UNCOVERING
EUROPEAN PRIVATE LAW

A STUDENT HANDBOOK

EDITED BY MARIJA BARTL,
LAURA BURGERS, AND CHANTAL MAK

UNCOVERING EUROPEAN PRIVATE LAW

Uncovering European Private Law

A Student Handbook

Edited by Marija Bartl, Laura Burgers, and Chantal Mak

OpenBook Publishers

https://www.openbookpublishers.com

Marija Bartl, Laura Burgers, and Chantal Mak (eds), *Uncovering European Private Law: A Student Handbook*. Cambridge, UK: Open Book Publishers, 2025, https://doi.org/10.11647/OBP.0448

Digital material and resources associated with this volume are available at https://doi.org/10.11647/OBP.0448#resources

Information about any revised edition of this work will be provided at https://doi.org/10.11647/OBP.0448

ISBN Paperback: 978-1-80511-505-2
ISBN Hardback: 978-1-80511-506-9
ISBN PDF: 978-1-80511-507-6
ISBN HTML: 978-1-80511-509-0
ISBN EPUB: 978-1-80511-508-3

DOI: 10.11647/OBP.0448

Cover image: Black redstart with a bright red tail (2023), https://unsplash.com/illustrations/black-redstart-with-a-bright-red-tail-drinks-water-from-the-lake-reflected-in-the-mirror-water-stylization-TxrxnAAfRdc, licensed under the Unsplash+ License

Cover design: Jeevanjot Kaur Nagpal

Contents

V. METHODS

13. Data Subjects in European Private Law

Antonio Davola

Abstract

This chapter seeks to examine the discourse surrounding the involvement of private law in promoting the rights of data subjects, particularly within the evolving landscape of digital environments. To achieve this, it initially delves into the existing regulations within the European Union, exploring their foundational principles. Subsequently, it provides an overview of the key provisions of the General Data Protection Regulation, elucidating how the regulation currently recognises control over data as a significant—arguably, the primary—mechanism for safeguarding individuals when participating in digital interactions. However, as the far-reaching impact of data analyses on human lives suggests a need for a broader viewpoint, the chapter scrutinises the potential role of private law in complementing and enhancing the traditional stance of data protection law.

1. Introduction

The advent of digitalisation, together with the increasing interaction between individuals and virtual environments characterising the information society,[1] entails a growing risk, that citizens are deprived of control and lack awareness regarding which information about them is available on the web, as an inner corollary of the computerisation of interactions.

Nowadays, the industry accumulates knowledge about individuals, which is mined from interactions occurring online—and oftentimes offline as well, mainly by means of interactions occurring between users and Information and Communication Technologies (ICTs).

Through data acquisition, companies can innovate their strategies to gain a

1 L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era* (Berlin: Springer, 2014).

 https://doi.org/10.11647/OBP.0448.13

competitive edge, deliver services, and market their products by engaging in comprehensive analyses of their target audience, allowing for the customisation of each user's experience.[2] The execution of these processes relies on automated algorithms that operate across various dimensions, employing a diverse range of techniques. For instance, companies may utilise artificial intelligence (AI) models to process user information and generate 'persuasion profiles',[3] enabling the creation of personalised content that serves the functional needs of product and service provision and, more broadly, the establishment of contracts and relationships.[4]

Amidst the pervasive sense of disorientation and disempowerment resulting from the structural changes and imbalances fostered by digital infrastructures,[5] privacy and data protection laws are increasingly viewed as pivotal instruments for enhancing individual protection. These regulations aim to ensure that individuals have meaningful oversight over information held by third parties. While privacy has traditionally been construed as the 'right to let alone',[6] functioning as a deterrent against unwarranted intrusions into personal space and as a prerequisite for exercising fundamental rights,[7] data protection laws seek to bolster individuals' effective (and, to some extent, proactive) control over the collection and utilisation of the information. In essence, these laws emphasise the right of individuals to have complete control over their analogical and digital identities.[8]

This progression can be traced, reaching at least as far back as the early 1970s. During this period, an initial strand of legal scholarship emerged, highlighting the potential new risks associated with data processing for citizens, particularly in the context of computers and large databases. In Europe, this concern led to the formulation of early sets of national laws and court decisions that established an individual right to informational self-determination,[9] building on the idea that a society, in which citizens remain unaware of who possesses information about them, is not acceptable.

Simultaneously, international agreements began to recognise a set of obligations for those involved in data processing, along with corresponding rights for individuals:

2 I. Domurath, 'Technological Totalitarianism: Data, Consumer Profiling, and the Law', in L. de Almeida, M. Cantero Gamito, M. Durovic, and K. P. Purnhagen (eds), *The Transformation of Economic Law: Essays in Honour of Hans-W. Micklitz* (Oxford: Hart Publishing, 2019), pp. 65–90.

3 B. J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (Burlington: Morgan Kaufmann, 2002).

4 S. C. Boerman, S. Kruikemeier, and F. J. Z. Borgesius, 'Online Behavioural Advertising: A Literature Review and Research Agenda', *Journal of Advertisings* 46.3 (2017), 363–376; R. Walker, *From Big Data to Big Profits: Success with Data and Analytics* (Oxford: Oxford University Press, 2015).

