Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The battle of power: Enforcing data protection law against companies holding data power

Tuulia Karjalainen

Faculty of Law, University of Helsinki, P.O. Box 64, 00014, Finland

ARTICLE INFO

Keywords:
Data protection
Privacy
Data power
Platforms

ABSTRACT

The EU General Data Protection Regulation (2016/679, GDPR) was enacted to regulate digital platforms who process excessive amounts of personal data and dominate today's online markets. However, the Regulation has not fully succeeded in meeting this goal. This article argues that effective regulation of digital platforms should be based on understanding the data power these companies hold. Data power, stemming from control over personal data, weakens monetary sanctions due to the monopolistic position digital platforms have obtained by data processing, reduces accountability and democratic control over data processing practices, and limits individual control over one's own data. This power sets digital platforms apart from other companies and calls for sector-specific data protection rules for the platform industry.

Introduction

A small number of platforms who process excessive amount of personal data control today's online market. It is often argued that the dominant role of these data monopolies has led to a decrease in privacy, and dysfunctional competition.[1] Therefore, finding effective remedies against data power is topical in both legal scholarship and world politics.

Data power can be defined as power exercised by digital platforms that stems over their control of data flows.[2] These platforms provide free services to consumers but build their business on the user personal data that they collect and sell to other companies for targeted advertising.[3] That the data power companies hold an unprecedented kind of power is widely accepted.[4] Due to the fast development of these businesses during the early 2000s, the legislator has not been able to address all the challenges related to them. Different ways to regulate data power have been widely discussed in legal research, but to date there is little agreement. In competition law, the dominant market position of these data monopolies

E-mail address: tuulia.karjalainen@helsinki.fi

[1] Wolfgang Kerber, Digital markets, data, and privacy: competition law, consumer law and data protection (2016) 11 *Journal of Intellectual Property Law & Practice* 856, 859; and Marco Botta and Klaus Wiedemann, The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey (2019) 64 *The Antitrust Bulletin* 428, 444.

[2] Orla Lynskey, Grappling with "Data Power": Normative Nudges from Data Protection and Privacy (2019) *Theoretical Inquiries L.* 189, 196.

[3] Beatriz Kira, Vikram Sinha and Sharmadha Srinivasan, Regulating digital ecosystems: bridging the gap between competition policy and data protection (2021) 30 *Industrial and Corporate Change* 1337, 1340.

[4] See, for example, José van Dijck, David Nieborg, and Thomas Poell, Reframing platform power (2019) 8 *Internet Policy Review*; European Data Protection Board Statement of the EDPB on the Data Protection Impacts of Economic Concentration 27 August 2018 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf>; and Lynskey op. cit. (n 2).

https://doi.org/10.1016/j.clsr.2022.105742

has been discussed in terms of market power, unfair competition, and merger control.[5] In data protection law, the introduction of the EU General Data Protection Regulation (2016/679, GDPR) in 2016 was meant to target these companies through enhanced data subject rights, increased accountability, and considerable fines. However, the GDPR has not fully reached this goal.

In this article, I argue that in order to find effective data protection remedies against digital platforms we need to identify and understand the power these companies hold in contemporary societies. Understanding that power also helps to identify the problems that regulatory measures should target. I approach data power in context of European data protection law drawing concrete examples on the effects of power to different regulatory approaches. The main contribution of this paper is towards creating a more comprehensive understanding about the role of data power in the society and identifying the challenges this power poses to enforcement.

The article is structured as follows: The second chapter presents the main characteristics of data power and its effects. Next, I will identify core consequences of the power in terms of data protection law, namely dominance over data, limitations to individual control over their own data, and effects on enforcement and democracy. Last, I will discuss alternative regulatory models and suggest that sector-specific data protection rules taking data power into account might be the solution for the platform industry.

About data power and platforms

Many forms of platform power

Platform power has been widely debated in recent years, and the role of platforms has been addressed from many different angles. In this chapter, I will take an overview of some of these approaches. Digital platforms, or platform companies, are companies that create digital communities and marketplaces for interaction and transaction.[6] The concept of a platform is not unanimously defined but most descriptions share the idea of the platforms using digital technology to interact between users and suppliers.[7] Sometimes these platforms are also called data monopolies, and usually include at least Google, Facebook, Microsoft, Apple, and Amazon.[8]

The platforms have created new kinds of economic models and disrupted traditional markets in many ways. This is why the role and the effects of digital platforms has been the subject of passionate political debate in recent years. While platforms can be observed from many interesting viewpoints, in this paper I concentrate on the discourses around the power these platforms hold. The notion of power is central to distinguishing these companies from more traditional economic actors, and also to analyzing their regulation.[9] Platform power has been conceptualized in many different ways, for example power based on data, infrastructural effects of platforms, and their role as gatekeepers. While these concepts start from slightly different premises, they all share a core idea of the platforms having power that sets them apart from other companies, and their extensive personal data processing being a primary source of this power.

First, data power is a term defined by Orla Lynskey as "*a multifaceted form of power available to digital platforms, arising from their control over data flows*".[10] The concept of data power underlines this control over data as *power*. The main factor of data power is the omnipresence of a platform in the digital environment, providing it with access to large volumes of data from different applications.[11] Approaching these platforms as holders of data power underlines that the processing of data is not problematic as such but the power arising from the data volume and variety can be.[12] The concept and existence of data power also emphasizes the power disparity between companies.[13]

The platform companies are also considered to have so-called gatekeeping power. The position of these companies in the online market makes them gatekeepers of information flows between different users of the platform, such as consumers, content providers, and advertisers. The gatekeepers are able to collect information about their users and get competitive advantage from the volume and variety of data they then employ for advertising.[14] The gatekeeping power manifests itself as control of access not only to individual services but to the ecosystem as a whole.[15] Similarly to the concept of data power, gatekeeping power underlines the volume of platform data processing, ability to combine data from different sources, and the use of this data to control access to products and services.

