Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act

*Maximilian Gartner**

Individual autonomy has been explicitly recognized in the European Union's 2022 Data Act proposal. This article shows that such unprecedented inclusion of autonomy in an EU regulatory framework targeting the digital domain marks a paradigm shift for digital-sector legislation away from mostly tacit recognition of autonomy as a meta-principle to a more aggressive regulatory posture. It contextualizes this nascent development by highlighting the turn towards the protection of mental privacy in recent sector-relevant legislation and investigates the intent and scope of Article 6 of the Data Act proposal in light of an increasing regulatory focus on so-called dark patterns.

Keywords: Individual Autonomy | European Digital Legislation | Data Act | Article 6

I. Introduction

Under the umbrella of its digital strategy, and in particular its European Strategy for Data (ESD),[1] the European Commission has intensified its regulatory presence in the digital domain in recent years. One of the most recent proposals in this space is the Data Act (DA)[2], an instrument that primarily (but not exclusively) regulates data access and use between businesses themselves (B2B) and the public sector (B2G). Curiously, with this proposal, the European Commission has now introduced the term 'autonomy' into the (prospective) legislative body that regulates the European digital landscape. From there, similar references to autonomy have also been added to the Digital Service Act (DSA), which has recently entered into force.[3] This paper shows that this marks a milestone in a turn towards protection of mental privacy, surfacing a hidden trend that has been growing in recent years.

How did we get here? One of the main goals of the DA (which is still in its draft stage at the time of writing) is to 'increase legal certainty for companies and consumers' in relation to the generation and use of data.[4] To this end, the DA proposal will mandate that data-collecting devices (ie IoT-devices)[5] must be designed in a way that the data their use generates is accessible by the user either direct-

DOI: 10.21552/edpl/2022/4/6

* Maximilian Gartner, PhD Candidate, University of Bologna | KU Leuven | Mykolas Romeris University. For correspondence: <maximilian.gartner@kuleuven.be> | <maximilian.gartner2@unibo.it>, https://last-jd-rioe.eu/maximilian-gartner.html
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD 'Law, Science and Technology Rights of Internet of Everything' grant agreement No 814177.

1 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European Strategy for Data COM (2020) 66 Final' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

2 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) [2022] COM/2022/68 final.

3 Rec 67 DSA.

4 See eg the communication material at 'Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy' (2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113>.

5 See eg ibid Rec. 14, 19.

ly[6] or through request to the respective data holder.[7] This requirement seemingly mirrors the General Data Protection Regulation's (GDPR) right of access, but now applies to data beyond personal data. The DA offers a shortcut of sorts to the user, who now has discretion over this data and may want to make it available to a third party. Upon request of either the user or another party acting for the user, the data holder must make the aforementioned data available to a third party directly.[8] These third parties, upon obtainment of the data by the data holder, are subject to a number of requirements. Interestingly, the first of these requirements reads as follows:

'The third party shall not [...] coerce, deceive or manipulate the user in any way, by subverting or impairing their autonomy, decision-making or choices of the user, including by means of a digital interface with the user.'[9]

This provision marks the first time that the term autonomy is used in the main text of data-related European legislation as proposed by the European Commission, and the first time it is used to refer to human autonomy. Since then, a similar provision has also been added to the Digital Service Act that has since entered into force. However, neither the draft nor the DSA provide a definition of the term, so the scope of the obligation to not impair a user's autonomy appears somewhat opaque.

While the explicit wording is novel, it is by no means a new idea. This text aims to trace the legal recognition of self-determination in recent European data-related legislation and provide the context in which this regulatory approach is grounded. Through a short survey of legal sources, this article shows that individual autonomy has already been held as a meta-principle informing regulatory measures, in particular in the field of privacy and data protection. The explicit inclusion of individual autonomy in the DA must be seen as a consequential next step following increased focus on mental privacy and the mental aspects of self-determination.

The analysis after this introduction proceeds as follows. The second section gives a short overview over the common meaning of the term as the basis for subsequent interpretation. The third section provides context by highlighting how the link between data protection, privacy and autonomy has been recognized by a now famous German court case pertaining to informational self-determination. The fourth section argues that the mental aspect of autonomy and decision-making have enjoyed increased attention as more recent legislative proposal aim to strengthen protection for mental privacy. The fifth section investigates the scope of Article 6 under the DA proposal under this context and considers if the provision is aimed purely at adversarial design. The sixth section connects these threads and highlights that recognition and protection of individual autonomy is no longer limited to a status of meta-principle but has surfaced as an explicit value. I conclude in section seven.

II. First Delimitations of Autonomy

The DA and its related legislative instruments give no legal definition of the term autonomy. Because the term is used colloquially and as a technical term in certain scientific disciplines, this section provides a first delimitation of autonomy as a high-level concept to serve as context for the remaining analysis.

1. Ordinary Meaning of Autonomy

Proper legal methodology suggests that a good place to start interpreting this newly introduced term is to consider its ordinary meaning.[10] By translating literally from its Greek origin words *αὐτο* (meaning 'self') and *νόμος (*meaning rule or law), we derive at an original meaning of a state or capacity to govern oneself, or more liberally, self-determination. In the present case, grammatical interpretation of Article 6 DA makes clear that we must consider individuals (ie the users of a product or service collecting data) as the subject of this self-determination. Autonomy in the meaning of Article 6 DA hence clearly refers to individual (or personal) autonomy, ie the capacity of individuals to exercise their self-determination capacities.

6 Ibid Art 3.

7 Ibid Art 4.

8 This as long as the third party is not considered a gatekeeper under the DMA, see ibid Art 5.

9 Ibid Art 6 para 2 (a)

10 Koen Lenaerts and José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Colum. J. Eur. L. 3; Hannes Rösler, 'Interpretation of EU Law' (2012) 2 Max Planck Encyclopaedia of European Private Law 979.

