UtrechtLawReview

Data Protection Without Romance: The Power Asymmetries that the GDPR Does Counter

ARTICLE

CHARLOTTE DUCUING

ABSTRACT

A clear and consensual conceptualization of the power asymmetries that data protection seeks to address is missing. That modern bigness translates into multifaceted power issues results in multiple branches of the law being increasingly called upon to respond, illustrated by the recent adoption of the EU digital package. Such an endeavor requires consistency between them and thus also a clear vision of which legal framework addresses which power issue(s) and how. To spin a musical metaphor, for the choir to be harmonious requires that every singer sings their own score. This article unpacks the nature and ways in which data protection addresses power asymmetries through 'data control'. It does it through an enquiry into the conceptual relationship between 'data' and 'control' or power under data protection.

CORRESPONDING AUTHOR:
Charlotte Ducuing
Post-Doctoral research, Centre for IT and IP Law of the KU Leuven (CiTiP), BE
charlotte.ducuing@kuleuven.be

KEYWORDS:
data control; data commodification; data protection; data objectification; modern bigness

TO CITE THIS ARTICLE:
Charlotte Ducuing, 'Data Protection Without Romance: The Power Asymmetries that the GDPR Does Counter' (2025) 21(2) Utrecht Law Review 78–94. DOI: https://doi.org/10.36633/ulr.1124

DOI: 10.36633/ulr.1124

1. INTRODUCTION

That there are power issues in the digital environment is widely agreed upon. The expression 'Big Tech' is often used[1] to refer to companies such as Alphabet, Meta, Amazon and Apple, that have acquired a multifaceted bigness and power over society through technology. Key to this is the power element, which Gerbrandy and Phoa conceptualized as a multifaceted 'modern bigness'.[2] Modern bigness raises serious issues, including the reconfiguration of social relationships through data for profit[3] that structurally favours the dissemination of harmful content and fake news,[4] a detrimental impact on the performance of identity[5] and on the agency and autonomy of individuals through digital addiction and the manipulation of user behaviour.[6] 'Sensory' power,[7] through data-driven surveillance, is often found to discriminate against vulnerable groups. Issues also arise from the ability of Big Tech to build conglomerates or ecosystems[8] and to otherwise take advantage of power asymmetries. This leads to rent-seeking behaviours to the detriment of innovation[9] and of the principle of decentralized economic decision-making that liberal market societies are purported to be premised on. Power is also manifested in the possibility for Big Tech to influence democratic processes[10] and to reshape sectors, including in the public sphere, that are to their own benefit and create new dependencies,[11] generating inequalities. The heightened power of Big Tech goes along with a disempowerment of weaker actors and especially of individuals, broadly referred to as 'power asymmetries', namely the differential power between Big Tech and individuals.

Equally agreed upon is the statement that data protection – and especially the GDPR[12] – aims to counter power asymmetries in the digital environment.[13] This is even considered by some

1 Including by the European Commission. For example, the Impact Assessment of the Data Governance Act proposal includes 15 occurrences (with no definition) of the term 'Big Tech platforms'; see European Commission, Commission Staff Working Document – Impact Assessment Report accompanying the document 'Proposal for a Regulation [...] on European data governance (Data Governance Act), 25.11.2020 SWD(2020), 295 final.

2 A Gerbrandy & P Phoa, 'The Power of Big Tech Corporations as Modern Bigness and a Vocabulary for Shaping Competition Law as Counter-Power' in M Bennett et al. (eds.), *Wealth and Power* (Routledge, 2022), 166–185, s 3. Other conceptualizations have been proposed, such as 'data power', see O Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 *Theoretical Inquiries in Law*, and 'platform power', see D Nieborg et al., 'Introduction to the Special Issue on Locating and Theorising Platform Power' (2024) 13 *Internet Policy Review*, no. 2.

3 S Viljoen, 'An Argument for Positive Political Theories of Data Governance' (2022) 6 *Georgetown Law Technology Review*, 464, 467.

4 N Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8 *Digital Journalism*, no. 6, 842; J Cohen, 'Infrastructuring the Digital Public Sphere', (2023) 25 *Yale Journal of Law & Technology*. Special Issue: The Yale Information Society Project and Yale Journal of Law and Technology Digital Public Sphere Series.

5 B Roessler, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy', in B Roessler & D Mokrosinska *Social dimensions of privacy – Interdisciplinary perspectives* (Cambridge University Press, 2015), 157.

6 P Helm & S Seubert, 'Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies' (2020) 18 *Surveillance & Society*, no. 2, 185.

7 E Isin & E Ruppert, 'The Birth of Sensory Power: How a Pandemic Made It Visible?' (2020) 7(2) *Big Data & Society,* no. 2, 1.

8 M Bourreau & A de Streel, 'Digital Conglomerates and EU Competition Policy' (CERRE 2019) CERRE report <https://www.cerre.eu/news/digital-conglomerates-and-eu-competition-policy> (last visited 25th April 2025); J Crémer et al., 'Competition Policy for the Digital Era' (European Commission, 2019), 108; B Lundqvist, 'Competition and Data Pools' (2018) 7 *Journal of European Consumer and Market Law*, 146.

9 Birch coined the notion of 'parasitic innovation', see K Birch, *Data Enclaves* (Palgrave Macmillan, 2023).

10 P Parvin, 'Hidden in Plain Sight: How Lobby Organisations Undermine Democracy' in *Wealth and Power* (n 2), 229; Cohen (n 4).

11 J Montero & M Finger, 'Platformed! Network Industries and the New Digital Paradigm' (2017) 18 *Competition and Regulation in Network Industries*, nos. 304, 217; K Sabeel Rahman, 'Infrastructural Regulation and the New Utilities' (2018) 35 *Yale Journal on Regulation*, 911; L Taylor, 'Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector' (2021) 34 *Philosophy & Technology*, no. 4, 897; T Sharon & R Gellert, 'Regulating Big Tech Expansionism? Sphere Transgressions and the Limits of Europe's Digital Regulatory Strategy' (2023) 27 *Information, Communication & Society*, no.15, 2651.

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

13 B van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?' (2014) 5 JIPITEC, no. 3, 229, para 2.

authors to constitute the very added-value[14] or even essence or 'core'[15] of the right to data protection, tied to the popular notion of 'data control'. Data protection is thus expected to contribute to countering the detrimental effects of modern bigness, alongside other legal frameworks such as competition law as well as the new Digital Markets Act[16] and Digital Services Act.[17]

Yet, at the same time, many lament that, as a matter of fact, the GDPR has not delivered on such expectations. Nine years after the adoption of the GDPR, the Facebooks and Googles of this world are still alive and kicking. Gal and Aviv showed that, in certain circumstances, the GDPR actually *favours* Big Tech over smaller companies.[18] Data protection is notoriously used as a trump card by Big Tech to shield themselves from other obligations designed to tame bigness, such as data sharing obligations to the benefit of smaller companies.[19] Finally, the lack of empowerment that the GDPR has provided to individuals constitutes the discursive background for the adoption of a new wave of data-related legislation at the level of the EU. In other words, the adoption of EU data legislation is based on the observation that data protection has not countered power asymmetries well or not well enough. Individuals – like smaller companies – would notably be deprived of data use and value while they have contributed to their generation.[20] In this context, the EU aims to empower individuals with data control through the use of, for example, 'personal information management services' (PIMS) or personal 'data spaces'.[21]

Actually, a clear and consensual conceptualization of the power asymmetries that data protection seeks to address is missing. That modern bigness translates into multifaceted power issues results in multiple branches of the law being increasingly called upon to respond, illustrated by the recent adoption of the EU digital package. Such an endeavour requires consistency between those branches of the law and thus also a clear vision of which legal framework addresses which power issue(s) and how.[22] This article unpacks the nature and ways in which data protection addresses power asymmetries through 'data control'. It does it through an enquiry into the conceptual relationship between 'data' and 'control' or power under data protection.