5 See L. A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limit* (Alphen aan den Rijn: Kluwer, 2002), p. 117.

6 S. D. Warren and L. D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4.5 (1890), 193–220.

7 W. L. Prosser, 'Privacy', *California Law Review* 48.3 (1960), 383–423; E. J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review* 39 (1964), 962–1007.

8 A. Westin, *Privacy and Freedom* (New York: Athenum, 1967); G. J. Stigler, 'An Introduction to Privacy in Economics and Politics', *Journal of Legal Studies* 9.4 (1980), 623–644.

9 Bundesverfassungsgericht 15 December 1983, 1 BvR 209/83, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983.

the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, established by the Organisation for Economic Co-operation and Development (OECD; guided by the principle of openness shaping data treatment), clarified that individuals should have the ability to ascertain the existence and nature of their personal data undergoing processing, and that they should also be informed about the main purposes of data use, the identity of data controllers, and how to engage with them.[10] The openness principle evolved alongside and as a prerequisite to the principle of individual participation, granting individuals the right to access information about data concerning them held by others. This principle also aligned with the collection limitation principle, emphasising that the collection of data should generally occur with the knowledge of the individuals to whom the data pertains.[11]

A year later, these principles received additional reinforcement through the 1981 Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[12] The Convention mandated that individuals should have the ability to confirm the existence of any automated data files containing information about them, understand the primary purposes of these files, and know the residence or place of business of the file's controller.

Contemporary technological advancements have further intensified the imperative for data protection. In today's context, individuals function as 'informative agents', consistently sharing information through online activities and interactions with IoT (Internet of Things) products and wearable devices. Consequently, the scale of personal data collection and sharing has significantly expanded, with technology playing a crucial role in facilitating the seamless flow of personal data.

As a consequence, a discernible shift occurred in contemporary legal practice: the right to the protection of personal data was enshrined as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) (2000/C 364/01),[13] and individuals were endowed with specific rights pertaining to the legal safeguarding of their personal data and information, being designated as 'data subjects' in this context.

The concept of 'data subject' was further defined in the now-repealed Directive 95/46/EC on the protection of individuals concerning the processing of personal data.[14] According to the directive (Article 2), a data subject is an identified or identifiable

10 OECD, *Recommendation of the Council of 23 September 1980: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publishing, 1980), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188, para. 12.

11 *OECD Guidelines*, paras 13 and 27.

12 Council of Europe, 'Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data', Strasburg (28 January 1981), https://rm.coe.int/1680078b37

13 (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

14 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.

natural person whose personal data is processed by a controller or processor. This definition remained unaltered following the adoption of the EU General Data Protection Regulation (GDPR) in 2016,[15] where the term 'data subject' is qualified in identical terms under Article 4 within the broader definition of 'personal data'.[16]

It should be noted that the term 'data subjects' specifically refers to individuals, excluding non-physical entities such as corporations and public authorities from this classification—and hence excluding them from the normative coverage provided by the GDPR. Within the category of natural persons, the GDPR generally avoids differentiation based on specific characteristics, be it European Union citizenship or residency. This broad and inclusive approach aligns with the universal scope outlined in the GDPR's Recital 14, emphasising its application to any natural person within the EU's territory regarding the processing of their personal data, without discrimination.

The notion of a data subject is intricately tied to the notion of personal data, wherein information pertaining to individuals receives protection only if it either directly identifies the person or renders them identifiable.[17] Consequently, the processing of anonymous data falls outside the purview of data protection law. To determine the identifiability of a person, a test of reasonable likelihood must be conducted, taking into consideration the prevailing state-of-the-art technology pertaining to the processing, its foreseeable advancements, and various objective factors, including the costs and time required for identification.[18] This definition is intentionally broad and adaptable to technological advancements, with the sole stipulation that the data in question pertains to a specific individual.[19]

Even if, among data subjects, there is no explicit differentiation based on individual characteristics at the rule level—in order for everyone to be afforded equal protection—it is noteworthy that certain features, such as the public interest associated with a person, may be considered in assessing the fairness of data processing.[20] A notable exception to this uniform approach pertains to children: the General Data Protection Regulation specifically addresses the situation of children by imposing special requirements for consent[21] and transparency obligations.[22] Data related to children is deemed particularly crucial, given their presumed lack of awareness and

15 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 (GDPR).

16 Article 4 GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

17 See P. Blume, 'The Data Subject', *European Data Protection Law Review* 4 (2015), 258–264.

18 Recital 26 GDPR.

19 See N. Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', *Law, Innovation and Technology* 10 (2018), 40–81.

20 See ECJ Case C-131/12 *Google Spain SL and Google Inc v. Agencia Española de Protecciòn de Datos (AEPD) e Mario Costeja Gonzàles* [2014] ECLI:EU:C:2014:317.

