law and economics, two major works have recently been published which summarize some of the main approaches in the normative.[84]

The issue of fairness as an object of laws regulating economic activity, such as competition law, has been the subject of fierce debate among law and economics scholars, where the contours of the debate have progressed along the asserted dichotomy between efficiency v justice as regards the object of competition law. Should competition law deliver "fair" outcomes, or should it be more concerned by protecting the competitive process, thereby ensuring a competitive market, where efficient outcomes are produced?

As noted by White: "The deeper problem with externalities from a Kantian point of view is that the economic analysis focuses on the harm imposed rather than the wrong done. Economics, based on brute utilitarianism, treats all harms the same and recommends any measures to make harms efficient. But not all harms are wrongful, and in fact some harms are protected by rights."[85]

---

[82] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market [2019] OJ L11/3, Preamble 1.

[83] European Commission, 'New Competition Tool Initiative', <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12416-Single-Market-new-complementary-tool-to-strengthen-competition-enforcement_en> accessed 15 November 2024.

[84] Erik O Cappelen and Bertil Tungodden, *The Economics of Fairness* (Edward Elgar Publishing, 2019); Lee Anne Fennell and Richard H McAdams (eds), *Fairness in Law and Economics* (Edward Elgar Publishing, 2013).

[85] Mark D White, 'With All Due Respect: A Kantian Approach to Economics' in Mark D White (ed), *The Oxford Handbook of Ethics and Economics* (Oxford University Press 2019).

This "Kantian" interpretation of the *ratio legis* behind excessive pricing prohibition in European competition law is reflected in the wording in the leading case of United Brands on unfair pricing,[86] where "unfair pricing" per Article 102a TFEU were defined as prices having "no reasonable relation to the economic value of the product."[87]

According to the seminal test developed in the case, the excess in turn could be determined objectively if it would be possible to calculate it through a comparison between the selling price of the product and its cost of production, which would disclose the "profit margin". Finally, the question to be determined would consist in answering the question if the disclosed difference is "either unfair in itself or when compared with competing products".[88]

If notions and preferences relating to fairness were only treated as externalities by "mainstream" economics which have influenced competition law to a great extent during the past decades, this approach would run the risk of being in direct conflict with the core *ratio legis* of a statute such as Article 102a TFEU.

Concluding on the matter of fairness in European competition law, as evident from the above, fairness is a core tenet of the European approach to regulating economic activity, although the issue of efficiency and the so-called more economic approach, inspired by the Welfarist and Chicago school of competition theory dominated the field for several decades.[89]

There is thus a solid body of case law relating to issues such a unfair pricing,[90] which helps clarify the study of fairness norms in the DMA, Data Act and AI Act, but also a body of legal acts exists that, in one way or another, elevates the matter of fairness, with particular emphasis and most importantly, on its connection to Union competition law.[91]

The next section moves on to discuss the interaction between intellectual property law and competition law, as much of digital, data and AI-driven markets are protected by various intellectual property rights, enabling the rightsholders to certain practices which might come in conflict with Union competition law.

The next section discusses the interaction between competition law and intellectual property law in general.

[86] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECLI:EU:C:1978:22, paras 250-253 regarding the test for excessive pricing.
[87] In turn defined in Case 26-75 *General Motors Continental NV v Commission of the European Communities* [1975] ECLI:EU:C:1975:150, para 12.
[88] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECLI:EU:C:1978:22. See paras 250-253 regarding the test for excessive pricing.
[89] Bartalevich (n 21).
[90] Behrang Kianzad, 'Are Excessive Pricing Cases Few and Far Between? A Quantitative Analysis of Fifty Years of European Jurisprudence 1971-2021' (2023) 3 *Concurrences*.
[91] See e.g. DMA point 10 in the preamble; EU Data Act point 32 in the preamble and EU AI Act point 45 in the preamble.

