A Single European Data Space and Data Act for the Digital Single Market: on Datafication and the Viability of a PSD2-like Access Regime for the Platform Economy

Federico Ferretti*

In its new digital strategy for Europe, the EU highlights the need for better data-access and sharing. In line with this priority, it is working on a proposal for a Data Act that aims to provide the underlying legal framework. This paper seeks to disentangle key legal concepts and issues related to datafication that affect the envisaged European Data Space. It reveals that the EU already has a suitable regulatory model under the Payment Services Directive 2 ('PSD2'). The strategy focuses on market imbalances of the platform economy and challenges the legitimacy of large technological companies ('Big-Techs'). The latter act as gatekeepers to maintain a key role in data-access and monetise their data dominance. The paper casts into question the existence of a data market, suggesting that the EU already has a viable legislative model provided by the 'PSD2' sectoral legislation. Its data-access model could be applied horizontally across data-driven markets and the platform economy without engineering new rules or adding regulatory layers.

Keywords: Digital Single Market; Data Act; data; data rights and control; data access; data sharing; platform economy; PSD2

* Associate Professor of Law, Alma Mater Studiorum University of Bologna; Director of the Jean Monnet Centre of Excellence 'Consumers and SMEs in the Digital Single Market (Digi-ConSME)'; Jean Monnet Chair of EU Digital Market Law (E-DSM). Co-funded by the Erasmus+ Programme of the European Union. The author is grateful to the three anonymous reviewers for their insightful and helpful comments. The usual disclaimer applies.

TABLE OF CONTENTS

I. INTRODUCTION

The EU strives to attain a leading role in the data economy by exploiting an expanding amount of data to create innovative products and services in the Single Market. It views digitalisation as a tool for relaunching economic growth and social welfare.

This paper focuses on the key issue of data-access and sharing in the current market imbalances of the platform economy, where dominant undertakings act as gatekeepers. First, it explores the limits of existing EU laws addressing different aspects of data-access and sharing such as proprietary rights, data protection and competition that prevent the creation of a genuine market for data-driven products and services. Next, it investigates the extent to which the objectives set forth by proposed EU legislation can be met through the model of cognate regulatory instruments like the one governing the payment sector. Ultimately, this study claims that the latter provides a feasible regulatory model capable of creating the envisaged market in conjunction with current data laws. This model could be replicated for the entire digital market.

As part of the Digital Single Market Strategy,[1] the European Commission's latest policy goal is to create a single European Data Space, conceived as a 'genuine single market for data (…) where personal as well as non-personal data (…) are secure and businesses also have easy access to an almost infinite amount of high-quality data'.[2]

The digital expansion has placed data at the centre of major economic and social transformations. To the extent that data are the lifeblood of innovation, they have become an essential resource in economic terms. Data are no longer seen as mere outputs generated by the use of technology.

---

1 Commission, 'A Digital Single Market Strategy for Europe' (Communication) COM (2015) 192 final.

2 Commission, 'A European strategy for data' (Communication) COM (2020) 66 final.

Instead, they are increasingly regarded as inputs for the creation or improvement of products and services such as information services, processes, or decision-making tools.[3]

To achieve its policy objectives, the EU has committed to combining fit-for-purpose cross-sectoral (horizontal) legislation and governance to ensure the free flow, access and sharing of data within the Union.[4] The legislation will integrate existing data laws such as the GDPR[5] and few others[6] to support the viability and sustainability of an alternative model for the data economy that is at once open yet fair, transparent, and accountable.[7] In addition to furnishing a legislative framework for the governance of a common data space and the reuse of public sector data, data sharing among market players has a preeminent role to be achieved by means of a Data Act.[8] Two major problems for the achievement of policy goals are the intense

---

3 Ikujiro Nonaka, 'A Dynamic Theory of Organizational Knowledge Creation' (1994) 5 Organization Science 14; Francesco Mezzanotte, 'Access to Data: the Role of Consent and the Licensing Scheme' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 159.

4 Commission, 'A European strategy for data' (n 2).

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR).

6 See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56.

7 European Data Protection Supervisor, 'Opinion 3/2020 on the European Strategy for Data' (16 June 2020) <https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf>.

8 Commission, 'A European strategy for data' (n 2).

concentration of data in the hands of limited large online platforms (also known as 'Big-Techs') and market imbalances in the access and (re)use of data.[9] Big-Techs raise a number of different problems, some of which have already been addressed in legislative proposals.[10] Of concern here is that they are large multinational corporations that dominate the digital business. Within such a vast industry, Big-Techs dominate their respective niche market using the data to expand subsequently into other markets. Big-Techs may have very different business models, levels of maturity and financialisation, or corporate governance. They share in common the capacity to act as intermediary infrastructure and become gatekeepers of the indispensable facility represented by the data. They also become market gatekeepers in this way.[11] Their models build on creating, maximising, and monetising network effects and economies of scale to dominate the market, reduce competition and consumer welfare, and stifle innovation driven by others. Due to their distinctive features, Big-Techs have given rise to the so-called 'platform economy' which, overall, enjoys largely unchecked power in a regulatory vacuum.[12]

---

9 Ibid.

10 See e.g. Commission 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM (2020) 842 final, which proposes new ex-ante rules for gatekeeper platforms as well as a new supervisory framework at EU level to address conduct and competition harm risks.

11 The European Commission defines a gatekeepers as 'a provider of core platform services', where core platform services are any online intermediation services, online search engines, online social networking services; video-sharing platform services; number-independent interpersonal communication services; operating systems; cloud computing services; advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services. See ibid art 2.

12 Anne Helmond, 'The Platformization of the Web: Making Web Data Platform Ready' (2015) 1 Social Media + Society 1; Rodrigo Fernandez and others, *The Financialisation of Big Tech* (SOMO 2020).

This paper disentangles key legal aspects of datafication in the policy and market context discussed above that impact the envisaged European Data Space and a prospective data-access regime under the Data Act. These aspects include proprietary data rights, data protection and competition law. Particular attention is granted to the market imbalances in the platform economy created by Big-Techs and the extent to which such organisations should be allowed to monetise data acting as gatekeepers. This analysis ultimately suggests that the objectives of the proposed EU Data Act are already met by the model of cognate regulatory instruments governing the payments sector. The model could be applied horizontally as a norm of general application for all data without adding regulatory layers to current standards.

The study employs a doctrinal approach, analysis, and analogy to sustain its claims. Its contribution to the literature is to propose the extension of an existing regulatory framework for the novel purpose of data-access and sharing in the digital single market as a whole.

Section 2 explores the concept of data and their features to identify the extent and reach of data ownership or control rights and how these influence the idea of a 'single market for data'.[13] The analysis of the existence of a single market for data-driven products and services, rather than a 'data market', serves to highlight the relationship among players in the digital market. In turn, market characteristics shape the horizontal data-access regime needed for a Data Act that could correct the problems created by the imbalances of the platform economy. Section 3 demonstrates the limits of competition law enforcement to offer solutions for the creation of a genuine market for data-driven products and services. Designing an adequate data-access regime for the European data strategy and Data Act requires an understanding of the inherent limitations of available legal tools. The essential question is what form the Data Act should take. This is examined in Section 4, which studies

[13] As framed by Commission, 'A European strategy for data' (n 2).

the sectoral EU legislation on payment services to explore its viability as a model of horizontal general application for the entire digital market.

The EU does not have to reinvent any measures, nor would it need to engineer new rules.

II. The Limits of Competition Law Enforcement: A Single Market for Data-Driven Products and Services, Not a Single market for Data

The strategy for creating a single European Data Space presupposes maximum data availability. These are considered an essential component—or raw material—for the development of a competitive digital market, especially in terms of data-access and (re)usability. The policy vision and debate centre around the creation of a 'single market for data' and the rebalancing of market power in relation to data-access and sharing.[14]

Inevitably, the idea of a 'data market' prompts questions about its nature and reintroduces the long-debated issue of data ownership or titles to data, i.e. the extent of exclusive right to use, exploit, and disclose data, subject only to the rights of persons with a superior interest or legal or contractual restrictions.

One fundamental reservation is the extent to which recognition of a title in rem to data, and therefore the resultant market type, can be justified. Claims to proprietary rights are linked to commercial exploitation and the delineation of the market. Simply put, the allocation of a title in rem to data, in whatever form this may be recognised, would give rise to important consequences. These lead in turn to the question of how to strike a balance between the rights, obligations, and limits of those claiming title and a general interest in access to - and reuse of - data for the innovation and development of the digital market.