Also the consequences of power have been analyzed from different viewpoints. Digital platform power has been viewed as soft policy power that allows the platforms to participate and influence public and policy discourses,[16] media power through which they can control the content visible to users, affecting the public opinion,[17] and what is called "search engine manipulation effect", commonly abbreviated as SEME, referring to the power to affect public opinion through search results that are seen as neutral and objective.[18] Also these aspects of power have their origin in the data processing. However, they emphasize the consequences of power.

[5] Maria Wasastjerna, *Competition, Data and Privacy in the Digital Economy : Towards a Privacy Dimension in Competition Policy?* (Kluwer Law International 2020) 85-90.

[6] Joost Rietveld and Melissa A Schilling, Platform Competition: A Systematic and Interdisciplinary Review of the Literature (2021) 47 Journal of management 1528, 1529.

[7] Martin Kenney and John Zysman, The Rise of the Platform Economy (2016) 32 *Issues in science and technology* 61–69, 65.

[8] These companies are also sometimes referred with the acronym GAFAM, or FAAMG.

[9] van Dijk, Nieborg & Poell op. cit. (n 4) 3.

[10] Lynskey op. cit. (n 2) 199.

[11] Lynskey op. cit. (n 2) 198.

[12] Lynskey op. cit. (n 2) 212.

[13] Lynskey op. cit. (n 2) 196-198.

[14] ibid.

[15] van Dijk, Nieborg & Poell op. cit. (n 4) 7.

[16] Lynskey op. cit. (n 2) 192.

[17] ibid.

[18] Robert Epstein and Ronald E. Robertson, The Search Engine Manipulation Effect (SEME) and its Possible Impact on the Outcomes of Elections (2015) 112 *Proc. Nat'l. Acad. Sci.* E4512.

The power stemming from data processing to politics, media, and public opinion indicate that platform power has an infrastructural nature in our society. This infrastructural power extends beyond power of individual platforms over certain market segments. The concept of infrastructural power refers to the platforms operating in conjunction and arises from the role of platforms as gatekeepers.[19] It affects politics and society beyond monopolistic market power.[20] Alike the other power concepts, the infrastructural power stems from the platforms' ability to combine data from multiple sources due to the large number of services each of them offers, and the lack of transparency to these connections.[21] The concept of infrastructural power acknowledges elements of both data power and gatekeeping power. What the approach contributes to them is an emphasis on these companies working in conjunction.[22] Platform power is not a feature of a single company but a characteristic of an entire ecosystem.

While the power of digital platforms has been conceptualized in many ways, these approaches have a common understanding of two things. First, digital platforms have power. Second, this power originates from their personal data processing. Each of the approaches presented above provide a different viewpoint to the power of digital platforms, allowing different kinds of discussions. In this paper, I mainly use the term data power in order to underline the connection of platform regulation and data protection law. Data processing is one defining feature of the platforms and the main factor in producing their power.[23] Data protection laws target that cornerstone of the platform economy. Understanding the different power dynamics that characterize the digital platform environment provide useful tools to identify legal problems and solutions and to analyze the effectiveness of different regulatory interventions in the field.

Current debates about platforms and data power

Data power may detrimentally affect the competition between companies and also be harmful to individuals subject to the power.[24] For this reason, regulation of platforms has been subject to active political and academic discussion in the EU in recent years. Digital platforms have been subject to investigations by supervisory authorities, the most well-known cases being perhaps the German Bundeskartellamt's competition decisions on Facebook[25] and French CNIL's data protection sanctions on Google.[26] Also, the European Court of Justice has issued multiple decisions against platforms.[27] Politically, the European Commission' Digital Services Act package, meant to upgrade the rules governing digital services, recently reached political agreement.[28] Many academic publications have also been dedicated to the topic.[29]

One concrete attempt to target data power was the introduction of the EU General Data Protection Regulation in 2016. Although the GDPR applies to all data processing regardless of size, one important motivation behind the Regulation was restricting the extensive online personal data processing conducted by platforms.[30] The GDPR has now been applied for four years, and some conclusions can be drawn about its effectiveness against data power. The relationship between data power and data protection law is interesting because processing of personal data seems to be one of the core factors affecting on the development of data power. Data protection law, and the GDPR in particular, restrict this processing creating a clear tension between the law and power.

In many ways, data protection law is at odds with the data processing practices of platforms. Their big data and targeted advertising-based business model is often difficult to align with the GDPR's requirements of pre-determined processing purposes and full transparency.[31] At the moment, it is possible to argue that the data power does not fully comply with the EU data protection framework especially when it comes to data minimization, necessity of data processing, validity of consents, and transparency – all these being features that, properly implemented, considerably limit the amount of available data. Since data power builds on the quantity and precision of available personal data, privacy-enhancing practices that potentially reduce the amount of data threaten the dominant position of data power companies.[32]

These effects to competing markets and individual privacy are an important motivation to find effective remedies against data power companies. However, the law and its enforcement attempts have not always proven effective. I suggest that these