4 The interface between competition law and intellectual property law

As Intellectual Property Rights (the "IPRs") are legally granted monopolies, shielding the rightsholder from actual or potential competition during the protection period (in case of patents, 20 years, plus secondary protection certificates etc.), the rightsholder is able to set and enforce supra-competitive, monopolist prices, which might at first look be in conflict with the roots of competition law.

Some, such as Joseph Schumpeter, indeed posit this possibility of monopolist prices and probability of monopolistic profits as the main driver behind innovation, in turn driven by dynamic competition.[92]

When "costs" increase relative to "value", and when markets are protected by exclusive rights conferred through of patents, thereby shielding them from competitive pressure, there is manifest risk for abuse of dominant position, including the imposition of unfair pricing, although prohibited by per Article 102a TFEU as detailed in the previous section.

Since all forms of data are mainly protected by some form of intellectual property rights (such as patents, copyrights, trade secrets or other sui generis rights relating to data and databases), the interaction between this body of law - granting exclusivity by way of legal-monopolies- and competition law, which traditionally challenges exclusivity and monopolies, is worth exploring, and in fact, this interaction is clearly articulated in the EU Data Act.[93]

At least on the face of it, these bodies of laws do indeed seem to be in conflict. The delicate interaction between competition law and intellectual property law is probably most evident in innovative, high-risk sectors, such as the data-driven and digital sectors or the pharmaceutical sector.

On the matter of boundaries between IP law and competition law, the CJEU has accepted that an intellectual property right allows its proprietor to charge higher prices compared to non-protected goods.[94] However, the CJEU also has consistently affirmed there an upper limit for prices that can be set by a dominant undertaking.

As in every introductory course on intellectual property law, it is important to distinguish between the existence and the exercise of granted and protected rights. Competition law should therefore fulfil the necessary check-and-balances function in this public-private rights equation and balancing of interests. The impact of IPR protection on

[92] Richard Gilbert, 'Looking for Mr. Schumpeter: Where Are We in the Competition Innovation Debate?', in *Innovation Policy and the Economy, vol. 6* (MIT Press, 2006), 159–215; Jonathan B Baker, 'Beyond Schumpeter vs. Arrow: How Antitrust Fosters Innovation' (2007) 74 Antitrust Law Journal 575.

[93] See e.g. EU Data Act, Point 32 in Preamble, noting "Whether a connected product competes with the connected product from which the data originates depends on whether the two connected products are in competition on the same product market. This is to be determined on the basis of the established principles of Union competition law for defining the relevant product market".

[94] Case 24/67 *Parke, Davis and Co. v Probel, Reese, Beintema-Interpharm and Centrafarm* [1968] ECLI:EU:C:1968:1.

innovation is a highly complex matter dependant on a range of factors beyond the legal incentives.[95]

Crucially, as the ratio legis and economic justification for providing innovators with intellectual property protection entail the prospect of supra-competitive prices in order to recoup costly and risky investments. The resulting trade-off between innovation and access can be approached by way of competition law, acting as a moderating and equalising force and arbiter.

Although it has been re-affirmed by the CJEU in the Parke Davis case[96] that a difference in price emanating from its legally exclusive nature compared to other non-exclusive goods would be justified, there are however other metes and bounds applying to the use of those exclusive rights. The legal discourse on FRAND in regard to Standard Essential Patents is one such example.[97]

In short, actions that are perfectly legal under IP law can be deemed illegal in a competition law setting, as was the case in the seminal AstraZeneca case where AstraZeneca made use of its legal rights to deregister an established product and its marketing authorization, allegedly as a conscious strategy to delay generic entry.

As held by the Court, "...the illegality of abusive conduct under Article 82 EC (now article 102 TFEU, author remark) is unrelated to its compliance or non-compliance with other legal rules and, in the majority of cases, abuses of dominant positions consist of behaviour which is otherwise lawful under branches of law other than competition law."[98]

Hence, the distinction between existence and exercise of IPRs builds the basis of European law and jurisprudential approach to the interface between IPRs and Competition Law, where CJEU has, on numerous occasions,[99] reiterated that the exercise of IPRs and possible anti-competitive practices arising from such exercise is well within the ambit of European competition law. This view was developed in the *Consten & Grundig* case,[100] where the European Court of Justice elaborated on the distinction between the granting of IPRs and the exercise of the IPRs, and the court has consistently reaffirmed this position ever since.[101]

---

[95] Yi Qian, 'Do National Patent Laws Stimulate Domestic Innovation in a Global Patenting Environment? A Cross-Country Analysis of Pharmaceutical Patent Protection, 1978–2002' (2007) 89 Review of Economics and Statistics 436.