In this context, the present paper explores the following hypotheses. The first hypothesis is that the disappointment as to the attainment of the objectives of data protection by the GDPR is due to over or misplaced expectation as the nature of the power asymmetries that this legislation addresses. The second hypothesis is that a conceptualization of the power asymmetries that

14 O Lynskey, 'Deconstructing Data Protection: The "added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 *International & Comparative Law Quarterly*, no. 3, 569.

15 D Clifford & J Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 *Yearbook of European Law* 130, 144; G Versaci, 'Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection' (2018) 14 *European Review of Contract Law*, no. 4, 374, 391; A Giannopoulou et al., 'Intermediating Data Rights Exercises: The Role of Legal Mandates' (2022) 12 *International Data Privacy Law*, no. 4, 316, 319.

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

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

18 M Gal & O Aviv, 'The Competitive Effects of the GDPR' (2020) 16 *Journal of Competition Law & Economics*, no. 3, 349.

19 A telling example of this is the seeming defence of data protection by BusinessEurope (the European lobby of large companies), in its position paper on the Data Act requiring Big Tech to share data, see Business Europe, Position Paper: The proposal for a Data Act, 01.09.2022, https://www.businesseurope.eu/publications/the-proposal-for-a-data-act-a-businesseurope-position-paper/ (last visited 14 March 2024).

20 Commission, SWD, Impact Assessment accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), SWD/2022/34 final, 2022'.

21 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act or DGA), Rec. 30. The reference to such instruments in the Second Report of the Commission on the application of the GDPR shows how relevant the Commission considers them to be for data protection, European Commission, Communication to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25.7.2024, 17.

22 The consistency of the EU digital package – that they refer to as 'Technology Regulation' – is explored in and throughout the monograph, edited by I Graef & B van der Sloot, see 'The Legal Consistency of Technology Regulation in Europe' (Hart Publishing, 2024).

DOI: 10.36633/ulr.1124

data protection addresses is needed to preserve its specificity and effectiveness. The GDPR seeks to advance fundamental rights while new EU digital legislation pursues also, and mainly, economic goals, namely to allocate data as a resource and to enhance its tradability and thus data-driven growth. This heightens the risk that the lack of clarity surrounding how data protection addresses power asymmetries results in a dilution of the specificity of data protection into such economic goals. A third hypothesis is that the notion of 'data control', because it comes across as unclear and catch-all, should be clarified for that aim. In turn, it also requires the clarification of the nature and function of the fundamental notion of 'personal data' to begin with.

The article proceeds as follows. Section 2 explores the patchwork of the various conceptualizations of data control and clusters them together depending on the nature and function ascribed to (personal) data. The nature and function(s) ascribed to the notion of 'personal data' then form the basis for the conceptualization of the power asymmetries that data protection seeks to address, throughout the article. Section 3 goes back to the basics of data protection and clarifies the nature and function(s) of the notion of personal data, both within and outside the GDPR, and in particular in the digital package of the EU. Section 4 outlines how the legal data protection literature conceptualizes (or does not conceptualize) the power asymmetries that data protection seeks to address. Section 5 turns to the non-legal literature dedicated to the relationship between data and power, which can be found in the field of critical data studies (CDS) and infrastructure studies. The clustering of data-related power asymmetries then serves as an interpretation grid for the conceptualization of the types of power asymmetries that data protection seeks to address (Section 6). Finally, Section 7 concludes with a discussion on how data protection contributes to tackling modern bigness issues, as part of the EU digital package.

2. DATA CONTROL, THE GDPR APPROACH TO COUNTER POWER ASYMMETRIES

The GDPR counters power asymmetries by seeking to enhance data control. Yet, neither the nature nor the function of data control are consensual in the legal literature. This Section identifies the two conceptualizations that come across as most contradictory to one another, in order to identify a (the) bone of contention. Section 2.1 outlines what is referred to here as a 'dual view' of data control. Then, Section 2.2 outlines the 'control of risks' view of data control.

2.1. THE DUAL VIEW OF DATA CONTROL

At one end of the spectrum, for example by Giannopoulou et al., data control is conceptualized as comprising both a positive and a negative dimensions. According to them, the positive dimension consists of the ability of data subjects to '*actively* manage their personal data' (emphasis added) through data subjects' rights, consent and other (possibly technological) tools or, in other words, in personal data self-management. While the positive dimension implies an active engagement of data subjects with respect to the processing of data related to them, the negative dimension features the opposite characteristics. Allegedly referring to the remainder of the GDPR provisions where the data subject is not actively engaged, the negative dimension, according to them, consists of 'safeguarding an environment where control over one's personal data is not subsumed by power asymmetries'.[23] Giannopoulou et al. consider the negative dimension to be instrumental to the positive one, resulting in personal data self-management, expressed as data control, being considered as the concept of data protection.[24] Implicitly, this interpretation endorses the view that data protection

23 Giannopoulou et al. (n 15), 32.

24 This same logic is endorsed – albeit not always so clearly – in other works. Lazaro and Le Métayer are not explicit on the relationship between individual data control and the rest of the GDPR provisions. They seem to assume that, by leveraging what they refer to as collective and/or technological and organizational (i.e. the role of DPAs) control, the GDPR would indeed strive for individual data control, namely data self-management thus viewed as the ultimate goal, to be made possible. See C Lazaro & D Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 *SCRIPTed* 3. The same view is expressed extensively throughout N Anciaux et al., 'Empowerment and "Big Personal Data": From Portability to Personal Agency' (2021) 2 *Global Privacy Law Review*, no. 1, 16. The same reasoning seems to be underlying the argument by Ursic that certain obligations of data controllers – such as the right to provide information – are instrumental to the individual control of data subjects, see H Ursic, 'The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?' in M Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Nature, 2018), 60–61.

would generally be deprived of positive objectives and rather geared towards a – somewhat negative – management of harm.[25]

The conceptualization by Giannopoulou et al. finds an echo with data control as put forward by EU data legislation, with its strong focus on *data* and data self-management by individuals seemingly endorsed as the final goal. Comprising both the Data Governance Act (DGA) and the Data Act,[26] EU data legislation claims to empower individuals with respect to 'their' data *beyond* the GDPR, through the further development of data access and data portability(-like) rights.[27] In particular, while the GDPR is considered to grant mainly a *negative* protection to individuals, namely concerning detrimental data processing activities conducted by others, EU data legislation aims to empower individuals to *positively* conduct the activities that they wish with 'their' data, i.e. data self-management. For example, the Data Act enables users of connected products to claim data generated throughout the use of such products and to use them as they see fit or have them processed by a third party of their choice under strict regulation.[28] For its part, the DGA aims to enable individuals (and also businesses) to generate value from data by resorting to trustworthy data intermediaries when transacting data such as 'PIMS' (personal information management systems),[29] notably based on data access and data portability rights that enable individuals to have some factual control of data and thus to initiate further processing.[30]

Thus defined, the empowerment of individuals – and businesses – constitutes a key objective of the EU data policy.[31] The countering of power asymmetries in the digital environment through an enhanced data control lies at the core of the 'European way of data governance',[32] expected by the EU to form the EU alternative for the digital environment, namely one that is not dominated by Big Tech.[33]

2.2. THE CONTROL OF RISKS VIEW

On a conceptual level, the dual view of data control (outlined in Section 2.1) appears to have common ground with what Rouvroy and Poullet warned against as a form of commodified – and thus pointless, according to them – data protection.[34] Rouvroy and Poullet define commodified data protectioni as the reunion of two elements: (i) personal data 'propertization' with data as a commodity;[35] and (ii) the featuring of data protection as an ultimate value consisting in the satisfaction of individuals' immediate preferences with regard to personal data. Against the commodified view, Rouvroy and Poullet consider that the right to data protection should be intermediate and instrumental to other fundamental rights and freedoms.[36]

25 This view is put very explicitly by Prins: 'Typical of the human-rights perspective is the idea that privacy is negative in nature: It is viewed as a right of non-interference, not as a right of positive entitlements'. See C Prins, 'Property and Privacy: European Perspectives and the Commodification of Our Identity' in L Guibault & P Hugenholtz (eds.), *The Future of the Public Domain, Identifying the Commons in Information Law*, vol 16 (Kluwer Law International, 2006) 234.