[19] van Dijk, Nieborg & Poell op. cit. (n 4) 8-9.
[20] ibid.
[21] van Dijk, Nieborg & Poell op. cit. (n 4) 7-8.
[22] ibid.
[23] van Dijk, Nieborg & Poell op. cit. (n 4) 3.
[24] Lynskey op. cit. (n 2) 197.
[25] Bundeskartellamt 6th division decision B6-22/16 on 6 February 2019.
[26] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC; Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED; see also decision about data transfers in Google Analytics of 10 February 2022 (the decision was only published in an anonymized form at <https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf>).
[27] See, for example, cases Wirtschaftsakademie C-210/16, Schrems C-311/18, and Fashion ID C-40/17.
[28] European Commission, Europe fit for the Digital Age: Commission proposes new rules for digital platforms, Press release 15 December 2021 < https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347>; European Commission, Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets, Press release 25 March 2022 <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1978>.
[29] About academic discussion on platforms, see for example Rietveld and Schilling op. cit. (n 6).
[30] European Commission 'Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation' published 24 May 2018 STATEMENT/18/3889 <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889>.
[31] Viktor Mayer-Schönberger and Kenneth Cukier '*Big Data : A Revolution That Will Transform How We Live, Work, and Think*' (First Mariner Books 2015) 173-174.
[32] Samson Y. Esayas, Competition in (Data) Privacy: 'Zero'-Price Markets, Market Power, and the Role of Competition Law (2018) 8 *International Data Privacy Law* 8, 187.

challenges are due to a lack of understanding of the *power* these platforms hold.

While there seems to be some kind of agreement that the platforms are powerful, it seems an equally accepted fact that they provide useful services. Therefore the main challenge in regulating data power is to identify and target the negative consequences of power. The concept of data power helps to underline what sets the platforms apart from other companies: the power stemming from access to personal data. Understanding how the power functions in terms of regulation therefore allows us to target the rules better to the negative consequences.

In this article, I focus on the efforts to regulate data power by data protection law because the structural incompatibilities of personal data protection and large-scale data processing provide an interesting basis for analysis. I will start by looking into the effectiveness of some measures the GDPR targets data power with. This assessment helps us better understand the effects power has on regulation attempts.

The effects of data power on data protection

Monopoly over data and knowledge

In the previous chapter we concluded that extensive processing of personal data is common for all concepts conceptualizing platform power. This chapter will looks into how the power stemming from extensive processing affects the regulatory approaches adopted in the GDPR.

Digital platforms typically build their business on the processing of personal data. Their services rely on personalization and profiling conducted based on data from users' behavior collected on their services and across the internet.[33] Many platform services are also free for consumers but financed by advertising targeted based on highly detailed user profiles created from their behavioral data.[34] Another thing typical to digital platforms is that they provide multiple services and can combine data between them. For example, recently rebranded Meta, former Facebook, owns Facebook, Messenger, Instagram and WhatsApp. This extensive collection of personal data provides data power companies with substantial amounts of information and knowledge. These companies probably have access to more data than any other actor does in the contemporary society, and they have means to process that data to obtain information about the data subjects.[35] This access to massive amounts of data is one of the defining characteristics of data power and one of the most significant factors that produce the power.

Another typical feature of the platform ecosystem is that the data and processing capacity lie with a small number of private actors. The platform companies have access to knowledge and information that no other actors do. This gives data power control over knowledge production and the external disclosure of this knowledge. When no other actors than platforms have access to similar amounts of data and processing power, information about the nature of the data, and, more importantly, the conclusions drawn on it, is not publicly available. The monopoly over data comes with the authority to decide what information is worth learning, and who will have access to learn it.[36] Because only a handful of operators have access to this information, and each of them only parts of it, the rest of society becomes dependent on them, both for the free, valuable services, and for the processing of that information for other purposes too.[37] The concentration of this power to only a few private companies constitutes a fundamental and extraordinary change in the traditional division of learning in an information society.[38] In addition, the automated decision-making about what consequences are drawn from the data and who gets to see it makes the processing opaque and also subject to weaker democratic control and public oversight than human power over information resources.[39]

Besides informational power, the monopoly over data processing also produces economic and financial power for the platform companies. Large-scale data processing has made the platforms some of the biggest organizations globally. For example, Amazon ranks the 2nd largest in the world in terms of revenue, Apple 3rd, and Alphabet (Google) 9th.[40] The direct connection between data processing and profit creates an important incentive for the platforms to continue data processing, and a challenge for data protection enforcement if the lucrative processing does not comply with the law.[41] Monetary sanctions alone may not sufficiently incentivize compliance if the fines are not proportional to the potential financial gains of non-compliance.

The GDPR provides for maximum sanctions of 20 million euro or up to 4% of the company's global annual turnover (GDPR Article 83.6). During the first three years after the GDPR took effect, the platforms have already been subject to supervisory inspections and the first fines have been issued. At the time of writing (July 2022) the biggest sanctions have been issued to Amazon in Luxembourg (746 MEUR), WhatsApp in Ireland (225 MEUR), and Google in France (50 MEUR). However, many of these sanctions are being appealed and are therefore not final. While the GDPR allows for other measures, such as the prohibition of processing (article 58.2), these measures have not yet been used against the platforms on a large scale.

Balancing sanctions with the potential financial gains of data processing has been one of the issues with the GDPR enforcement so far. The GDPR might not sufficiently incentivize

[33] Viktoria H.S.E. Robertson, Excessive data collection: Privacy considerations and abuse of dominance in the era of big data (2020) 57 *Common Market Law Review* 161, 163.

[34] ibid.

[35] Lynskey op. cit. (n 2) 197.

[36] Shoshana Zuboff, The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power (Profile Books 2019) 192.

[37] Zuboff op. cit. (n 36) 341-344.

[38] Zuboff op. cit. (n 36) 180. However, it is worth noting that the questions about access to and power over information resources and learning, or concentration of this power to a limited number of actors, are not new. For example, in a traditional society the learning has been a privilege of the religious or academic actors.