21 GDPR Article 8.

22 GDPR Article 12(1).

understanding regarding the consequences of data processing and their legal rights, which results in a diminished decision-making capability.[23]

The categorisation of an individual as a data subject serves as the normative foundation for the award and enforcement of a set of rights established by the General Data Protection Regulation. Despite their diverse structures, these rights share a common premise: the acknowledgement that, during digital interactions, data subjects often lack sufficient knowledge about the collection and processing of their data. Consequently, there is a need for substantial rectification of the information asymmetry between data subjects and their counterparts. This rectification is crucial to empower data subjects to make informed decisions about consenting to data-related practices[24] and to oversee that data processing aligns with their preferences.

2. Legal Context: Data Subjects and Their Rights in the European Normative Framework

In accordance with the structure outlined by the GDPR, measures to empower data subjects encompass both *ex ante* and *ex post* processing rights, that afford individuals a range of powers to be exercised both before and after the execution of data processing. This dual approach is designed to facilitate individuals' control over information across the entire lifecycle of personal data. Granting data subjects rights that can be asserted after data acquisition provides them with a meaningful opportunity to reassess the utilisation of their data in evolving contexts. This recognises the inherent challenge that individuals may not be able to anticipate all the consequences that may arise from the use of their personal data in advance.[25] Hence, *ex post* rights play a crucial role in guaranteeing the substantive fairness of data processing activities. Moreover, it is important to note that certain rights bestowed upon data subjects serve as prerequisites to others. For instance, the right to access information is a necessary precursor to exercising the distinct right to rectify incomplete or inaccurate data.[26] Ultimately, all data subject rights must be interpreted within the overarching framework of the general principles of transparency and fairness embedded in the GDPR.[27] These rights are operationalised through the observations and considerations made by the Court of Justice of the European Union (CJEU).

23 See Recital 38 GDPR, with regards to the special protection accorded to children under the GDPR see, among others, A. Mantelero, 'Children Online and the Future of EU Data Protection Framework: Empirical Evidences and Legal Analysis', *International Journal of Technology Policy and Law* 2 (2016), 169–181; E. Lievens and V. Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', *Computer Law and Security Review* 34.2 (2018), 269–278.

24 See G. G. Fuster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *Revista de Internet, Derecho y Política* 9 (2014), 92–104.

25 J. Ausloos and P. Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice', *International Data Privacy Law* 8.1 (2018), 4–28.

26 See ECJ Case C-454/16 *Peter Nowak v Data Protection Commissioner* [2014] ECLI:EU:C:2014:317; Case C-73/16 *College van burgemeester en wethouders van Rotterdam v Mee Rijkeboer* [2009] ECLI:EU:C:2009:293.

27 ECJ Case C-49/17 *Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629, p. 102.

Data subject rights are mostly communication-based and inspired by an overall duty to enhance transparency and comprehensibility: accordingly, the General Data Protection Regulation requires information to be concise, transparent, intelligible, and expressed in an easily accessible form, using clear and plain language.[28]

The primary and foundational mechanism for safeguarding data subjects and establishing the initial legality of data-related activities is obtaining their aware consent for data processing. According to Article 4(11), this consent must be freely given, specific, informed, unambiguous, and involve an affirmative indication that the data subject agrees to the processing of personal data related to them. Even after consent is granted, data subjects retain a set of rights that they can exercise in their interactions with the involved party.

Such rights can be organised into five categories: a) right of access; b) right to rectification and erasure; c) data portability; d) right to be forgotten; and e) rights about profiling.

The entitlement of each data subject to access their personal data, as articulated in Article 15 of the GDPR, finds its roots in the Charter of Fundamental Rights of the European Union (Article 8, Paragraph 2) and is an offshoot of the broader right to the protection of personal data. As per Article 15 GDPR, a data subject has the right to receive confirmation from the controller regarding whether personal data concerning them are undergoing processing. In cases where processing is occurring, the data subject has the right to access that personal data, along with information concerning various aspects of the processing. This includes details such as the purposes of the processing, the recipients, or categories of recipients to whom the personal data have been or will be disclosed, the expected duration for which the personal data will be retained, and the existence of the right to request rectification, erasure, or restriction of the processing activity from the controller. It is imperative that all this information be presented to the data subject in a comprehensible format. Consequently, any technical abbreviations, codifications, or acronyms in the data format are unacceptable unless their meanings are adequately clarified for the recipient.

The right to rectification—as outlined in Article 16—serves as a crucial complement to the right to access, as the accuracy of stored data is paramount in maintaining the integrity of the data subject's identity. Consequently, the data subject holds the right to request the controller to modify, correct, or update the data concerning them at any time. This includes the ability to supplement incomplete personal data. This mechanism is designed to safeguard the personal identity of individuals, ensuring that statements pertaining to them are truthful and do not compromise the personal identity they have cultivated throughout their lifetime.

Closely tied to the right of access is the right to data portability, as articulated in Article 20 of the GDPR: this right empowers the data subject to receive all the personal data previously provided to the controller, with the purpose of having that

28 GDPR Article 12.

data transmitted to another data controller. For example, individuals have the right to retrieve their contact list from a webmail application for transfer to a cloud service provided by a different operator.

Additionally, the right to be forgotten, as specified in Article 17 of the GDPR, addresses the enduring presence of data on the internet and is a direct outcome of the conclusions drawn by the Court of Justice of the European Union in the landmark *Google Spain* case.[29] In its ruling, the Court affirmed the data subject's right to request the de-indication of a link associated with news about them when that information no longer holds public interest.