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

27 DGA (n 25), Rec. 5, 30, 32 and 33; Data Act (n 26), Rec. 33.

28 Data Act (n 26), Rec. 35, Arts. 3 to 6.

29 DGA (n 25), Chapters III and IV.

30 DGA (n 25), Rec. 30 and Chapter III.

31 Commission, Communication 'A European strategy for data' 2020 (COM/2020/66 final) s C.

32 DGA (N 25), Rec. 32.

33 Commission, Communication (n 31), s C.

34 A Rouvroy & Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth at al. (eds.) *Reinventing Data Protection?* (Springer, Dordrecht, 2009).

35 'Possessive individualism combined with the perception of personal information as a commodity freely exchangeable on the market [...]', ibid 50.

36 '[...] in an era of possessive individualism such as ours, data protection – or the empowerment of individuals with regard to their personal data – risks being interpreted as making the satisfaction [of] individuals' immediate preferences with regard to their personal data, their choices to keep undisclosed or to commodify personal information a final value.' ibid.

DOI: 10.36633/ulr.1124

Building upon Rouvroy and Poullet with the ambition to conceptualize *how* data protection is intermediate and instrumental to other fundamental rights and freedoms, von Grafenstein also criticizes the focus on 'data'. He conceptualized data control as the control of future data processing-induced risks to the autonomous exercise of fundamental rights and freedoms by individuals.[37] His conceptualization of data protection – and especially of data control – is centred on the cornerstone notion of 'purpose'. According to him, compliance with the GDPR is tailored, through the notion of purpose, to the control of risks incurred by the processing of data by other actors. That way, data protection constitutes a legal reaction to the risks resulting from the power asymmetries caused by data processing by such other actors ('data controller(s)'), which could translate into harm if not adequately acted upon.[38] Against this background, individual data control enables individuals to take part in such legislative endeavour, in a continuum of control of data processing-incurred risks. With this conceptualization, data – namely the notion of 'personal data – plays an instrumental role with the focus being mainly placed on data processing-incurred *risks*.

To conclude, data protection is widely agreed to be geared towards the countering of power asymmetries, including in the context of 'modern bigness'. Yet, the various interpretations of this function of data protection in the literature and by the EU legislature suggest that *how* data protection does that is under-conceptualized. More precisely, an understanding of the *nature* of the power asymmetries – and of the ensuing issues – that data protection seeks to address, is missing for the calibration of the expectations. Despite the consensual agreement that data protection – and especially the GDPR – addresses power asymmetries through the enhancement of data control, severe contradictions can be found. Rather than random disagreements, these contradictions have to do with how data protection relates to data commodification, which speaks to the nature of the objective pursued by data protection and to the nature and function of the notion of 'personal data'. The following Sections 3 to 6 explore the hypothesis that a clearer understanding of the nature and function(s) of the notion of 'personal data' under the GDPR will in turn help to clarify the nature of the power asymmetries that this legislation seeks to address.

3. NATURE AND FUNCTION OF THE NOTION OF 'PERSONAL DATA'

This Section returns to the basics of data protection and seeks to clarify the nature of the notion of 'personal data', as used in the GDPR, with relation to its function(s). The nature and function(s) of 'personal data' are addressed in the law, first and obviously, under the GDPR (Section 3.1) but also, more recently, in other legislation as part of the EU digital package. Section 3.2 focuses on the dichotomy arising in the law between 'personal data' and 'non-personal data'.

3.1. UNDER THE GDPR

The notion of 'personal data' under the GDPR[39] mainly follows a risk-based approach in line with the overall approach of the GDPR. The question is not whether some data qualify as personal data in the abstract. As famously demonstrated by Purtova, the label, 'personal data'

37 M von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (2020) 6 *European Data Protection Law Review* 509; M von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II Controlling Risks Through (Not to) Article 8 ECFR Against Other Fundamental Rights' (2021) 7 *EDPL* 190; M von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III Consequences for the Interpretation of the GDPR (and the Lawmaker's Room for Manoeuvre)' (2021) 7 *EDPL* 373.

38 von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II (n 37), 194–195. The 'risks to rights' approach of the GDPR has been criticized for problematically turning rights into risks. For a recent summary of such critiques, see K Yeung & L Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 *Regulation & Governance*, no. 1, 137, s 3.3.2; A Christofi et al., 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?' in Information Resources Management Association (eds.) *Research Anthology on Privatizing and Securing Data* (IGI Global, 2021). However, von Grafenstein conceptualizes the 'risks to rights' approach of the GDPR as rather illustrative of a *precautionary and preventive* approach, see von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I (n 37), 520; von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II (n 37), 199. In other words, the GDPR is about regulating the *likelihood* of harm, precisely to prevent such likelihood materializing into genuine harm.

39 GDPR, Art. 4(1), Rec. 26.

DOI: 10.36633/ulr.1124

is relational or 'situational', or in other words subjective.[40] It notably depends on the nature of the actor processing the data and on the (technological and organizational) means that they have at their disposal to identify individuals through data. In that light, the label 'personal data' reflects the likelihood of an ensuing risk of harm, i.e. in the form of interference with fundamental rights and freedoms, that could ensue,[41] of which the likelihood of identification of individuals through data constitutes a proxy.[42] The important question is then which *level of risk* should be admitted in this regard, account being had to the resulting risk of harm, which is circumstantial (especially in the big data era). The notion of 'personal data' under the GDPR is thus mainly a conceptual one, namely as a proxy for the likelihood of harm that could be inflicted on individuals.

The nature of the notion of 'personal data' is directly connected to its function to *trigger the application* of the GDPR. Any processing of data allowing the identification of (an) individual(s) must comply with the GDPR.[43] The notion of 'personal data' acts as a dividing line between those risks (if any) that are acceptable and those that are acceptable only provided that they are regulated under the GDPR. This constitutes the main function of the notion of 'personal data', already in place before the GDPR with the Data Protection Directive.[44]

Besides this foundational function, Hallinan and Gellert identified another function of the notion of 'personal data' as a regulatory subject-matter, particularly since the adoption of the GDPR.[45] While the GDPR does not affect the overall regulatory system compared to the Data Protection Directive, the development of data subjects' rights mainly takes the form of the development of rights 'on' personal data.[46] A particularly striking case is the new right to data portability, which grants data subjects, under certain circumstances and conditions, a 'right to receive the personal data concerning [them]' and to have them ported to another controller.[47] This has unsurprisingly caused some scholars to read the GDPR through the lens of property law.[48] The question has arisen whether the right to data portability belongs to data protection or whether it rather serves market, consumer protection and/or innovation purposes.[49] The data portability right is not ownership in the absence of exclusive rights.[50] However, it serves a property function in the sense that, both in object and in effect, it constitutes personal data as an object and regulatory subject-matter and allocates them as a resource. A minor consideration under the GDPR, the function of 'personal data' as an object and a regulatory subject-matter is importantly closely connected, under the GDPR, to 'data control' with a proprietary vocabulary ('his or her data').[51]

---

40 N Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation and Technology*, no. 1, 40.

41 ibid 40.

