BANCA D'ITALIA

EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Data governance and the regulation of the platform economy

by Oscar Borgogno and Michele Savini Zangrandi

November 2021

Number 652

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Data governance and the regulation of the platform economy

by Oscar Borgogno and Michele Savini Zangrandi

Number 652 – November 2021

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6627 (print)
ISSN 1972-6643 (online)

Printed by the Printing and Publishing Division of the Bank of Italy

DATA GOVERNANCE AND THE REGULATION OF THE PLATFORM ECONOMY

by Oscar Borgogno*, Michele Savini Zangrandi*

Abstract

Systematic data exploitation through digital means lays at the very heart of the current platform economy. The regulatory boundaries posed by legislation to what firms and individuals can do with this intangible asset fall under the broad concept of data governance. We argue that the three major regulatory policy fields critical in shaping a country's data governance framework are data control, national security and competition law. These legislative strands have a profound impact on the platform economy and overlap with each other in a significant manner. In exploring the complex trade-offs, this paper reaches three broad conclusions. First, multiple and diverse regulatory domains intersect the digital space, with overlapping and sometimes unpredictable consequences. Second, given the transnational nature of digital activity, international coordination and dialogue are of the utmost importance. Third, as the data governance framework has important consequences for the financial sector, sectoral regulators should be open to taking an active part in national and international discussions.

JEL Classification: F53, K21, L38.
Keywords: digital platforms, data, competition policy, national security, data access, privacy.
DOI: 10.32057/0.QEF.2021.0657

Contents

* Bank of Italy, International Relations and Economics Directorate

1. Introduction: Data Governance.

Data governance can be broadly defined as the set of rules and enforcement mechanisms that discipline collection, access, storage and processing of third party data. In the context of the increasing degree of digitalization, this is a topic of intuitive importance, and vast complexity: the ability to collect, merge or exploit datasets, can make the fortune of firms or countries, yield enormous opportunities, or generate unmanageable risks.

Yet, data governance is seldom discussed outside of limited policy circles. This is partly due to its fuzzy definition: no individual regulation disciplines the subject in a comprehensive fashion while several regulations discipline sections of it. This is partly due to its heavy politics: because of the dominance of digital platforms, data governance amounts, for most intents and purposes, to platform governance – an activity that in the global race to digital supremacy escalates quickly into (geo)political tensions.

By means of sweeping simplification, three major regulatory fields appear critical in shaping a country's data governance framework: data control, national security and competition policy. Data control regulation defines the rules for access, use and re-use of data. National security regulations determines (the increasingly broad) set of data-types and uses which are off-limits. Competition regulation sanctions the behavior and business practice of the digital "market makers". These legislative strands have a profound impact on the digital economy and substantial degrees of overlap with each other: tinkering with elements of one regulation, often leads to unintended effects in the others' domain.

This paper discusses the role that each of these regulatory levers play, and the complex web of overlaps and trade-offs that exist when they apply to the digital sphere. In exploring these interactions, this note aims to support the policy maker and regulators in understanding the key levers under the fuzzy hood of data governance.

The analysis brings to three broad conclusions.

First, regulation of the digital space suffers from an extreme degree of complexity. Multiple and diverse regulatory domains intersect the digital space, with overlapping and sometimes unpredictable consequences. As regulators strive to "put order" in their digital corner, it appears particularly important that this complexity is factored in.

Second, given the trans-national nature of digital activity, coordination and dialogue can hardly be confined to a set of national regulators. However, while a set of internationally agreed principles for the regulation of the digital sector would appear necessary, this seems a complex task for the very broad-basedG20 and WTO negotiations. Convergence might instead be found within smaller groups of like-minded countries.. At the end of October 2021, Trade Ministers of G7 countries issued a set of commonly agreed Digital Trade Principles,[1] pledging to work towards a common framework for cross-border data transfers, and limiting the use of data-localization measures for protectionist purposes. These principles constitute a first step towards overcoming structural differences within the block of advanced economies.

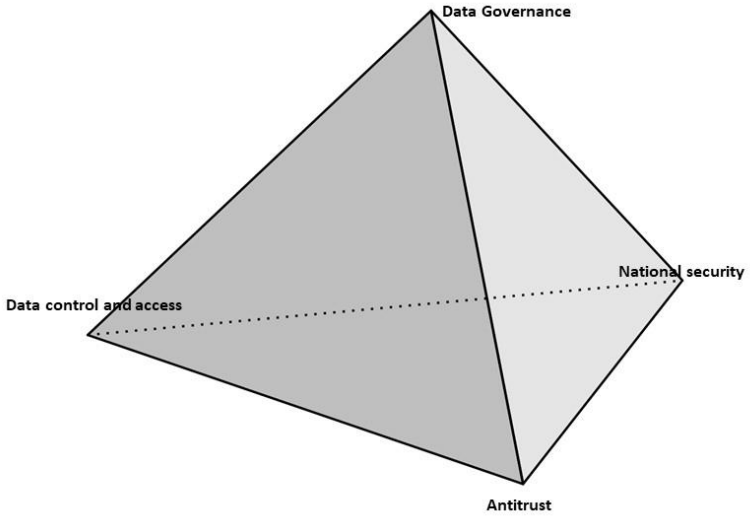
Third, the definition of the global data governance framework has important consequences for the financial sector, and its regulators. Finance, more than other sectors, is a data-centric business. Financial regulators should therefore take active part in national and international discussions on this matter. Given the pervasive nature of digitalization, the analysis presented here should be considered

[1] G7 Trade Ministers, "Digital Trade Principles", October 22, 2021.

as both partial and preliminary. Additional policy levers, such as digital taxation and content liability rules, also play a role and come with specific complexities.

The structure of this note can be thought of as a triangle-based pyramid (Fig. 1), where data governance, at the top, rests on three separate regulatory levers – which are nonetheless all connected with each other at the base. Sections 2, 3 and 4 are respectively dedicated to the role that data control, national security and antitrust regulations play in the definition of national data governance frameworks. Section 5 is dedicated to the multiple overlaps and trade-offs among the three legislations. Section 6 concludes.

Fig. 1: the data governance pyramid



2. Three levers of data governance.

2.1. Lever 1: data control and data access regulations.

The multifaceted set of rules on access, sharing and re-use of data between firms, individuals and public entities is a major pillar of data governance. Owing to the economic potential of data-enabled applications, such as Internet of Things (IoT) and Artificial Intelligence (AI), these regulations are often flagged as crucial factors in unlocking economic growth.[2]

In its very essence, data control is the overarching element at the base of modern privacy legal frameworks.[3] Indeed, such a broad concept encompasses different aspects of how personal information can be legitimately gathered and used by third parties. First, we find rules that determine the conditions for primary collection of personal data. Second, there are rules setting the legal perimeter within which data-enabled service providers can access personal information that has already been collected by other providers (business-to-business data sharing, B2B data sharing).[4]

[2] OECD (2019), 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies', OECD Publishing.

[3] As rightly pointed out by Acquisti A., Taylor C., and Wagman L. (2016), 'The economics of privacy', 54 Journal of Economic Literature 2, 442–492, different dimensions and definitions of privacy emerge from the literature, such as privacy as control over usage versus privacy as protection against access of personal information.

[4] This is the case of the access-to-account rule enshrined in the Payment Service Directive (PSD2) in Europe. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal

Third, there are rules providing for the flow of privately held data into the public sphere (business-to-government data sharing, B2G data sharing).[5] Fourth, we find provisions mandating public bodies to share publicly held data with businesses and individuals (government-to-business, G2B data sharing).[6]

Data access regulations – including privacy – generally find their expression in the right of control over data. In those jurisdictions where a comprehensive personal data protection legal framework is in place, such as the European Union, the right of control empowers individuals to move their own data from one data controller to another,[7] setting the balance of powers between data subjects and controllers and mitigating issue personal data lock-in.[8] Moreover, data control also applies in business-to-business and business-to-government dealings, where the growth enhancing potential of data sharing is tapered both by the legitimate interests of individuals and by the reticence and mistrust of private firms.