Lastly, the GDPR provides data subjects with a set of rights pertaining to profiling and automated decision-making. According to Article 22, data subjects have a general entitlement not to be subject to decisions based solely on the automated processing of their data. Exceptions to this rule include cases where the processing is necessary for the conclusion or execution of a contract (e.g. automatically sending an email to all participants in a mailing list), when the treatment is based on the data subject's explicit consent, or when required by EU or Member State law.

It is important to note that, in addition to the explicit provisions in the GDPR, the specifics of all data subjects' rights are further elucidated by guidelines developed by European authorities and agencies, such as the Article 29 Data Protection Working Party and the European Data Protection Supervisor.[30]

3. Societal Relevance: Control over Data as a Core Concept for Individuals' Freedom

The establishment of a comprehensive set of rights for each data subject, coupled with the principle that consent should serve as the primary condition for lawful data processing in the absence of other legal bases,[31] originates from the acknowledgement that control over data is crucial for the self-determination and free will of data subjects.[32] This notion of control primarily encompasses the right to determine the utilisation of

29 Case C-131/12 *Google Spain SL.*

30 Amongst the most relevant documents drafted by these entities, see Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017), https://ec.europa.eu/newsroom/article29/items/611236, p. 10; European Data Protection Supervisor, 'Preliminary Opinion "Privacy and Competitiveness in the Age of Big Data"' (2014), https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en; European Data Protection Supervisor, 'Opinion 8/2016 "On the Coherent Enforcement of Fundamental Rights in the Age of Big Data"' (2016), https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf; Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679 WP259 rev.01' (2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

31 See Article 6 GDPR.

32 D. J. Solove, *The Digital Person* (New York: New York University Press, 2004), p. 77; A. F. Westin, *Privacy and Freedom*.

personal information, including decisions regarding its collection and disclosure.[33]

Over time, both national and European courts have scrutinised the concept of control to provide a functional interpretation of the provisions outlined in the GDPR in favour of data subjects. Even before the European framework for data protection was established, the German Constitutional Court underscored the idea that individuals' control over their data is indispensable to enable the freedom of individuals to make plans or decisions relying on their personal self-determination.[34] In a recent judgment involving the regulation of data monitoring through cookies, the CJEU clarified that expressing consent through a pre-selected checkbox does not constitute active behaviour, as it would 'appear impossible' to objectively ascertain whether a user has given informed consent by not deselecting a pre-ticked checkbox.[35]

As a result, it is reasonable to assert that the rights and entitlements granted by the GDPR shall be interpreted to provide substantial protection to users, in line with a perspective that views privacy and data protection as fundamentally serving to shield individuals from imbalances created by data-driven technologies.[36]

a. The Role of Information in Defining and Exercising Control over Data Processing

In consideration of the abovementioned aspects, and of the prominent focus of data protection and privacy law on principles such as informational self-determination and autonomy,[37] it is not surprising that decision-making studies, following the neoclassical approach,[38] have been playing a crucial role in shaping the application of data subjects' rights, with the 'information paradigm' operating as a key focal point in shaping data subjects' rights.[39] Drawing on the established concept of individuals as *homini oeconomici* and building upon the expected utility theory for decisions made under uncertainty, data protection traditionally presents individuals as rational actors capable of processing available information to make logical decisions aligned with their priorities. Consequently, user empowerment heavily depends on the use of disclosures and information rights (as seen in Article 15 GDPR), recognised as a fundamental tool in addressing the information asymmetry operating at the core of their vulnerability. While disclosures are not the exclusive means of protecting users, coexisting with supervisory and structural obligations like privacy by design and

33 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* (Berlin: Springer, 2018), pp. 55–83.

34 Bundesverfassungsgericht 15 December 1983.

35 ECJ Case C-673/17, *Planet49* [2019] ECLI:EU:C:2019:801.

36 R. Calo, 'Privacy, Vulnerability, and Affordance', *DePaul Law Review* 66 (2017), 592–593.

37 D. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

38 See, among others, A. Acquisti, C. Taylor, and L. Wagman, 'The Economics of Privacy', *Journal of Economic Literature* 54.2 (2016), 442–492.

39 See A. L. Allen, 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm', *Faculty Scholarship at Penn Carey Law* 32 (2000), 861–875.

by default principles, informational duties still remain a primary, if not the primary, normative resource to advance the protection of data subjects.

Additionally, it should be mentioned that, beyond the influence of the neoclassical theory, several other reasons have been adduced to support the prominence of the information paradigm as a benchmark for developing regulatory tools and disclosure duties. For instance, disclosure is observed to be a relatively low-cost form of intervention and one that is transparent for all parties involved. *Ex-ante* disclosure rules are efficiently enforceable for supervisory authorities and simultaneously provide companies with a clear means of determining compliance with relevant provisions. Finally, it is often argued that disclosure obligations garner a form of 'bi-partisan' support, striking a favourable balance between paternalistic and liberalist approaches to market regulation.[40]

b. Critiques to the Information Paradigm and to Data Protection as the Main Resource to Advance Users' Protection in Digital Environments

Against this background, it is widely recognised that a considerable body of research, particularly in behavioural studies, contends that individual decision-making frequently diverges from the neoclassical paradigm.[41] These studies present evidence of interaction dynamics—including the ones pertaining to data processing and online relations more in general—that contradict the rigidity of conventional economic theories of individual behaviour, particularly in scenarios involving standard-form contracts.