42 Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> (last date of visiting 25 April 2025); M Finck & F Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 *International Data Privacy Law*, no. 1, 11, 14; Purtova (n 40), 46.

43 GDPR (n 12), Art. 2(1).

44 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Art. 3(1).

45 D Hallinan & R Gellert, 'The Concept of "Information": An Invisible Problem in the GDPR' (2020) 17 *SCRIPTed*, no. 2, 269.

46 For a clustering of data subjects' rights, see L Drechsler, 'The Sword in the Stone: The Potential of Data Subject Rights of the General Data Protection Regulation' [2023] *Revue Européenne du Droit de la Consommation*, 87.

47 GDPR (n 12), Art. 20(1).

48 H Pierce, 'Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law' (2018) 4 *European Data Protection Law Review*, 190; N Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table … and Back on Again?' (2014) 30 *Computer Law & Security Review*, no. 1, 6.

49 P De Hert et al., 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' [2017] *Computer Law & Security Review*; I Graef et al., 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 *German Law Journal*, no. 6, 1359, 1363–1367; O Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' (2017) 42 *European Law Review*, no. 6, 793, 809–810.

50 Graef et al., (n 49), 1368.

51 Rec. 68 GDPR indicates that the right to data portability aims to 'further strengthen the control [of data subjects] over his or her own data'. Not connected to any specific GDPR provision in particular, the reference

3.2. UNDER OTHER EU POLICY AND LEGAL FRAMEWORKS: PERSONAL DATA VERSUS NON-PERSONAL DATA

With its recent data policy project, the EU repeatedly refers to the notion of 'personal data'. In this respect, two closely related elements require further consideration.

The first element consists of the introduction of the new notion of 'non-personal data' into EU policy[52] and legislation[53] led to a new 'personal data versus non-personal data' divide. Non-personal data are defined as data which are not personal, namely by default compared to the notion of personal data under the GDPR.[54] This notion has led legal scholarship to question the *feasibility* of this divide in law, because of the dynamicity of the personal data label.[55] Interestingly for the present paper, Janeček connects this issue to data commodification: 'The property and market advocates [...] would want to utilize the data and therefore *secure stabile control over them*' (emphasis added).[56] He pictures the problem as an epistemological one, due to both the confusion between 'data' and 'information' and to the misaligned label of data as either personal or non-personal *in time*. While 'property and market advocates' want to secure a data label – and thus allocation – *ex ante* to use and trade data, the label as 'personal data' can be attracted at any time, possibly *ex post* (i.e. after data collection) depending on the semantic *information* contained in a dataset.[57]

However relevant, this discussion does not exhaust the debate and should be complemented with a clarification of the underlying conceptualization of (personal) data and of the function(s) of the notion of 'personal data' under the GDPR. The 'personal versus non-personal data' divide relies on an implicit twofold premise. The first premise is that the respective categories of data refer to realities *of a same nature,* namely 'data'. The second premise is that both personal and non-personal data are 'things' and especially regulatory subject-matters. In other words, this divide implicitly but necessarily relies on data objectification, namely of *both* personal and non-personal data. Yet, it is now clear that such data objectification does not appropriately report on the nature and main function of personal data under the GDPR, as a conceptual notion acting as a proxy for the likelihood of harm (see Section 3.1 above).

The second element consists of the function assigned to the notion of 'personal data' in EU data legislation. The DGA equates the 'making available of data' by data subjects with the exercise of data subjects' rights under the GDPR.[58] Then, personal data sharing is defined as the provision of data by data subjects to a data user (namely a data acquirer) *based on,* among others, the GDPR.[59] And ultimately, the definition of a data user implies that, as a result of data sharing, they get a 'right to use data [...] under [the GDPR]'.[60] This definition[61] relies on the GDPR, as an external legal source, to provide for an initial allocation of data to individuals – i.e. data

to data control in Rec. 7 GDPR uses the same terminology: 'natural persons should have control of *their own* personal data' (emphasis added).

52 European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European Data Economy', COM(2017) 9 final, 10.1.2017; European Commission, Data Strategy (n25), s. C.

53 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Free Flow of Non-Personal Data Regulation). The notion of non-personal data was then upheld in many other data-related laws, such as DGA, Art. 2(4) and Data Act, Art. 2(4).

54 Free Flow of Non-Personal Data Regulation (n 53), Art. 3(1); DGA, Art. 2(4); Data Act, Art. 2(4).

55 I Graef et al., 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3256189 4 <https://papers.ssrn.com/abstract=3256189> (last visited 29 July 2019). For similar arguments, see J Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' <https://ssrn.com/abstract=3274519> (last visited 13 November 2018); V Janeček & G Malgieri, 'Commerce in Data and the Dynamically Limited Alienability Rule' (2020) 21 *German Law Journal*, no. 5, 924.

56 V Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34 *Computer Law & Security Review,* no. 5, 1039, 1043.

57 ibid.

58 DGA (n 21), Art. 10(b) and Rec. 30.

59 ibid, Art. 2(10).

60 ibid, Art. 2(9).

61 This formulation could attract two interpretations. It could mean, first, that data subjects could *dispose of* their data subjects' rights. In a slightly less proprietary reading, it could mean that compliance with the GDPR by the data user would amount to the GDPR granting them, positively, a right to use data.

DOI: 10.36633/ulr.1124

subjects – that serves as a prerequisite legal instrument underpinning different types of data sharing relationships and in particular personal data commercial transactions. This denotes a proprietary reading of data subjects' rights, envisaged as rights or entitlements *on* – or related to – *data* acting as a functional alternative to property to enable data transactions. Relatedly, the notion of 'personal data' acts as a data allocation mechanism. Here again, personal data are considered as an object, as a regulatory subject-matter, and even as a resource. This function of the notion of personal data goes with the promotion of data self-management by data subjects, portrayed as a manifestation of data control by individuals.

3.3. CONCLUSION

The notion of 'personal data' constitutes a foundation of the GDPR – and of data protection more in general. Under the GDPR, the label as 'personal data' is based on a risk-based approach rather than as an objective categorization. The notion of 'personal data' is a conceptual one that serves as a proxy for the likelihood of harm, thus triggering the application of the law. Alongside this classical function – very much connected to the *nature* of the notion of personal data – arose a new – and minor – function of the notion of 'personal data' as a regulatory subject-matter, with the development of personal data-focused data subjects' rights under the GDPR. The prime example of this is the data portability right, which goes so far as to play a property role by allocating personal data as a resource. This was accompanied with a new proprietary terminology in connection to references to data control.

After the adoption of the GDPR, EU data legislation has continued this function of personal data as an object and a regulatory subject-matter *from the outside.* This trend was identified, in this Section, with two phenomena. First, the new notion of 'non-personal data', which has forced a new 'personal data versus non-personal divide' where both are implicitly considered as objects and regulatory subject-matters. Second, and going even further, the DGA uses the notion of 'personal data' as a proxy for a data allocation mechanism, thus reinterpreting the GDPR as doing just that.