2. Individual Autonomy as a Technical Term

It is useful to remember that insofar terminology is used colloquially or without definition, this happens before a backdrop of other disciplines with a more granular or sharper understanding of the term in question. Awareness of the (interdisciplinary) underpinnings of autonomy is useful, not only because they can seep into general use but also because they represent a basis from which issues are identified and criticisms are offered.[11] In the domain of philosophy, where individual autonomy is best situated as a technical term,[12] autonomy is often considered as a congruence between an individual's choices, the motivations (or mental states) that inform those choices, and the motivations behind those motivations.[13] In this sense, autonomy is mostly internal to the individual. Simplified, an individual is autonomous if they make autonomous choices, and they make autonomous choices if their choices are aligned with their preferences. This view is not uncontested, with critics voicing the need for recognition of other, non-internal factors.[14] In summary, autonomy under this view describes self-determination through valid decision making.

The term autonomy is also already used in the legal domain. The concept of self-determination is found eg in the principles of contractual autonomy where it describes the capacity of self-governance through freedom of contract.[15] And more broadly still, an individual's capacity to govern oneself is considered by the legal philosopher Hans Kelsen as one underlying characteristic of the legal domain itself.[16]

The term autonomy is hence not new but comes pre-charged with meaning. Insofar it is used as a reference point in legislative instruments without definitions, we may understand it as a reference to an extra-legal value, diffuse in scope and potentially subject to change in what the reference entails.[17] At the same time, it is important to remember that the definition attempts from different disciplines, be they legal or other, may inform but cannot simply be transplanted into the context of European digital legislation. Hence, it is necessary to identify the connection points between the broader concept of autonomy and the ESD. The first contextual clue comes from the centrality of the tenet of privacy within the digital strategy of the European Union. The second clue here comes from the domain, which is targeted by the regulation, namely the domain of data protection.

III. Informational Privacy and Autonomy

To understand the motivation behind the inclusion of explicit autonomy safeguards within the ESD, it is useful to consider it an extension of existing privacy

11 For example, the Independent High-Level Expert Group on Artificial Intelligence that has advised on the European Strategy for Artificial Intelligence also has ethicists and philosophers in its ranks, propagating their respective disciplines' discourses into the political process. The later discussed proposed amendments to the draft AI Act explicitly call out the Group's work on Trustworthy AI and have suggested enshrining their findings in a series of principles within the regulation, see the proposed Rec 5b, Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties Justice and Home-Affairs, 'Amendments - Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' <https://bit.ly/3Mboami>.

12 See eg Andrews Reath, 'Ethical Autonomy', *Routledge Encyclopedia of Philosophy* (Taylor and Francis 1998); Markus Christen, 'Autonomie – Eine Aufgabe Für Die Philosophie' (2007) 66 Schweizerische Zeitschrift für Philosophie <https://schwabeonline.ch/schwabe-xaveropp/elibrary/openurl?id=doi%3A10.24894%2FStPh-de.2007.66012>.

13 Harry Frankfurt, 'Freedom of Will and Concept of a Person' (1971) 68 The Journal of Philosophy 5; Andrew Sneddon, *Autonomy* (1st edn, Bloomsbury Academic 2013); Gerald Dworkin, 'The Nature of Autonomy' (2015) 2015 Nordic Journal of Studies in Educational Policy 28479 <https://www.tandfonline.com/doi/full/10.3402/nstep.v1.28479>.

14 Natalie Stoljar, 'Autonomy and the Feminist Intuition' in Catriona MacKenzie and Natalie Stoljar. (eds), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency and the Social Self* (Oxford University Press 2000); Susan Brison, 'Relational Autonomy and Freedom of Expression' in Catriona Mackenzie and Natalie Stoljar (eds), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency and the Social Self* (Oxford University Press 2000); Catriona Mackenzie, 'Relational Autonomy, Normative Authority and Perfectionism' (2008) 39 Journal of Social Philosophy 512 <http://doi.wiley.com/10.1111/j.1467-9833.2008.00440.x>.

15 See for the nuances in terminology eg Salvatore Patti, 'Contractual Autonomy and European Private Law', *Rules and Principles in European Contract Law* (Intersentia) <https://www.cambridge.org/core/product/identifier/CBO9781780685434A032/type/book_part>.

16 Hans Kelsen, 'Causality and Imputation' (1950) LXI Ethics passim. Kelsen uses the term freedom of will here. Nb that there are two implications here: First, autonomy serves as the prerequisite to create legal rules in the first place. In the literature, this is often explored at the intersection of autonomy and democracy. Second, autonomy of some form serves as a requirement for laws to apply or attribute consequences to actors. See for these also Brian Barry, 'The Politics of Free Will' (1997) 59 Tijdschrift voor Filosofie 615 <http://www.jstor.org/stable/40887805> and for an overview 'Autonomy in Moral and Political Philosophy', *The Stanford Encyclopedia of Philosophy* (2020) <https://plato.stanford.edu/entries/autonomy-moral/>.

17 See for this concept eg Leszek Leszczyński, 'Extra-Legal Values in Judicial Interpretation of Law: A Model Reasoning and Few Examples' (2020) 33 International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique 1073 <https://link.springer.com/10.1007/s11196-020-09773-y>.

safeguards. This section outlines the connection between autonomy and privacy generally, and informational privacy specifically.