[39] Frank Pasquale, *The Black Box Society: the Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 61.

[40] Fortune 500 list of 2021, available at: <https://fortune.com/fortune500/2021>.

[41] Esayas op. cit. (n 32) 187.

data power to comply with its provisions if compliance requires abandoning or decreasing the targeted advertising that currently finances the services.[42] To put it another way, fines should be substantial enough to counterweigh the large profits, and strong enforcement is needed to ensure that compliance becomes profitable. Due to the economic power of the platforms and the high profits they make by processing data, fines are not necessarily an effective remedy against them, especially if their amounts remain low.

The size of data power companies also imposes special requirements on the authorities supervising them. The supervisory authorities are being criticized for insufficient resources and weak enforcement, sometimes even by their peers.[43] The biggest challenges arguably lie with the Irish Data Protection Commissioner who acts as a lead supervisory authority of Google, Facebook, Microsoft, and Apple.[44] Supervision of platform companies requires considerable resources and expertise from the authorities. However, lack of transparency can make obtaining sufficient information about data processing operations challenging.[45] In addition, the platforms have considerable legal resources to argue their cases and to contest decisions.

The GDPR attempts to solve the imbalance of resources between supervisors and their targets through accountability and a risk-based approach to data protection. In most cases, the Regulation does not set forth detailed instructions but rather high-level objectives. The practical measures required for an appropriate and adequate level of data protection are then determined case by case based on the risks related to processing.[46] This approach imposes the responsibility to know the details of the data processing and conduct any necessary risk assessments on the companies processing the data, who should prove accountable for their actions.[47] At the same time, risk-based data protection has been criticized especially in the platform context for entrusting companies with too much responsibility and control over their own compliance.[48] Furthermore, risk-based approach intends to facilitate the work of authorities but it may also complicate supervision by setting the agenda on the adequacy of risk assessment instead of the sufficiency of protection of individuals.[49]

The strong correlation between data processing and financial gains is one of the core challenges to platform regulation. The size and resources of the platforms imposes challenges on enforcement and, consequently, effectiveness of data protection law. To conclude, the monopoly over data processing is one of the main factors contributing to data power. Furthermore, data processing is also extremely profitable for the platforms, who have become some of the biggest companies on the planet. The scope of data processing conducted by digital platforms and the data power they hold makes their supervision challenging. At the same time, accountability and self-regulatory approaches may prove problematic due to the high financial interests for data processing. Furthermore, the lack of transparency into data power processing practices complicates monitoring data power further but it also affects the relationship between data power and individuals.

Impact on individual behavior

One important tool the GDPR adopts to protect personal data is the enhanced control of individuals over their own data. The idea of individual control is a longstanding approach to data protection relying on the data subject's free and informed choice to disclose their data for processing.[50]

Nevertheless, the control-based approach is ill-suited to data power for two reasons. First, the amount of online data processing is overwhelming, and an average individual is unlikely to understand and exercise choice over the processing of their data in various platform services.[51] Second, the power of the platforms as gatekeepers and somewhat essential service providers does not necessarily allow individuals to make free choices in the fear of social exclusion.[52] Today, many platforms justify the unrestricted availability of data as prioritizing quality of service over data protection, or even as a devaluation of privacy by consumers.[53] However, even if individuals were willing to trade their privacy for better services to some

[42] Esayas op. cit. (n 32) 188.

[43] For example, Germany's Federal Data Protection Commissioner publicly criticized his Irish counterpart on inefficiency, see Derek Scally, German regulator says Irish data protection commission is being 'overwhelmed, *Irish Times* 3 February 2020 <https://www.irishtimes.com/business/financial-services/german-regulator-says-irish-data-protection-commission-is-being-overwhelmed-1.4159494>.

[44] Under the GDPR art. 56 the lead supervisory authority is the data protection authority of the country where the company has its main establishment in the EU. The lead authority supervises the company on the entire EU area. Currently 4/5 GAFAM companies are headquartered in Ireland with the exception of Luxembourg-based Amazon.

[45] Maria Eduarda Gonçalves, The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward (2017) 26 *Information & Communications Technology Law* 90, 101.

[46] Lachlan Urquhart, Tom Lodge, and Andy Crabtree, Demonstrably Doing Accountability in the Internet of Things (2019) 27 *International Journal of Law and Information Technology* 7, 7.

[47] Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation (2016) 7 *J Intell Prop Info Tech & Elec Com L* 271, para 43.

[48] ibid.

[49] Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach (2018) 9 *European Journal of Risk Regulation* 502, 518.

[50] Helen Nissenbaum, A Contextual Approach to Privacy Online' (2011) 140 *Daedalus* 32, 34; and Attila Kiss and Gergely László Szöke, Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation in Gutwirth S., Leenes R., de Hert P. (eds.) *Reforming European Data Protection Law*. Springer 2015, 318.

[51] Brendan Van Alsenoy, Eleni Kosta and Jos Dumortiera, Privacy notices versus informational self-determination: Minding the gap (2014) 28 *International Review of Law, Computers & Technology* 185, 190; Woodrow Harzog, The Case Against Idealising Control (2018) *EDPL* 423, 426.

[52] Gordon Hull, Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data (2015) 17 *Ethics Inf Technol* 89, 94.