[96] Case 24-67 (n 94).

[97] Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee setting out the EU approach to Standards essential Patents, 29 November 2017, COM(2017) 712 final.

[98] C-457/10 P *AstraZeneca v Commission* [2012] ECLI:EU:C:2012:770, para 132.

[99] See e.g. Joined cases 56 and 58-64 *Établissements Consten S.à.R.L. and Grundig-Verkaufs-GmbH v Commission of the European Economic Community* [1966] ECLI:EU:C:1966:41; Case 78-70 *Deutsche Grammophon Gesellschaft mbH v Metro-SB-Großmärkte GmbH & Co. KG* [1971] ECLI:EU:C:1971:59; Case 24-67, *Parke, Davis and Co. v Probel, Reese, Beintema-Interpharm and Centrafarm* [1968] ECLI:EU:C:1968:11; Case C-372/19, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Weareone.World BVBA and Wecandance NV* [2020] ECLI:EU:C:2020:959.

[100] Joined cases 56 and 58-64 *Établissements Consten S.à.R.L. and Grundig-Verkaufs-GmbH v Commission of the European Economic Community* [1966] ECLI:EU:C:1966:41, see recital 10-11.

[101] Case 78-70 *Deutsche Grammophon Gesellschaft mbH v Metro-SB-Großmärkte GmbH & Co. KG* [1971] ECLI:EU:C:1971:59 ;Case 238/87 *AB Volvo v Erik Veng (UK) Ltd* [1988] ECLI:EU:C:1988:477; Case 40/70 *Sirena Srl v Eda Srl and others* [1988] ECLI:EU:C:1979:236; Case 24-67 *Parke, Davis and Co. v Probel, Reese, Beintema-Interpharm and Centrafarm* [1968] ECLI:EU:C:1968:11.

Other cases such as Magill[102] and Deutsche Grammophon[103] can also be read in that light. One might point to numerous cases at both the EU level[104] and on the Member State level that have dealt with abusive pricing issues related to intellectual property rights, albeit not innovative medicines as such, beyond the cited AstraZeneca and Servier cases, where the excessive price resulted from other practices.

Furthermore, the impact of competition law enforcement on innovation has been investigated to some extent, and has been demonstrated to be a positive, as noted by one the most comprehensive studies on the matter, which uses a unique firm-level dataset on patenting activities that includes over 1.2 million firm-year observations across 66 countries, from 1991 through 2015.

The study confirmed a strong connection between competition laws and firm innovation. More stringent competition laws were associated with sharp increases in firm innovation, as measured by the number of patents, forward citations to patents, citations per patent, the number of very highly cited patents, and the number of explorative patents. The results were stronger among firms that are less financially constrained, publicly listed firms, and non- family-controlled firms.[105]

As long-standing research[106] on the matter demonstrates, neither more protection, nor perfectly competitive markets, invariably lead to more innovation, but many other factors such as firm size, industry sector and overall innovation policy, also interact to a high degree.

In sum, a conceptual framework related to the anti-competitive exercise of IPRs has long been developed in European law and jurisprudence, making a distinction between the lawful existence and unlawful exercise of IPRs, where charging unfair (excessive) pricing is one of the anti-competitive abuses that might arise from the exercise of IPRs.

Hence, the settled case law[107] of CJEU makes it clear that EU competition law can be utilised against breaches of other bodies of laws, more importantly, intellectual property

[102] Joined cases C-241/91 P and C-242/91 P *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities* [1995] ECLI:EU:C:1995:98.