Much of the current and prospective legislation surrounding the ESD is firmly aimed at measures to safeguard privacy, and its derivative, but now mostly emancipated concept of data protection.[18] Presently, the right to data protection is understood to extend beyond the protection of the right privacy.[19] This is highly relevant, as privacy is often seen to serve as a prerequisite to autonomy[20], or at least as an enabling state hereto.[21] As a result, due to their entangled nature, measures that safeguard autonomy tend to do so informed by privacy concerns as well.[22] At the same time, apprehensions about autonomy inform the consideration of privacy concerns.[23] The prospective legislation under the ESD continuously emphasizes its grounding in the catalogue of fundamental rights. And naturally, two of these fundamental rights, as codified in the European Charter of Fundamental Rights, are the right to privacy and data protection. This is only further substantiated when considering the substantively similar Article 8 of its 'precursor', the European Convention on Human Rights and its attached case-law. Under this provision, one's psychological integrity, personal beliefs and personal development, as well as one's physical and moral integrity sphere of relations to and between other people (and oneself) were found to be protected.[24] This aligns well with the scope of autonomy explored previously, in which mental coherence and integrity are paramount.[25]

It is common to distinguish different types of privacy, generally representing different aspects of freedom from certain interferences. Based on work by Tavani and Floridi, we distinguish broadly between two types of privacy that are particularly relevant here: informational privacy and mental privacy. Informational privacy is the freedom from informational interferences and intrusions. Such intrusions arise then out of the collection and use of information about an individual. Likewise, mental privacy is the freedom from psychological interferences and intrusions.[26] Consequently, informational privacy intrusions are collection and exploitation measures of information of inappropriate type or amount while mental privacy intrusions are exploitation measures of psychological features, including cognitive biases.[27] The most obvious connection between these aspects of privacy and autonomy is the following: informational privacy protects from autonomy constraints made (more) effective because they are based on facilitating information, while mental privacy protects from autonomy constraints by ensuring the integrity of an individual's decision-making and deliberation process.

18 See eg M Tzanou, 'Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right' (2013) 3 International Data Privacy Law 88 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipt004>; J Kokott and C Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipt017>; Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 522 <https://www.sciencedirect.com/science/article/pii/S0267364913001325>.

19 Alexander Roßnagel and Christian Geminn, '"Privatheit' Und 'Privatsphäre' Aus Der Perspektive Des Rechts - Ein Überblick' [2015] Juristenzeitung 703.

20 See eg Stanley Benn, 'Privacy, Freedom, and Respect for Persons' in Ferdinand Shoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984) pp 241ff.

21 See eg Joseph Kupfer, 'Privacy, Autonomy, and Self-Concept' (1987) 24 American Philosophical Quarterly 81, 83.

22 Indeed, there seems to be considerable overlap in concerns of privacy and autonomy. Holvast, surveying existing literature notes that the terms freedom, control and self-determination are used in almost all publications relating to privacy, from which the relevance to autonomy is self-evident; see Jan Holvast, 'History of Privacy' in Vashek Matyáš and others (eds) (Springer Berlin Heidelberg 2009) p 16.

23 For example, the European Court of Human Rights has found that Article 8 of the ECHR (ie Right to Privacy) is based on the concept of 'human autonomy'; see eg Pretty v. The United Kingdom (2002) ECHR para 61; (2002) Christine Goodwin v. The United Kingdom (2002) ECHR para 90; Evans v. The United Kingdom (2007) para 71.

24 Cf. Nicolae Virgiliu Tănase v. Romania [GC] (2019) ECHR para 128 and Bensaid v. the United Kingdom (2001) ECHR para 47.

25 For a closer analysis on how the case law aligns with the philosophical concept of autonomy compare also Maximilian Gartner, 'Fit for the Future: A Pragmatic Account of Human Autonomy to Understand Emerging Issues in The Internet of Everything' in Marie Bourguignon and others (eds), *Technology and Society: The Evolution of the Legal Landscape* (Gompel&Svacina 2021).

26 See H Tavani, 'Informational Privacy: Concepts, Theories and Controversies' in KE Himma and HT Tavani (eds), *Handbook of Information and Computer Ethics* (Haboken: John Wiley 2008); Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford University Press 2014) 208f; Note that the distinction between different types of privacy conceptions is not clean. In particular, conceptions of decisional privacy, i.e. privacy that protects the ability to make decisions, may overlap largely with mental privacy, depending on how decisional privacy is scoped, see Marjolein Lanzing, '"Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies' (2019) 32 Philosophy & Technology 549 <http://link.springer.com/10.1007/s13347-018-0316-4>. For clarity, this text adopts the lens of mental privacy.

27 DSA 67 offers a few examples in which psychological intrusions can undermine the decision making capabilities, such as making the cancellation of a service more cumbersome, certain choices more difficult or time-consuming to select or deceiving individuals by nudging them into decisions e.g. through default-settings. Nb that by themselves none of these measures are truly difficult to overcome.

In the domain of technology regulation, informational privacy (or information privacy) seemed to be historically established as a primary motivator. Informational privacy is an intuitive prerequisite to autonomy to the extent that interference with an individual's autonomy becomes more effective as more information about the individual is known and can be acted upon. Connecting the concepts of privacy and autonomy is then the notion that the right to privacy encompasses (partly) the concept of individual autonomy and concerns itself specifically with the human being as an autonomous subject.

Somewhat prescient to the issues of emerging technologies, the German Constitutional Court (*Bundesverfassungsgericht*) recognized the concept of informational self-determination as encompassed in the general personality rights of German Citizens, as imbued by the German Constitution as early as 1983.[28] The decision noted that automated information gathering and processing allowed for an exceedingly complete profile of the personality of individuals and, consequentially, ever more effective means of influence.[29] Consequently, the court recognized the right of an individual to determine use and disclosure of their personal data.[30] Naturally, this decision, affirming the arguments that German legal scholars had been bringing forward for a while,[31] had significant impact beyond the jurisdiction it was reached in.[32] Rephrasing this in the context of this analysis, the court recognized the increased leverage over individual self-determination that technology enabled, and as a result strengthened their informational privacy, as informational privacy intrusions, i.e. the collection and use of personal information, was limited.