[53] Esayas op. cit. (n 32) 183. See also Facebook's CEO Mark Zuckerberg who announced in a 2010 speech that "Privacy is no longer a social norm". For example: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

extent, there are behavioral factors that prevent them from acting on their privacy concerns and demanding better data protection. The most important element reducing demand for privacy is the existence of information asymmetry between the individuals and companies: The individuals do not know how their data is processed and what risks the processing entails.[54] For example, privacy policies are often notoriously hard to understand.[55]

This *Privacy Paradox* refers to research findings showing that even individuals who are aware of their rights and consider them important rarely use them. This phenomenon is often explained by uncertainty making the individuals easily nudged towards more lenient data protection settings.[56] Certain characteristics of data power reinforce the *Privacy Paradox* and reduce individuals' ability to freely express control over their own data. To start with, the way digital platforms process data is often opaque and lacks transparency. Digital platforms often collect and process users' behavioural data collected from their online interactions in order to target and personalize content.[57] This big data is processed in connection with large-scale predictive analytics used to detect patterns and trends in human behavior.[58] The processing is based on the principle of collecting all available data without prior selection and then analysing it to find useful correlations.[59] The approach makes it difficult to communicate the extent and details of data processing in public, since the purposes and means of processing are not necessarily known beforehand.[60]

Furthermore, many platforms have been hesitant to disclose the extent and details of their data processing in public for reasons of business secrecy.[61] This lack of information essentially means that even the most capable individuals are not able to obtain sufficient knowledge about the processing to make informed choices about it. The opaqueness and lack of transparency contribute to data power and even constitute an essential element of it. The lack of transparency can hinder supervision, thus protecting the source of data and enabling continuity of current surveillance practices.[62] One more explanation for the secrecy is the gap between the data processing and the cultural understanding of privacy.[63] In other words, the details of the processing are kept secret in the fear of the public not approving them.

Data power also hinders individual control in a more subtle manner. The power establishes itself in relation to the individuals in a way that makes it seem a natural feature of the internet, and free services funded with behavioral advertising a standard business model. This process of social surveillance determines normal and desirable behavior that the subjects reproduce.[64] The consequence of unacceptable behavior is social exclusion.[65] For example, it can be socially difficult not to use platform services, such as social media or online messaging applications, when everyone else uses them.

Besides individual behavior, data power also affects democracy and the core structures of our society on a more fundamental level.[66] One example of such an effect is the Cambridge Analytica scandal where a British consulting company collected information of up to 87 million Facebook users and used the data mostly to target political advertising during the US Presidential Election 2016 and British Brexit Referendum the same year.[67] The scandal became public through a document leak by a former employee in 2018. In public discourse, the ability to target political advertising on an individual level was considered as interference on election results, and the development of such methods outside of public control and regulation was seen as a threat to democracy. Whether Cambridge Analytica made an innocent business decision to apply targeted advertising in a lucrative field of elections, or whether they interfered into democratic processes for malicious purposes, may not be known, but the scandal showed that platform data processing may extend to unforeseen areas without transparency and public oversight.

The *Privacy Paradox* illustrates the challenges in regulating data power, underlining the fact that attempts to resist power involve complex social factors. The data power manifests in social structures that make acting against the power difficult and unappealing. Consequently, compliance with the power seems an individual choice, based on a rational cost-benefit analysis.[68] Besides individuals, the internalization affects public discourse at large. For example, data power is

[54] Esayas op. cit. (n 32) 189.

[55] See also New York Times 2019 article concluding that Facebook's privacy policy was more difficult to understand than Stephen Hawking's A Brief History of Time, at Kevin Litman-Navarro, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster., *New York Times* 6 December 2019 <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

[56] Susan B. Barnes, A privacy paradox: Social networking in the United States (2006) 11 *First Monday*, URL: <http://firstmonday.org/issues/issue11_9/barnes/index.html>.

[57] Robertson op. cit. (n 33) 163.

[58] Robert Nisbet, Gary Miner and Ken Yale, *Handbook of Statistical Analysis and Data Mining Applications* (Elsevier 2018) 39.

[59] Ira S Rubinstein, Big Data: The End of Privacy or a New Beginning? (2013) 3 *International Data Privacy Law* 74, 78.

[60] Bart van der Sloot and Sascha van Schendel, Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study (2016) 7 *J Intell Prop Info Tech & Elec Com* L 110, 119-120.

[61] Mateusz Grochowski, Agnieszka Jabłonowska, Francesca Lagioia & Giovanni Sartor, Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises (2021) 8 *Critical Analysis of Law*, 46.

[62] Grochowski, Jabłonowska, Lagioia & Sartor op. cit (n 61) 48, 61-62.

[63] Zuboff op. cit. (n 36) 89-91.

[64] Alice Marwick, The Public Domain: Surveillance in Everyday Life (2012) 9 *Surveillance & society*, 378–393.

[65] Reginald Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality* (1999) quoted in John Edward Campbell & Matt Carlson, Panopticon.com: Online Surveillance and the Commodification of Privacy (2002) 46 *Journal of broadcasting & electronic media*, 598.

[66] Robert Epstein, Manipulating Minds: The Power of Search Engines to Influence Votes and Opinions, in Moore, Martin, and Damian Tambini (eds) *Digital Dominance : the Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018), 297-298.

[67] About the Cambridge Analytica scandal, see, for example: The Guardian's Cambridge Analytical files <https://www.theguardian.com/news/series/cambridge-analytica-files>.

[68] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Penguin Books 1977)176-177.

often downplayed as an inevitable functionality of technology, extensive data processing practices as an essential consequence of technical development.[69] Also the GDPR has been blamed for preventing innovation and economic success if the EU, and the fierce lobbying at the time of drafting the Regulation shows its provisions are not meaningless. Furthermore, other political challenges could include effects on employment or tax revenues created by these companies. Against this background, public opinion has an effect on the willingness of politicians to regulate these companies.