[103] Case 78-70 *Deutsche Grammophon Gesellschaft mbH v Metro-SB-Großmärkte GmbH & Co. KG* [1971] *ECLI:EU:C:1971:59* (n 121).

[104] Case 40-70 *Sirena S.r.l. v Eda S.r.l. and others* [1971] ECLI:EU:C:1971:18; Case 24-67, *Parke, Davis and Co. v Probel, Reese, Beintema-Interpharm and Centrafarm* [1968] ECLI:EU:C:1968:1; Case 238/87 *AB Volvo v Erik Veng (UK) Ltd* [1988] ECLI:EU:C:1988:477.

[105] Ross Levine and others, 'Competition Laws and Corporate Innovation' (National Bureau of Economic Research, 2020) w27253.

[106] Lawrence M Debrock, 'Market Structure, Innovation, and Optimal Patent Life' (1985) 28 The Journal of Law and Economics 223–44; William D Nordhaus, *Invention, Growth, and Welfare: A Theoretical Treatment of Technological Change* (The MIT Press 1969).

[107] See e.g. Case 24-67 *Parke, Davis and Co. v Probel, Reese, Beintema-Interpharm and Centrafarm* [1968] ECLI:EU:C:1968:11; C-457/10 P *AstraZeneca v Commission* [2012] ECLI:EU:C:2012:770, para 132; Joined cases 56 and 58-64 *Établissements Consten S.à.R.L. and Grundig-Verkaufs-GmbH v Commission of the European Economic Community* [1966] ECLI:EU:C:1966:41; Case C-372/19 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Weareone.World BVBA and Wecandance NV* [2020] ECLI:EU:C:2020:959.

law and exclusive rights, thus being applicable also on matters regulated by DMA; Data Act and the AI Act, where these acts indeed refer to Union competition law, also.[108]

The next section delves more deeply into comparing the *ex ante* approach to fairness in regulation of data-driven markets with the *ex post* approach of competition law.

5 The interaction between ex ante regulation and ex post competition law enforcement in digital markets

The above conceptual framework is also well-suited for the challenges posed by the data-driven markets and the abuse of dominant positions by those possessing massive amounts of data which gives them a competitive lead and, in many cases, an entrenched market position with high markets shares. This can at times come close to monopolistic situations when discussing certain tech giants and their services, as well as their unassailable lead over would-be competitors.

This matter has also been referred to as "network effects" and is one of the motivating factors behind the enactment of Digital Markets Act, the EU Data Act, the EU AI Act and so on. Network effects entail that the value of a product, service, or platform depends on the number of buyers, sellers, or users who leverage it.

Typically, the greater the number of buyers, sellers, or users, the greater the network effect—and the greater the value created by the offering.[109] This in turn leads to a "winner-takes-all" scenario that influence strategies, such as pricing and quality,[110] but also entrenches market power for those firms enjoying such network effects, further insulating them from competition, and competition law enforcement.

This matter becomes even more complex in the case of so-called data network effects, a concept that has emerged from advances in artificial intelligence and the growing availability of data, where a platform exhibits data network effects if, the more it learns from the data it collects on users, the more valuable the platform becomes to each user.[111]

One prime example in the literature is the case where Microsoft succeeded in making MS Office (spanning Word, Excel, and PowerPoint) the dominant suite of office productivity applications, encouraging users to standardize on MS Office for both business

[108] Digital Markets Act, Para 10.
[109] Tim Stobierski, 'What are Network effects?' (*Harvard Business School*, 12 November 2020) https://online.hbs.edu/blog/post/what-are-network-effects, accessed 2024-11-15.
[110] Rietveld J and Schilling MA, 'Platform Competition: A Systematic and Interdisciplinary Review of the Literature' (2021) 47(6) *Journal of Management* 1528 - 1563.
[111] Robert Wayne Gregory et al., 'The Role of Artificial Intelligence and Data Network Effects for Creating User Value' (2021) 46(3) *Academy of Management Review* 534.

and personal use. The direct network effects for these applications were based on easy file sharing across users.[112]

Another example concerns the increased use of algorithms and AI solutions in to product price monitoring and algorithmic price changes, where a bulk of previously human-made decisions are now increasingly automated, complicating the matter further. Such was the defence by Lufthansa when investigated by German *Bundeskartellamt* alleged unfair and excessive pricing[113] by Lufthansa on some selected routes following the exit of rival Air Berlin.