Since then, informational privacy is still safeguarded by current legislation and judicial decisions. One of the more prominent matters of discussion with respect to informational privacy and autonomy was the so-called *right to be forgotten*.[33] Following the same logic as in the German court case above, restricting access to personal information limits or remedies the informational privacy intrusion of large-scale information collection. Since then, the power to modulate how personal data can be collected, stored and used has been enshrined as a core tenet of the General Data Protection Regulation's catalogue of data subject rights.[34]

The draft DA also entitles users of services to information about non-personal data they produce. We take from this that if autonomy is inherent to (informational) privacy and data protection,[35] the existing safeguards for those values mean that the protection of autonomy has been a non-explicit goal of legislation already, even if left unnamed.

IV. The Turn Towards Explicit Mental Privacy Protection

Informational privacy is seen as a prerequisite safeguard to an individual's exercise of autonomy. But mental privacy is even closer entrenched with an individual's autonomy, if not identical to the concept[36], as it describes the very ability of an individual to make decisions.[37] Revisiting the definitions outlined

28 See eg Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (1st edn, Springer 2009).

29 *1 BvR 209/83 (Volkszählung)* [1983] German BVerfG BVerfGE 65, 1 – 71 [93].

30 Ibid para 1.

31 Cf in particular Wilhelm Steinmüller and others, 'Grundfragen Des Datenschutz - Gutachten Im Auftrag Des Bundesministeriums Des Innern (Drucksache VI/3826)' (1971) 93,96,120.

32 With some scholars going as far as calling it an '*avant-garde* decision', see Rouvroy and Poullet (n 28) 45.

33 See Section 4.1f in Cécile de Terwangne, 'The Right to Be Forgotten and Informational Autonomy in the Digital Environment', *The ethics of memory in a digital age* (Springer 2014).

34 It is noteworthy in this context that the data subject's control over their information adds an additional layer to their "informational self-determination": Not only can they deny opportunity to be affected by information-fed technology, they can also choose to yield (or not restrict) information, which would have the validation of their conscious (and autonomous) approval.

35 Which is the contention of many, see e.g. Kupfer (n 21); Benn (n 20); Holvast (n 22). Similarly, the ECHR has also found that the right to privacy is based on the concept of "human autonomy", see e.g. . ECHR (2002) Pretty v. The United Kingdom § 61; ECHR (2002) Christine Goodwin v. The United Kingdom § 90; ECHR (2007) Evans v. The United Kingdom § 71.

36 Finding a distinction between mental privacy and autonomy *per se* is difficult and beyond the scope of this text. The interested reader is referred to Marjolein Lanzing, ''Strongly Recommended' Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies' (2019) 32 Philosophy & Technology 549 <http://link.springer.com/10.1007/s13347-018-0316-4> (nb the slightly different terminology in the article).

37 Bert-Jaap Koops and others, 'A Typology of Privacy ' 38 University of Pennsylvania Journal of International Law 483, 50ff <https://heinonline.org/HOL/P?h=hein.journals/upjiel38&i=489>. Note the distinction between decisional and intellectual privacy (freedom of mental intrusions), in which the authors suggest that decisional privacy is the active exercise of intellectual privacy. This tracks well with the conception of autonomy as a product of congruent mental states and highlights the necessity of valid decision-making capacity.

in Section II, the mental aspects of autonomy relate to the process of valid decision-making in line with an individual's preferences and interests. This section shows that current and upcoming regulations seem to have taken a turn towards more explicit protection of this aspect of privacy and autonomy *per se* as well, as evidenced by the following data points.[38]

1. Autonomy Considerations in the GDPR

Following in the footsteps of the Data Protection Directive 95/46/EC, the GDPR represented the first comprehensive European regulation of the digital domain. While much of the measures of data protection generally relate closely to informational privacy as mentioned in the previous section, there are similarities to the above-mentioned Article 6. The most salient protection of mental privacy comes with the provisions concerning a data subject's consent. As is well known, consent represents one of the main justifications for data processing, and this consent must be given freely. As highlighted by the European Data Protection Board (EDPB) and its predecessor, the Article 29 Data Protection Working Party, deception, intimidation, coercion, compulsion, pressure or 'inability to exercise free will' can preclude the validity of consent given.[39] The wording of Article 6 DA is strongly reminiscent of this language and can be considered as translating the assessment of the EDPB into code (albeit in a different overall context).[40] Another autonomy-safeguarding measure is the protection awarded by the principle of lawful, fair and transparent processing outlined in Article 5 para 1 (a) of the GDPR. The fairness principle not only precludes data processing that is detrimental or discriminatory, but also unexpected or misleading.[41] For example, the EDPB has interpreted the fairness principle encoded in the GDPR as being incompatible with autonomy-constraining nudges and dark patterns (see for this below) even prior to their guidelines on adversarial design.[42] Similarly, the EDPB has also stated that data subject autonomy is covered by the lawfulness principle.[43]

2. Autonomy Considerations in the European Approach to Artificial Intelligence

Another important testament to the increasingly explicit focus on autonomy is the report by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. In it, the expert group lists respect for human autonomy, including mental autonomy, as a core ethical principle (and equates the concept with decision-making).[44] The report identifies practices of coercion, deceiving, manipulating conditioning or herding individuals as particular threats to this principle.[45] This is also in line with international trends; a 2019 survey of ethical guidelines for AI found that 'freedom and autonomy' was considered an explicit core principle in almost half of the frameworks investigated.[46] Following this, a draft of the Artificial Intelligence Act, leaked by the online journalism company Politico, included the prohibition of an AI system if it was

38 The following represents but a short survey of the legal instruments referenced therein. A full analysis of each instrument through the lens of autonomy would be beyond the length requirements for this text and is left for another time.