Importantly, the two functions of the notion of 'personal data' are conceptually misaligned and contradictory. The *nature* of the notion of 'personal data' aligns with its foundational function as a conceptual proxy for the likelihood of harm and *not* as an object, which would instead require an objective categorization of data. Overall, a recent historical pattern is unfolding in EU law that the original and foundational function of 'personal data' as a conceptual proxy for the likelihood of harm is eroding to the benefit of increasing personal data objectification, arising both from *within* data protection and then reinforced from the *outside*.

4. THE DATA PROTECTION LEGAL LITERATURE ON POWER ASYMMETRIES

This Section explores how the legal literature conceives of the power asymmetries that data protection seeks to counter and how this question is connected to the nature and function of the notion of 'personal data'. Although data protection is considered to have the countering of power asymmetries as its main added-value or even as its essence, the legal literature actually offers a rather frustrated understanding of this notion.[62]

Most of the literature – even when discussing data control as the expected fix to counter power asymmetries – simply does not substantiate what power asymmetries are and which *types* of power asymmetries the GDPR addresses. A prime example is Lynskey, a leading author on the relationship between data protection, power and control In developing the argument that the countering of power asymmetries with data control constitutes the added-value of data protection, Linskey develops a compelling analysis of the *implications* and scope of 'data power' of Big Tech. She identifies that they go well beyond market power to, amongst other things, media and political power, yet she discusses neither the *nature* nor the *object* of such

62 Power asymmetries is often used interchangeably with – or in close connection to – harm, see for example A Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 *Computer Law & Security Review*, no. 2, 238, 250–251. While power asymmetries are often viewed as the *cause* of (the likelihood of) harm, Vrabec considers that the very existence of power asymmetries constitutes a harm, see H Vrabec, *Data Subject Rights under the GDPR* (Oxford University Press, 2021), 54.

power.[63] She discusses power asymmetries by and large as the main issue addressed by data protection, yet she does not untangle the different types of power (asymmetries) nor does she attempt to identify with which of these types data protection is concerned. Rather, she includes an illustrative list of power asymmetries that can in practice be found with Big Tech.[64] She does not reflect upon either the question of personal data objectification or upon the relationship between the nature and function of 'personal data' and the conceptualization of the power asymmetries that the GDPR counters.

A distinction which is often found in the literature is the one made between 'individual' and 'systemic' – or collective – data-related power asymmetries. Often, this distinction has the normative function of dismissing the sole focus on *individual* power asymmetries – i.e. through the sole emphasis on individual data control – to the benefit of a more comprehensive vision encompassing 'systemic' ones as well.[65] Janssen et al. constitute a telling example. They apply the 'individual versus systemic' distinction to the question of data control – or data subjects' empowerment – in the context of 'personal information management systems' (PIMS), a form of privacy-enhancing technology. Individuals, expressed as 'users', are equipped with a technical device that enables them to manage data generated by or stored through it, and especially to make decisions on the use of such data.[66] Janssen et al. challenge the self-promotion of PIMS as data control enhancement tools as follows. PIMS do indeed empower individuals *in the context of a PIMS application* through self-data management. But they do not address *systemic* power asymmetries such as those 'inherent in surveillance' that typically take place *after* self-data management within a PIMS application. Rather, PIMS *facilitate* the advent of such power asymmetries through deceptive data control promises.[67] The authors do not engage with the literature dedicated to data-related power asymmetries. They do not engage with the question of how the nature and function(s) of the notion of 'personal data' may impact on the conceptualization of the power asymmetries that data protection counters. However, in light of Section 2 of the present paper, it is easy to see that what Janssen et al. identify as 'individual' data control consists of the control *of personal data* with personal data as the object of control. In contrast, this is not the case with what they identify as 'systemic' power asymmetries arising, for example, from data-driven surveillance.

In his (re-)conceptualization of the right to data protection, von Grafenstein considers 'control' as the core of data protection and thus pays particular attention to power asymmetries. He considers that the GDPR addresses the category of power asymmetries '*caused by the processing of data*' (emphasis added) by other actors, which he calls 'informational power asymmetries'.[68] For example, data-driven surveillance practices by other actors make individuals powerless and especially unable to go about their lives autonomously, so as to exercise their freedom of movement. This echoes the 'powerlessness' identified by Solove to result from data processing, which 'alter[s] the kind of relationships people have with the institutions that make important decisions *about their lives*' (emphasis added).[69] Obviously, such 'powerlessness' not only affects standalone individuals but also has systemic (or 'collective') impacts.[70] In contrast to the literature outlined above, von Grafenstein does identify a *type* of power asymmetries that the GDPR addresses. However, he does not engage with the literature dedicated to data-related power asymmetries and does not consistently

63 Lynskey, 'Grappling with "Data Power"' (n 2).

64 Lynskey, 'Deconstructing Data Protection' (n 14).

65 Mantelero (n 62); Y Ivanova, 'The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World' in D Hallinan et al. (eds), *Data Protection and Artificial Intelligence*, vol 13 (Hart Publishing, 2020), s 3.1; S Calzati & B van Loenen, 'Beyond Federated Data: A Data Commoning Proposition for the EU's Citizen-Centric Digital Strategy' [2023] 40 AI & SOCIETY, 945; J Duncan, 'Data Protection beyond Data Rights: Governing Data Production through Collective Intermediaries' (2023) 12 *Internet Policy Review*, no. 3, 15–17.

66 H Janssen et al., 'Personal Information Management Systems: A User-Centric Privacy Utopia?' (2020) 9 *Internet Policy Review*, no. 4, 2.

67 ibid, 19–20.

68 M von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II (n 37), 195.

69 D Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review*, 745, 757.

70 ibid, 770.

DOI: 10.36633/ulr.1124

stick to his own categorisation.[71] Von Grafenstein does engage with the nature and function(s) of 'personal data': he explicitly rejects that personal data must be considered as an object and must constitute the regulatory subject-matter of the GDPR.

From a different perspective, namely this of how the GDPR engages with vulnerability, Malgieri distinguishes the 'causal' from the 'modal' understandings of power. The former refers to the prevention of adverse effects while the latter refers to the specific situation of data subjects, both understandings of power being connected to various forms of vulnerability of data subjects. On the one hand, he connects vulnerability 'during the data processing' to the modal understanding of power. On the other, he connects vulnerability 'to the outcomes of data processing' with the causal understanding of power.[72] In his mapping exercise of the extent to which the GDPR addresses data subjects' vulnerabilities, he does not prioritise any of these different understandings of power in connection to the conceptualisation of the objectives of the GDPR. With his focus on vulnerability, he does engage neither with the alternative conceptualisations of power found in the legal literature on data protection law nor, *a fortiori,* with conceptualisations found outside of the legal literature. Finally, he does not engage with the nature and function of the notion of personal data.

To conclude, the countering of power asymmetries is often considered to constitute the specificity or added-value of data protection. However, the legal literature has surprisingly little engagement with this notion, even less so in connection to the nature and function(s) of the notion of 'personal data'. Most of the literature simply does not discuss this notion and does not, in particular, specify *which* power asymmetries the GDPR addresses. A distinction is often made between those power asymmetries that are 'individual' and those that are 'systemic' or collective, with the idea that the latter are more important or more serious than the former ones. This distinction does not consider the relationship with the nature and function(s) of the notion of personal data. Von Grafenstein interestingly identifies the power asymmetries that the GDPR does address, namely the ones 'caused by data processing' by other actors, which he conceptually connects to the nature and function of personal data – explicitly rejecting their objectification under the GDPR. A striking finding is that the data protection legal scholarship does *not* engage with the literature dedicated to data-related power asymmetries. In practice, data-driven surveillance generates the types of power asymmetries that, by general opinion, data protection primarily aims to address. However, there is no *conceptual* clarity on the types of power asymmetries that the GDPR counters, nor is there any clarity on the types of power asymmetries that data protection does *not* address.