Lufthansa pointed in this case to the algorithm being the reason behind price increases as a result of changes in demand. Although the case eventually was dropped by the *Bundeskartellamt*, citing the speedy entry of other competitors (Easyjet) into the market and subsequent price reductions Lufthansa's defence is interesting to note in regard to the boundaries of human-made law in relation to unfair pricing when faced with non-human, algorithmic "unfairness" as perceived by the human eye and according to human notions of fairness.[114]

Finally, in the context of fairness, data and competition law, the Meta / Facebook case brought by German *Bundeskartellamt* in 2019 and decided on as a preliminary ruling[115] by Court of Justice of European Union in 2021 is a seminal one which was recently concluded with Meta offering necessary commitments.

In February 2019 the *Bundeskartellamt* prohibited Meta (formerly Facebook) from combining personal user data from different sources without user consent. Meta appealed this decision. Over the years of legal proceedings, in which the Federal Court of Justice (2020) and the Court of Justice of the European Union (2023) confirmed the *Bundeskartellamt's* position on matters of principle, Meta and the Bundeskartellamt also intensively negotiated concrete measures to implement the authority's decision.

The CJEU ruled (Case C-21/23) that a competitor not classified as a "data subject" under the GDPR can enforce GDPR compliance through national competition rules. This case involved a German pharmacy owner marketing medicinal products on Amazon, requiring customer data entry. A competitor claimed this violated German unfair competition laws, arguing the lack of customer consent for processing health data constituted an unfair practice affecting market players and consumers.

---

[112] Catherine Tucker, 'What Have We Learned In the Last Decade? Network Effects and Market Power' (*The Global Antitrust Institute*, Spring 2018) <https://gai.gmu.edu/wp-content/uploads/sites/27/2021/05/Session-13_Tucker-Network-Effects.pdf> accessed 15 November 2024.

[113] Imposing so-called "unfair pricing" by a dominant undertaking (holding 40% or more of market shares in the relevant market) is prohibited by Union competition law per article 102a TFEU. See Kianzad (n 92).

[114] See Bundeskartellamt and Autorité de la concurrence, 'Algorithms and Competition' (November 2019) < https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=5> accessed 20 August 2020.

[115] Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537. It was held that GDPR concerns can indeed be pursued by competition law, a ruling which will have immense practical implication for abuses of DMA, Data Act and AI Act.

The CJEU found this consistent with the GDPR, allowing Member States to enable competitors to seek injunctions against GDPR breaches. It acknowledged such actions might not stem from data protection concerns but aim to ensure fair competition. The court emphasized personal data's role in digital economy competition and noted competitors' actions could strengthen GDPR compliance and safeguard data protection effectively.

Meta's individual measures are now deemed to be a sufficiently effective package allowing the *Bundeskartellamt* to close the case. Meta has withdrawn the appeal pending before the Düsseldorf Higher Regional Court (OLG Düsseldorf) against the *Bundeskartellamt's* decision. The decision is thus final.[116]

Although there is a clear presumption of the possibility of abuse with such market power, it must be observed that for example monopoly pricing of goods and services in the context of network effects at times can sometimes lead to lower markups, which can be even zero or negative in multi-sided markets. This context necessitates a somewhat different analysis than the traditional focus on, for instance SSNIP-based market power, particularly in the case of zero price products and services.[117]

The pre-supposed pre-occupation of sector regulator further targets all market players in the sector, whilst competition law is more concerned with market power and dominance as such, thereby being less intrusive and all-encompassing as opposed to sector regulator which is a per se intrusion upon market dynamics.