39 European Data Protection Board, 'Guidelines 5/2020 on consent under Regulation 2016/679, Version 1.1 (2020) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, para 24, 47.

40 The fact that the scope of the legislation is different between the instruments is not as relevant here. While the GDPR deals first and foremost with personal data, and the data act complements this by also dealing with non-personal data, the notion of giving justification to processing by a data controller (in the GDPR) or a third party (in the Data Act proposal) remains congruent. At this point it is noteworthy that the Data Act proposal does not verbatim use the concept of consent in its provisions dealing with third party data sharing, but instead describes a situation in which a request by the user or by the third party acting on behalf of the user issues a request to the data holder.

41 See e.g. European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2020) 19 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, para 70.

42 European Data Protection Board, 'Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them' (2022) <https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>

43 European Data Protection Board (n 42), para 68.

44 High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) 10,26 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>.

45 ibid 12.

46 Anna Jobin, Marcello Ienca and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1 Nature Machine Intelligence 389.

designed or used in a manner that 'manipulates human behaviour, opinions or decisions through choice architectures or other elements of user interfaces, causing a person to behave, form an opinion or take a decision to their detriment' or 'exploits information or prediction about a person or group of persons in order to target their vulnerabilities or special circumstances, causing a person to behave, form an opinion or take a decision to their detriment'.[47] While both of these provisions have been changed (and arguably weakened) by the final proposal by the European Commission, the adapted prohibitions still target the mental integrity of individuals under threat. Under Article 5 of the proposed AI Act, prohibition now applies to certain 'subliminal techniques' which 'distort a person's behaviour', or to certain systems that 'exploit any of the vulnerabilities' such as 'age, physical or mental disability' of persons. These formulations may very well be subject to further changes, as the LIBE and IMCO committees have tabled possible amendments to the language of the article.[48] Nonetheless, even with the narrower scope, the act clearly recognizes mental integrity of individuals as a matter of concern. Unlike the report of the High-Level Expert Group, the Act does not use the term autonomy in connections with individuals (and instead describes artificial intelligence as autonomous, somewhat exhausting the term for the purposes of the regulation).[49] However, a currently tabled amendment by Axel Voss, Deirde Clune and Eva Maydell would introduce a reference to (human) personal autonomy as well.[50] The suggested provision suggest high-level principles for "trustworthy AI systems, one of which is "human agency and oversight". This principle postulates that the development and use of AI as a tool must "serve people, respect human dignity and personal autonomy and [...] is functioning in a way that can be controlled and overseen by humans [...]." The stated goal of this addition is to influence future harmonisation efforts (eg through code of conducts or standardization requests).[51]

3. Autonomy Considerations in the European Data Strategy

While the European Approach to Artificial Intelligence was focused on the eponymous intelligent systems, the European Commission has introduced a swath of legislation that covers the European market for data as a whole under the umbrella of the European Data Strategy. The DA, which first explicitly introduced the notion of individual autonomy, is the latest of a few instruments under this strategy. Crucially, due to the long incubation period of European legislation, these instruments have been developed in parallel and have clearly influenced each other.

During this development phase, one phenomenon of technology design that is considered highly problematic for individual autonomy has demanded increased attention.[52] Increasingly, user interface design characteristics are recognized for their coercive or manipulative power and their ability to lead users to take actions against their interest. This phenomenon is typically called a 'dark pattern'. Dark patterns are design techniques that push or deceive consumers into decisions that have negative conse-

47 Art 6, leaked AI Act. An archived version is accessible at the following link at the time of writing: https://drive.google.com/file/d/1ZaBPsfor_aHKNeeyXxk9uJfTru747EOn/view

48 Protection and Committee on Civil Liberties Justice and Home-Affairs (n 11). It is notable that the IMCO committee particularly has scheduled hearings on the risks of dark patterns by external experts.

49 See eg Rec 6 of the AI Act as proposed by the European Commission, see Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised rules on artificial intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (2021) COM/2021/206 final.

50 See the proposed Article 4 a in Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties Justice and Home-Affairs (n 11).

51 This is not to be confused with the other references to human oversight in the AI Act draft, in particular Article 14, that imposes human-machine interface tools for control purposes as mandatory features for high-risk AI systems.

52 See eg Gregory Day and Abbey Stemler, 'Are Dark Patterns Anticompetitive? ' 72 Alabama Law Review 1 <https://heinonline.org/HOL/P?h=hein.journals/bamalr72&i=11>; Davide Maria Parrilli and Rodrigo Hernandez-Ramirez, 'Re-Designing Dark Patterns to Improve Privacy', *2020 IEEE International Symposium on Technology and Society (ISTAS)* (IEEE 2020); Diana MacDonald, 'Anti-Patterns and Dark Patterns', *Practical UI Patterns for Design Systems* (Apress 2019) <http://link.springer.com/10.1007/978-1-4842-4938-3_5>; Ari Ezra Waldman, 'Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'' (2020) 31 Current Opinion in Psychology 105; Than Htut Soe and others, 'Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets', *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (ACM 2020); Saul Greenberg and others, 'Dark Patterns in Proxemic Interactions', *Proceedings of the 2014 conference on Designing interactive systems* (ACM 2014); Colin M Gray and others, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective', *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021).

quences for them.[53] Examples of dark patterns include protracted procedures to withdraw from paid services or visual and procedural asymmetry in offering choices about data collection on websites through cookie-banners.[54] As a result of this attention, dark patterns also have received increased scrutiny from data protection watchdogs such as the European Data Protection Board and the local data protection authorities.[55] They have also led to substantial fines by regulatory authorities, such as in the cases brought against Google and Facebook by the French CNIL.[56] In both cases, the dark pattern identified as unacceptable was that opting out of cookie consent took more steps than opting in.[57] The issue was therefore located at the level of deciding (and acting) to give free consent, which highlights this as an individual autonomy issue.