In order to clarify the power asymmetries that the GDPR addresses and the relationship with the nature and function(s) of the notion of personal data, it is now necessary to look into the literature – outside the data protection legal literature – that does directly discuss this question.

5. DATA-RELATED POWER ASYMMETRIES: A CLUSTERING EXERCISE

Discussions on the relationship between data and power are prominently found in critical data studies (CDS)[73] and infrastructure studies.[74] The overarching question in these fields is that of

71 Some of the examples of power asymmetries that von Grafenstein discusses, are quite evidently not 'caused by' data processing by authors. For example, he justifies the household exclusion (GDPR, Art. 2(2)(c)) based on the somewhat equal status of members of a household; see von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II (n 37), 195. However, by doing so, he actually discusses the absence of a *preexisting* power asymmetry between them, rather than of a power asymmetry *caused by* data processing. On the merits of the argument, it can theoretically (and increasingly practically) not be excluded from the outset that data processing within a household *causes* power asymmetries. This has notably been demonstrated by feminist data protection studies. For a synthesis, see J Theilen et al., 'Feminist Data Protection: An Introduction' (2021) 10 *Internet Policy Review,* no. 4.

72 G Malgieri, '*Vulnerability and data protection law*' (2023), Oxford Data Protection & Privacy Law, Oxford, 94–96.

73 As part of critical data studies, the power implications of data are discussed every year in the 'data power conference', initiated in 2015 (see http://datapowerconference.org/). On the role of the data power conference in structuring the scholarly discussion, see A Hepp et al., 'New Perspectives in Critical Data Studies: The Ambivalences of Data Power—An Introduction' in A Hepp et al. (eds.), *New Perspectives in Critical Data Studies: The Ambivalences of Data Power* (Springer International Publishing, 2022), 1–23, 8–9.

74 Authors involved in infrastructure studies do not always identify it as a strand of literature as such. In the field of media and communication studies, for example, some authors instead refer to an 'infrastructural turn' or 'infrastructural approach'. On this, see S Flensburg & S Lai, 'Follow the Data! A Strategy for Tracing Infrastructural Power' (2023) 11 *Media and Communication*, no. 2, 319, 320–321; J-C Plantin & A Punathambekar, 'Digital Media Infrastructures: Pipes, Platforms, and Politics' (2019) 41 *Media, Culture & Society*, no. 2, 163–165.

the *specificities* of data with respect to power (asymmetries). This Section summarizes the main types of power asymmetries identified with respect to data and categorizes them in connection with the nature and function(s) of data and especially with the question whether data are an object or not.[75]

Ruppert et al. identify that data are not only subject to traditional political struggles around allocation and distribution, like any other valuable resources, but they are also generative of new forms of power relations and politics that manifest both in the production of data and in their use.[76] They distinguish power '*in*' data from the finding that data '*are*' power.[77] Data '*are*' typically power when used as a means to exercise power through surveillance that allows one to influence humans' behaviour.[78] Data are also power when collected online to micro-target individuals and nudge them into purchasing certain goods and services.

Fisher and Streinz conceptualize the 'power to datafy' through what they refer to as the 'data-generating infrastructure' of those actors that 'control the means of data production'.[79] They distinguish the power to datafy from the fact of having or not having data.[80] According to them, the focus on data allocation or distribution obfuscates the control, by a few concentrated and powerful actors, of data-generating infrastructures.[81] Their research leads them to challenge the view that data constitute a resource (i.e. like any other) that must thus be regarded and regulated as an object.

In their respective studies, both Montero and Finger, and Luque-Ayala and Marvin recognize an infrastructural power of data, against the background of infrastructure studies.[82] They identify data objectification as a *source* of power asymmetries. Data are powerful because they constitute a common language that can abstract from the local. Local elements are turned into a datafied input that can be acted upon. This enables one to turn data into influence in a vast range of different realms (the 'general-purpose criterion' of infrastructure in the parlance of Frischmann).[83] They challenge the view that data would be a discrete resource (i.e. a resource like any other), because of the infrastructural role that data can be leveraged to play in society. Importantly, they identify the same phenomenon in their respective case studies that, instead of simply 'optimizing' activities, data are used *to structurally reshape* them, resulting in new power dynamics. For example, Montero and Finger show how online platforms use data to (re-)intermediate sectors, such as in the field of media and transport – fragmented as a result of liberalisation processes, and restructure these fields around their own business (interests).[84] Luque-Ayala and Marvin show how data are used, in smart cities projects, to reconfigure cities as 'computable projects'. They all confirm the finding, introduced in the previous paragraph, that data constitute a *means for* the exercise of power, rather than (only?) an object of power struggle.

To conclude, the relationship between data and power is closely connected to the question of the nature and function(s) of data, and especially whether data is to be regarded as an object and a resource or not. The research dedicated to the relationship between data and power

75 This section elaborates on C Ducuing, Data as a Contested Commodity, (2024) 24 *Global Jurist*, no. 3, 277, 11–12.

76 E Ruppert et al., 'Data Politics' (2017) 4 *Big Data & Society*, no. 2. See also Hepp et al. (n 74), 5–6.

77 Ruppert et al. (n 75), 2.

78 Isin & Ruppert (n 7); S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019); A Kapczynski, 'The Law of Informational Capitalism (Book Review of The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff 2019 and Between Truth and Power: The Legal Constructions of Informational Capitalism by Julie Cohen 2019)' [2020] *Yale Law Journal*, 1460.

79 A Fisher & T Streinz, 'Confronting Data Inequality' (2022) 60 *Columbia Journal of Transnational Law*, no. 3, 829, 844.

80 ibid 831.

81 Fisher & Streinz (n 78).

82 Montero & Finger (n 11); A Luque-Ayala & S Marvin, 'Datafication: The Making of Data-as-Infrastructure' in *Urban Operating Systems: Producing the Computational City* (MIT Press, 2020).

83 B Frischmann, *Infrastructure: The Social Value of Shared Resources* (Oxford University Press, 2012).

84 Montero & Finger (n 11).

DOI: 10.36633/ulr.1124

– found in CDS and infrastructure studies – explicitly challenges that data be regarded and regulated as an object, a resource or even as a commodity, precisely because of their specific relationship to power.

Two categories of power asymmetries need to be distinguished. First, what this article identifies as 'extrinsic data-related power asymmetries' arise from the uneven allocation or distribution of data, *like any resource*, leading to 'data haves' and 'data have nots'. They relate to power *over* data, whereby data constitute the object of power struggles. Such power asymmetries are concerned, for example, with the question who can access data or generate economic value from data, namely such questions that are typically addressed by property law. For example, the question has arisen as to who should be entitled to access and use data generated by the use of connected products, such as cars, farming equipment or wearables. Second and *unlike other things*, data are characterized by 'intrinsic power asymmetries', caused by the specificities of data compared to other things.