Consequently, research on topics such as information overload, the impact and consequences of the no-reading problem, and the framing and saliency bias in information provision sheds light on the inherent limitations of traditionally conceived information duties.[42] These limitations pertain to the ability of disclosure-related rights to instil genuine awareness and, more specifically, to serve as effective strategies for preserving users' control over the collection and processing of their data.

Data protection law has not remained unaffected by these developments, prompting regulatory initiatives to integrate behavioural findings into the structure of the GDPR. This is primarily achieved by reconsidering the conventional approach to the principle of transparency and advocating for a substantive approach to disclosure as a means to foster informational self-determination. This shift is evident, for instance, in GDPR provisions mandating that information and communications regarding data processing

40 O. Ben-Shahar and C. E. Schneider, 'The Failure of Mandated Disclosure', *University of Pennsylvania Law Review* 159 (2011), 647–749 (pp. 681–684).

41 See, among others, C. Sunstein, *Behavioural Law & Economics* (Cambridge, UK: Cambridge University Press, 2000).

42 I. Ayres and A. Schwartz, 'The No-Reading Problem in Consumer Contract Law', *Stanford Law Review* 66.3 (2014), 545–609; Ben-Shahar and Schneider, 'The Failure of Mandated Disclosure'; F. Cheng and C. Wu, 'Debiasing the Framing Effect: The Effect of Warning and Involvement', *Decision Support Systems* 49.3 (2010), 328–334.

be easily accessible and comprehensible, employing clear and plain language for such disclosures.[43]

The increasing emphasis on ensuring awareness of consent, as evident in express statutory provisions[44] and judicial decisions from Member States and the European Commission,[45] lends further support to these considerations. Similar concerns have been raised regarding the effectiveness of consent and its associated rights in enhancing user protection: despite being equipped with the aforementioned rights, data subjects often find it challenging to exert practical control over data processing activities; limitations arise from the fact that terms and conditions are typically drafted unilaterally, offering only partially negotiable terms.[46] Consequently, the current conceptualisation of consent has been criticised as an inherently flawed mechanism,[47] unable to operate in practice.

In addition to criticisms directed at the information paradigm and consent as the primary means for advancing user protection in the digital environment, further doubts have been raised regarding the structural capacity of data protection law to provide a meaningful basis for protecting users' self-determination when subject to decisions based on data processing.

In particular, a competing narrative asserts that the concept of a data subject should primarily be interpreted as identifying a power imbalance, extending its scope beyond qualifying merely an informational imbalance between the parties and viewing information asymmetry as just one aspect of a much broader context. This alternative perspective has garnered increasing attention in recent legal scholarship. Scholars such as Daniel Solove have theorised privacy as a tool to address power imbalances—particularly between individuals and public administration.[48] Similarly, Julie Cohen has analysed privacy, surveillance, and self-exposure through the lens of relational power.[49]

---

43 Article 5(1)(a) and Recital 58 GDPR.

44 See Article 7 GDPR.

45 See, A. G. della Concorrenza e del Mercato, 'Sanzioni per 20 milioni a Google e ad Apple per uso dei dati degli utenti a fini commerciali (PS11147)', *AGCM* (16 November 2021), https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150; Bundeskartellamt, Decision No B6–22/16 [6 February 2019]; OLGDüsseldorf, VI-Kart 1/19 (V), Bundeskartellamt c. [Facebook 26 August 2019]; Bundesgerichtshof, KVR 69/19 [23 June 2020]; Datatilsynet, 'Grindr LLC (Administrative Fine)' (2021), https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf; ECJ Case 673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801. For a comparative analysis of these decisions and their implications, see A. Davola and G. Malgieri, 'Data-Powerful' (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4027370

46 ECJ Cases C-240/98 to C-244/98 *Océano Grupo Editorial and Salvat Editores* [2000] ECLI:EU:C:2000:346, para. 25: 'the consumer is in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge. This leads to the consumer agreeing to terms drawn up in advance by the seller or supplier without being able to influence the content of the terms'.

47 M. Durovic and F. Lech, 'A Consumer Law Perspective on the Commercialization of Data', *European Review of Private Law* 29 (2021), 701–732 (p. 712).

48 D. J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review* 53 (2001), 1393–1462 (p. 1399).

49 J. E. Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012), Chapter 6; on

These studies have been advancing an increasing argument that the characteristics of the data subject—and therefore the meaningful application of the rights provided by the GDPR—can be accurately understood only by considering the corresponding capabilities of the 'counterparty' or the powerful entities, specifically digital companies utilising their data. In essence, user protection should be scrutinised and customised based on the interplay between individual characteristics and the capabilities or power of the digital companies using their data. Ideally, one could suggest that data subjects could be more appropriately identified as 'individuals subject to data processing'.