A cooperation between competition authority and sector regulator would further cure many of the deficiencies pointed out by the those opposing an interventionist role of competition authorities regarding finding of proper benchmarks. Furthermore, as competition rules are part of the TFEU, they have superiority to sector regulation rules and as such can be invoked to cure deficiencies.[118]

Some commentators have maintained that the presence of a sector regulator would rebut competition law enforcement against alleged anti-competitive practices, such as unfair pricing. Looking at the settled jurisprudence and types of cases, there is support to the contrary, affirming the position that the existence of a sector (price) regulator does not preclude ex post competition law enforcement.

---

[116] Bundeskartellamt, 'Facebook Proceeding Concluded' (10 October 2024) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html> accessed 15 November 2024.

[117] Emilio Calvano and Michele Polo, 'Market Power, Competition and Innovation in Digital Markets: A Survey' (2021) 54 Information Economics and Policy 100853.

[118] OECD, 'Excessive Prices' (2011) Background Paper, para. 120, DAF/COMP/W2(2011)7; European Commission, Commission Notice on the Application of Competition Rules to Access Agreements in the Telecommunications Sector (98/C 265/02) *OJ C 265, 22.8.1998, p. 2-28*.

The legal position is evident from settled jurisprudence in Telekom,[119] Airport[120] and Energy[121] sectors, where despite being heavily regulated sectors, they still observed a non-trivial number of excessive pricing cases, where the price level set by the sector regulator could be invoked as a benchmark in the assessment.[122]

Many times the sector regulator has been unable to address the anti-competitive practices of unfair pricing, as evident from the string of excessive pharmaceutical pricing cases.[123] The aim of Digital Markets Act, the EU AI Act and the EU Data Act are in turn to curb deficiencies and shortcomings on part of Union competition law which is said not have been able to come to terms with the issues targeted by those aforementioned legal acts pertaining to digital, data and AI markets.

The interaction between sector regulation and competition law will thus be in the forefront regarding the application of said legal acts, as many cases might present themselves in the interface between these bodies of law and regulation.

6 Conclusions

Much of the ongoing research[124] elevating "fairness" related to data, digital markets and, most importantly, Artificial Intelligence, targets non-discrimination, ethics and bias. However, little work has been done on the matter of fairness as a competition law and regulatory concept applied to digital, data-driven and AI markets. This is unsatisfactory, since the recent legal acts elevate fairness to a great extent, while referring to norms and principles derived from and developed in EU competition law.

As EU competition law itself has long entertained contentious debates on whether fairness could and should act as a goal and concept for laws governing economic activity, among them competition law, it becomes even more important to have a clear discussion on whether the "fairness" norm elevated in legal acts such as DMA, EU Data Act and EU AI Act sustains the same understanding of "fairness" as within EU competition law, not least since there are multiple references in those legal acts to Union competition law.

EU competition law indeed includes rules prohibiting for example "unfair pricing", supported by settled case law and various doctrinal approaches, however it is apparent that the fairness dimensions in the aforementioned legal acts do not entirely mirror those

[119] Case C-280/08 P *Deutsche Telekom AG v European Commission* [2010] ECLI:EU:C:2010:603.
[120] Michele Giannino, 'Enforcement of Excessive Price Competition Provisions in the Airport Sector' (2012) SSRN Electronic Journal.
[121] Case AT.39816 –*Upstream gas supplies in Central and Eastern Europe (Gazprom)* - Final Committment Decision, 24/05/2018.
[122] See Commission Decision of 15 November 2011 in Case COMP/39.592 - *Standard & Poor's*, C (2011) 8209 final, para 26; referring further to Case C-66/86 *Ahmed Saeed*, paragraph 43; see also Case 30/87, Corinne Bodson, para 31.
[123] Behrang Kianzad and Timo Minssen, 'How Much Is Too Much? Defining the Metes and Bounds of Excessive Pricing in the Pharmaceutical Sector' (2018) 2(3) *European Pharmaceutical Law Review* 133 – 148.
[124] Anna Jobin, Marcello Ienca, and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1(9) Nature Machine Intelligence 389.