Regulatory approaches to personal data protection differ widely across countries.[9] In the European Union (EU), Canada, and Japan access to personal data is allowed within strict limits on which information can be collected, which uses it can be put to, who can access it, and how long it can be retained for. The United States does not have a comprehensive federal legislation, with privacy limitation broadly seen as an undue impediment to trade and innovation.[10] Russia and China, conversely, follow a different approach, centered on the concept of cyber-sovereignty. Here data is considered a national strategic asset, which must therefore be stored locally. Recent developments in China see strong personal data protection alongside unbounded access rights on part of state and government agencies.

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, Art. 67.

[5] In France, the law for a digital republic allows the public sector to access certain privately held data of general interest. French legislation, 'Loi No 2016-1321 du 7 octobre 2016 pour une République numérique'. See also: High-Level Expert Group on Business-to-Government Data Sharing (2020), 'Towards a European strategy on business-to-government data sharing for the public interest', p. 35. For an economic assessment of the matter at the EU level, see: Bertin M., Duch-Brown N. (2020), 'The economics of business-to-government data sharing' (JRC Technical Report). On how to shape effective data sharing partnerships between public and private actors, see: Biancotti C., Borgogno O., Veronese G. (2021) 'Principled data access: building public-private data partnerships for better official statistics,' QEF Banca d'Italia 629.

[6] This is the case of the EU the Open Data Directive on open data and the re-use of public sector information and the Australian New Australian Government Data Sharing and Release Legislation. Indeed, public sector information (PSI) is acknowledged as a valuable resource for the digital economy both in terms of raw material for data-enabled services but also for the delivery of more accurate decision-making in society.

[7] De Hert P., Papakonstantinou V., Malgieri G., Baslay L. and Sanchez I. (2018), 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', 34 Computer Law and Security Review 193.

[8] In economics, data lock-in, also known as customer lock-in, makes an individual dependent on a service provider because she is unable to opt for a rival provider without substantial switching costs. See European Commission, 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018', (Communication) COM (2018) 43 final: "Since it allows the direct transmission of personal data from one company or organisation to another, the right to data portability will also support the free flow of personal data in the EU, avoid the 'lock-in' of personal data, and encourage competition between companies." Cfr. Borgogno O., Colangelo G. (2020), 'Data, Innovation and Competition in Finance: The Case of the Access to Account Rule', European Business Law Review 31, no. 4 (2020): 573-610.

[9] Indeed, the dichotomy personal-non personal data is likely to prove extremely challenging to apply in real world scenarios when there is a need to deal with complex sets of data generated by different sources, ultimately capable of being referred to specific individuals thanks to big data analytics and cross-referencing.

[10] To date, the most relevant state data privacy state legislation within the US is the California Consumer Privacy Act (CCPA). Signed into law on June 28, 2018, it went into effect on January 1, 2020. The CCPA is cross-sector legislation that provides for broad individual consumer rights and imposes significant duties on entities or individuals that gather personal information about or from a California resident.

The reminder of this section provides an overview of the EU efforts at shaping its data-space. With the introduction of data access regimes sanctioned by the General Data Protection Regulation (GDPR) in 2016, the EU has spelled out – arguably – the most cohesive, principled approach to data governance so far. This approach has seen a reasonable degree of uptake in other countries. However, whether the EU's approach will prove appropriate, or even enforceable remains an open question.

The EU GDPR sets out a comprehensive legal framework on personal data protection with rules hinged on overarching principles of lawfulness, fairness, purpose limitation, data minimization and ultimately of transparency and accountability.[11] The right to data portability, enshrined in article 20 of the GDPR, has been recognized as a breakthrough in the realm of personal data protection law.[12] According to the Working Party 29[13], the right to data portability is framed as a building block of a wider framework of "workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data".[14]

In addition to GDPR-sanctioned data portability, the European Commission has put forward a large array of sector-specific regulatory initiatives on data access, also targeting non-personal data.[15] Notably, the Second Payment Service Directive (PSD2) sets out a sector-specific access to account data rule[16], the Regulation on free-flow of non-personal data addresses data sharing practices in the commercial arena (business-to-business)[17], and the recent Directive on open data aims at promoting the re-use of government information.[18] While these initiatives differ in terms of scope, they all aim to promote smooth and trusted forms of data sharing.[19]

Additional proposals aim at shaping the EU data governance landscape. In November 2020, the Commission presented a proposal for a Data Governance Act aimed at enabling the sharing of

[11] See for example the rules on data protection by design and by default rule under art. 25 GDPR; the reporting duties as the breach notification obligation under art. 33 GDPR; and the appointment of a Data Protection Officer under art. 37 GDPR, is a first precondition for the fulfilment of businesses' accountability. In this context, specific consideration is to be given to the data protection impact assessment and prior consultation under art. 35 and 36 GDPR, requiring data controllers to identify the risks to the fundamental rights and interests of natural persons directly stemming from processing technologies and to "be able to demonstrate that processing is performed in accordance with" data protection law. Moreover, as highlighted by art. 24(1) GDPR, controllers shall implement technical and organisational measures, which have to be adequate to the nature, the scope, the context and the risks of the enacted data processing.

[12] From a substantive point of view, data portability encompasses three different and complementary rights: (1) the right to receive data provided by data subject; (2) the right to move those data to another controller; and (3) the right to have the personal data transferred directly from one controller to another.

[13] The Article 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until the entry into application of the GDPR.

[14] Article 29 Data Protection Working Party (2013), 'Opinion 03/2013 on purpose limitation', 47.

[15] Indeed, businesses also collect, process and share data that are inherently of non-personal nature, as energy or environmental data.

[16] 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, Art. 67.

[17] Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union [2018] OJ L303/59.

[18] 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 (recast) [2019] OJ L172/56.

[19] It is worth pointing out that two main distinctions emerge from the access rules emerging worldwide. The first hinges on the binding character of each sharing regime. Whereas the GDPR, the PSD2 and the Open Data and Public Sector Information Directive entrust specific data holders with a duty to share data whenever so requested, the Regulation on a framework for the free-flow of non-personal data merely provides for a general freedom to move data within the Internal Market. The second involves the scope of the different mechanisms designed by the European legislator. Notably, whereas the XS2A rule is a sector-specific rule inherently aimed at delivering data sharing within the retail financial sector, the other frameworks establish general-purpose data sharing regimes that apply, with different degrees, across industries to the whole economy.

sensitive data held by public bodies and private actors.[20] By the end of 2021 the Commission is expected to present the proposal for a Data Act with the goal of fostering business-to-government data sharing for the public interest, supporting business-to-business data access, and assessing the intellectual property rights framework with a view to further enhance data access and use.[21]

The European data access framework is increasingly taken as an international benchmark, with particular emphasis on retail markets (such as banking services and energy).[22] In the US, the July 2021 Executive Order on Executive Order on Promoting Competition in the American Economy marks a renewed push towards data access regulation. The Order encourages the Director of the Consumer Financial Protection Bureau to introduce new rules facilitating "the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products".[23] In Australia, the Government proposed the "Data Availability and Transparency Bill 2020" in order to establish a scheme for the sharing of 'public sector data' by 'data custodians' to 'accredited users'.[24] In the same vein, the Australian Government set up the Consumer Data Right that gives individuals greater control over their own data, including the ability to securely share data with a trusted third party.[25] Also the Government of Canada, at the request of the Canadian Competition Bureau, undertook a review process of open banking in 2018 and by the end of 2021 the Advisory Committee is expected to deliver final considerations on consumer privacy, security, and data access.[26]

Overall, the introduction of the right to data portability under the GDPR offers an opportunity to gauge the impact of data sharing rules. On one hand, several studies questioned the effectiveness of data portability in fostering market contestability.[27] Others warned against the entrenchment of dominant incumbents data sharing might engender.[28] On the other hand, the benefits of an industry led approach – such as the Data Transfer Project launched by Microsoft, Google, Twitter and Facebook in 2018 to facilitate reciprocal movement of data[29] – appear equally uncertain and tilted in