In addition, from a structural perspective, it has been noted that the primary limitations in applying data protection law arise because, by definition, the GDPR only applies when personal data is processed to deliver interactions in digital environments. Therefore, the rules of the GDPR do not extend to data that is anonymised or to techniques that do not involve personal data processing, such as gamification strategies. Additionally, in cases where personal data is used after being subjected to pseudonymisation, obtaining the data subject's explicit consent, or establishing the necessity of data processing for contract performance serves as a legal basis for the treatment. This approach reflects a focus, consistent with the goals of data protection law, on ensuring the lawfulness of the structural requirement for shaping the digital environment around users (i.e. the acquisition of data) rather than on regulating its impact on self-determination,[50] which is often regarded as offering only partial protection to individuals.

c. Data Subjects, or Subject to Data? Framing the Debate under the Lens of European Private Law

While recognising that the implementation of the GDPR has notably enhanced the position of data subjects in digital markets, it is currently questioned whether the existing framework provides individuals with sufficient protection, especially considering the pervasive impact of data-based techniques on people's lives. The deployment of ICTs, AI, and their integration into society has brought about significant changes to the human condition, resulting in transformations that profoundly alter our ways of acting and decision-making: this often leads to a blurring of distinctions between reality and virtuality—sometimes referred to as the 'onlife paradigm'.[51]

In this context, data protection law is frequently viewed as providing only a partial perspective on a much broader and more complex issue:[52] in particular, as digital technologies deeply influence various aspects of individuals' lives, with data processing

---

the relation between privacy and power in the work of the same author, see also J. E. Cohen, 'Turning Privacy Inside Out', *Theoretical Inquiries in Law* 20 (2019), 1–32 (p. 22).

50 Ursic, 'The Failure of Control Rights in the Big Data Era'.

51 Floridi, *The Onlife Manifesto*.

52 C. Koolen, 'Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data', *European Review of Private Law* 31.2(2023), 427–468.

being the main conceptual antecedent for occurrences in digital environments, there is an ongoing debate about whether the discussion should be explored from a broader perspective under the purview of European private law.

Within this strand of analysis, growing attention is directed toward examining whether a set of contractual provisions or general clauses could be effectively applied to digital interactions to safeguard self-determination. For instance, provisions regulating defective consent are considered a temporary response to risks stemming from discriminatory processing.[53] More broadly, rules on fraud and misrepresentation are being explored as potentially applicable to situations where a party misunderstands the nature of an interaction due to conditions affecting their perception of the functioning or characteristics of the offered product or services, developed based on data processing and profiling strategies.

Building on similar conceptual foundations, some authors propose the use of general private law clauses to scrutinise manipulations of the digital environment that could impair users' rights. Specifically, departing from a critical evaluation of theories centred on digital operators as information fiduciaries, it has been suggested that the principle of good faith could serve as a tool to supplement and enhance existing legal standards not originally designed for digital economies.[54] This approach tailors the scope of parties' obligations based on their expectations and, ultimately, the characteristics of the online environment. More broadly, there is an ongoing debate about whether the current shortcomings observed in data protection law for protecting individuals in the digital environment could be addressed by referring to general principles rooted in private law. In this context, significant attention is given to two key concepts: vulnerability and self-determination (oftentimes coupled with autonomy).

Regarding the first aspect, the notion of digital vulnerability is currently being explored as a potential unified framework capable of establishing a comprehensive normative theory for individuals' protection.[55] This perspective aims to shift the focus from the technical activity of data processing to the societal implications of digital interactions. Accordingly, the characteristics of digital environments are seen as able to create conditions—whether contingent or structural—that expose users to exploitation by their counterparties. Consequently, the objective of private law is seen as dynamically identifying and rectifying these conditions by categorising them as unlawful or non-compliant with protection standards. In addition, in the context of peculiar contractual

53 C. Poncibò, 'Remedies for Artificial Intelligence', in C. Poncibò, M. Ebers, and M. Zou (eds), *Contracting and Contract Law in the Age of Artificial Intelligence* (London: Bloomsbury, 2022), pp. 201–220.

54 C. Goanta, 'The Ancient Alien: Good Faith as the Facilitator of Personalized Law', *The University of Chicago Law Review Online* (2022), https://lawreviewblog.uchicago.edu/2022/03/09/bp-goanta/. On the role of good faith in European Private Law, see also Chapter 6 by Talya Deibel in this volume.

55 With vulnerability being generally defined as a state of defencelessness and susceptibility to power imbalances as arising from structural inequalities, and other market or social conditions. S. Ranchordas and M. Beck 'Vulnerability', in M. Kaufmann and H. Lomell (eds) *Handbook of Digital Criminology* (Berlin: De Gruyter, 2024), pp. 509–518; G. Malgieri, *Vulnerability and Data Protection Law* (Oxford: Oxford University Press, 2023).

relations, such as business-to-consumer transactions, this approach may also involve referring to sector-specific bodies of law, such as consumer law.[56] Digital vulnerability is thus conceptualised as a pathological condition, potentially affecting individuals in their digital existence, leading to deviations from aware and self-conscious behaviours.