Data power affects the regulatory approaches adopted in the GDPR on many levels. The power weakens financial sanctions due to the monopolistic position digital platforms have obtained by extensive data processing, it reduces accountability and democratic control over data processing practices, and it limits individual control over their own data through secrecy and naturalization. It seems fair to conclude that the GDPR may not have found the most efficient means to address platform data processing. The next chapter will consider alternatives for these approaches.

Approaches and challenges to regulating data power

Challenges in regulating digital platforms through general laws

Regulation of platforms by means of data protection has not always been effective. The power these companies hold affect their relationship with individuals, other companies, and the legislator, creating a challenging environment for attempts at regulation. The fiercest criticism towards the GDPR as concerns platform regulation has been the lack of targeting the biggest players, inefficient enforcement, and the imposition of an unreasonable burden for smaller companies subject to similar rules as the big companies. The GDPR obligations are the same for everyone, and they scale mostly based on risk. Combined with a lack of resources in enforcement, the GDPR has not been as efficient at targeting the data power as was likely hoped.[70]

At the same time, the target of regulation is not entirely clear. The platform companies provide many useful products and services that have become essential to modern life. While the powerful position of platform companies is often deemed problematic, the companies and their services as such might still have value. How, then, should we regulate data power? In this chapter, I will consider alternative regulatory models outside data protection and cases where digital platforms have taken steps towards improving data protection, trying to draw lessons on the effects of data power to its regulation.

Besides data protection, regulation of digital platforms has been topical in competition law where the focus is on market effects and unfair business practices. While traditional competition law has not been able to address dysfunctionalities in the markets affected by data power because the data is not explicitly traded, i.e. it does not have direct monetary value, questions about data and privacy have nevertheless gained importance in the field.[71] The traditional separation of competition and data protection law as two distinct fields is losing its meaning, and data protection and privacy are increasingly being considered as parameters of competition assessment.[72] This is logical, since both data protection and competition law aim to target power asymmetries that affect individual welfare.[73] European competition and data protection authorities are cooperating in regulating digital platforms through investigations, for example in the German Bundeskartellamt's investigations of Facebook.[74] While it seems that the tools of one field are not sufficient to regulate the complex effects of power, the goals of competition and data protection law do not always align.

These conflicts are visible in two recent cases where Apple and Google implemented changes to their online advertising systems to improve privacy. Apple's update to its operating system iOS 14 in 2020 allowed users to opt out from many forms of tracking.[75] Most importantly, Apple started to require apps to obtain user consent for tracking across apps and websites, and to use the device's advertising identifier (IDFA).[76] The consent requirement likely reduces the amount of available data, since some users will inevitably refuse. This change can be described as dramatic since the financing models of data power mainly rely on cross-site tracking through online identifiers, and limiting available data reduces the precision of tracking. Therefore, Apple's new strategy could indicate a new direction for data power. However, the decision is also backed with strong economic incentives. Financial Times reports that in six months after introducing the tracking consent, Apple's own market share in targeted advertisements more than tripled.[77] It seems that the change effectively blocked Apple's

[69] Jockum Hildén, *The Politics of Datafication: The influence of lobbyists on the EU's data protection reform and its consequences for the legitimacy of the General Data Protection Regulation* (University of Helsinki 2019) 3.

[70] Lynskey op. cit. (n 2) 210.

[71] Inge Graef, When Data Evolves into Market Power – Data Concentration and Data Abuse under Competition Law, in Moore, Martin, and Damian Tambini (eds.) *Digital Dominance : the Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018) 76.

[72] Wasastjerna op. cit. (n 5) 126-131; See also Maurice E. Stucke and Ariel Ezrachi, When Competition Fails to Optimize Quality: A Look at Search Engines (2017) 18 Yale Journal of Law and Technology; and Esayas op. cit. (n 36).

[73] Francisco Costa-Cabral and Orla Lynskey, Family Ties: The Intersection Between Data Protection and Competition in EU Law (2017) 54 *Common Market Law Review* 20, 9.

[74] Bundeskartellamt decision B6-22/16 op. cit. (n 25).

[75] See, for example, Zack Whittaker, Apple's iOS 14 will give users the option to decline app ad tracking, *TechCrunch* 22 June 2020 <https://techcrunch.com/2020/06/22/apple-ios-14-ad-tracking>; and David Nield, The iOS 14 Privacy and Security Features You Should Know, *Wired* 20 September 2020 <https://www.wired.com/story/ios-14-privacy-security-features>.

[76] See Apple, App Store User Privacy and Data Use for Developers at <https://developer.apple.com/app-store/user-privacy-and-data-use/> accessed 20 October 2020.

[77] Patrick McGee, Apple's privacy changes create windfall for its own advertising business, Financial Times 17 October 2021 <https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d>.

competitors from advertising on Apple devices, leaving the company itself with a larger market share than before.

Besides Apple, Google has also implemented new practices in its online advertising. Google's Privacy Sandbox was announced for the Google Chrome browser in August 2019,[78] and for Android mobile devices in February 2022.[79] Essentially, the Privacy Sandbox aims to remove so-called third-party cookies and similar technologies used for cross-site tracking and to replace them with solutions processing data through the user's browser and device.[80] Moreover, advertising would be targeted based on aggregated cohorts rather than individuals.[81] The Privacy Sandbox effectively makes Google's Chrome browser a gate to online advertising.[82] Just as with Apple, Google's Privacy Sandbox has raised concerns about price discrimination and self-preferencing Google's own services.[83] The UK Competition and Markets Authority (CMA) has investigated the Privacy Sandbox for Chrome due to concerns of these changes being an abuse of dominant position in the web browser market and online advertising.[84] In March 2022, the CMA accepted Google's commitments to restrict the competition effects of the Privacy Sandbox.[85] These commitments include impact assessment criteria, greater transparency, restrictions of user data combination and self-preferencing, and external monitoring.[86]

Initially, the changes Apple and Google implemented indicate compliance with the GDPR's consent requirements, and also general principles about data minimization. Personalized advertising that is based on extensive amounts of data collected from users' online behavior is one of the most criticized practices of digital platforms, and also one of the defining factors of data power. Limitations to these practices could potentially have significant effects on the core features of data power, such as the monopoly over information. However, in these online advertising cases, the platforms' data protection measures also strengthened their positions against competitors by increasing their control over the advertising ecosystem. Consequently, the platform power over their competitors increased, and power over individuals may have increased too.