At the time of writing, the first instruments of the EDS have now been finalized and entered into force. In particular, the DSA has received amendments that have introduced language similar to the DA's mention of autonomy. While the original proposal focused on manipulative activities in the context of more systemic negative consequences to society and democracy, both the Council and the European Parliament have added specific provisions to prohibit dark patterns, making their mental privacy considerations much more explicit and concrete in turn.[58] The final version now mentions individual autonomy in its Recital 37, which calls for providers of online platforms to be prohibited from "*deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof [...] or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice*". This is of course mostly congruent with the text of the Data Act. However, it bears noting that the main text of the DSA now in force does not contain references to individual autonomy, and instead prohibits providers from deceiving, manipulating or otherwise materially distorting or impairing the ability of individuals to make "free and informed decisions".[59] We may note that the DA does not contain a materiality-qualifier (yet); time will show if the language between these instruments will converge. As it stands, the DSA excludes weak or innocuous dark patterns from its prohibition, while the situation under the DA is less clear.[60] All this means that the DA in its current form

53 See Rec 67 DA.

54 See eg Christoph Bösch and others, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) 2016 Proceedings on Privacy Enhancing Technologies 237; Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence', *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM 2020).

55 See European Data Protection Board (n 43). Already prior to this, the CNIL's digital innovation laboratory LINC published a report titled "Shaping Choices in the Digital Work", which explicitly connected the "nudging" power or dark patterns with concerns for individual autonomy, see LINC, 'Shaping Voices in the Digital World - From Dark Patterns to Data Protection: The Influence of Ux/Ui Design on User Empowerment' (2019) <https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf>.

56 The CNIL has fined Google LLC and Google Ireland Ltd a combined 150 million euros for adversarial cookie banner design, see *Délibération de la formation restreinte n°SAN-2021-023 du 31 décembre 2021 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED, Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société FACEBOOK IRELAND LIMITED.* The problem in both case was that rejecting cookies took more steps than accepting cookies, a practice the EDPB calls a "hindering" and "longer than necessary" dark pattern.

57 Nb that this decision was based on French Data Protection Act, but the findings will likely generalize well. Other DPAs have already communicated that they consider such measures as incompatible with the GDPR rules as well, see e.g. the FAQ section of the Austrian *Datenschutzbehörde* under https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html#Frage_7.

58 Council of the EU, 'Press Release: Digital Services Act: Council and European Parliament Provisional Agreement for Making the Internet a Safer Space for European Citizens'. Prior to that the proposal did mention manipulative advertising techniques in Rec 63 and 68 which can be further seen as a safeguard against infringements of mental privacy and autonomy. The European Parliament also suggested an amendment which used the term autonomy explicitly (and also in connection with dark patterns), see the proposal for a regulation Recital 39 a (new), European Parliament, 'Amendments Adopted by the European Parliament on 20 January 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC (COM(2020)0825' (2022) <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html>. The recital was functionally similar to the actual Recital 67, but was more explicit in its elaborations. This preceded the use of the term by the European Commission in the Data Act proposal.

59 See Art 25 DSA. Nb that this provision was introduced at the same time as the reference to autonomy, so after the Data Act draft was introduced. The Parliament and Council thus decided to rely on autonomy as a principle in the recitals but preferred the more descriptive nature of the phrase "free and informed" decision in the operative article.

60 However, we may note the reference in Rec 34 DA that "common and legitimate commercial practices" should not themselves be considered as dark patterns. Nonetheless, Art 6 DA as it currently stands is much more restrictive as it prohibits coercion, deceiving or manipulation "in any way".

remains the only instrument to include an explicit reference to autonomy in its main text.

V. Explicit Autonomy Protection in the Data Act

We now finally arrive at the Data Act draft. The creation of the DA has run in parallel to the previously mentioned instruments and intensive discussion of coercive or manipulative design on a European level has preceded its release. As a result, the proposal of the European Commission reflects this development and continues the trend towards a more explicit protection of mental privacy. For the first time, the commission has used the term autonomy as a descriptor of a subject's status that ought to be protected. This section aims to investigate, if the use of new terminology signals a more expansive protective umbrella in the DA or if the protection of one's autonomy is limited under the proposal.

At first glance, the structure and context of Article 6 DA seems to narrow its scope of application somewhat.[61] The language of the proposal prohibits the use of measures to subvert or impair user autonomy 'including by means of a digital interface with the user', a provision that focuses on hostile design that was previously also the subject of DSA amendments.[62] Clearly, the wording of Article 6 and its corresponding recital of the DA proposal see dark patterns as the main risk from which to guard users from prospective data recipients. After all, Article 6 references digital interfaces but no other examples.[63] Digital interfaces are clearly already a meaningful way to subvert or impair someone's autonomy, and do not need an explicit reference to be considered as such. Their explicit (and sole) reference suggests instead that these digital interfaces (ie dark patterns) are considered to be of unique relevance to this provision. Similarly, the wording of Recital 34 suggests a strong focus on regulating dark patterns and does not mention any other coercive or manipulative measures. In this sense, the language of the text may be read as more than illustrative application, and instead as concrete target-setting.[64] This also conforms with the previous analysis of the DSA. There, the term autonomy is again used exclusively in conjunction with dark patterns.