Two types of intrinsic power asymmetries can be distinguished. (1) Data constitute a *manifestation of power* (data 'as' power), namely of the power to datafy, which relates to the data production or generation phase. Certain actors have the 'power to datafy': they dispose of the means and are in a position which enables them to generate and use certain types of data. For example, the unique position of Big Tech as managers of large and almost unavoidable platforms enables them to generate data relating to individuals' and businesses' behaviour online. (2) Data also constitute a *means through which* new forms of power can be generated and exercised (power *through* data), which relates to the use of data (further processing after the collection or generation phase). Power *through data* is reinforced by the infrastructural capabilities of data, namely the fact that they can be used for a wide range of purposes in different realms. Importantly, the object of intrinsic data-related power asymmetries is *not* data but people and people's behaviour, whether natural persons or companies and whether standalone individuals or collectives (or even society at large), depending on the context.

The relationship between the two types of power asymmetries is not straightforward. On the one hand, they feed each other in a loop: more data means more (infrastructural) power, in turn allowing for more data capture and data use, etc. On the other hand, *addressing* these power asymmetries implies a trade-off. The identification of intrinsic power asymmetries fundamentally challenges the perception and regulation of data as an object and as a resource. In contrast, such perception constitutes the premise for addressing extrinsic power asymmetries – if addressed in isolation. The findings of this section can be visualized in Figure 1.

	Extrinsic power asymmetries	**Intrinsic power asymmetries**
Description of the problem	Unequal/unfair allocation of data ('data haves' versus 'data have nots'), data monopolies	Data as a means to generate and exercise power: - Data as a (manifestation of) power; - Power exercise through data
Object of power	Data (power *over* data)	People('s behaviour)
Example	'It is unfair that car manufacturers appropriate massive amounts of in-vehicle data to the detriment of independent repairers'	'It is unfair that smart farming equipment providers use farm data to tailor the prices of inputs (i.e. fertilizers) sold to farmers'
Conceptualization of the nature of data	Data as a resource	Data as *something else*
Relationship to data objectification	Congruent	Incongruent
Relationship to the other form of data-related power asymmetry	*Ambivalent* relationship - Power asymmetries *issues* feed each other in loops, because of the infrastructural potential of data; - But, addressing power asymmetries implies trade-offs and contradictions.	

Figure 1 Categorization of data-related power asymmetries.

DOI: 10.36633/ulr.1124

6. THE DATA-RELATED POWER ASYMMETRIES THAT THE GDPR DOES AND DOES NOT COUNTER

Bringing together the findings of the previous Sections, this Section now identifies the power asymmetries that the GDPR does address, in light of the nature and function(s) of the notion of 'personal data'. It shows that the application of the 'extrinsic versus intrinsic power asymmetries' distinction is not only *useful* (Section 6.1) but actually *necessary* to conceptualize the power asymmetries that the GDPR addresses and how it addresses them (Section 6.2).

6.1. THE GDPR AND INTRINSIC DATA-RELATED POWER ASYMMETRIES

In practice, data-driven surveillance – as the archetypal example of power asymmetries that, by general opinion, the GDPR aims to counter – relates to *intrinsic* power asymmetries. By engaging in data-driven surveillance, some actors acquire the power to influence the behaviour of individuals, for example by influencing the way they move in public spaces or at work. What von Grafenstein identifies as 'informational power asymmetries' – power asymmetries *caused by* data processing by other actors – constitute *intrinsic* power asymmetries. The term 'informational power asymmetries' sounds linguistically accurate in pointing to the *specific* relationship of data to power that the GDPR aims to address. The GDPR is indeed predominantly about regulating the conditions under which *other actors* – 'data controllers' – process data in a way that unduly prevents individuals from going freely about their lives. Personal data 'processing' includes both data collection (or generation) and other/further operations conducted with personal data,[85] with the presumption that the conduct of such activities can, as such, entail risks to the enjoyment by individuals of their fundamental rights and freedoms to go about their lives. This account is in line with the main and foundational function of the notion of 'personal data' as a conceptual proxy for the likelihood of harm (Section 3.1).

In contrast, personal data self-management constitutes a fix to *extrinsic* data-related power asymmetries whereby actors other than individuals are considered to 'have' data and be able to make use of them. Data are then considered as objects unevenly allocated or distributed to the detriment of individuals. Personal data self-management boils down to enabling individuals to *dispose of* personal data and make use of them or, in other words, in reallocating personal data, perceived as an object and a resource, partly in their hands. The countering of extrinsic data-related power asymmetries can be found under the GDPR with the more marginal function of personal data as an object, a regulatory subject-matter and a resource. For example, the data portability right aims to enable individuals to *dispose of* personal data. Centered on *data*, this right aims to enable individuals to manage data, for example by choosing to have data – collected and further processed for an initial purpose by one data controller – moved to another data controller of their choice.[86]

The data access right under the GDPR constitutes a borderline case here. Although visibly designed originally to enable individuals to participate in controlling the risks that can arise from data processing by data controllers,[87] this right can also be used as a data allocation mechanism so that data subjects get factual control over personal data in order to make further use of data themselves. In this case, that data are processed – and especially that they are collected (or generated) – is not viewed as a problem as such, but only insofar as the individual cannot dispose of the resulting data. Within this line of thought, data collection constitutes a logical prerequisite for individuals to manage them and benefit from their use.

Yet, clearly, the fundamental *raison d'être* of the GDPR is *not* to enable personal data self-management, on which this article disagrees with Giannopoulou et al. Finally, the GDPR takes into account other – namely not necessarily data-related – power asymmetries. Such is the nature of the prohibition that consent is to be the legal basis for personal data processing in the case of a 'clear imbalance' between data controllers and data subjects. This provision is irrespective of the *cause* of power asymmetries and demonstrably aims to protect the consent of individuals against power asymmetries possibly *predating* personal data processing.[88]

85 GDPR (n 12), Art. 4(2).

86 ibid, Art. 20.

87 ibid, Art. 15.

88 ibid, Rec. 43, Art. 4(11) and Art. 6(1)(a).

DOI: 10.36633/ulr.1124

To conclude, the distinction between intrinsic and extrinsic data-related power asymmetries finds a fertile ground in the GDPR and applies very naturally to it. It appears that the GDPR is predominantly and wholly geared towards the countering of intrinsic data-related power asymmetries. More specifically, the GDPR addresses such intrinsic data-related power asymmetries that arise from the processing of data relating to individuals and that, if left unaddressed, could result in harm being caused to them and especially in individuals being prevented from autonomously enjoying their fundamental rights and freedoms. While this constitutes the very *raison d'être* of the GDPR, this Regulation also takes into account other types of power asymmetries, such as the relative power situation of actors (data controllers and data subjects), which can play a role in the system of checks and balances of personal data processing. With the adoption of the GDPR, data protection also plays – marginally but decidedly – a data allocative function that aims to address extrinsic data-related power asymmetries.

6.2. WHY AN APPROPRIATE CONCEPTUALIZATION OF THE COUNTERING OF POWER ASYMMETRIES UNDER THE GDPR MATTERS

That the conceptual distinction between intrinsic and extrinsic data-related power asymmetries is *useful* to understand the GDPR is one thing. This Section goes one step further in arguing that this conceptual distinction is actually *necessary*, in particular to preserve the autonomy of the GDPR against commodified corrupted interpretations of it.