---

14 Ibid.

Moreover, if rights in rem are recognised and allocated, they must have limits and exceptions that serve the public interest.[15]

Therefore, defining the nature of data is key to informing public policy and establishing the legal basis for claims of title, including the very existence of a 'data market'.[16] It is also instrumental in defining the boundaries of the public interest in access to, and (re)usability of, data as an essential resource.[17]

As previous scholarship suggests, delineating the concept of data and their economic properties is a challenging exercise.[18] Yet it is a necessary one if data are to be treated as a commodity in the market.

1. The Nature of Data

The first difficulty is one of terminology and derives from the misleading interchangeability, in everyday jargon, of terms like 'data' and 'information'. However, the distinction between the two matters for policy and legal discourse. In information science, data is conceptualised in two ways: as signals, i.e. unprocessed reinterpretable digital representations, and as measurable and discrete observations of facts or acts in a formalised manner (such that there is a clear separation between the different possible values). However they are conceptualised, data must be suitable for communication,

---

15 Also argued by Teresa Scassa, 'Data Ownership' (2018) CIGI Paper No 187 <https://www.cigionline.org/publications/data-ownership/#:~:text=Teresa%20Scassa%20is%20a%20CIGI,of%20data%20ownership%20and%20control> accessed 10 June 2022.

16 See also Vincenzo Zeno-Zencovich, 'Do "Data Markets" Exist?' (2019) 2 Media Laws 22.

17 Josef Drexl, 'Data Access and Control in the Era of Connected Devices' (BEUC, The European Consumer Organisation, 15 January 2019) <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 12 April 2021.

18 See e.g. Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (2017) JRC Digital Economy Working Paper 2017-01 <https://joint-research-centre.ec.europa.eu/system/files/2017-03/jrc104756.pdf> accessed 10 June 2022.

interpretation or processing.[19] The definition of data is often supplemented with the requirement that signals be readable, generated or observable by a machine.[20] Data are often viewed as a by-product of other activities.[21] Yet they are also a resource in their own right when converted into information - that is the number of discernible signals or data points necessary to transmit a message.[22]

Other characterisations distinguish between a syntactic level (signs and their relationship with each other) and a semantic level (the meaning of data), which leads to a distinction between the content and code layers.[23] Information is instead a broader concept than data that depends on context and usage to convey meaning.

In the end, data are most appropriately defined in relation to the other parameters in their lifecycle, which can be illustrated in sequential order: data

---

19 Russel Ackoff defines data as 'symbols that represent the properties of objects and events. Information consists of processed data, the processing directed at increasing its usefulness'. 'From Data to Wisdom' in Russel Ackoff (ed), *Ackoff's Best* (John Wiley and Sons 1999) 170. See also Chaim Zins, 'Conceptual Approaches for Defining Data, Information, and Knowledge' (2007) 58 Journal of the Association for Information Science and Technology 479; Commission, 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final; Commission, 'Proposal for a Regulation on European data governance (Data Governance Act)' COM (2020) 767 final, art 2(1).

20 Herbert Zech, 'Data as a Tradable Commodity' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market* (Intersentia 2017) 51.

21 Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) 65 Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int) 989.

22 Max Boisot and Agustì Canals, 'Data, Information and Knowledge: Have We Got It Right?' (2004) 14 Journal of Evolutionary Economics 43; Ronaldo Vigo, 'Complexity over Uncertainty in Generalized Representational Information Theory (GRIT): A Structure-Sensitive General Theory of Information' (2013) 4 Information 1. See also Robert M Losee, 'A Discipline Independent Definition of Information' (1997) 48 Journal of the American Society for Information Science 254.

23 Zech (n 20).

(any representation of something in digital form) are the raw material for information, information (structured data with a discernible meaning) is the raw material for knowledge, and knowledge (information whose validity has been established through tests of proof or intellectual virtue) is the raw material for wisdom (the ability to use knowledge to achieve and establish desired goals).[24]

This multichotomy implies a linear flow and hierarchy that do not remain on a purely theoretical level but have important economic and legal consequences.

2. The Data Value Chain

From an economic perspective, data represent a primary material. A sequential process of transformation adds value to the data, especially when combined with the resourcefulness, capability and experience of the agents who utilise the outcomes at each stage.[25] This is the value extraction process. The extensive availability of large volumes of diverse datasets from various unrelated sources (big data) is decisive to extracting maximum value.[26] The

---

24 Paul Bierly, Eric Kessler and Edward Christensen, 'Organisational Learning, Knowledge and Wisdom' (2000) 13 Journal of Organisational Change Management 595; Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access' (2000) 52 Federal Communications Law Journal 561. According to Rob Kitchin, data are not neutral. They reflect choices about which data to collect or exclude and cannot exist independently of the ideas, instruments, practices, contexts and knowledges used to generate, process and analyse them. *The Data Revolution: Big Data, Open Data, Data Infrastructure and their Consequences* (Sage 2014) 1.

25 Antti Aine, Tom Bjorkroth and Aki Koponen, 'Horizontal Information Exchange and Innovation in the Platform Economy – A Need to Rethink?' (2019) 15 European Competition Journal 347.

26 Kitchin (n 24).

value of data grows progressively through the information, knowledge and wisdom conveyed by the data on the semantic level.[27]

In practical terms, the value chain distinguishes between data production, processing, collection, organisation and analysis and the achievement of set goals, including innovations based on the insights gained in the previous steps. As a raw material, data are an infinite resource generated at an insignificant cost. Moreover, they are immaterial and non-consumable (non-rival), which means usage does not exhaust the supply and they may be used simultaneously by more than one agent. These features are a novelty in economic theory, which considers limited or restricted resources, as well as production costs.[28]

Consequently, the economic value of data in their essential form is trivial and irrelevant.[29]

The paradox of the debate over titles to data is precisely that where there is no value, one would conclude that ownership or other rights of economic exploitation are not an issue. This deduction is reinforced by the unique nature of data as limitless and non-rivalrous, which fits uneasily with the

---

27 Zech (n 20); Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17).

28 Jean-Sylvestre Bergé, Stephane Grumbach and Vincenzo Zeno-Zenchovic, 'The "Datasphere", Data Flows beyond Control, and the Challenges for Law and Governance' (2018) 5 European Journal of Comparative Law 144.

29 See Commission, 'Decision of 27.6.2017 relating to the proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 – Google Search (Shopping))' C (2017) 4444 final (Google Search case). See also Edouard Bruc, 'Data as an Essential Facility in European Law: How to Define the "Target" Market and Divert the Data Pipeline?' (2019) 15 European Competition Journal 177.

legal concept of a title in rem. As in the case of ideas, these features are the foundations for the classification of data as public goods.[30]

If property rights are difficult to extend to data, this, in turn, creates challenges in establishing usage rights.[31] Instead, the issue arises as soon as value is provided, i.e. at the later stage when data provide information, knowledge and wisdom.

Another complication that surfaces is the contribution of multiple actors to the datafication process and the relationship between them. Different persons (natural and/or legal) may contribute to generating data through human activities or technologies (e.g. data created or observed by a sensor, search engine, or website), or may add value during the processing, observation, aggregation, storage, selection, verification and analysis stages. Data can be directly generated by the person or by that person's use of services.[32] Value may also reside in the immediacy and instant availability of data.[33]

---

30 Harold Demsetz, 'Toward a Theory of Property Rights' (1967) 57 The American Economic Review 347; Priscilla Regan, 'Privacy as a Common Good in the Digital World' (2010) 5 Information, Communication and Society 382. See also Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17), which also makes reference to constitutional principles of freedom of information and the EU Charter of Fundamental Rights (Article 11(1)).

31 Some scholarship, forcing the established economic and legal notion of property, debates whether its concept should be flexible enough to extend to new immaterial goods and eventually allow the commodification of data. See Nadezhda Purtova, 'The Illusion of Personal Data as No One's Property' (2015) 7 Law, Innovation and Technology 83; Alberto De Franceschi and Michael Lehmann, 'Data as Tradable Commodity and New Measures for their Protection' (2015) 1 Italian Law Journal 51.

32 Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 World Competition 473; Josef Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' (2018) Max Planck Institute for Innovation & Competition Research Paper No 18-23 <https://ssrn.com/abstract=3274519> accessed 12 April 2021.