From a competition perspective, Apple and Google's dominance over the advertising market within their dominant services is not necessarily positive. From a data protection perspective, processing of data by one entity instead of many can have either a positive or negative effect on the protection of individuals. These conflicting effects illustrate the challenges of regulating data power in a manner that takes into account its effects on many areas at once.[87]

Data protection and competition law have addressed different aspects of data power and digital platforms in recent years both together and separately. However, it seems that these measures have not fully managed to address the effects of data power on markets and individuals. One common feature in these attempts is that they address data power by means of general, non-targeted law. These tools, often created to apply to all companies, do not appear to grasp the special nature of digital platforms. For example, the examples about Apple and Google show us is that we can target clearly determined problems, such as giving individuals the right to decide whether their data can be used to target advertisement. However, targeting the spill-over effects can be much more difficult. The infrastructural and autonomous character of data power means that suppressing a part of it does not necessarily limit the power as a whole but rather recreates it in new areas. An answer to these challenges could be to regulate platforms as an industry sector of their own, issuing special rules that acknowledge the unique character of these companies. The EU is already taking first steps in this direction.

Towards industry regulation of digital platforms

The EU is taking another approach by targeting digital platforms as an industry of their own, perhaps as a response to the criticism on the effectiveness of data protection and competition law in targeting platforms. The Digital Services Act package consisting of the Digital Markets Act (DMA) and the Digital Services Act (DSA) is meant to upgrade the rules governing digital services and to ensure fundamental rights and fair competition.[88] The new DMA will specifically regulate platforms, aiming to stop them from relying on unfair conditions to business and consumers.[89] The DMA has been seen as the EU's attempt to regulate digital platforms and will have important implications on digital platforms when adopted.[90] It can be seen as sector-specific competition law although the Regulation expands beyond traditional competition rules.[91]

The DMA covers eight types of so-called core platform services that are gateways between businesses and consumers,

[78] Justin Schuh, Building a more private web, Blog post 22 August 2019, <https://www.blog.google/products/chrome/building-a-more-private-web/>.

[79] Anthony Chavez, Introducing the Privacy Sandbox on Android, blog post 16 February 2022, <https://blog.google/products/android/introducing-privacy-sandbox-android/>.

[80] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, Google as a defacto privacy regulator: analysing the Privacy Sandbox from an antitrust perspective (2021) 17 *European Competition Journal* 617, 651-652.

[81] ibid.

[82] Geradin, Katsifis & Karanikioti op. cit. (n 80) 668.

[83] Oliver Latham, Mikaël Hervé and Romain Bizet, Antitrust concerns in AdTech: formalizing the combined effect of multiple conducts and behaviours (2021) 17 *European Competition Journal* 353, 358-362.

[84] UK Competition and Markets Authority, Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals, Case number 50972 11 February 2022 <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>.

[85] ibid.

[86] ibid.

[87] Geradin, Katsifis & Karanikioti op. cit. (n 80) 675.

[88] European Commission op. cit. (n 28).

[89] European 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.

[90] Pierre Larouche and Alexandre de Streel, The European Digital Markets Act: A Revolution Grounded on Traditions (2021) 12 *Journal of European Competition Law & Practice*, 542.

[91] Pablo Ibáñez Colomo, The Draft Digital Markets Act: A Legal and Institutional Analysis (2021) 12 *Journal of European Competition Law & Practice*, 561-562.

and whose position risks of unfair practices.[92] After the Commission has designated a company as a provider of core platform services, the DMA's obligations to improve consumer control over their data, restrict data combination, limit data collection, promote data access and portability, and increase fairness and transparency will apply. When it comes to data, the DMA provides for interoperability and data portability aimed to prevent lock-in effect and facilitate switching between services.[93] These obligations can be described as self-executing, since the burden of compliance lies with the company.[94] This feature aligns DMA to the GDPR, especially to its obligations on accountability.

While the DMA can be characterized as competition law, it differs from traditional competition law in the sense that it assigns rules to entities defined as gatekeepers regardless of whether they actually misuse this position.[95] In this sense, the DMA can be compared to other industry-specific rules such as those in telecommunications or finance.[96] What sets the DMA apart from other rules applicable to digital platforms is that the Regulation directly addresses only certain companies that are considered to hold data power. After a company has been designated a core platform service provider, there is no additional evaluation of potential misuse of power. This approach may help avoid the current pitfalls of the GDPR when it comes to evaluating the actions of data power. At the same time, the definition of a core platform service might be one of the biggest challenges of the DMA, since the threshold system used to designate gatekeepers may create adverse selection issues incentivizing near-gatekeepers to adapt their business in a manner that keeps them under the threshold.[97]

Even though the GDPR and the DMA address very different aspects of data power, it is interesting to compare their approaches, since the two laws adopt almost opposite means of targeting what they perceive as the most harmful activities. While the GDPR obligations apply to all companies regardless of size, and the balancing of obligations relies on the risks of processing (not the company), the DMA first identifies risky gatekeeper companies and imposes specific obligations on them.[98] The move towards seeing digital platforms as an industrial sector subject to its own specific rules, as indicated by the DMA, could be a step towards a new direction in European platform regulation. However, the DMA being mainly a competition law instrument, it should be considered that also specific data protection laws could apply to digital platforms.