While widely spread, the distinction between individual and systemic (or collective) power asymmetries (and related harms) is insufficient to adequately report on the GDPR. To demonstrate it, I base myself on the analysis of the paper of Calzati and Van Loenen, which relies on the distinction between individual and systemic power asymmetries. Their paper offers a critical perspective on the discourse underpinning EU data policy, namely mainly the European Data Strategy.[89] On the one hand, the authors consider that the focus of EU data policy on market building is detrimental to societal values and in particular to the *collective* dimensions of data. On the other hand, they imply that data protection would not be detrimentally affected by EU data policy. They base this conclusion on their perception that the GDPR has an 'individual outlook' because it provides *individual rights*.[90]

This raises several issues. First, the authors conflate 'individual rights' with a data market perspective, thereby implicitly perceiving the GDPR as a bundle of rights on personal data as an object and a resource likely to legally support data markets. As discussed in the previous Sections, in the main the GDPR does *not* do that. Second by doing so, they fail to recognize that the *raison d'être* of the GDPR is to address *intrinsic* data-related power asymmetries, which is possibly, at least in practice, what they have in mind when referring to collective dimensions of data. Third, what they refer to as collective dimensions of data says nothing about the *nature* of the collective and how its/their interests relate to personal data. Following on from the other issues mentioned, the 'collective dimensions of data' could easily get wrongly depicted as collective property of data, with data being regarded and regulated as an object and a resource.[91] Fourth, the authors consider the 'collective dimension of data' necessarily more relevant than the 'individual' one. Yet, the 'collective dimension of data', if viewed as collective property of data, could actually interfere with well-founded 'individual' concerns arising from intrinsic data-related power asymmetries.

The distinction between individual and systemic (or collective) power asymmetries is obviously relevant. However, what the present analysis shows is that this distinction alone does *not suffice* to report conceptually on how the GDPR counters power asymmetries. What remains missing with the individual versus systemic distinction is an understanding of the *nature* of the power asymmetries at hand, namely mainly intrinsic – as opposed to extrinsic – data-related ones.

The distinction between intrinsic and extrinsic data-related power asymmetries is also critical in preserving the autonomy of data protection against commodified corrupted mis-interpretations. It now becomes obvious that the data control that EU data legislation aims

89 Calzati and van Loenen (n 65).

90 ibid s 3.2.

91 The same ambivalence can be observed with M Mannan et al., 'Data Cooperatives in Europe: A Preliminary Investigation' (2022) 24 *Network Industries Quarterly*, no. 3, 12, 15.

DOI: 10.36633/ulr.1124

to enhance – and thus the power asymmetries that this legislation aims to counter – are different from the GDPR's. EU data legislation sides with a vision of data control as personal data self-management by data subjects whereby personal data are perceived as an object and a resource that EU data legislation aims to better allocate and distribute. This approach is undoubtedly affiliated with personal data-focused data subjects' rights under the GDPR such as data portability. But this EU data legislation approach resolutely deviates from the *raison d'être* of the GDPR to counter *intrinsic* power asymmetries. That EU law leans towards a vision whereby data – both 'personal' and 'non-personal' data – are perceived and regulated as objects and resources that should be better allocated, is a political choice. Legally speaking, it is not a problem in itself. The legal issue lies in pretending that such an approach is tantamount to the approach of the GDPR, thus forcing a commodified interpretation of data protection as warned against by Rouvroy and Poullet. As the present paper has shown, this confusion finds sources in both the pervasive – and seemingly self-evident to many – objectification of personal data and the lack of a clear identification of the types of power asymmetries that the GDPR counters.

To conclude, this Section shows that conceptualizing the GDPR following the distinction between intrinsic and extrinsic data-related power asymmetries is not only relevant but it is also *necessary*, both conceptually and in practice in order to avoid an erosion of data protection by the means of its commodified corrupted mis-interpretation. A commodified interpretation of data protection – with its ultimate value being data control, expressed as personal data self-management by data subjects – can be observed in the data protection legal literature and in EU data legislation.

7. CONCLUSIONS

This article contributes to unpacking the relationship between data protection and modern bigness. More specifically, it offers a conceptualization of the relationship between data protection and power asymmetries. Data protection – and especially the GDPR – has as its main function to tackle power asymmetries. However, *which* power asymmetries the GDPR seeks to address is under-conceptualized in the legal literature. This should be associated with the pervasiveness of data commodification narratives both within data protection to some limited extent but also mainly *outside* of data protection with the EU digital package.

First, the article highlights the – until now – silent and implicit endorsement of personal data objectification. Mainly and foundationally used in data protection as a conceptual proxy for the likelihood of harm, the notion of 'personal data' has recently been increasingly used to regulate personal data as an object, a regulatory subject-matter and a resource.

Second, the article identifies that such personal data objectification results in a mis-interpretation of the power asymmetries that data protection seeks to address. The article conceptualizes the power asymmetries that data protection seeks to address as 'intrinsic data-related' ones, whereby data constitute a manifestation and means for exercising power. Specific to data, intrinsic data-related power asymmetries have people as an object. For example, data-driven surveillance deployed in the public space consists of exercising intrinsic data-related power asymmetries over passers-by, by controlling their behaviour. In contrast, the conceptualization of personal data as an object, regulatory subject-matter and a resource, leads to considering power asymmetries (solely) as 'extrinsic' ones, namely as matters of data allocation and distribution.

The findings of this article have manifold implications. They put in question the ways in which the EU digital package conceives of its internal consistency and thus seeks to address modern bigness. In particular, EU data legislation builds its consistency and compatibility model with data protection at the cost of a commodified corrupted mis-interpretation of data protection, as warned against by Rouvroy and Poullet some 15 years ago. Data protection is mis-portrayed as a personal data allocation mechanism, thus fixing *extrinsic* data-related power asymmetries. Irrespective of the normative worth of this objective, unlike the Data Act and the Data Governance Act, the GDPR does not seek to redistribute data, appropriated by Big Tech, with individuals.

Actually, and however controversial it may sound, the taming of the power of Big Tech – as such and put in the abstract – is not the primary objective of data protection. That data protection addresses *intrinsic* data-related power asymmetries speaks to the specificity of data protection. The fundamental right to data protection seeks to preserve the autonomous exercise of one's fundamental rights and freedoms, or in other words, the possibility for one to go freely about one's life, in the face of the power exercised and/or manifested by others over one through data. That Big Tech are big or that they have a lot of data are not, as such, issues that data protection seeks to address. Yet, of course, these constitute relevant criteria for the legal analysis of how Big Tech exercise power over individuals through data so that data protection does and should play a role in regulating modern bigness.

More in general, data protection should not be expected to solve all types of power issues in the digital environment, to the risk of diluting or deprioritizing its true core.

This article should also be read as a warning signal against the power of data commodification discourses to re-shape and thus corrupt data protection as we know it. Data commodification discourses have gradually and increasingly eroded data protection, with EU data legislation being the climax of this phenomenon. This article casts doubts on whether the GDPR can accommodate the new, and however accessory, function ascribed to it to *allocate* personal data with the data portability right. Of little *practical* impact, this right has played a huge and problematic *discursive* role. Indeed, the data allocation function relies on a conceptualization of personal data as an object, a regulatory subject-matter and a resource, which is misaligned with its main and foundational conceptualization as a proxy for harm.

Finally, this article invites the legal scholarship on data protection to engage with relevant non-legal scholarship with respect to power issues, mainly found in CDS and infrastructure studies.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATIONS

Charlotte Ducuing orcid.org/0000-0003-1160-0637
Post-Doctoral research, Centre for IT and IP Law of the KU Leuven (CiTiP), BE

TO CITE THIS ARTICLE:
Charlotte Ducuing, 'Data Protection Without Romance: The Power Asymmetries that the GDPR Does Counter' (2025) 21(2) Utrecht Law Review 78–94. DOI: https://doi.org/10.36633/ulr.1124

Published: 01 October 2025