33 Duch-Brown, Martens and Mueller-Langer (n 18).

From this perspective, the distinction between personal and non-personal data—which has thus far remained indistinct—assumes relevance. Data may be non-personal or personal in nature, where the latter are broadly defined in relation to an identified or identifiable natural person.[34]

Natural persons would intuitively assert that they own data about themselves, as these comprise personal attributes. However, individuals do not own information about themselves. Personal data do not pre-exist prior to their expression or disclosure. They are always to some extent constructed or created by more than one agent.[35] They pertain to a person yet do not belong in a proprietary sense to him/her. Those who process personal data (data controllers) have the right to process data pertaining to data subjects as long as such processing is lawful, i.e. they abide by procedural rules established by law (in the EU, the GDPR - infra) with the objective of protecting individual citizens not against data processing per se but against unjustified collection, storage, use and dissemination of the data pertaining to them.[36] Moreover, personal data may be turned into anonymous data, but

---

34 Descriptive definition based on GDPR, art 4(1). See also the earlier Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (European Commission, 20 June 2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 12 April 2022.

35 Federico Ferretti, *Competition, the Consumer Interest, and Data Protection* (Springer 2014). See also Annette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).

36 E.g. individuals do not own their criminal records or credit history. Ferretti, *Competition, the Consumer Interest, and Data Protection* (n 35). See also the discussions about individuals not owning information about themselves in Jerry Kang and Benedikt Bunter, 'Privacy in Atlantis' (2004) 18 Harvard Journal of Law and Technology 230; Rouvroy and Poullet (n 35).

they are still data (of a non-personal nature) that remain in existence without allocation to data subjects.[37]

In the end, the value chain and the role of different stakeholders are crucial from the legal perspective. Each transformation, creation of value, and interaction of different subjects at different levels epitomises a separate legal construction and allocation of rights. For this reason, it is crucial to determine whether and at what stage data may become a commodity giving rise to transferable rights, and whether legal protections should intervene.[38]

3. Data-related Rights

The value chain determines when legal rights should be allocated, who is entitled to claim a title over the data, and how to exercise such rights.

The fluid nature of data and their unsuitability to being defined and regulated in the same way as other tangible or intangible goods has generated debates about the potential creation of a new right in rem specific to data.[39] Under existing laws, however, no data property right can exist. Nor do there seem to be legal grounds for recognising rights of economic

---

37 Gintare Surblyte, 'Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy' (2016) 65 Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int) 1121.

38 Barbara Evans, 'Much Ado About Data Ownership' (2011) 25 Harvard Journal of Law and Technology 70; Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data – A Revolution that Will Transform How We Live, Work and Think* (John Murray 2013).

39 For all, see Zech (n 20).

exploitation over data per se.[40] Likewise, no EU jurisprudence satisfactorily deals with the matter.[41]

Instead, rights over data usability and allocation can be constructed as a bundle of other rights. These originate from a patchwork of existing laws, protecting other goods or values, that affect interested parties in data use without allocating property rights. Not surprisingly, these rights shift from a sales or transfer paradigm to a licence model based on access.[42]

Access requires a subject to hold the data, which presupposes control. In the debate over data accessibility, the point is to define the precise extent of control rights and entitlements, as well as the legal mechanisms to deal with access restrictions in a framework that does not presuppose a comprehensive data regime.

---

40 Zech (n 20); Mezzanotte (n 3); Sjef van Erp, 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects' (2017) Maastricht European Private Law Institute Working Paper No 2017/6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046402> accessed 12 April 2021; Francesco Banterle, 'Data Ownership in the Data Economy: A European Dilemma' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era* (Springer 2020) 199.

41 See Ivan Stepanov, 'Introducing a Property Right Over Data in the EU: The Data Producer's Right – An Evaluation' (2020) 34 International Review of Law, Computers & Technology 65. According to the author, however, although no property rights as such over data exist, when faced with gaps some national Courts seem to adapt and in certain aspects treat data as property offering points of divergence. German Courts ruled on the proprietary aspects of data on matters of mishandling by company employees, albeit in criminal and labour law cases. The Courts concluded that for the purposes of those fields of law, data can be owned, thus exhibiting traits associated with property. In the Netherlands, the Supreme Court stated that from the perspective of criminal law data could be the object of theft. Finally, Luxembourgian law gives the right to reclaim ownership in data from the cloud in bankruptcy proceedings if the circumstances provide for such an opportunity. Ibid 73-74.

42 Aaron Perzanowski and Jason Schultz, *The End of Ownership. Personal Property in the Digital Economy* (MIT Press 2016).

The assortment of laws that assign rights and obligations over data are discussed below.

A. Intellectual Property Laws

Intellectual property is the traditional form of protection of intangible assets. Its normative frameworks, including related rights, are often used to provide some form of protection for rights over data.

-*Copyright Law*

Copyright protects the original expression of ideas or facts, but there is no protection for ideas or facts in the abstract. What is protected is originality in the form, not in the contents.[43] To enjoy protection, data must therefore result from creative choices, not merely technical ones, and cannot be the straightforward result of investments. Accordingly, raw data aggregations or compilations do not satisfy the requirement of originality.[44] Human authorship is moreover essential. This element excludes generations, aggregations or compilations of data performed by software or automated processes (the latter, by contrast, are protected as intellectual property).[45]

Considering that the utilitarian value of data in the big data context does not derive from creativity or originality, copyright protection offers very limited rights, if any, over data control and access restrictions.

---

43 Commission, 'Towards a thriving data-driven economy' (n 19); Commission, 'A Digital Single Market Strategy for Europe' (n 1).

44 Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH and Others* EU:C:2011:798; Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd and Others v QC Leisure and Others* and *Karen Murphy v Media Protection Services Ltd* EU:C:2011:631; Case C-604/10 *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others* EU:C:2012:115.

45 *Football Dataco* (n 44).

-Trade Secrets and Confidentiality

In a business setting, anything may be confidential or secret in nature. Typically, the values protected by law are confidentiality and secrecy rather than the good itself. For example, ideas that cannot be protected under copyright law may find protection when shared under the private law setting of a confidentiality agreement. Likewise, information about customers and suppliers, business plans, market research and strategies can be used as business competitiveness or research innovation management tools.[46]

Thus, data may constitute the subject matter of confidential information or a trade secret, whether collected automatically or not and without any requirement of originality or creativity.

The Trade Secrets Directive sets forth a liability regime in tort against the unlawful acquisition, use and disclosure of trade secrets.[47] A trade secret is defined as information at the semantic level (i.e. it is different from data).[48] To enjoy protection, the information must be secret, i.e. it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question.[49] Its commercial value derives from secrecy, and should be subject to adequate security measures to keep it secret.[50] Trivial information is excluded.[51] Here, the right holder controls the secret rather than the data that turn into information.[52]

As the scope of such protection is confidentiality and secrecy, both contracts and trade secrecy law confer rights in personam, applying only to the

---

46 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (Trade Secrets Directive).

47 Ibid recital 2.

48 Zech (n 20).

49 Trade Secrets Directive, art 1.

50 Ibid art 2(1).

51 Ibid recital 14.

52 Ibid art 2(2).

contractual parties or persons who have unlawfully acquired, used or disclosed a trade secret.[53] Third parties are not bound by access restrictions and further dissemination. Equally, the law offers remedies only if parties knew or should have known of their secret nature.

Moreover, contracts or secrets presuppose a party holding the data. Questions remain regarding the legal title of control over data. This can be a de facto situation when data are generated internally by one agent only, with no other agent claiming rights over them.[54] This is already a substantial limit on value in the data economy.

As regards commercial value, the doubtful or trivial value of raw data has already been noted above. This is especially the case for data generated by multiple agents and/or interconnected machines.[55] The causal link between the secrecy of individual data and the commercial value of information or knowledge can be challenged too.[56] Some scholars use this point to argue that in a big data environment, trivial information may also have economic value when compiled in sufficient quantities, showing false premises in the law.[57] Nevertheless, whether their prospective value derives from their secrecy remains uncertain. Allocating value in a network environment may be unattainable.[58] By contrast, it is the secrecy of algorithms that holds value.

In light of the above considerations, some authors conclude that trade secrets legislation can nonetheless be better suited to serving the purposes of the

---

53 Ibid art 2(3).

54 See e.g. Andreas Wiebe, 'Protection of Industrial Data – A New Property Right for the Digital Economy?' (2017) 12 Journal of Intellectual Property Law & Practice 62.

55 E.g. in the Internet of Things, which describes the network of physical objects owned by one or more parties that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

56 Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17); Banterle (n 40).

57 Zech (n 20).

58 Wiebe (n 54); Stepanov (n 41).

data economy by focussing on the specific way someone has unlawfully gained access to the data, allowing a more flexible regime than erga omnes rights over the data.[59]

Overall, it appears clear that trade secrecy law grants relative protection over data control.