found in competition law, as per literal wording in acts such as DMA which note that DMA is enacted to curb deficiencies not being able to be curbed by Union competition law.[125]

As noted by one critique offered by Wolfgang Kerber "the objectives of the DMA (contestability, fairness) differ from the competition objective of Articles 101 and 102 TFEU, and any investigations and assessments have to refer to the still not sufficiently clarified objectives of contestability and fairness, i.e., consumer welfare might not be the sole and decisive criterion anymore".[126]

Nevertheless, it can be claimed that the concept of unfairness in competition law, e.g. when talking about "unfair pricing", has a rather solid "conceptual basis" in both law and economics, as the matter of unfair pricing has laid the groundwork of Nobel Prize in Economics, following the work of Kahneman et alia.[127] who demonstrated that people hold strong fairness in transaction preferences. People are willing to forgo increases in utility if they perceive a transaction as unfair, or when they are faced with manifest price increases without objective reasons such as an increase in the costs of supplying the product.[128]

As aptly summarized by Klaus Mathis "In people's minds, justice – however it is defined – has an immanent value, which is very difficult to weigh up against an increase in economic efficiency."[129] Fairness becomes relevant in these contexts simply because the core analytical structure of neoclassical and welfarist theories of harm do not neatly encompass the law and economics of digital and AI markets, nor the traditional political economy focus on "equitable exchange", which came to build the foundation of laws governing market activity and exploitation.[130]

The marginalist and welfarist approach to competition law and economics is not fully suited to come to terms with the observed phenomena of the unassailable competitive lead gained through access to Big Data, Network effects and the ability to invest in costly AI systems which in turn build upon the treasure-trove of Big Data in the hands of few Big Tech corporations.

---

[125] Digital Markets Act, point 5, preamble, noting "It follows that the market processes are often incapable of ensuring fair economic outcomes with regard to core platform services. Although Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) apply to the conduct of gatekeepers, the scope of those provisions is limited to certain instances of market power, for example dominance on specific markets and of anti-competitive behavior, and enforcement occurs ex post and requires an extensive investigation of often very complex facts on a case by case basis. Moreover, existing Union law does not address, or does not address effectively, the challenges to the effective functioning of the internal market posed by the conduct of gatekeepers that are not necessarily dominant in competition-law terms".

[126] Wolfgang Kerber, 'Taming Tech Giants with a Per Se Rules Approach? The Digital Markets Act from the "Rules vs. Standard" Perspective' (2021) 3 Concurrences 28.

[127] Daniel Kahneman, Jack L Knetsch and Richard H Thaler, 'Fairness and the Assumptions of Economics' (1986) 59(4) The Journal of Business S285-S300.

[128] Robert Piron and Luis Fernandez, 'Are Fairness Constraints on Profit-Seeking Important?' (1995) 16(1) Journal of Economic Psychology 73–96.

[129] Klaus Mathis, *Efficiency Instead of Justice?* (Springer, 2009) 48.

[130] von Nell-Breuning (n 73).

In this context the recently introduced ex ante regulatory approaches such as EU AI act, EU Data act as well as Digital Markets act, all elevate "fairness" and "fair processes" in various forms, ranging from safety in AI systems, to disclosure of data, non-discrimination and various ethical aspects of AI and the use of Big Data.
Thus, when DMA notes that "for the purpose of this Regulation, unfairness should relate to an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage",[131] then it is possible to argue that this is the same Aristotelian norm regarding equality in exchange, that in turn built the basis for "just price" and later, the prohibition against "unfair pricing".

The recent approaches by behavioural economics also contribute to our understanding of human bias towards fairness and aversion towards unfairness, especially regarding transactions and pricing. The works of Kahneman, Knetch and Thaler,[132] Piron and Fernandez,[133] Fehr and Schmidt,[134] Varian,[135] Ulen,[136] Sunstein and Jolls[137] et alia. in combination with research on neuro-economics experiments[138] further contributes to the normative understanding when trying to make sense of what role fairness should and could play in the law and economic analysis of allegedly "unfair behaviour" or "unfair prices".