In parallel, digital techniques are scrutinised for their potential to undermine individuals' self-determination and autonomy, where these concepts are commonly perceived as the right of users to make meaningful choices about their lives without coercion.[57] This perspective encourages a re-interpretation of traditional legal notions rooted in self-determination. These notions, such as agency, unfairness, and good faith, are reconsidered in the context of the distinctive characteristics of contemporary online environments. Indeed, as data processing strategies isolate individuals' characteristics, transforming them into 'dividuals' (i.e. sets of categories)[58] used as predictors for the design of provided content, and establishing connections among the shared characteristics of various data subjects, the difficulty of comprehending the dynamics of such a process is seen as compromising individuals' capacity to make genuine decisions and fully exercise their autonomy, which constitutes a core value of private law.

4. Points for Reflection

This chapter aims at tracing the debate on the role of private law in advancing data subjects' rights, with a specific focus on the dynamics of processing occurring in contemporary digital environments. In order to do so, it provides a first insight into the relevant rules in the European Union, inspecting their conceptual underpinnings; then, it offers an overview of the main contents of the GDPR, so as to clarify how control over data is currently identified as a major—if not the major—resource to protect individuals engaging in digital interactions. Against this background, though, criticisms suggest that there is wide consensus that the field is not sufficiently robust to ensure a high level of user protection and that the pervasive impact of data analyses on human lives suggests embracing a wider perspective. Hence, private law could be inspected as potentially able to complement and enrich the traditional standpoint of data protection law. Current questions, though, still animate the debate and should inspire further reflections: first and foremost, given the absence of a structural unification of private law in the EU, solutions moving from the extension of its general clauses always encompass a major element of uncertainty within the discourse on the regulation of digital interactions, also considering its intrinsic transnational dimension.[59]

56 In this regard, see Chapter 9 in this volume.

57 H. Dagan and M. Heller, *The Choice Theory of Contracts* (Cambridge, UK: Cambridge University Press, 2017).

58 M. Hildebrandt, 'Privacy as Protection of the Incomputable Self. From Agnostic to Agonistic Machine Learning', *Theoretical Inquiries in Law* 20.1 (2019), 83–121.

59 S. Grundmann (ed.), *European Contract Law in the Digital Age* (Cambridge, UK: Intersentia, 2018); M. Bartl, 'Socio-Economic Imaginaries and European Private Law', in P. F. Kjaer (ed.), *The Law of Political*

In addition, the transformative effects—especially in terms of conceptualisation of self-determination—that could arise from a more substantive application of private law to digital techniques based on data processing are still largely unexplored: in particular, it is worth evaluating if, as self-determination in contemporary digital ecosystems emerges as a structural byproduct of the exposition of users to the unique characteristics of such environments, this could further reshape our understanding of self-determination itself, establishing ways for re-conceptualising its role within private law theory and moving beyond the primary qualification of users as 'data subjects' in the digital realm.

Q1: How might we reconceptualise the notion of 'data subject' to better capture the broader power dynamics at play in digital environments?

Q2: What specific limitations of the regulatory approach based on information and control have emerged in practice, and what alternative frameworks might better safeguard individuals' rights?

Q3: What advantages and challenges might arise from applying traditional private law doctrines to digital interactions?

Q4: How might this concept of 'digital vulnerability' be operationalised in legal practice, and what specific protections might it offer that current approaches do not?

Q5: How might consent mechanisms be redesigned to better align with the realities of digital interactions? Or should we move beyond consent-based models entirely?

Q6: What might a reconceptualised notion of self-determination look like in the digital age?

Bibliography

A. G. della Concorrenza e del Mercato, 'Sanzioni per 20 milioni a Google e ad Apple per uso dei dati degli utenti a fini commerciali (PS11147)', *AGCM* (16 November 2021), https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150

Acquisti, A., C. Taylor, and L. Wagman, 'The Economics of Privacy', *Journal of Economic Literature*54.2 (2016), 442–492, https://doi.org/10.1257/jel.54.2.442

Allen, A. L., 'Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm', *Faculty Scholarship at Penn Carey Law* 32 (2000), 861–875

Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679 WP259 rev.01' (2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Economy: Transformations in the Function of Law (Cambridge, UK: Cambridge University Press, 2029), pp. 228–253.

Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017), https://ec.europa.eu/newsroom/article29/items/611236

Ausloos, J., and P. Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice', *International Data Privacy Law* 8.1 (2018), 4–28, https://doi.org/10.1093/idpl/ipy001

Ayres, I., and A. Schwartz, 'The No-Reading Problem in Consumer Contract Law', *Stanford Law Review* 66.3 (2014), 545–609

Bartl, M., 'Socio-Economic Imaginaries and European Private Law', in P. F. Kjaer (ed.), *The Law of Political Economy: Transformations in the Function of Law* (Cambridge, UK: Cambridge University Press, 2029), pp. 228–253, https://doi.org/10.1017/9781108675635

Ben-Shahar, O., and C. E. Schneider, 'The Failure of Mandated Disclosure', *University of Pennsylvania Law Review* 159 (2011), 647–749

Bloustein, E. J., 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review* 39 (1964), 962–1007

Blume, P., 'The Data Subject', *European Data Protection Law Review* 4 (2015), 258–264, https://doi.org/10.21552/EDPL/2015/4/4