-*Database Rights*

At first sight, the legal protection of databases may appear the simplest model for data rights. The growing importance of data over time has given rise to support for and protection of investments in databases, without which early EU policymakers believed the database industry could not emerge.[60]

With the creation in the Database Directive[61] of a sui generis right akin to copyright, EU legislature has provided a right for database creators able to demonstrate that 'there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database'.[62] No originality obligation is required.[63]

---

59 Banterle (n 40).

60 It can be questioned whether any backing law was needed and the scope of its success, especially if the experience of other non-EU jurisdictions is compared. See Bernt Hugenholtz, 'Something Completely Different: Europe's Sui Generis Database Right Book' in Susy Frankel and Daniel Gervais (eds), *The Internet and the Emerging Importance of New Forms of Intellectual Property* (Wolters Kluwer 2016) 205; Scassa (n 15), comparing EU law with the experience of the US and Canada that have no specific database protection law.

61 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20 (Database Directive).

62 Ibid art 7.

63 Bernt Hugenholtz, 'Intellectual Property and Information Law' in Jan Kabel and Gerard Mom (eds), *Intellectual Property and Information Law: Essays in Honour of Herman Cohen Jehoram* (Kluwer Law International 1998).

The subject of the right is the substantial investment in the creation of a database, not the data themselves.[64] Under established jurisprudence, the investment should be in data that have been obtained, verified or presented. By contrast, investment in data created or generated by the person is excluded.[65] This is a limit of protection in the context of big data and artificial intelligence.

In addition, the protection is circumscribed to extraction and/or reutilisation of the 'whole' or a 'substantial part' of the contents of a database, not individual datasets. Unauthorised insubstantial extractions or reutilisations do not qualify as infringement.

Another difficulty that emerges is that big data, given their volume and diversity, are incongruent with traditional databases as conceived by the law. The Directive defines databases as collections of 'data or other materials which are systematically or methodically arranged and can be individually accessed'.[66] With big data, new technologies produce non-relational databases; that is, software associated with databases provide a mechanism for data storage and retrieval that is modelled using different means than the tabular schemas of relational databases. The 'systemic or methodical arrangement' elements are lacking and data are not compiled in a way that

---

64 Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final. See also Case C-46/02 *Fixtures Marketing Ltd v Oy Veikkaus Ab* EU:C:2004:694; Case C-338/02 *Fixtures Marketing Ltd v Svenska Spel AB* EU:C:2004:696; Case C-444/02 *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)* EU:C:2004:697.

65 Case C-203/02 *The British Horseracing Board Ltd and Others v William Hill Organization Ltd* EU:C:2004:695.

66 Database Directive, recitals 17, 21 (emphasis added). See also Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35, art 1(2) (PSD2).

preserves the semantic value of data. These circumstances have induced scholars to conclude that protection does not apply.[67]

Although it pertains to the field of data protection law, the recent *Schrems*[68] case confirms in a novel way that the data in a database, regardless of their substantiality, do not automatically belong to the database owner. Invalidating the agreement between the EU and the US on the international transfer of personal data, the CJEU prevented the database owner from moving the data to a different jurisdiction that did not offer adequate protection under EU standards. The case imposed new limits on the proprietary rights to databases composed of personal data.

As the above analysis suggests, database protection legislation prevents the simple extension of real rights or legal control over individual or raw data.

B. Personal Data Protection Law

Data protection law dictates important rights and obligations in data usability and allocation relating to an identified or identifiable natural person.

The GDPR details the conditions under which data processing is legitimate. It forces processing to be transparent, enabling data subjects to control it where the processing is not authorised by the law itself as necessary for social reasons. In short, data protection law focuses on the activities of processors and enforces their accountability, thus regulating an accepted exercise of power.[69] The law is rooted in the idea that democratic societies should not

---

67 Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 22.

68 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559.

69 Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action' in Serge Gutwirth and others (eds) (n 35). On a critical view that data protection acts are seldom

be turned into societies based on control, surveillance, actual or predictive profiling, classification, social sorting, and discrimination. It is not only a question of individual liberty, privacy, integrity and dignity, but a wider personal right aimed at fostering the social identity of individuals as citizens and consumers alike. Accordingly, the data protection regime provides legal protection to pursue the common goal of a free and democratic society where citizens develop their personalities freely and autonomously through individual, reflexive self-determination. It provides for collective deliberative decision-making about the rules of social cooperation.[70] Granting individuals control over their personal data is more than a mere tool allowing them to control the persona they project in society, free from unreasonable or unjustified associations, manipulations, distortions, misrepresentations, alterations or constraints on their true identity. It is the fundamental value of humans developing their personality in a way that allows them full participation in society without having to make thoughts, beliefs, behaviours, or preferences conform to those of the majority or those dictated from above by commercial interests.[71]

The conceptual principles outlined above are reflected in the provisions of the GDPR, the scope of which is to ensure those who determine the purposes and methods of personal data processing (the 'data controllers') engage in good data management practices. The GDPR incorporates a series of general rules on the lawfulness of personal data processing.[72] Data subjects must be informed of the processing, which has to be performed for legitimate, explicit and precise purposes. Processing is limited to the necessary time

---

privacy laws but rather information laws, protecting data before people, see Simon Davis, 'Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997) 143.

70 Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?' (2014) 51 Common Market Law Review 843 (citing Rouvroy and Poullet (n 35)).

71 Ibid.

72 GDPR, art 13-14.

frame (principles of purpose specification and data minimization).[73] Finally, data subjects are granted the right to access their data[74] and non-absolute data portability rights.[75]

A data controller can claim a valid basis for processing only if it meets one of the exhaustive criteria established by the law. If the data controller's processing does not satisfy one of them, it is unlawful.[76]

4. De Facto Control

What emerges from the previous Sections is that the existing framework is not resolutive in allocating data rights.

Intellectual property protections or related regimes are unsuitable to grant legal recognition of exclusive powers of control over datasets.[77]

When data are personal, the law grants stronger control. Even here, however, legal control is not absolute but relative. The speciality is that the debate on data control and allocation is enriched with the respect of fundamental rights. Nonetheless, data protection does not provide economic rights.

If there are no legal rights in rem or title transfer of data, in principle the latter should be freely available and access to them unrestricted. The 'data market' should not exist. The conception of data as a collective good is not an unfamiliar one (res communis)[78], with the caveat of the control conferred by the GDPR.

---

73 Ibid art 5.

74 Ibid art 15.

75 Ibid art 20.

76 Ibid art 6.

77 This conclusion is in line with those of Zech (n 20); Wiebe (n 54); Gervais (n 67).

78 Demsetz (n 30); Yoram Barzel, *Economic Analysis of Property Rights* (Cambridge University Press 1997). Collective goods (technically, things that are common to humankind) are not appropriable but the public may acquire certain usufructuary

Yet this scenario does not reflect reality. Data are regarded as a valuable economic asset, characterised by data gatekeeping, access restrictions, entry barriers, and lock-ins.

The question of how such power materialises conclusively leads to de facto control. This control allocates economic exploitation and allows sole use or access contracts. It transforms data from a non-rival good into a rival one. De facto control—which can also be termed 'possession'—is typically ensured by technical means and the ability of platforms to mine data from users. Simply put, de facto controllers are incentivised to invest in data collection because they appropriate the gains.

This finding could lead EU lawyers toward a nest of wasps regarding the law of possession in the absence of a legal title. Sharp divergences persist between civil and common law. Countries and doctrinal debates differ over the existence or nature of possessors' titles and the extent of protection.79 These fascinating discussions would deviate from this study. Here, it is sufficient to acknowledge that the law of possession would lead to weak non-resolutive protection.[80] In any event, it would not fall within the competence of EU law, but follow an impassable path for EU intervention that would frustrate from the outset any idea of harmonisation and a Single Digital Market.

---

rights (a limited real right of *usus*), directly and without altering them, and their fruits (*fructus*, the right to derive profit from them). They should be kept separate from no one's good (*res nullius*), in that the latter derives from private Roman law whereby they are considered ownerless property appropriable by means of occupation or possession if not regulated otherwise (e.g. wild animals). See Paul Du Plessis, *Borkowski's Textbook on Roman Law* (Oxford University Press 2020).

79 For a comprehensive account of comparative doctrines on the law of possession, see James Gordley and Ugo Mattei, 'Protecting Possession' (1996) 44 The American Journal of Comparative Law 293.

80 Ibid.

Rather than a market for data, factual control defines a market for access to data holding. Due to regulatory gaps, the gatekeepers are dominant technological companies.