[20] European Commission (2020), 'Proposal for a Regulation of the European Parliament And of the Council on European data governance' (Data Governance Act) COM/2020/767 final.
[21] See the legislative train schedule of the Data Act.
[22] Interestingly, data access regulations can be regarded as a prominent example of the regulatory power gained by the European Union worldwide. As these reforms are followed by foreign legislators and policy makers, they complement the market-led "Brussels effect", namely the process of unilateral regulatory globalisation caused by the European Union *de facto* (but not necessarily *de jure*) externalising its laws outside its borders through market mechanisms. Cfr. Bradford A. (2020), 'The Brussels effect: How the European Union Rules the World', Oxford University Press.
[23] The White House (July 9, 2021), 'Executive Order on Promoting Competition in the American Economy'.
[24] Australian Government (December 9, 2020), 'Data Availability and Transparency Bill 2020'.
[25] The Consumer Data Right was enacted by the Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth), which inserted a new Part IVD into the Competition and Consumer Act 2010.
[26] Financial Consumer Agency of Canada (2021), 'Open Banking'.
[27] See Batikas M., Bechtold S., Kretschmer T., and Peukert C. (2020), 'European Privacy Law and Global Markets for Data', CEPR Discussion Paper No. 14475. In the same vein, Gal M. and Aviv O. (2020) 'The Competitive Effects of the GDPR', 16 Journal of Competition Law and Economics 3. See also Wing MW L. and Liu X. (2020), 'Does data portability facilitate entry?', 69 International Journal of Industrial Organization, arguing that data portability may hinder switching and entry due to the demand-expansion effect where the prospect of easier switching due to data portability may induce consumers to provide even more data to the incumbent, hence strengthening the incumbency advantage. See also Bessen J., Impink S.M., Reichensperger L., and Seamans R. (2020), 'GDPR and the Importance of Data to AI Startups', Boston University School of Law, Law & Economics Series Paper No. 20-13, evaluating how the GDPR may negatively impact firms that need data to develop.
[28] Geradin D., Karanikioti T. and Katsifis D. (2020), 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech', TILEC Discussion Paper No. 12; and Johnson G. and Shriver S. (2020), 'Privacy & market concentration: Intended & unintended consequences of the GDPR', Working Paper.
[29] See Facebook, Google, Microsoft, and Twitter (2018), 'Data Transfer Project Overview and Fundamentals', White Paper, 4. The four firms announced the launch of a joint open-source initiative called the Data Transfer Project with the objective of easing user data transfer among their platforms. According to their declarations, such a new data portability

favor of big players. Leaving market players free to determine data rules and standards can lead to breaches and abuse, as demonstrated by the Cambridge Analytica scandal.[30]

Finally, one cannot understate the issue of enforceability. Since its launch, the application of GDPR has been mired by circumvention and lack of enforcement,[31] a precedent that does not bide well to the incoming set of additional EU measures in the data-space. While a host of private lawsuits by civil society groups could prod regulators into action, the interconnected nature of the data economy implies extraterritorial enforcement – a measure with geopolitical consequences.

2.2. Lever 2: national security regulations.

Data governance is increasingly recognized as a topic of national security relevance.[32] Preserving sensitive government and military information as well as the physical and logical integrity of the communication infrastructure has long been a core mission of a country's security apparatus. In recent years, however, concerns have been raised with the national security implications of hostile access – legal or otherwise – to sensitive personal information.

In its traditional form, national security issues affect the data governance space through cybersecurity regulation. Novel concerns, conversely, motivate heightened investment screening as well as increased scrutiny over retail personal data collection and handling. This section addresses the impact of these measures on data governance.

First, cybersecurity norms aim at preventing illicit access to information by imposing heightened security requirements on critical infrastructures or entities. While cybersecurity regulation does not discipline data access per se, it recognizes the critical nature of information and the presence of hostile actors. These technical and legal requirements shape a country's data governance landscape by limiting digital operators' ability to rely on certain service providers. In the EU, the 2016 Network Information Security (NIS) Directive[33] identifies digital infrastructure and critical digital service providers (online market places, cloud and online search engines) subject to heightened security requirements. The NIS2 proposal might expand further the perimeter in the digital services space to include the likes of social media platforms data centers.[34] In the financial sector, the Digital Operational Resilience Act (DORA) proposal[35] subjects all critical third party services providers to the financial sector to heightened security standards and regulatory supervision. Crucially, as critical third party services providers are required to establish a business presence within the European

mechanism will remove the infrastructure burden on providers and users related to portability of data from one company to another: "[T]he future of portability will need to be more inclusive, flexible, and open. We believe users should be able to seamlessly and securely transfer their data directly from one provider to another." Even though the project unfolded quite slowly over the years, it is still actively pursued by its proponents. For instance, on 30 July 2019, Apple announced that it will be joining the project, allowing data portability in iCloud. Moreover, on 2 December 2019, Facebook announced the ability for users to transfer photos and videos to Google Photos, originally available only in a select few countries.

[30] Polański P.P. (2018), 'Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal', 7 Journal of European Consumer and Market Law 141.

[31] Lancieri F. (Forthcoming 2022) 'Narrowing Data Protection's Enforcement Gap', 74 Maine Law Review, Issue 1.

[32] Slaughter M.J. and McCormick D.H. (May/June 2021), 'Data Is Power. Washington Needs to Craft New Rules for the Digital Age', Foreign Affairs.

[33] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194.

[34] European Commission (2020), 'Proposal for directive on measures for high common level of cybersecurity across the Union Proposal for directive on measures for high common level of cybersecurity across the Union'.

[35] European Commission (2020), 'Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM/2020/595 final'.

Union' territory in order to serve the financial sector, the regulation bans data flows towards nonresident operators.

Second, foreign investment screening in critical sectors is a well-established practice to ensure national security objectives. The scope of investment screening regulation, however, has recently seen a substantial expansion in recognition of the strategic importance of personal information.

In the US, the 2018 Foreign Investment Risk Review Modernization Act (FIRRMA) extended the definition of *screenable* transactions to foreign investments yielding non-controlling stakes on sensitive personal data of United States citizens that may be exploited in a manner that threatens national security. This includes identifiable (or re-identifiable) personal data regarding financial conditions, insurance, private communication, geolocation, health, biometric information, government and security status, and genetic test results. With the exception of genetic test results, transactions in these data-categories are considered relevant when they involve specific populations (such as security or government personnel) or more than one million US citizens.

In the EU, the 2019 FDI screening Regulation, which sets out a procedure for investment screening coordination within the common market, includes transactions involving access to sensitive information, including personal data, within a specific *screenable* activity. Given the broad definition of personal data under the GDPR, the set appears particularly broad.[36] In practice and as an example, concerns over the treatment of sensitive personal data appear to have prompted the Italian Government to apply its investment screening powers to a transaction involving the acquisition of a minority stake in the payment company Satispay on part of Chinese behemoth Tencent.[37]

Third, concerns have been raised with the national security implications of hostile-yet-legal access to sensitive personal data. These constitute the logical extension of the concerns over safety and integrity of the communication infrastructure that led the US and several allied countries to ban Huawei (and sometimes ZTE) components from their telecom infrastructure. Whereas concerns with Huawei contemplated the risk of mass espionage through network control, the same risks apply to app-enabled retail data collection.

Although national security issues arising from the activity of hostile retail apps have yet to result in specific regulations, this appears in the works. In the US, for instance, they resulted in the August 2020 Trump administration Executive Orders banning Chinese Apps TikTok and WeChat. The bans never effectively entered into force as they were stayed in first-circuit court,[38] and subsequently withdrawn by the Biden administration for reformulation. Their language is nonetheless instructive, and (as shown in the subsequent paragraph) the concern they spell out appears still present in the current Administration.

According to the Executive orders: "*the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States. […] TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such*

[36] GDPR, art. 4(1): "A*ny information relating to an identified […] natural person [or a] natural person […] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*",

[37] Bechis F. (2021), 'Cina e fintech, golden power su Tencent. Cosa c'è dietro', Formiche.net. Satispay S.p.A. is an Italian company that controls the Luxemburg registered Payment institute Satispay Europe SA

[38] See https://www.ft.com/content/cf02c37f-a46f-4fb0-a7ae-3c21c20fbdd6 and https://www.ft.com/content/84c73841-ef42-4d97-8a6e-b7d02d5fda20

as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[39] And, "*Like TikTok, WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information.*"[40]

The Biden administration followed a more institutional approach by withdrawing the outright bans and ordered a major assessment of concerns related to hostile apps. Specifically, and in line with Trump Executive Orders, the June 9, 2021 Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, recognizes that the increased use of apps developed by foreign adversaries, including China, threatens the national security, foreign policy, and economy of the United States. Thus, the new order mandates a thorough evaluation of the threat and the assessment of policy options, which is expected for the last quarter of 2021.