Adding to this normative conundrum, the practical applicability of many competition law concepts and benchmarks such as dominance, definition of relevant market, differential pricing, MFN-clauses, unfair pricing and so on merit further exploration in the case of multisided-platforms due to their dual character.

However, less attention has been focused on the emergence of AI as a practical challenge for competition law enforcement when dealing with for example, instances of algorithmic price collusion, refusal to license data by a dominant undertaking and price gouging / excessive pricing resulting from AI information sharing and collusive behaviour.

A string of recent cases[139] nevertheless, demonstrates the legislative appetite for bringing such cases, enabled by *ex ante* regulatory approaches. As evident from the

[131] Digital Markets Act, Point 33, preamble.
[132] Kahneman, Knetsch and Thaler (n 27).
[133] Robert Piron and Luis Fernandez, 'Are Fairness Constraints on Profit-Seeking Important?' (1995) 16 Journal of Economic Psychology 73.
[134] Fehr and Schmidt (n 28).
[135] Hal R Varian, 'Distributive Justice, Welfare Economics, and the Theory of Fairness' (1975) 4 Philosophy & Public Affairs 223.
[136] Thomas S Ulen, 'Law and Economics, the Moral Limits of the Market, and Threshold Deontology' in Aristides N Hatzis and Nicholas Mercuro (eds), *Law and Economics: Philosophical issues and fundamental questions* (1st edn, Routledge 2015).
[137] Cass R Sunstein, Richard H Thaler and Christine Jolls, 'A Behavioural Approach to Law and Economics' (1998) 50 Stanford Law Review 1471.
[138] A W Cappelen et al., 'Equity Theory and Fair Inequality: A Neuroeconomic Study' (2014) 111(43) *Proceedings of the National Academy of Sciences* 15368 - 15372; Mario F Mendez, 'The Neurobiology of Moral Behavior: Review and Neuropsychiatric Implications' (2009) 14(11) *CNS Spectrums* 608 - 620; M Hsu, C Anen and SR Quartz, 'The Right and the Good: Distributive Justice and Neural Encoding of Equity and Efficiency' (2008) 320 Science 1092.
[139] See e.g. US District Court for the Middle District of North Carolina, RealPage, Case No. 1:24- cv-00710, Complaint, 23 August 2024; DC Court of Appeals, Amazon, Case No.22-CV-0657, Opinion, 22 August 2024; Case T-334/19 *Google and Alphabet v Commission (Google AdSense for Search)* [2024] ECLI:EU:T:2024:634.

section on law and economics approaches to fairness, the concept of fairness and its practical application in law and economics is not without challenges in overcoming the inherent "subjective" elements entailed in fairness considerations.

Focusing on the practical issue of "unfair pricing" as an anti-competitive practice under EU competition law – one that most readily lends itself for comparison with the type of "unfair behaviour" that legal acts such as DMA, EU Data Act and EU AI act aim to combat- would be a practical approach to devise a clear, objective and practical framework to enforce and implement the fairness norms in these legal acts. Fairness can indeed act as an objective and operational concept in both law and economics of laws governing economic activity, such as the Digital Markets Act, Data Act and AI Act, provided that the enabling conditions for defining what constitutes fair / unfair are clearly established.
As noted by Gerard, "instead of weakening legal certainty, the candid exposure of the fairness rationale underlying competition principles…might increase the predictability of individual assessment by shedding light of some of the variables capable of affecting outcomes".[140] Since EU competition law, which the aforementioned acts seem to be inspired by, and also refer to, entails concepts such as "unfair pricing" with long-established case law and doctrinal development, it would be advisable to analogously interpret the fairness dimension in the these legal acts in light of such competition law rules, particularly on unfair pricing.

[140] Damien Gerard, 'Fairness in EU Competition Policy: Significance and Implications' (2018) 9 Journal of European Competition Law & Practice 211.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 4 - 1/2025