On the other hand, grammatical and syntactical interpretation yield that the perceived risk to an individual's autonomy is not exhausted by adversarial design. The provision's wording leaves room for coercion, deceiving, manipulation subversion and impairment in 'any [other] way', beyond the aforementioned adversarial digital interfaces. Under this reading, the concepts of 'autonomy, decision-making or choices of the user' seem to suggest one broad protected element, and the prohibition on prospective data recipients to negatively affect their users' exercise of these capacities is extensive as a result. This is reinforced by the enumeration of protected elements quoted above and their relationship to each other: Clearly 'decision-making' of the user precedes their 'choice' in time and abstraction but is inextricably linked. In a similar way, 'autonomy' is clearly connected (and not separate to) the element of decision-making but describes it merely at another preceding level of abstraction. Including these concepts in the prohibitive provisions of legislation is a strong indicator that the protection users enjoy in relation to their self-determinative capacities should be interpreted holistically. Here, we may draw parallels to the regime of consent under the GDPR. As mentioned above, the EDPB has found coercion, deception or similar practices to be incompatible with valid (free) consent. Despite the slightly different wording, it is clear that practices deemed to be problematic under Article 7 of the GDPR, in particular with respect of freely given consent, are also prohibited under Article 6 DA, as they would invariably subvert or impair the autonomy, decision-making or choices of the relevant users.

As a result, it seems likely that the unprecedented and equivocal wording present in Article 6 would be fertile ground for expansive interpretation by regulatory authorities and the ECJ alike. While the motivation behind Article 6 DA is clearly derived from increasing public attention on the matter of dark patterns, the current text of the proposal leaves the door wide open for holistic (and correspondingly hard to

61 Art 6 Data Act Proposal (n 2).

62 Further limiting the scope, not every nudge that affects an individual's decision-making will be outlawed by these provisions. Recital 34 of the Data Act proposal lays out that 'common and legitimate commercial practices that are in compliance with Union law' are not 'in themselves […] constituting dark patterns'.

63 Ibid.

64 Ibid Rec. 34

predict) decisions about user-data recipient interactions.[65]

VI. Discussion: From Meta-Principle to Explicit Protection

As is often the case with European legislation covering the digital sector, much of the ambiguity of certain provisions stems from the lack of explicit definitions. Article 6 DA is no exception. This section argues that the inclusion of individual autonomy in the DA signals a paradigm shift, the opacity and the many potential amendments to the proposal that will surely be brought up in the ongoing legislative process notwithstanding.

Beyond the digital domain, individual autonomy, as a concept situated somewhere between the domains of ethics, law and cognitive science, has long held the position of a meta-principle in the legal domain. Its status as an underlying foundation of legal systems generally and fundamental rights specifically is well established.[66] There is also considerable reflection of different aspects of individual autonomy in specific fundamental rights. Arguably, more physical aspects of an individual's autonomy have commanded the majority of attention for a long time. For example, the right to liberty or the prohibition of forced labour interdict palpable and direct constraints of an individual's factual capacity to make choices. But as the digital domain has grown in relevance and our understanding of its potential to interfere with an individual's non-physical autonomy has improved, new tools within the catalogue of fundamental rights have emerged as appropriate safeguards.[67] As Diggelmann and Cleis have shown, the modern conception of a right to privacy has only emerged relatively recently, and this has been at least correlated with the rise of (information) technology.[68] Clearly, this right to privacy (and by an extension, the right to protection of personal data) is closely connected to an individual's mental capacity of self-determination, just as the German *Bundesverfassungsgericht* found. Similarly, the right to mental integrity, freedom of thought, conscience and religion, and the freedom of holding opinions without interference capture concerns for an individual's mental autonomy.[69] And while the original legal instruments have eschewed the term autonomy, secondary literature such as legal commentaries have recognized the concept when discussing the underlying motivating principles of fundamental rights.[70] Even more granularly, many legal provisions can be traced to the purpose of shielding some aspects of an individual's mental autonomy, and they often do so in light of emerging technologies. For example, legal scepticism towards subliminal or misleading advertising, non-validity of legal consent under duress or exposure to false information or limits to data collection all connect to a collective concern over individual autonomy. The current focus on adversarial design or 'dark patterns' in European legislation is the most recent testament to this, and the substantial fines for these practices on the basis of existing legislation suggests that this is not going to change. Indeed, the DA proposal is also outfitted with the now typical GDPR-esque penalties in case of infringements, further discouraging autonomy-constraining measures. Finally, some scholars have noted a perceived disconnect between the value placed on the mental aspects of individual autonomy and the protection fundamental rights award in light of neuroscientific advancements and the manipulative impact they may pro-

65 This would create a situation not dissimilar from the impact of principles relating to processing of personal data enshrined in Art 5 of the GDPR as mentioned above, see European Data Protection Board (n 43).

66 Kelsen (n 16); Jaunius Gumbis, Vytaute Bacianskaite and Jurgita Randakeviciute, 'Do Human Rights Guarantee Autonomy?' [2008] Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol 77. It is also worth noting that the original use of the term autonomy was not in the context of individuals but for politic collectives.

67 In a similar notion, the European Court of Human Rights maintains a collection of decision related to new technologies, where the application of the human rights catalogue that entered into force in 1953 is summarized, see European Court of Human Rights - Press Unit, 'Factsheet: New Technologies' <https://www.echr.coe.int/documents/fs_new_technologies_eng.pdf>.

68 Oliver Diggelmann and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' [2014] Human Rights Law Review. In the United States, the concept of modern privacy is often thought to have been heralded by Brandeis and Warren and their seminal article, see Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193. Interestingly, Warren and Brandeis too discuss emerging technology in detail as a threat to privacy, in their case the advent of photography and the logistic of newspaper circulation. However, the notion of privacy in the context of United States legislation is somewhat idiosyncratic and not fully congruent with European understanding of the same. See also Dorothy J Glancy, 'The Invention of the Right to Privacy' (1979) 21 Ariz. L. Rev. 1.