2.3. Lever 3: competition policy.

Due to the dominant role that digital platforms play in the digital economy, data governance issues are interrelated with their business conducts and often undistinguishable from platform governance. Digital platforms are the "market makers" of the digital economy, shaping its governance through business decisions. In disciplining anti-competitive behaviour of digital operators, allowing or denying mergers of digital businesses – and thus of datasets – and imposing remedial actions such as fines, divestments and commitment decisions, competition law enforcement plays a critical, albeit unrecognized role, in defining a country's data governance framework.

This section explores recent developments in competition regulations and its impact on data governance frameworks.

The rise of digital markets poses structural questions for competition policy. Digital markets are characterized by network effects, economies of scale and scope, and cross-sectoral spill-overs. Taken together, these generate barriers to entry that make digital markets not easily contestable, prone to tipping, and highly concentrated.

Digital platforms, in their twin role of market makers and market participants, are the crux of the problem. In the digital environment, platforms operate the marketplace while they provide their own products and services in competition with rival sellers. Unlike other market participants, they also act as private regulators (they set the market's rules) and gatekeepers (they control market participant's access to their clients or their clients' behavioural data). This conflation of roles is likely to entrench their dominant position, shielding them from effective competitive pressures.

Traditional antitrust struggles to keep up. Timely application of antitrust law is crucial to ensure healthy competitive dynamics. However, traditional ex-post antitrust enforcement proved unfit to tackle the challenges generated by rapidly changing digital markets. Competition investigations are lengthy processes, often unable to address structural market problems. By the time an infringement is condemned, and remedies imposed, the firm at stake is likely to have already monopolized the target market. When this happens, the antitrust toolkit is unable to restore the conditions existing before the infringement. The seven-year-long European Google Shopping investigation provides a

[39] Trump D.J. (Ausgust 6, 2020), 'Executive Order on Addressing the Threat Posed by TikTok'.
[40] Trump D.J. (Ausgust 6, 2020), 'Executive Order on Addressing the Threat Posed by WeChat'.

good example of how complex and burdensome the competitive assessment can be when it comes to some practices performed by vertically integrated platforms.[41]

Also preventive antitrust action, in the form of merger control, struggles to cope with the challenges posed by the data economy. In theory, merger scrutiny represents a major tool to address structural competitive problems. Nonetheless, it is widely acknowledged that competition authorities have under-enforced antitrust rules in the digital environment.[42] Over the last five years, tech giants have been probed for engaging in "killer acquisitions" and erecting barriers by creating "digital conglomerates". Despite such concerns, very few of the mergers in question have faced scrutiny by competition agencies, or were successfully challenged by private plaintiffs and public agencies in the EU and US.

Under most merger control frameworks, enforcers are often expected to apply traditional business metrics to the digital environment. The main metric for guiding merger control regimes is turnover rather than more relevant ones, like the amount paid by the acquirer. As many digital start-ups provide their services free of charge, they generate low revenues while retaining a substantial economic value in terms of user knowledge, user data or network effects. Good examples were the $1 billion acquisition in 2012 of Instagram by Facebook and the acquisition in 2013 of the Israeli mapping services provider Waze by Google for $1.3 billion. Similarly, the $19 billion acquisition of WhatsApp (a company with a turnover of around ten million dollars) by Facebook was reviewed by the EC only based on a specific request by Facebook in order to benefit from the one-stop-shop review provided by the European Commission.[43] None of these transactions would have attracted merger scrutiny at the EU level under current law.

Across the world, policy makers are considering options to overhaul competition law to make it fit for the new digital era. Options span from lowering legal standards and the evidentiary burdens faced by public agencies, to a wide range of ex-ante prohibition or obligations[44] that sidestep traditional case-by-case economic analysis. Revamped merger control also plays a central role, for example, in proposals for the overhaul of European competition.[45]

Calls for revamped antitrust or tailored platform regulation however hold digital economy wide consequences. Two instances provide a sense of the impact of recent, or perspective regulation.

---

[41] European Commission, Case AT.39740 (2017), Google Search (shopping).

[42] Walker M. (2020), 'Competition policy and digital platforms: six uncontroversial propositions', 16 European Competition Journal 1.

[43] Article 4(5) of the EU Merger Regulation (EUMR).

[44] Austrian Competition Authority (2020), 'Digitalisation and Competition Law – Position Paper', 10; European Commission (2020) 'New Competition Tool', Inception Impact Assessment, 3, stating that the aim of the proposal for a new competition tool is to fill enforcement gaps in the current antitrust rules by expanding the toolkit in order to address anticompetitive behaviours that standard antitrust analysis would strive to tackle; U.S. House of representatives (2020), 'Investigation of competition in digital markets, majority staff reports and recommendations' (Subcommittee on antitrust, commercial, and administrative law), 392. Conversely, a remarkable exception is represented by the common position of G7 competition authorities and, apparently, by the report prepared for the European Commission. According to this view, the challenging issues raised by digital markets can be successfully addressed with existing toolkits since antitrust ensures a flexible framework and a fact-based, cross-sectoral and technology-neutral analysis. See: G7 Competition Authorities (2019) 'Common Understanding on Competition and the Digital Economy'; Crémer J., de Montjoye Y.-A., and Schweitzer H. (2019) 'Competition policy for the digital era', Report for the European Commission.

[45] Germany, for instance, has already introduced a new jurisdictional €400 million threshold based on the value of the transaction rather than the turnover of target companies. Motta M., Peitz M., (2019) 'Challenges for EU Merger Control', CRC TR 224 Discussion Paper Series (University of Bonn and University of Mannheim, Germany); Gautier A., Lamesch J. (2020), 'Mergers in the Digital Economy', CESifo Working Paper Series 8056.

The first instance is one where reforms that aggressively target large platforms take limited consideration of the diversity in platforms' business model. The European Commission's infringement decision against Google in 2018 provides an example. In 2018 the Commission issued a $5.1 billion fine to the firm for abuse of its dominant position with reference to its mobile operating system Android,[46] mandating Google to unbundle Google Play Store, Google Search App and Google Chrome from the operating system. The injunction – currently challenged at the European Court of justice – would force a major change in Google's business model. Simply put, mobile operating systems follow two different business models. Google's business method is hinged on an open platform that generate revenues through targeted advertisement. Apple's model, conversely, is based on a closed environment, that generates revenue through the sale of mobile devices.

The second instance relates to tailored regulatory interventions aimed at constraining platform's business freedom. There is a growing consensus that competition enforcement should be supplemented by tailored regulation. Notably, the European Commission released in December 2020 a proposal of a new regulation (the Digital Market Act) under which firms considered as gatekeepers would be prevented from engaging in a wide ranging of self-preferencing conducts.[47] On April 7, 2021 the UK the Government established a Digital Market Unit (DMU) within the CMA that will be tasked with overseeing a new regulatory regime for platforms deemed to have "strategic market status".[48] Similarly, Germany in January 2021 amended its Competition Act to better protect competition in times of digitization. The new law empowers the Bundeskartellamt, with a competition instrument meant to address large digital platforms' behaviors.[49] Finally, in June 2021, the U.S. House of Representatives has unveiled a five-bill antitrust package designed to curb the market power of large online platforms representing "critical trading partners."[50]

Due to the alleged inability of traditional competition law enforcement to address competitive distortions in digital markets, these regulatory proposals depart from the experience and lessons developed by antitrust legal systems over the years with an inevitable impact on digital platforms' business model. Limitations on self-preferencing included in the Digital Market Act (DMA) proposal constitute a remarkable example of such new regulatory approach to competition policy.[51] A substantial fraction of the disputes involving digital platforms stem from their degree of vertical integration, with the corresponding incentive to favor their own activities. Yet, vertical integration is not by itself detrimental to competition. To the contrary, vertical integration has been found to increase consumer welfare and foster competition in many instances.[52] Leaving aside the complexities

[46] European Commission, Case AT.40099, Google Android (July 18, 2018). According to the Commission, Google engaged in the following illegal conducts: (1) tying Google's search and browser apps, (2) illegal payments to device manufacturers and mobile network operators conditional on exclusive pre-installation of Google Search; and, (3) illegal obstruction of development and distribution of competing Android operating systems.