Big data are a game-changer. They have been exploited by new technologies for the collection, storage, mining, synthesis, pattern recognition, and analysis of large volumes of wide-scoped, varied, and accurate data almost in real-time.[81] The value lies in the cumulative features of the 4 Vs: volume, velocity, variety, and veracity.[82] The maximum value of data is created by mining and analytical tools of artificial intelligence and machine-learning technologies. Competitiveness is a function of the sophistication of technologies and analyses they can perform. Arguably, data analysis is the real commodity rather than the data themselves.

As discussed above, 'data markets' should have no reason to exist, at least in conventional economic and legal terms. Rather, data are an essential, non-rivalrous, and infinite component of novel product or service markets best represented as 'data-driven markets', with different markets employing different types of big data as inputs for different outcomes.

As things stand, it seems that 'data markets' exist as the de facto result of unsuitable regulation over a fluid res that is collective in nature.[83]

To the extent that this conclusion is plausible, de facto control negatively impacts the ensuing data-driven markets. Hence, it is not only conceivable but also desirable that data-access should become unrestricted.

---

81 Mark Lycett, 'Datafication: Making Sense of (Big) Data in a Complex World' (2013) 22 European Journal of Information Systems 381.

82 Ibid. See also Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford University Press 2016); Daniel Rubinfeld and Michal Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339.

83 But see Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer 2016), according to which competition authorities and courts should define and analyse a potential market for data in addition to relevant product markets.

In principle, the enforcement of competition law should overcome abuses of market power and anticompetitive practices such as barriers to the access of essential facilities and market development.

III. The Limits of Competition Law Enforcement

1. The Unsuitability of Data as an Essential Facility

In principle, the importance ascribed to data as an indispensable input for the Digital Single Market could trigger the application of competition law. In its traditional application to dominant firms,[84] the question is the extent to which the de facto control of gatekeeping platforms over data qualifies as anticompetitive conduct harming the competitive process, innovation and entrepreneurship. A market where a data-dominant firm may restrict or impose unfair conditions on access can create a bottleneck. Provided there is abuse, the natural suggestion would be to use competition law as a tool for creating a level playing field of unrestricted data-access through a duty to share.

Competition law provides two legal grounds to remedy gatekeeping: the prohibition of anticompetitive agreements under Article 101 TFEU if the gatekeeper's refusal is based on an agreement with other firms, or in the absence of such an agreement, the prohibition of the abuse of dominant position under Article 102 TFEU.

To the extent that data constitute the essential input in the hands of monopolists, the most appropriate enforcement instrument is offered by the 'essential facility doctrine' under Article 102 TFEU. The doctrine may require a dominant firm to share its assets with others if those assets are indispensable to competing in the market and refusing access would eliminate effective competition. The market failure arising because control

---

[84] Giorgio Monti, 'Abuse of Dominant Position: A Post-Intel Calm?' (2019) 3 CPI Antitrust Chronicle <https://www.competitionpolicyinternational.com/abuse-of-a-dominant-position-a-post-intel-calm/> accessed 12 April 2021.

of data infrastructure and network effects (direct or indirect) force competing firms to depend on platforms, which become indispensable in the same fashion as physical infrastructures like railroads or ports.

The imposition of dealing with a dominant undertaking interferes with fundamental principles of freedom of contract and party autonomy. This is a controversial point that demands a limited application of the doctrine.[85] Moreover, it should be borne in mind that this is a measure meant to stimulate competition in the market and not for the market.[86] In the context of data and the European strategy, it may emerge as an important factor since competition in the market and for the market each lead to a different form of innovation: sustaining innovation that improves existing products/services in the former case, and disruptive innovation that discontinues products or services in the latter. The scholarly literature highlights how competition authorities need to balance the two in determining whether or not to intervene.[87] In this scenario, competition law enforcement may be only partially useful to the goals of the European Data Strategy.

Given this caveat, there is no general approach for applying the essential facility doctrine. It is a test based on the analysis of the specific circumstances of each case: the specific characteristics of the relevant facility, the conduct under scrutiny, and its economic context. To apply the essential facility

---

85 Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' (2019) 53 Revue Juridique Thémis de l'Université de Montréal 33; Jaques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era – Final Report* (European Commission 2019). See also Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co KG and Mediaprint Anzeigengesellschaft mbH & Co KG* EU:C:1998:264, Opinion of AG Jacobs; Case T-41/96 *Bayer AG v Commission of the European Communities* EU:T:2000:242.

86 Ibid. See also Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17).

87 Ibid.

doctrine, the facility (data) must be defined as a distinct relevant market from derivative markets. However, there is no market for (big) data as such. Moreover, platforms act as gatekeepers in different service markets. Therefore, one would need to examine the competitive reality of the markets in which each platform operates and to which the data content relates.[88] Next, robust evidence of likely anticompetitive effects should be provided.

The application of the doctrine is notoriously narrow and cumbersome.

The first step in establishing dominance is to define the relevant market. However, a digital market per se cannot be identified. Instead, platforms are heterogeneous with different business models. Relevant markets must be defined anew each time. Moreover, the potential harm to competition posed by platforms' dominance may not be always recognised if measured in terms of price and output.[89] Instead, the economic feature of platforms is their multi-sidedness; they interconnect and operate in two or more markets with network economy effects and economies of scale, where the basis for deriving income may be very diverse. In so operating, the benefits that one market (one side) derives from the platform depends on the participants of one or more other markets (other sides).[90] Data obtained in one market offer

---

88 Joined Cases 6 and 7/73 *Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission of the European Communities* EU:C:1974:18.

89 Lina Khan, 'Amazon's Antitrust Paradox' (2017) 126 The Yale Law Journal 710; Inge Graef and Francisco Costa-Cabral, 'To Regulate or Not to Regulate Big Tech' (2020) 1 Concurrences 24. See also Google Search case (n 29), according to which, even if users do not pay a monetary consideration for the use of search services on the internet, they contribute by providing data with each query.

90 For example, a search engine provider offers its services to users for free, at the same time providing advertising services or tools to other companies for profit. Likewise, a retailer may offer its intermediation services to buyers for free, at the same time operating as retailer in competition with other retailers but with the advantage of having more complete profiles of users. On the two or multi-sidedness of platforms, see Inge Graef, *EU Competition Law, Data Protection and Online Platforms* (n 83); Geoffrey Parker, Marshall van Alstyne and Sangeet Choudary, *Platform Revolution* (Norton 2017); Crémer, de Montjoye and Schweitzer (n 85).

a competitive advantage in the other(s). Therefore, the definition of the relevant market depends not only on diverse data-driven markets to which undertakings may require access but also on the markets for the several types of information that can be extracted from the data.[91] In the big data age, defining relevant markets for the essentiality of data may prove highly complex if not impossible.[92]

Second, the degree of dependence needs to be established. A successful claim must demonstrate the indispensability of the facility to business activity and that there are no other actual or potential substitutes for the facility. Moreover, there should be technical, legal, or economic obstacles that make it impossible, or unreasonably difficult, for competitors to obtain the facility.[93] Accordingly, exclusivity does not necessarily imply either essentiality or monopolistic power. Resources are not essential as such, but relative to something or in comparison with other available inputs. With big data, it is impossible to recognise a certain set of data that could identify a product/service market. In principle, all data may be useful and they can be replaceable or interchangeable in connection with the purpose for which they are needed.[94] The very notion of big data suggests that they are an extremely heterogeneous resource, whose applications cannot be known in advance. However, to be essential, a facility should serve a defined product/service in a cause-and-effect relationship.[95] Therefore, data should be divided into different categories and access granted only to the truly

---

91 Giuseppe Colangelo and Maria Teresa Maggiolino, 'Big Data as Misleading Facilities' (2017) 13 European Competition Journal 249; Mark Patterson, *Antitrust Law in the New Economy* (Harvard University Press 2017).

92 Patterson (n 91).

93 *Oscar Bronner* (n 85); Case C-418/01 *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* EU:C:2004:257; Case T-201/04 *Microsoft Corp v Commission of the European Communities* EU:T:2007:289.

94 Niels-Peter Schepp and Achim Wambach, 'On Big Data and its Relevance for Market Power Assessment' (2016) 7 *Journal of European Competition Law and Practice* 120; Colangelo and Maggiolino (n 91).

95 Ibid.

indispensable ones. From this perspective, the solution offered by the application of the doctrine appears far removed from the reality of big data and the goals of the European data policy.