69 See Maximilian Gartner (n 25).

70 See eg Manfred Nowak, *U.N. Covenant on Civil and Political Rights - CCPR Commentary* (2nd edn, NP Engel, Publisher 2005).

vide,[71] and the matter has subsequently received attention in a parliamentary question to the European Commission.[72]

Thus, to repeat the obvious, the concept of autonomy is not foreign to the legal domain. What is new to a certain extent is first, the increased consideration of non-physical aspects of autonomy and second, its recognition not only as a meta-principle but as explicit protected value. As outlined above, European legislation in the digital domain has inched closer to explicit recognition. Both within the European Approach for Artificial Intelligence and the European Strategy for Data, the constraining effects technology can have on an individual's autonomy have been targeted with increasing precision while maintaining technology-neutral language. With its pending explicit recognition in the DA (and to a certain extent through references in the Digital Service Act), individual autonomy is now on the cusp of being explicitly recognized by a European legal instrument regulating the digital domain; hence facilitating the transfer of theoretical and ethical concerns highlighted in advisory bodies and scholarship into more durable code. Should the regulation pass in its current or similar form, individual autonomy will have shed its status as meta-principle and take the position of explicitly protected characteristic. But even if the wording is not adapted in the future legislative process, its inclusion in the European Commission's proposal is already indicative of the trend outlined in this paper.

In any case, actors in the digital domains that collect and process data will likely be faced with another opaque, but wide-ranging limit on how to structure interactions with their users. As the increasingly hostile approach of legislation and regulatory enforcement towards autonomy-subversion and impairment is continuing, careful considerations will be necessary for data collecting and processing entities.

VII. Conclusion and Outlook

With the DA proposal, the regulatory grasp of the European Union in the digital domain has further caught up with the need voiced by technology ethicists and stakeholders[73] to protect the mental aspects of an individual's capacity to self-determination. While the immediate attention of regulatory authorities applying the provisions in its current form would likely focus on combating instances of adversarial design such as dark patterns, the trend towards more holistic protection of individual autonomy and mental privacy in the digital domain will continue.

This analysis has shown that (individual) autonomy has already served as a meta-principle informing relevant legislation. Nevertheless, its 'emancipation' as an explicitly protected concept raises questions to what extent this newly adopted posture will affect the envelope of acceptable interactions in the digital space going forward. The provisions of the DA proposal prohibit impairment or subversion of an individual's autonomy only in the context of user-data recipient relationships. However, autonomy is not constrained solely in these contexts. The recognition of autonomy may very well spill over into a more confident posture of regulatory authorities and courts when considering autonomy constraints under other existing regimes. There, the application of general principles (and extrapolation of the underlying fundamental rights), such as the aforementioned fairness principle, or the instantiation of autonomy as free consent in the GDPR, may herald a more aggressive stance against technology-assisted autonomy impairment or subversion without the need for further legislative change. Considering the function of the DA proposal, this may even be necessary to maintain regulatory consistency. For example, Article 6 DA functionally complements the GDPR's right to data portability, enshrined in its Article 20. But of course, this provision does not mention coercion or subver-

71 See eg Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life sciences, society and policy 1.

72 Emmanouil Fragkos, 'Question for Written Answer E-004810/2021 to the Commission (Legislation against the Manipulation of the Human Brain through Neuroscience)' <https://www.europarl.europa.eu/doceo/document/E-9-2021-004810_EN.pdf>.

73 See eg Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75; Council of Europe, 'Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes' (2019); Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Seventy-Third Session Item 74 (b) of the Provisional Agenda** Promotion and Protection of Human Rights: Human Rights Questions, Including Alternative Approaches for Improving the Effective Enjoyment of Human Rights and Fundamental Freedoms' (2018); Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data and Society.

sion of the data subject's autonomy.[74] It seems questionable that users under the DA proposal are meant to enjoy more thorough protection from autonomy-undermining measures pertaining to potentially non-personal data than data subjects under the GDPR pertaining to personal data. As a result, revisitation of these existing regimes under the now explicit recognition of autonomy may be needed, if not through legislative means, then through enforcement based on 'updated' interpretation of the existing instruments. Future research examining the effect of the more explicit posturing with respect to mental privacy and individual autonomy to the interpretation of existing legislative instruments such as the GDPR would be welcomed.

74 Originally, this may have been due to the fact that the GDPR does not explicitly mention the right of the future data controller to issue its own request for data transfer but considers this right to lay exclusively with the data subject. Here, the Data Act proposal uses different language with an explicit inclusion of a third party 'acting on behalf' of the user. But in both cases, the justification for transferring the data originates from the original data subject or user. It seems unlikely, that the wording of Art 20 of the GDPR ought to be interpreted in a way that precludes potential receiving data controllers equipped with power of attorney and valid consent of data subjects from issuing a request on behalf of the data subject. This is true in particular, as the GDPR foresees controller-to-controller transfers in the context of data portability. Instead, this is likely a sign of an evolved understanding of the power dynamics between data subjects and users on the one hand and data service providers on the other handle. See also Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (2016) <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> pp 6f, as endorsed by the EDPB. On the other hand, recent communication of the EDPB and the EDPS seem to suggest a different view. In one of their joint decisions they proclaim that the Data Act would 'in practice likely extend to entities other than the data subject'; ostensibly different than under the GDPR, see European Data Protection Board and European Data Protection Supervisor, 'DPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (2022) <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf> para 14. A more thorough investigation into receiving data controller's standing and legitimation to make requests on the data subject's behalf is left for another time. In the meantime, the interested reader may consider Teodora-Lavola-Spinks and Daniela Spajic, 'The broadening of the right to data portability for Internet-of-Things products in the Data Act: who does the act actually empower (Part II) (2022), <https://www.law.kuleuven.be/citip/blog/the-broadening-of-the-right-to-data-portability-for-internet-of-things-products-in-the-data-act-part-ii/>.