[47] The proposal is currently pending for approval by the European Parliament and the Council.

[48] As recommended by the UK Digital Competition Expert Panel (2019), 'Unlocking digital competition', 5.

[49] Jens-Uwe Franck, Martin Peitz (2021) Taming Big Tech: What Can We Expect from Germany's New Antitrust Tool?, Oxford Business Law Blog.

[50] See H.R. 3816, 'American Innovation and Choice Online Act'; H.R. 3825, 'Ending Platform Monopolies Act'; H.R. 3826, 'Platform Competition and Opportunity Act'; H.R. 3843, 'Merger Filing Fee Modernization Act', and H.R. 3849, 'Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act'.

[51] European Commission (2020) 'Proposal for regulation on contestable and fair markets in the digital sector (Digital Markets Act)'.

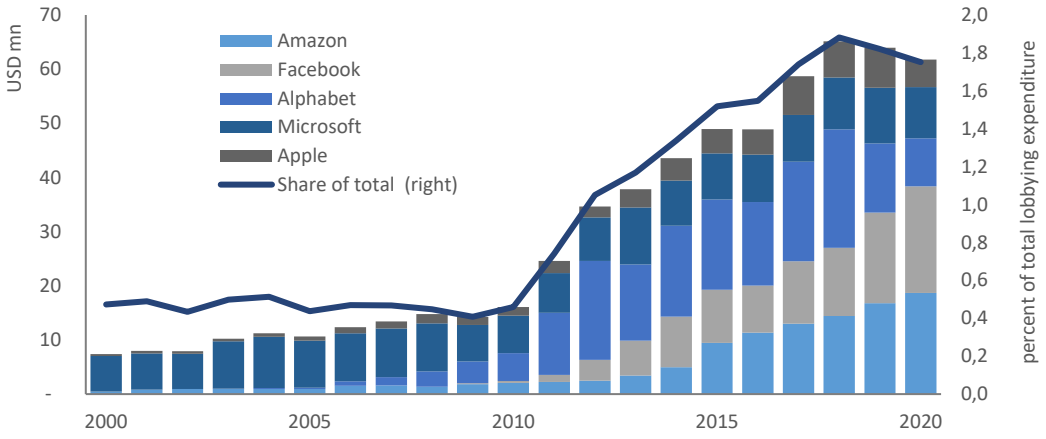
[52] This is acknowledged by the Commission in its Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2008] OJ C265/6. Fumagalli C., Motta M., Calcagno C. (2018) 'Exclusionary Practices. The Economics of Monopolisation and Abuse of Dominance', Cambridge University Press, p. 480.

of economic analysis, mandating an overarching neutrality obligation on gatekeepers might simplify the work of antitrust agencies, but it could as well hinder the benefits of competition and innovation.

Both instances demonstrate the large, if indirect, impact that antitrust policy can have on a country's data governance framework. In the first instance, forcing Google to adopt a more closed ecosystem (similar to Apple's) would send an economy-wide signal against certain types of open data-intensive business models. In the second instance, restrictive ex-ante regulation might calcify (or permanently disband) existing business models, with a lasting impact on innovation dynamics within the platform economy.

Finally, as regulation is rarely shaped by cost-benefit analysis alone, it is important to keep in check the two factors of broad influence in the re-shaping of competition policy. The first is the agenda of digital platforms. Platforms count amongst the most lavish lobbyists, on both sides of the Atlantic, and wield therefore margins of influence on the legislative process. Lobbying expenditure on part of digital platforms has increased substantially over the years in the US, both in absolute and relative terms (Fig. 1). In the EU Google and Microsoft class as the top two in lobbying expenditure since 2017, while Facebook ranked fourth in 2020.[53] The second is the (geo)political role that platforms play in the global race for digital supremacy, discussed in section 3.3.

Fig. 2: Platform lobbying expenditure in the US



Source: author's elaboration from www.opensecrets.org[54]

3. Overlaps and trade-offs.

This discussion has thus far dealt with the data governance implication of three major, yet separate, strands of regulation. To complete it, we need to discuss the most apparent overlaps and trade-offs among these strands regulations.

This section proceeds in this sense. Section 3.1 addresses overlaps and trade-offs between competition and data protection, section 3.2 between data access and national security and section 3.3 between national security and competition.

[53] Author's extrapolation from https://lobbyfacts.eu/

[54] OpenSecrets is a Nonpartisan, independent and nonprofit, research group that tracks money in U.S. politics and its effect on elections and public policy

3.1. Competition and Data Protection.

The regimes of competition and data protection have developed in silos for the last 20 years. Their respective rules and principles have thus been applied irrespective and in isolation of each other. According to the traditional "law and economics" approach, data protection together with consumer law tackle information asymmetries and behavioural weaknesses of individuals whereas antitrust law focuses on anti-competitive practices (such as cartels and abuse of monopoly power).

This clear separation hardly applies in the context of the digital economy, where information asymmetries are intertwined with competitive dynamics. As the conduct of firms in digital ecosystems has blurred the boundaries between legal fields, antitrust has increasingly crossed the path of data protection. Indeed, several scholars argue that there is room to apply data protection and competition regimes in a more coherent way to better protect consumer welfare.[55]

The digital economy differs from its physical counterpart in that the "relevant locus of competition" is often product quality rather than mere price. A healthy competitive environment should therefore see competition take also place in terms of privacy-related quality of services. In this sense, data protection should be regarded as a non-price parameter of quality, allowing consumer choice over their optimal level of data protection.[56] It follows that antitrust enforcers should pay attention not only to prices and innovation dynamics, but also to the effective level of privacy granted to consumers. Sound antitrust enforcement should therefore be able to tackle anti-competitive practices based on data exploitation.[57]

Competition in the privacy-space might already be visible in the market. The recent Facebook-Apple spat regarding the introduction of privacy friendly default options on Apple devices provides a clear example. In April 2021, Apple announced that the new version of its operating system would have a default option denying access to certain types of user information, used (among others) by Facebook to provide targeted advertising.[58] While Facebook publicly complained of Apple's purportedly anti-competitive behaviour, observers hailed Apple's decision as the result of healthy competition in the privacy-space.[59] To Facebook's credit, concerns that Apple's behaviour might serve to its own advantage led the European Commission to make clear that privacy policies must not give preferential treatment to a provider's apps over those of its competitors. On the same issue, the French antitrust authority has recently rejected the request for interim measures against Apple's adoption of the App

[55] Graef I., Clifford D., Valcke P. (2018), 'Fairness and enforcement: bridging competition, data protection, and consumer law', 8 International Data Privacy Law 3; Botta M., Weidemann K. (2020), 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: the Regulatory Dilemma in the Facebook Odyssey', 64 The Antitrust Bulletin 3.

[56] At the Subcommittee's oversight hearing in November 2019, Makan Delrahim, the Assistant Attorney General of the Justice Department's Antitrust Division, testified that because privacy is a dimension of quality, protecting competition "can have an impact on privacy and data protection.", Antitrust Agencies Hearing at 15 (statement of Makan Delahim, Assistant Attorney General, United States Dep't of Justice Antitrust Div.), 56.

[57] Kuner C., Cate F.H., Millard C. et al. (2014), 'When Two Worlds Collide: The Interface Between Competition Law And Data Protection', 4(4) International Data Privacy Law 247, 247.

[58] Financial Times (26 April 2021), 'How Apple's iOS 14.5 update is shaking up the app economy'.

[59] Facebook complained that Apple is using its "*dominant market position to self-preference their own data collection while making it nearly impossible for their competitors to use the same data*". Financial Times, 'Apple and Facebook trade accusations over data privacy'; Also the Germany's largest media, tech and advertising companies have accused Apple of antitrust abuse, see Financial Times (26 April 2021), 'German groups file Apple antitrust complaint as it makes privacy changes'. Langhe B., Puntoni S. (2021), 'Facebook's Misleading Campaign Against Apple's Privacy Policy', Harvard Business Review.