Third, the refusal to provide access to the facility should exclude all effective competition on the market.[96] Mutatis mutandis, the features of platform business models and those of the facility (data) could impede the realisation of such a condition.

Finally, the refusal to provide access should not be justified by objective reasons.[97] When data are personal, data protection rules may be used as a defence against data-access requests based on competition law.

All the above illustrates that the already cumbersome enforcement of the essential facility doctrine finds additional obstacles when platforms and data are involved, making competition law enforcement an inadequate tool for the goals of unrestricted data-access and innovation.

2. Data Portability

When data are personal, Art. 20 of the GDPR recognises the right of data portability. Data subjects have the right to have their data transmitted to another controller in a structured, commonly used and machine-readable format, as long as the processing is based on consent or a contract.

Consent and contract necessity are only two of the grounds for lawful data processing as per Article 6 GDPR. The processing grounds of compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest, and the pursuit of legitimate interests of data controllers or third parties are therefore excluded from the data portability right.

---

96 *Microsoft* (n 93).

97 Ibid.

Under the circumscribed range of situations in which the right is applicable, data subjects continue to have their data processed by the original controller after a data portability operation, since this operation does not trigger the erasure of the data from the former controller but simply a transfer to another controller for the provisions of services from the latter.[98] The decision of consumers to switch service providers becomes consent to pass their data to another provider, but the possibility of erasing their data from the former provider remains subject to a separate request and conditions as per Article 17 GDPR.

The absence of a general right to data portability in the GDPR already portrays a narrow scope. This is further restricted to data which data subjects have provided themselves to the data controller—so-called volunteered data. The scope of the provision includes observation of the data but excludes derived or inferred data, or anything resulting from the analysis of the data.[99]

The norm also reduces the reach of the right by adding that controllers may transfer data where it is 'technically feasible'[100] without providing any indication about its meaning. This vagueness allows significant leeway to data controllers unwilling to make a transfer.[101]

Data protection rights of third parties provide an additional constraint when the request involves data of other individuals. This situation is not infrequent in social media where individuals share activities and intertwine their data.[102]

---

98 Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (European Commission, 5 April 2017) <https://ec.europa.eu/newsroom/article29/items/611233/en> accessed 12 April 2022.

99 Ibid. see also GDPR, recital 68.

100 GDPR, art 20(2).

101 Aysem Vanberg and Mehmet Unver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8 European Journal of Law and Technology 1.

102 Barbara Engels, 'Data portability amongst online platforms' (2016) 5 Internet Policy Review <https://policyreview.info/articles/analysis/data-portability-among -online-platforms> accessed 12 April 2021.

Last but not least, true individual control over personal data – hence effective portability - has proven difficult to achieve due to the disproportionate costs or efforts borne by data subjects, especially with the advent of technologies utilising big data and the ability to turn anything into personal data without individuals' knowledge or communication.[103]

Keeping the above limitations in mind, legal scholars have already analysed the control mechanism of horizontal application of the right and its relationship with competition law.[104] The right is analogous to the control approach of data protection and its limited application (see above, Section 2.3.2). The GDPR addresses the issue from the perspective of data subjects' rights. The main policy objective is to ensure that individuals are in control of their data and trust the digital domain. However, the perspective of competition remains outside the remit of the GDPR, which must be complemented by the limited applicability of competition law (above).[105] The primary aim of data portability is data subjects' control, not competition concerns. It enables access and transferability to or via individuals without creating an access system at the disposal of competitors for product development. Thus, even if data portability impacts on competition for the prevention of service lock-ins alongside the equally limited Regulation

---

103 Nadezhda Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (2017) 10 Journal of Law and Economic Regulation 64.

104 Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335; Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359; Inge Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (2020) 2 CPI Antitrust Chronicle 1.

105 Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74; Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law and Security Review 193.

2018/1807 on the free flow of non-personal data,[106] its applicability is narrow. The measure is very far from providing an appropriate data-access regime to satisfy the sharing obligation of European policy goals.[107]

IV. THE CASE FOR PSD2-LIKE REGULATION OF THE PLATFORM ECONOMY

1. Ex-ante Regulation and the PSD2 Model[108]

The Sections above aimed to demonstrate the shortcomings of property, competition, and data protection law enforcement to offer a regulatory framework hospitable to a data-access and sharing regime for the European Data Strategy. A major drawback in digital markets is that they move too fast and are too varied and complex to be supervised ex-post and comprehensively. Moreover, the amorphous nature of big data complicates their 'essentiality' in legal terms. This does not mean that competition law is

---

106 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59. The Regulation operates on two specific obstacles to data mobility, i.e. data localization requirements imposed by Member States and contractual vendor lock-in practices in the private sector (situations where customers are dependent on a single provider and cannot easily switch to a different vendor without substantial costs, legal constraints or technical incompatibilities). On the latter aspect, it facilitates and encourages EU companies to develop self-regulatory codes of conduct to improve the competitive data economy based on the principles of transparency, interoperability and open standards. Companies that provide data processing services should introduce some self-regulatory codes of conduct to ensure the provision of clear and transparent information and thereby avoiding vendor lock-ins. In the case of a dataset composed of both personal and non-personal data, the Regulation applies to the non-personal data part of the dataset.

107 See also the Commission recognition that 'as a result of its design to enable switching of service providers rather than enabling data reuse in digital ecosystems the right [to data portability] has practical limitations'. Commission, 'A European strategy for data' (n 2) 10.

108 PSD2.

generally unfit to preserve the contestability of markets or other structural aspects not covered in this contribution.[109] However, legal intervention could give regulators the power to require or prohibit behaviours to reach desired economic and social outcomes without having to engage in proving unfit competition rules on a case-by-case basis.

Unsurprisingly, ex-ante regulation of the platform economy is gaining popularity in EU policy circles. In preventing a level playing field and obstructing innovation, the bottlenecks created by data are a difficult issue that could be better addressed by the regulatory realm.[110]

On the one hand, regulation ensures higher technical specialisation and can be more effective in addressing the structural problems of markets like the digital ones that cannot be tackled under EU competition rules. On the other hand, it is also capable of more effectively addressing the unfair allocation of resources, welfare, and social harms.[111]

The EU already has sector-specific legislative instruments enabling data-access in place.[112] Before engineering a new one, the question is whether any

---

109 Nicolas Petit, *Big Tech and the Digital Economy: The Moligopoly Scenario* (Oxford University Press 2020).

110 Commission, 'A European strategy for data' (n 2) especially 8, 14.

111 Niamh Dunne, *Competition Law and Economic Regulation, Making and Managing Markets* (Cambridge University Press 2015); Jean Tirole, *Economics for the Common Good* (Princeton University Press 2017); Crémer, de Montjoye and Schweitzer (n 85).

112 See e.g., in the payment services sector, PSD2; in the motor vehicles sector, Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L151/1; in the digital content sector, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1; in the energy sector, Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on

of these could be suitable as a horizontal regulatory model of general applicability. The financial sector is an interesting case to investigate due to the precursory and more mature role it has traditionally played as a data-driven market.[113]

The PSD2 is the EU sector-specific legislation providing a normative data-access framework for payment services within the Internal Market.

Its objective is to lay down the terms for achieving integrated retail payments in the EU that are inclusive not only of existing but also new payment services and market players. Its ambitious goal is to take advantage of innovative technology-enabled solutions (fintech) to generate efficiencies and reach a broader market with more choice and integrated services, at the same time pursuing transparency and consumer protection.[114]

The Payment Services Directive ('PSD1')[115] was the first attempt to comprehensively regulate the sector and provide the necessary infrastructure for the perfection of the internal market. It specified the allocation of risk among service providers and customers, regulated a vast array of payment instruments, enhanced market transparency, and strengthened competition

---

common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L158/125.

113 George Akelof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 Quarterly Journal of Economics 488; Joseph Stiglitz and Andrew Weiss, 'Credit Rationing in Markets with Imperfect Information' (1981) 71(3) American Economic Review 393; Douglas Diamond, 'Monitoring and Reputation: The Choice between Bank Loans and Directly Placed Debt' (1991) 99 Journal of Political Economy 689; Allen Berger and Gregory Udell, 'Relationship Lending and Lines of Credit in Small Firm Finance' (1995) 68 Journal of Business 351; More recently, see Dirk Zetzsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (2020) 57 Common Market Law Review 331.