Sector-specific data protection laws already exist, among others, in the telecommunications sector where the so-called ePrivacy Directive (2002/58/EC, EPD) is currently being updated into a Regulation.[99] The EPD complements the GDPR in the telecommunications sector mainly by restricting the possibility of operators to process data for purposes other than conveyance of communication (EDP Articles 5–6). These strict industry-specific rules have been justified by the essential role of teleoperators as gateways to basically all communication and the fundamental rights to confidentiality of communication, data protection, and privacy.[100] It is worth noting that while the ePrivacy rules are being renewed, there has been no serious political discussion about removing the restrictions altogether. Sector-specific data protection rules thus seem to remain important in the era of the GDPR.

A similar approach to the EPD and the DMA, consisting of industry-specific data protection rules, could effectively regulate platform data processing and, as a consequence, restrict data power by affecting data collection. Approaching data power as an industry with characteristics and regulatory needs of its own could help to address the development and reproduction of the power through data. In addition, these industry-specific data protection rules could acknowledge the challenges in individual control and enforcement endemic to a platform setting. While the DMA is a clear step towards this type of regulation, its provisions target the competition and market effects of data power. In data protection, a platform privacy act could address the data protection concerns stemming from data power.

Conclusions

Data power of a small number of platform companies has been a topic of both political and academic debates in recent years. The data processing and the market power of the platforms has been addressed by legal means in competition and data protection law. However, while the need to regulate these companies seems to be widely accepted, the exact goals and purposes of this intervention appear vaguer. In this article, I have argued that to determine appropriate and effective legal remedies for platforms, we should first understand the special power they hold in our society. This power-centric approach helps to identify the problems that regulatory measures should target.

Data power stemming from large-scale processing of personal data is one of the defining features of digital platforms

[92] Filomena Chirico, Digital Markets Act: A Regulatory Perspective (2021) 12 *Journal of European Competition Law & Practice*, 494.
[93] Matthias Leistner, The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer (2021) 16 Journal of Intellectual Property Law & Practice, 780.
[94] Colomo op. cit. (n 98) 574.
[95] Nicolas Petit, The Proposed Digital Markets Act (DMA): A Legal and Policy Review (2021) 12 *Journal of European Competition Law & Practice*, 532.
[96] Chirico op. cit. (n 92) 493.
[97] Petit op. cit. (n 95) 534.
[98] ibid.
[99] In terms of data power, ePrivacy is also an interesting comparison because the applicability of ePrivacy rules to interpersonal communications in non-public networks, i.e. most messaging applications provided by platforms, has been subject to fierce debate over the years. After the European Electronic Communications Code (2018/1972, EECC) took effect in 2020 the EPD also covers communication over private networks, meaning that many platform services are already subject to these rules too. However, when it comes to data power, ePrivacy only applies to the services that consist of interpersonal communications. This leaves many areas of data power out of scope for specific privacy regulation.
[100] European Commission Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final, recitals 1-2.

and distinguishes them from many other companies. Especially when it comes to data protection and privacy, data power imposes unique challenges on regulation due to the unforeseen amounts of data these companies hold. Therefore, digital platforms would merit an industry-specific data protection law of their own, similar to the ePrivacy Directive in the telecommunication sector or the upcoming Digital Markets Act targeting competition issues in the platform market. Since data power is mainly established by processing personal data, a platform privacy act targeting those practices could directly affect the production and development of that power.

While the GDPR is criticized for taking insufficient measures against data power, it is worth underlining that the Regulation has nevertheless increased the importance of data protection in business and public discourse. The political will to regulate data processing and the market effects of the platforms, and citizens raising concerns about privacy, steer data power into a new direction. It seems that we are currently undergoing a cultural shift from a trust in new technologies to a need to regulate them. The platform power developed by private actors is largely motivated by financial gains and mostly remains outside of the legal controls for data processing. That era underlined the possibilities of new technologies and the opportunities a better understanding of human behavior could create for business, politics, and society. However, the unforeseen social and democratic effects of this processing have raised concerns about the lack of public control over these companies. The number of applicable and planned laws targeting platforms seems to indicate that, at least in the EU, attitudes towards big data processing and predictive analytics are changing.

There are also signs of change in data power although it might be too early to identify their direction. The political pressure for transparency and data protection has made the platforms change their operations to an extent. Even though data protection and privacy can be identified as current megatrends, data use and analytics are also of increasing importance. It seems unlikely that large-scale data processing would diminish, but instead legal and political control over the rules and principles of processing may intensify.

It is worth remembering that while data power has negative effects, such as gatekeeping control over infrastructure and relationships, and influence over many social and democratic functions of society, it has also been a productive force both in the technological development of useful services and in creating new spaces for collaboration, communication, and human interaction. The regulation of data power should therefore concentrate on goals and purposes along with effectiveness. We should ask ourselves: what exactly is the problem with data power we want to solve?

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

Acknowledgements

This work was supported by Academy of Finland research project *Is This Public or Private? – A Study of the Philosophical Foundations of European Privacy Regulation*. The author wishes to thank participants of the workshop 'Regulating Digital Markets: Enforcement and Remedies' as well as the two anonymous reviewers of this manuscript for their invaluable comments.