Tracking Transparency (ATT) framework for applications on iOS 14, which creates new consent and notification requirements for app publishers.[60]

Market authorities have already started to work across regulatory borders. The antitrust investigation of the Bundeskartellamt (German competition authority) against Facebook in 2016, constitutes the first attempt to integrate privacy interests into an abuse investigation.[61] Taking data protection law as a benchmark for evaluating exploitative behaviour under competition law, the Bundeskartellamt reached the view that Facebook's collection and use of data from third-party sources is an antitrust violation with serious exclusionary effects on competitors. According to the Bundeskartellamt, Facebook would have achieved an unlawful competitive advantage vis-a-vis users and competitors by imposing terms of service in violation of European data protection law. As a result, the social platform was able to entrench its dominant position in the market for social media and consolidate its influence on advertising markets. The decision is currently litigated in the Dussendorf court, which has recently decided to refer questions for preliminary ruling to the European Court of Justice.[62]

There are also signs that data protection parameters can be integrated into merger control analysis. In the 2014 Facebook/WhatsApp merger clearance, the European Commission noted that security and privacy were one of the many parameters of competition applicable to the case, along with the user base, price, perceived trendiness, and the reliability of the communications service.[63] The merger was nonetheless allowed because Facebook and WhatsApp were not considered as close competitors and consumers would have continued to have a wide choice of alternative communications apps after the transaction.[64] Conversely, in the 2016 clearance of the Microsoft/LinkedIn merger, the European Commission required Microsoft to enter in addition a number of commitments to avoid that the market for professional social networks would tip in favour of LinkedIn ultimately marginalizing competitors offering a greater degree of privacy protection than LinkedIn.[65] More recently, the European Commission cleared the acquisition of FitBit by Google despite several economists publicly calling for the Commission to block the transaction.[66] They worried that the merger would have allowed Google becoming dominant in 'health tech' markets, uniquely combining its existing data with the information gathered from Fitbit thereby undermining the ability of rivals to compete.[67]

From a welfare perspective, the integration of data protection principles into competition enforcement is a welcome development.[68] As competitive dynamics within the digital economy show, antitrust problems are intertwined with information and behavioural imbalances between firms and consumers. A separate application of the two disciplines might therefore lead to suboptimal enforcement

[60] Autorité de la concurrence, 'Decision 21-D-07 of 17 March 2021 regarding a request for interim measures submitted by the associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, and Syndicat des Régies Internet in the sector of advertising on mobile apps on iOS', (2021).
[61] Bundeskartellamt (2 March 2016) Press Release.
[62] Botta M., Weidemann K. (2020), 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: the Regulatory Dilemma in the Facebook Odyssey', 64 The Antitrust Bulletin 3.
[63] European Commission (3 October 2014), Case No COMP/M.7217, Facebook/WhatsApp, paras 87–90.
[64] European Commission (3 October 2014), Press Release. Following the WhatsApp's updates to its terms of service in August 2016 allowing the possibility of linking WhatsApp users' phone numbers with Facebook users' identities, the European Commission imposed as 110 million euro on Facebook for providing misleading information during the merger investigation. European Commission (18 May 2017), Press Release.
[65] Consequently, Microsoft entered into a number of commitments to address the competition concerns in the market for professional social networks that were also linked to the impact on privacy as a non-price parameter of competition.
[66] Borreau M. et al. (2020), 'Google/Fitbit will monetise health data and harm consumers', CEPR Policy Insight No 107; See Régibeau P. (2020), 'Why I agree with the Google-Fitbit decision', Voxeu, for an opposite view, arguing: "If combining data in a manner that leads to more discrimination in the health market is undesirable, then why use merger review to prevent such combinations from Google only? Regulation would be far superior in that it would at least preserve a level playing field."
[67] Caffara C., Ryan J. (2021), 'The antitrust orthodoxy is blind to real data harms', Voxeu.
[68] Stucke M. and Grunes A. (2016), 'Big Data and Competition Policy', (Oxford University Press), p. 82.

decisions.[69] Prioritizing economic efficiency over data protection might exacerbate the market failures the two practices are supposed to tackle.[70]

Coordination between competition and data or consumer protection authorities appears therefore necessary within the digital space. An example of this is the recent joint statement of the UK's Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA) setting out their shared views on the relationship between competition and data protection in the digital economy.[71]

Coordination is needed as frameworks regulating third party data collection, access, use and retention have a direct impact on the competitive landscape. Lack of data governance frameworks during the early days of the digital economy – when user metadata was considered an industrial byproduct – enabled and fostered digital disruption. Fast forwarding to present days, the same data governance frameworks, recognizing unbridled exploitation rights to data custodians, cement oligopolistic positions in the digital economy.

3.2. National Security and Data Protection.

As data protection regulations set forth the conditions and safeguards under which personal information can be processed, they inevitably interact with countries' national security structures. Data protection regulation allow the creation of large data pools which are often exploited by national or foreign security services, or by malicious actors. Excessive, unjustified or malicious exploitation of personal data often sparks conflicts between individual rights and national security prerogative, both within and between jurisdictions.

The conflict between the national security and the individual rights is particularly evident between the US and the EU. Such tensions is epitomized in the recent Schrems II decision, whereby the Court of Justice of the EU (CJEU) struck down the European Commission's EU-US data protection equivalence decision which served as legal basis for most of the transatlantic data transfers.

Since the September 2001 attack on the Twin Towers, the world experienced a marked increase in security screening, particularly with respect to digital communication. In this context, data protection regulation shifted, on both sides of the Atlantic, from economic, to security actors – from DG Internal Markets to security structures and interior ministries in the EU and from the Department of Commerce to Homeland Security and Treasury in the US – resulting in vast increase in cross-border security related arrangements,[72] such as the SWIFT agreements. [73]

As the Snowden revelations shed light on US mass surveillance operations, however, the pendulum started swinging back. According to Edward Snowden, under section 702 of the Foreign Intelligence Surveillance Act (FISA), US security agencies gained warrantless access to private data from Facebook, Google, Apple, Microsoft, and five other major platforms under a secrete programme

[69] Jin G.Z., Wagman L. (2020), 'Big data at the crossroads of antitrust and consumer protection', 54 Information Economics and Policy, 20.
[70] Lynskey O. (2018), 'Non-price Effects of Mergers – Note', OECD DAF/COMP/WD, 70.
[71] UK Competition and Market Authority (2021) Press Release.
[72] Zalnieriute M. (Forthcoming 2022), 'Transfers after Schrems II: the EU-US Disagreements over data Privacy and national Security', 55(1) Vanderbilt Journal of Transnational Law 35.
[73] In July 2010, the European Parliament approved a five-year agreement with the U.S. for the transfer of financial and other information collected by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to the U.S. the SWIFT information exchange. Such systems have been used for national security purposes more regularly and significantly since 9/11. For instance, in 2006, US authorities including the CIA attempted to gain access to SWIFT for terrorist finance tracing. In 2013, it was reported that the NSA intercepted and retained data transmitted via SWIFT.

called PRISM.[74] Private lawsuits, led by privacy activist Max Schrems, contested the US Government unbridled access to Facebook data as in violation of GDPR rights. The judicial process that followed led the CJEU to invalidate two EU-US data protection equivalence decisions known as *safe harbor* (struck down in 2015)[75] and *privacy shied* (struck down in 2020) [76].

In its ruling, the CJEU held that the US does not provide for an *essentially equivalent*, and therefore sufficient, level of protection as guaranteed by the European data protection legislation. Notably, the judges pointed out that the legal bases of US surveillance programmes such as PRISM and UPSTREAM[77] amount to a disproportionate interference with the rights to protection of data and privacy enshrined in article 45(1) of the GDPR. In its very essence, the US legal framework does not limit in a sufficient manner the powers conferred upon US authorities and lack actionable rights for EU subjects against US authorities.