114 PSD2, recital 6.

115 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC [2007] OJ L319/1 (PSD1).

by harmonising market access requirements, licencing and access to technical infrastructures.[116] Taking a pro-competition attitude, the PSD1 also enabled the operations of new end-to-end providers, i.e. new firms, in the form of closed platforms that digitally intermediate between the payer and the payee, arranging the payment transaction within their closed system with no dependence on other providers such as the firm where the payment account is held.[117]

At the same time, the market witnessed the emergence of infant front-end providers, i.e. third-party providers (TPP) of digital services based on the customer's payment account held by banks. These services could include payment initiation (Payment Initiation Services or 'PIS')[118] or account information (Account Information Services or 'AIS'),[119] either requiring direct and continuous access to the customer's account and the data therein contained. However, the banks where the payment account are held could legitimately refuse access to their infrastructure on grounds of intellectual

---

116 See e.g. ibid recitals 10, 16-17, 42 and arts 10, 28. In the literature, see Despina Mavromati, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market* (Kluwer Law International 2008).

117 A typical example of end-to-end are e-money schemes such as the one provided by PayPal, a well-known firm operating as a payment processor and online payments system that supports instant online money transfers and serves as an electronic alternative to traditional methods like checks or money orders. Other end-to-end examples are virtual currencies/crypto-assets, or electronic money providers.

118 PIS operate as a bridging software between a trader's website and a payer's bank account. Examples of PIS are internet payment gateway providers or mobile wallets that position themselves as interfaces between the payers or the payees and the bank of the payment account.

119 AIS provide a single source of information on the current state of the aggregated finances of payment service users. Examples of AIS are services consolidating in one all the accounts of a person, money management, credit-risk analysis and scoring, financial advice, comparisons, access to targeted offers of other financial services such as credit or insurance, etc. They all analyse a person's transactions on their accounts to provide services based on information.

property protection, security risks, or persistent unclear rules regarding liabilities towards customers.[120]

Whilst applying in principle to online payment services, the PSD1 ignored both the specific issues and new developments of the fast-growing digital market. As a regulatory instrument conceived for payment services offered by traditional incumbents, the legal framework of the PSD1 displayed essentially two limits: i) the de facto low competition in the retail-banking sector characterised by low elasticity of demand, lock-in problems, and exclusivity of payments services linked to the holding of bank accounts;[121] ii) obsolescence in the face of fintech acceleration, with new unregulated market players and services operating outside the relationship between the banks and their account-holding customers.[122]

---

120 Giuseppe Colangelo and Oscar Borgogno, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule' (2020) 31 European Business Law Review 573.

121 The Netherlands Authority for Consumers and Markets, 'Barriers to Entry Into the Dutch *Retail* Banking Sector' (June 2014) <https://www.acm.nl/sites/default/files/old_publication/publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf> accessed 12 April 2021; Commission, 'Impact Assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions' SWD (2013) 288 final; European Central Bank, 'Financial Stability Review' (November 2016) <https://www.ecb.europa.eu/pub/pdf/fsr/financialstability review201611.en.pdf> accessed 12 April 2021; UK Competition and Market Authority, 'The Retail Banking Market Investigation Order 2017' (gov.uk, 2 February 2017) <https://www.gov.uk/government/publications/retail -banking-market-investigation-order-2017> accessed 12 April 2021.

122 European Banking Authority, 'Discussion Paper on Innovative Uses of Consumer Data by Financial Institutions' (2016) EBA/DP/2016/01 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1455508/68e9f120-8200-4973-aabc-c147e9121180/EBA-DP-2016-01%20DP%20on%20innovative%20uses%20of%20consumer%20data%20by%20financial%

The fundamental drawbacks of this market physiognomy were the high profit margins of the traditional banking industry to the detriment of consumer welfare and the weak protection of consumers exposed to the legal vacuum of the alternative market of emerging, highly demanded fintech.[123] These trends occurred in a legal environment unfavourable to innovation, where the growth of the digital market played almost no role in policy decisions.[124]

This historical primer on EU payments law suggests similarities with the platform economy in terms of the rationale and extent of the changes heralded by the PSD2. The directive launched the banking industry into uncharted territory, to the extent that many observers have branded the resulting EU payments market a 'revolution'.[125]

20institutions.pdf?retry=1>; European Banking Authority, 'Discussion Paper on the EBA's Approach to Financial Technology (FinTech)' (2017) EBA/DP/2017/02 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20%28EBA-DP-2017-02%29.pdf?retry=1>. In the literature, see Dirk A Zetzsche and others, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) EBI Working Paper Series no 6 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959925> accessed 12 April 2022; Federico Ferretti, 'Consumer Access to Capital in the Age of FinTech and Big Data: The Limits of EU Law' (2018) 25 Maastricht Journal of European and Comparative Law 476.

123 E.g. consumer protection concerns related to data protection, money laundering and fraud risks, and the difficulties of proof in establishing authorisation in cases of unauthorised payments. See Commission, 'Towards an integrated European market for card, internet and mobile payments' (Communication) COM (2011) 941 final.

124 Mary Donelly, 'Payments in the Digital Market: Evaluating the Contribution of Payment Services Directive II' (2016) 32 Computer Law and Security Review 827.

125 Inna Oliinyk and William Echikson, 'Europe's Payment Revolution' (2018) CEPS Research Report No 2018/06 <https://www.ceps.eu/ceps-publications/europes-payments-revolution/> accessed 12 April 2022, recalling industry trade and consumer groups.

2. The Access to Account Rule as a Game-changer: Open Banking and the Data Economy

With the PSD2, the EU legislature shifted its policy approach to digitalisation and undertook a significant intervention in the single payments market.[126]

Broadly, the law operates on two interrelated levels. Like the PSD1, it intervenes in the establishment, authorisation, and supervision of payment firms and the regulation of payment transactions. Adjusting to the digital market, the directive enlarges the scope of coverage of the law, clarifies the extent of consumer rights and service provider obligations, and reinforces security and authentication requirements.[127] In addition, the PSD2 recognises and incorporates into the regulation those TPPs emerging from new fintech endeavours in payment services. It brings TPPs under the same harmonised standards, requirements, and obligations as traditional payment providers and on an equal footing with them, regardless of the business model they apply.[128] Introducing the so-called 'access to account rule', it opens the market to new services by granting TPPs access to the customer payment accounts held by banks. The latter must allow TPPs authorised by the competent authority in their home Member State[129] access to the data contained in payment accounts in real-time and on a non-discriminatory basis.[130] By accessing and exploiting the large quantity of real-time data of the banking realm, technology firms have started disrupting retail financial markets.[131]

---

126 See, in particular, PSD2, recital 95.

127 See the various provisions of ibid, titles II-IV.

128 Ibid, recitals 27-33.

129 Ibid art 36.

130 Ibid arts 64-68.

131 Oscar Borgogno and Giuseppe Colangelo, 'The Data Sharing Paradox: BigTechs in Finance' (2020) 16 European Competition Journal 492; Oscar Borgogno and Giuseppe Colangelo, 'Consumer Inertia and Competition-sensitive Data

The 'access to account rule' has therefore become the tool to unlock the data power of dominant banks over innovative fintech firms.

The TPPs access payment accounts. Such access must occur securely, under the guidelines laid down by the European Banking Authority ('EBA'),[132] and does not require any payment to the holding banks. The access is only carried out upon the conclusion of a contractual relationship between the account holder and a TPP for the provision of PIS or AIS and is instrumental to providing those kinds of services that require the data contained in the account.[133]

Governance: The Case of Open Banking' (2020) 4 Journal of European Consumer and Market Law 143; Fabiana Di Porto and Gustavo Ghidini, 'I Access Your Data, You Access Mine. Requiring Reciprocity in Payment Services' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 307.

132 PSD2, art.95, followed by European Banking Authority, 'Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)' (2017) EBA-RTS-2017-02 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf> accessed 12 April 2022; Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782 [2018] OJ L69/23; European Banking Authority, 'Opinion of the European Banking Authority on the Implementation of the RTS on SCA and CSC' (2018) EBA-Op-2018-04 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1> accessed 12 April 2022.

133 For PIS, see PSD2, art 66, stating that 'when the payer gives its explicit consent for a payment to be executed and (…)'. For AIS, see PSD2, art 67, providing that 'the account information service provider shall: (a) provide services only where based on the payment service user's explicit consent; (…)'.

These provisions have given rise to the novel concept of 'Open Banking', a market model that shifts from the money business to the data business and vice versa. Account data are shared with new market players of the fintech industry capable of capturing or creating value around existing un- or under-exploited assets.[134] By law, banks must share the data they control for the benefit of fintech firms for the creation of new products or the provision of new services.