Boerman, S. C., S. Kruikemeier, and F. J. Z. Borgesius, 'Online Behavioural Advertising: A Literature Review and Research Agenda', *Journal of Advertisings* 46.3 (2017), 363–376, https://doi.org/10.1080/00913367.2017.1339368

Bygrave, L. A., *Data Protection Law: Approaching Its Rationale, Logic and Limit* (Alphen aan den Rijn: Kluwer, 2002)

Calo, R., 'Privacy, Vulnerability, and Affordance', *DePaul Law Review* 66 (2017), 592–593

Cheng, F., and C. Wu, 'Debiasing the Framing Effect: The Effect of Warning and Involvement', *Decision Support Systems* 49.3 (2010), 328–334, https://doi.org/10.1016/j.dss.2010.04.002

Cohen, J. E., *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012)

Cohen, J. E., 'Turning Privacy Inside Out', *Theoretical Inquiries in Law* 20 (2019), 1–32

Council of Europe, 'Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data', Strasburg (28 January 1981), https://rm.coe.int/1680078b37

Dagan, H., and M. Heller, *The Choice Theory of Contracts* (Cambridge, UK: Cambridge University Press, 2017)

Datatilsynet, 'Grindr LLC (Administrative Fine)' (2021), https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf

Davola, A., and G. Malgieri, 'Data-Powerful' (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4027370

Domurath, I., 'Technological Totalitarianism: Data, Consumer Profiling, and the Law', in L. de Almeida, M. Cantero Gamito, M. Durovic, and K. P. Purnhagen (eds), *The Transformation of Economic Law: Essays in Honour of Hans-W. Micklitz* (Oxford: Hart Publishing, 2019), pp. 65–90

Durovic, M., and F. Lech, 'A Consumer Law Perspective on the Commercialization of Data', *European Review of Private Law* 29 (2021), 701–732

European Data Protection Supervisor, 'Opinion 8/2016 "On the Coherent Enforcement of Fundamental Rights in the Age of Big Data"' (2016), https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

European Data Protection Supervisor, 'Preliminary Opinion "Privacy and Competitiveness in the Age of Big Data"' (2014), https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en

Floridi, B., *The Onlife Manifesto. Being Human in a Hyperconnected Era* (Berlin: Springer, 2014)

Fogg, B. J., *Persuasive Technology: Using Computers to Change What We Think and Do* (Burlington: Morgan Kaufmann, 2002)

Fuster, G. G., 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *Revista de Internet, Derecho y Política* 9 (2014), 92–104

Goanta, C., 'The Ancient Alien: Good Faith as the Facilitator of Personalized Law', *The University of Chicago Law Review Online* (2022), https://lawreviewblog.uchicago.edu/2022/03/09/bp-goanta/

Grundmann, S. (ed.), *European Contract Law in the Digital Age* (Cambridge, UK: Intersentia, 2018)

Hildebrandt, M., 'Privacy as Protection of the Incomputable Self. From Agnostic to Agonistic Machine Learning', *Theoretical Inquiries in Law* 20.1 (2019), 83–121, https://doi.org/10.1515/til-2019-0004

Koolen, C., 'Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data', *European Review of Private Law* 31.2(2023), 427–468, https://doi.org/10.54648/erpl2023018

Lievens, E., and V. Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', *Computer Law and Security Review* 34.2 (2018), 269–278, https://doi.org/10.1016/j.clsr.2017.09.007

Malgieri, G., *Vulnerability and Data Protection Law* (Oxford: Oxford University Press, 2023)

Mantelero, A., 'Children Online and the Future of EU Data Protection Framework: Empirical Evidences and Legal Analysis', *International Journal of Technology Policy and Law* 2 (2016), 169–181, https://doi.org/10.1504/IJTPL.2016.077189

OECD, *Recommendation of the Council of 23 September 1980: OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publishing, 1980), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Poncibò, C., 'Remedies for Artificial Intelligence', in C. Poncibò, M. Ebers, and M. Zou (eds), *Contracting and Contract Law in the Age of Artificial Intelligence* (London: Bloomsbury, 2022), pp. 201–220

Prosser, W. L., 'Privacy', *California Law Review* 48.3 (1960), 383–423

Ranchordas, S., and M. Beck 'Vulnerability', in M. Kaufmann and H. Lomell (eds) *Handbook of Digital Criminology* (Berlin: De Gruyter, 2024), pp. 509–518

Solove, D. J., *The Digital Person* (New York: New York University Press, 2004)

Solove, D. J., 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review* 53 (2001), 1393–1462

Solove, D., *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008)

Stigler, G. J., 'An Introduction to Privacy in Economics and Politics', *Journal of Legal Studies* 9.4 (1980), 623–644

Sunstein, C., *Behavioural Law & Economics* (Cambridge, UK: Cambridge University Press, 2000)

Ursic, H., '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* (Berlin: Springer, 2018), pp. 55–83

Walker, R., *From Big Data to Big Profits: Success with Data and Analytics* (Oxford: Oxford University Press, 2015)

Warren, S. D., and L. D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4.5 (1890), 193–220

Westin, A., *Privacy and Freedom* (New York: Atheneum, 1967)