These landmark judgments are at the cross road of data protection and national security. In the shifting balance between conflicting policy objectives, the CJEU asserted the primacy of fundamental principles of human dignity and freedom over (foreign) national security prerogatives. The ruling also came in the context of increasing scrutiny of security-related transfers.[78] In the US the ruling was harshly criticized as an EU legislative overreach into US security interests. Officials were reportedly mesmerized at the thought that citizens of one country should have the right to review their intelligence files from other countries. The ruling was also deemed unjust as the CJEU has examined the national security practice of the US while it is precluded from doing so in EU member states.[79]

The two Schrems rulings might have lasting impact on the global data governance framework. While transatlantic data transfers are still permitted, their legal basis has become substantially less certain. The issue appears compounded by the implementation of the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, which amends the US Stored Communications Act to give US courts access to data held by US subjects outside of US territories. While the October 2021 G7 Digital Trade Principles spell a political wish to overcome the differences across the two sides of the Atlantic, achieving actual convergence might not be so straightforward. Finally, the rulings will most likely impact data transfers between the EU and other jurisdictions, such as China, where government access to privately held data sanctioned by the 2017 cybersecurity law appears in equal, if not starker, conflict with EU principles. Scrutiny in this sense might stem from a recent complaint against Huawei's data transfers in a German court.[80]

---

[74] PRISM is a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies.

[75] CJEU, 6 October 2015, Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner of Ireland*.

[76] CJEU, 16 July 2020, Case C-311/18, *Data Protection Commissioner of Ireland v. Maximillian Schrems.* The second case arose as US surveillance law was not significantly changed following the invalidation of the Safe Harbour in *Schrems I*.

[77] UPSTREAM collection is a term used by the National Security Agency (NSA) of the United States for intercepting telephone and Internet traffic from the Internet backbone, i.e. major Internet cables and switches, both domestic and foreign.

[78] On 27 July 2017 the CJEU declared that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data could not be concluded in its current form. The provisions would have allowed systematic and continuous transfer of PNR data of all air passengers to a Canadian authority with a view to that data being used and retained, and possibly transferred subsequently to other authorities and to other non-member countries, for the purpose of combating terrorism and forms of serious transnational crime. The Court established that the envisaged agreement interfered with the fundamental right to respect for private life as well as the fundamental right to the protection of personal data. CJEU, Grand Chamber, Opinion 1/15 of the Court, OJ C 138 (2017).

[79] Swire P. (2020), 'Schrems II' backs the European legal regime into a corner — How can it get out?', IAPP.

[80] Politico (2020), 'Huawei data flows under fire in German court case'.

While much of the discussion in this section has focused on the degree of legally sanctioned access that national or foreign security services might have to personal data, it is important to point out that malicious operations also take place outside, or at the limits of national and international norms. The 2016 Cambridge Analytica scandal, whereby lax security standards on part of Facebook led to the leak of detailed psychometric user profiles, constitutes an eminent example of the risks of subversion[81] that derive from malicious access to personal data.

3.3. Competition and National Security.

Given the rich information content intermediated, and their role as critical infrastructures, digital platforms have increasingly acquired relevance in the national security sphere, much like the financial sector and other forms of physical infrastructures.

Since antitrust action pursues the objective to preserve innovation and contestability within digital markets, sometimes it might clash with the overarching interest of national states to preserve their security apparatus as well as their means of international power projection. While conflicts of this sort can and do emerge in other sectors of the economy, the size and pervasiveness of the digital economy, coupled with the increasing weaponization of cyberspace make this trade-off particularly thorny.

Against this backdrop, it comes as no surprise that antitrust discussions involving the digital economy will increasingly have to weigh the national security consequences of limiting platforms' business freedom against the risk of shielding them from antitrust scrutiny.

Over the last decade, digital platforms have been targeted by antitrust investigations for killer acquisitions, self-preferencing and other forms of abuse of dominance. For such violations, competition law contemplates fairly extreme remedies, including break-ups. Indeed, proposals of structural interventions have gained momentum in the US over the last five years among policy makers and scholars. The recent appointment of Lia Khan as Chairperson of the Federal Trade Commission and of Tim Wu as special assistant to the US president for technology and competition policy at the National Security Council – both vocal critics of Big Tech's market power – is a clear sign that the Biden administration is open to radical options.

Antitrust ambitions, however, are set to clash with national security considerations. In the United States, both the intelligence and the military rely on private tech companies – for hardware, information and talent alike. From a security perspective, these firms' market power and scale constitute irreplaceable strategic assets.

Two examples might put the issue in the right perspective. First, as pointed out in section 2.2, the Foreign Intelligence Surveillance Act (FISA) compels American firms to hand over data on suspected foreign agents. US intelligence agencies rely extensively on this legal tool to gather information. FISA court orders constituted the basis the PRISM dragnet. Second, as the US Defense Department needed to build an enormous cloud project (under the name of Joint Enterprise Defence Infrastructure Cloud), aimed at supporting its operations, it was only able to identify two viable bidders: Microsoft and Amazon. Only these two massive companies could provide the resources needed to establish the needed hardened data centres with the right analytical skills. Although the contract – awarded to

[81] Kastner J., Wohlforth W.C. (July/August 2021), 'A Measure Short of War', Foreign Affairs.

Microsoft – has recently been recalled, [82] it is unlikely that firms outside the limited US Big Tech circle might have the capabilities and the US government's trust to deliver on similar projects.

According to this line of argument, dominant firms should be shielded from antitrust enforcement. Market dominance can finance the innovation that guarantees the US military and intelligence cutting edge capabilities. Further, should antitrust action curtail platforms' innovative prowess, foreign competitors such as Baidu or Alibaba, would stand to benefit, to the advantage of US strategic adversaries.

The Qualcomm antitrust case serves a material example of this antitrust conundrum. In 2019 the Department of Justice (DoJ) intervened in appeal, asking the Ninth Circuit to stay the Federal Trade Commission's injunction against Qualcomm for abusing its dominant position as a supplier of semiconductor devices to the detriment of cell phone manufacturers and direct competitors, claiming that it "would significantly impact U.S. national security".[83] According to the DoJ, such action would have hampered Qualcomm's ability to invest in R&D, ultimately reducing America's potential to lead the global race in 5G. In 2020, the Ninth Circuit overturned the District Court's decision, implicitly recognizing also the national security argument against Chinese competitive pressure.[84]

The influence of wider public interests other than consumer welfare on antitrust enforcement however is far from uncontroversial.[85] It has been argued that national security may actually benefit from a more vigorous antitrust enforcement in the digital economy.[86] First, as private sector agents, platforms work in foreign markets and are therefore subject to incentives and blackmail that could backfire against their own country national security policy. Second, their anticompetitive behaviour might ultimately crush innovation, thereby eroding rather than sustaining the US' strategic advantage.

4. Conclusion.

The rise of digitalization, and the opportunities and risks that it engenders has sparked an increasingly lively debate on the rules that should govern the digital sphere. Data governance remains however a fuzzy concept, whose discussion is limited to selected policy circles. The reasons behind this phenomenon lie both in the complexity of the phenomenon and in its political load. For starters, no individual regulation disciplines the subject in a comprehensive fashion, while several regulatory actions try to tackle adjacent (but interrelated) problems. To follow, a limited number of extremely large and heterogeneous firms – digital platforms – hold critical roles within the digital space. Regulation of digital platforms is a highly political endeavor, both domestically and internationally.

By means of sweeping simplification, three major regulatory fields appear critical in shaping a country's data governance framework: data control, national security and competition policy. Data control regulations defines the rules for access, use and re-use of data. National security regulation determines (the increasingly broad) set of data-types and uses which are off-limits. Competition regulation sanctions the behavior and business practice of the digital "market makers". These legislative strands have a profound impact on the digital economy and substantial degrees of overlap

[82] US Department of Defense (July 6, 2021), 'Future of the Joint Enterprise Defense Infrastructure Cloud Contract'.
[83] US Department of Justice (2019), 'Statement of Interest Concerning Qualcomm's Motion for Partial Stay of Injunction Pending Appeal', 1.
[84] FTC v. Qualcomm Inc., 969 F.3d 974 (9th Cir. 2020).
[85] Phillips J. - FTC Commissioner (2020), 'The Role of National Security in Antitrust Enforcement'.
[86] Sitaraman G. (2020), 'The National Security Case for Breaking Up Big Tech', Vanderbilt Law Research Paper No. 20-18; O'Keefe C. (2020), 'How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents', Technical Report, Centre for the Governance of AI at the University of Oxford.

with each other: tinkering with elements of one regulation, often leads to unintended effects in others' domain.