Payment accounts contain a vast amount of data for analysis: financial data relating to incoming and outgoing transactions, balances, preferences, patterns, dependencies, behaviours, aspects of social life, etc. They are an exceptional tool for product development, especially when integrated with data from other unrelated sources ('big data') and processed by algorithms powered by artificial intelligence technologies.

The new paradigm of the Open Banking model thus reflects the unbundling of the provision of financial services in multiple market segments and the disintermediation of the banking industry.

Under the PSD2, TPPs are subject to business conduct restrictions and requirements that do not allow them to hold the payer's funds in connection with the service, store sensitive payment data of the service user, or process data beyond that necessary to provide the service.[135] The services can only exist via the traditional providers, creating a new market structure where the latter become digital platforms for the distribution of financial services. They facilitate and create a dependency for the contractual interactions of two or more market agents, but without having any contractual relationship with one of them (the TPP) and at the same time allowing the other one (the customers) to continue the fruition of their own services. The consent of customers is sufficient to allow TPPs to access account data.

---

134 Henry Chesbrough, 'Business Model Innovation: Opportunities and Barriers' (2010) 43 Long Range Planning 354.

135 PSD2, art 66(3).

Thus, the Open Banking environment generates indirect network effects, enabling bilateral ventures not otherwise attainable with other means.[136]

The Open Banking market structure is moving towards a confluence of traditional financial service providers transforming into technological firms (while still engaging in their core business) and technological firms entering the financial services market, where the latter may be infant fintech businesses or established Big-Techs.[137]

From this point of view, the PSD2 is a law that encourages the expanding use of personal data. By forcing data sharing, it enables a vast array of newcomers to access an increasing amount of data sources for novel purposes.

Moreover, the 'access to account rule' does not entail access to an essential facility. It escapes the precise definition of the relevant market, which is a highly discretional exercise.[138] The rule permits the exploitation of a facility controlled by others and at the same time, reinforces the control requirements of data protection law.

The PSD2 also grants stronger bargaining power to consumers in the digital market. Unlike the one-off transfer upheld by the right to data portability, data-access under the PSD2 allows for continuous access to real-time data.

---

136 Markos Zachariadis and Pinar Ozcan, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking' (2016) SWIFT Institute Working Paper No 2016-001 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199> accessed 12 April 2021; Diana Milanesi, 'A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom and the United States' (2017) Stanford Law School TTLF Working Papers Series No 29 <https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/> accessed 12 April 2021.

137 René Stulz, 'FinTech, BigTech, and the future of banks' (2019) NBER Working Paper No 26312 <https://www.nber.org/papers/w26312> accessed 12 April 2021; Dirk Zetzsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (n 113); Di Porto and Ghidini (n 131).

138 Di Porto and Ghidini (n 131).

Adopting a pro-competitive perspective, the directive arguably strengthens subjects' control over their data by complementing the data protection right of portability. This way, it addresses the opening-up of retail financial markets. Together, the PSD2 and the GDPR may be regarded as a building block targeting the difficult relationship between competition and consumer protection.

Even as the PSD2 has broken the gatekeeping position of banks in the payment financial services sector, by analogy its regulatory model may well interrupt the gatekeeping role of Big-Techs in the platform economy. The PSD2 has disrupted the financial services sector traditionally dominated by large banks. Likewise, it can unlock the data power of Big-Techs and disrupt the digital market.

In short, it can be argued that the PSD2 attains for a single sector the same goals that the EU aims to achieve more generally with its recent data-access and sharing policies - that is, to ensure competition and consumer protection in the Digital Single Market. It already provides a regulatory model that would not require the reinvention of rules. A fragmented legislative strategy with a diverging data act could have the undesirable result of creating an uneven playing field among sectors, where technological firms enjoy unjustified advantages over traditional market players without reciprocity. Asymmetrical regulatory measures are prone to tilt the market in favour of platforms to the detriment of new market players. This is already the case in the Open Banking market structure, where the Big-Techs are entering the financial services market without reciprocity.[139]

---

[139] Borgogno and Colangelo, 'Consumer Inertia and Competition-sensitive Data Governance' (n 131). For example, note that Google has secured an e-money license after Lithuania granted authorisation. The license enables the company to process payments, issue e-money, and handle electronic money wallets. It gives permission to operate across the EU via the passporting rights system. Likewise, Facebook and Amazon obtained licenses in Ireland and Luxembourg. See Milda Seputyte and Jeremy Kahn, 'Google Payment Expands With E-Money License

A one-size-fits-all Data Act built on the model of the PSD2 may set a fairer playing field, leaving room for competition law enforcement to challenge other anticompetitive practices in the market.

V. Conclusion

The EU has launched an ambitious policy for a Single Data Space. It seeks to combine legislation and governance across business sectors to ensure the free flow, access and sharing of data for competition and innovation. This paper analysed the legal aspects of the datafication process in the context of the market imbalances created by Big-Techs and how they influence the prospective Data Act for the establishment of a data-access and sharing regime for digital market players. It contributes to the field by assessing a recent policy and legislative announcement and advancing a novel suggestion for an alternative and simplified approach. It aimed to show that to build a genuine data-driven market for products and services and accomplish the latest policy goals, the EU should take stock of its legislation in the payments sector. The access to account rule of the PSD2 could be reproduced to grant free access to and sharing of data for innovation, at the same time breaking the gatekeeping role of Big-Techs in the same fashion as it did for banks in the financial services sector.

Many Big-Techs have built their business models on monetising data and acting as gatekeepers. Because data are so important for the digital economy, it is rational to assess the extent to which 'data markets' exist or take shape. No matter how tempting it may be, in legal terms, data cannot be qualified as tradable goods. Their fluid nature finds no parallel with existing concepts and traditional legal doctrines deriving from property and contracts. Likewise, competition principles cannot be directly applied.

From Lithuania' (Bloomberg, 21 December 2018) <https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania> accessed 12 April 2021.

Therefore, a market for data cannot exist without further complications or elaboration. Instead, digital markets can be considered 'markets for data-driven products and services', where competition and innovation lie in the ability to exploit the data, e.g. through the use of software algorithms, digital infrastructures, or product/service engineering and design. This distinction matters as it hardly justifies gatekeeping practices, where data are controlled de facto without proper legal title except in those established circumscribed situations where intellectual property rights or data protection law intervene.

However, the controls granted by intellectual property escape individual data. Likewise, when data are personal, data protection law addresses data subjects' control as a relative right that does not necessarily exclude the possibility of others accessing or using the data. Moreover, third parties may well access personal data upon data subjects' consent.

De facto control and gatekeeping negatively impact data-driven markets. Yet competition law enforcement is limited in application and does not offer a regulatory framework capable of challenging them. Not only are data amorphous and challenging to traditional legal constructs, but digital markets move too fast and are too varied and complex to be supervised ex-post by the competent authorities. Moreover, competition law does not provide a general approach for applying the essential facility doctrine to dominant platforms; enforcement would depend on the specific circumstances of each case, in terms of the specific conduct in question and its economic context. Competition law may continue to serve the purpose of limiting anticompetitive practices but appears unsuitable to tackle data concentration and bottlenecking.

It seems inevitable that ex-ante regulation, as expressed in the Data Act, will eliminate the limits or uncertainties of competition law enforcement. Yet the question remains of how it can achieve the expected results established in the policy goals.

Arguably, an analysis of the existing sectoral legislation advanced by the PSD2 reveals that the EU does not have to reinvent the wheel. The directive already enacts, in the financial services market, the results envisioned by the EU for the entire digital market. The PSD2 has set a precedent of user-driven data-access, enabling the real-time sharing of data, favouring interconnectedness, and facilitating innovation. By providing for the 'access to account rule', the PSD2 breaks the data monopoly of the traditional banking sector. It has given rise to the Open Banking model that is disrupting the sector, allowing for a free data-access regime where fintech companies (including Big-Techs) enter the market, design new products and provide new services. In such a renewed market, consumers continue to enjoy the usual protections afforded by data protection law. At the same time, the expanded applicability of data portability and reinforced ability to consent to data-access enables consumers to drive the process. More transparent control over data-access further empowers them.

The PSD2 has disrupted the retail financial market and unlocked the data and service power of dominant banks in favour of innovative firms. By analogy, its regulatory model could disrupt the digital market and unlock the data power of Big-Techs.

To the extent that the market failure of the platform economy mirrors the one that existed in the banking sector, the 'access to account rule' could be a replicable legislative model that addresses the market imbalances caused by the Big-Techs. If it works for banks, why shouldn't it be suitable for gatekeeping platforms?