This piece discussed the role that each of these regulatory levers play, and the complex web of overlaps and trade-offs that exist when they apply to the digital sphere with the aim of supporting policy maker and regulators in understanding the key levers under the fuzzy hood of data governance.

The analysis in this paper leads to three main conclusions.

First, regulation of the digital space suffers from an extreme degree of complexity. Multiple and diverse regulatory domains intersect the digital space, with overlapping and sometimes unpredictable consequences. As regulators strive to "put order" in their digital corner, it appears particularly important that this complexity is factored in.

Second, given the trans-national nature of digital activity, coordination and dialogue can hardly be confined to a set of national regulators. However, while a set of internationally agreed principles for the regulation of the digital sector would appear necessary, this seems a complex task for very broad-based the G20 and WTO negotiations. Convergence might instead be found within smaller groups of like-minded countries. At the end of October 2021, Trade Ministers of G7 countries issued a set of commonly agreed Digital Trade Principles, pledging to work towards a common framework for cross-border data transfers, and limiting the use of data-localization measures for protectionist purposes. These principles constitute a first step towards overcoming structural differences within the block of advanced economies.

Third, the definition of the global data governance framework has important consequences for the financial sector, and its regulators. Finance, more than other sectors, is a data-centric business. Financial regulators should therefore take active part in national and international discussions.

Given the pervasive nature of digitalization, the approach presented in this note could be considered as a blueprint to expand the analysis to additional policy levers, such as digital taxation and content liability rules.

References.

Acquisti A., Taylor C., and Wagman L. (2016), 'The economics of privacy', 54 Journal of Economic Literature 2, 442–492

Article 29 Data Protection Working Party (2013), 'Opinion 03/2013 on purpose limitation'

Australian Government (December 9, 2020), 'Data Availability and Transparency Bill 2020'

Austrian Competition Authority (2020), 'Digitalisation and Competition Law – Position Paper'

Bertin M., Duch-Brown N. (2020), 'The economics of business-to-government data sharing' (JRC Technical Report)

Biancotti C., Borgogno O., Veronese G. (2021) 'Principled data access: building public-private data partnerships for better official statistics,' QEF Banca d'Italia 629

Borgogno O., Colangelo G. (2020), 'Data, Innovation and Competition in Finance: The Case of the Access to Account Rule', European Business Law Review 31, no. 4 (2020): 573-610

Batikas M., Bechtold S., Kretschmer T., and Peukert C. (2020), 'European Privacy Law and Global Markets for Data', CEPR Discussion Paper No. 14475

Bechis F. (2021), 'Cina e fintech, golden power su Tencent. Cosa c'è dietro', Formiche.net

Bessen J., Impink S.M., Reichensperger L., and Seamans R. (2020), 'GDPR and the Importance of Data to AI Startups', Boston University School of Law, Law & Economics Series Paper No. 20-13

Borreau M. et al. (2020), 'Google/Fitbit will monetise health data and harm consumers', CEPR Policy Insight No 107

Botta M., Weidemann K. (2020), 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: the Regulatory Dilemma in the Facebook Odyssey', 64 The Antitrust Bulletin 3

Bradford A. (2020), 'The Brussels effect: How the European Union Rules the World', Oxford University Press

Caffara C., Ryan J. (2021), 'The antitrust orthodoxy is blind to real data harms', Voxeu

Crémer J., de Montjoye Y.-A., and Schweitzer H. (2019) 'Competition policy for the digital era', Report for the European Commission

De Hert P., Papakonstantinou V., Malgieri G., Baslay L. and Sanchez I. (2018), 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', 34 Computer Law and Security Review 193

European Commission, 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018', (Communication) COM (2018) 43 final

Fumagalli C., Motta M., Calcagno C. (2018) 'Exclusionary Practices. The Economics of Monopolisation and Abuse of Dominance', Cambridge University Press

Graef I., Clifford D., Valcke P. (2018), 'Fairness and enforcement: bridging competition, data protection, and consumer law', 8 International Data Privacy Law 3

European Commission (2020), 'Proposal for a Regulation of the European Parliament And of the Council on European data governance' (Data Governance Act) COM/2020/767 final

European Commission (2020) 'New Competition Tool', Inception Impact Assessment

European Commission (2020) 'Proposal for regulation on contestable and fair markets in the digital sector (Digital Markets Act)'

Facebook, Google, Microsoft, and Twitter (2018), 'Data Transfer Project Overview and Fundamentals', White Paper

Financial Consumer Agency of Canada (2021), 'Open Banking'

Gal M. and Aviv O. (2020) 'The Competitive Effects of the GDPR', 16 Journal of Competition Law and Economics 3

Gautier A., Lamesch J. (2020), 'Mergers in the Digital Economy', CESifo Working Paper Series 8056

Geradin D., Karanikioti T. and Katsifis D. (2020), 'GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech', TILEC Discussion Paper No. 12

G7 Competition Authorities (2019) 'Common Understanding on Competition and the Digital Economy'

High-Level Expert Group on Business-to-Government Data Sharing (2020), 'Towards a European strategy on business-to-government data sharing for the public interest'

Jens-Uwe Franck, Martin Peitz (2021) Taming Big Tech: What Can We Expect from Germany's New Antitrust Tool?, Oxford Business Law Blog

Jin G.Z., Wagman L. (2020), 'Big data at the crossroads of antitrust and consumer protection', 54 Information Economics and Policy, 20

Johnson G. and Shriver S. (2020), 'Privacy & market concentration: Intended & unintended consequences of the GDPR', Working Paper

Kastner J., Wohlforth W.C. (July/August 2021), 'A Measure Short of War', Foreign Affairs

Kuner C., Cate F.H., Millard C. et al. (2014), 'When Two Worlds Collide: The Interface Between Competition Law And Data Protection', 4(4) International Data Privacy Law 247

Lancieri F. (Forthcoming 2022) 'Narrowing Data Protection's Enforcement Gap', 74 Maine Law Review, Issue 1

Langhe B., Puntoni S. (2021), 'Facebook's Misleading Campaign Against Apple's Privacy Policy', Harvard Business Review

Lynskey O. (2018), 'Non-price Effects of Mergers – Note', OECD DAF/COMP/WD, 70

Motta M., Peitz M., (2019) 'Challenges for EU Merger Control', CRC TR 224 Discussion Paper Series (University of Bonn and University of Mannheim, Germany)

OECD (2019), 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies', OECD Publishing

O'Keefe C. (2020), 'How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents', Technical Report, Centre for the Governance of AI at the University of Oxford

Phillips J. - FTC Commissioner (2020), 'The Role of National Security in Antitrust Enforcement'

Polańsky P.P. (2018), 'Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal', 7 Journal of European Consumer and Market Law 141

Régibeau P. (2020), 'Why I agree with the Google-Fitbit decision', Voxeu.

Slaughter M.J. and McCormick D.H. (May/June 2021), 'Data Is Power. Washington Needs to Craft New Rules for the Digital Age', Foreign Affairs

Stucke M. and Grunes A. (2016), 'Big Data and Competition Policy', (Oxford University Press)

Swire P. (2020), 'Schrems II' backs the European legal regime into a corner — How can it get out?', IAPP

The White House (July 9, 2021), 'Executive Order on Promoting Competition in the American Economy'

U.S. House of representatives (2020), 'Investigation of competition in digital markets, majority staff reports and recommendations' (Subcommittee on antitrust, commercial, and administrative law)

US Department of Defense (July 6, 2021), 'Future of the Joint Enterprise Defense Infrastructure Cloud Contract'

US Department of Justice (2019), 'Statement of Interest Concerning Qualcomm's Motion for Partial Stay of Injunction Pending Appeal', 1

Walker M. (2020), 'Competition policy and digital platforms: six uncontroversial propositions', 16 European Competition Journal 1

Wing MW L. and Liu X. (2020), 'Does data portability facilitate entry?', 69 International Journal of Industrial Organization

Zalnieriute M. (Forthcoming 2022), 'Transfers after Schrems II: the EU-US Disagreements over data Privacy and national Security', 55(1) Vanderbilt Journal of Transnational Law 35