CiTiP Working Paper Series

An analysis of IoT data regulation under the Data Act proposal through property law lenses

Charlotte Ducuing

CiTiP Working Paper 2022

KU Leuven Centre for IT & IP Law - imec

20 September 2022

Title

Charlotte Ducuing[1]

Table of Contents

[1] Charlotte Ducuing is a doctoral researcher at CiTiP (KU Leuven). The author can be contacted at charlotte.ducuing@kuleuven.be.

Abstract

The paper provides an analysis of the regulation of IoT data under the Data Act proposal from the European Commission, through property law lenses. The hypothesis is indeed that the regulation constitutes a property institution, in the broad sense of an institution organising the use of data as resources in society. However, the pursuit of such objective is closely intertwined with market ordering objectives. The approach followed in this paper allows to propose a conceptualisation of the novel regulation of IoT data and to help assess it. It also serves to explore the concept and operationalisation of 'data control' and, more generally, the interpenetration between economic law of data and personal data protection law.

Keywords

Data Act, IoT data, data control, FRAND, data ownership

This paper is a work-in-progress. Any constructive comments made to the author are very much welcome.

1. Introduction

The long-awaited Chapter II of the Data Act proposal[2] constitutes a pioneering regulation of IoT data – namely data generated by the use of IoT products and related services. IoT ('Internet of Things') products are tangible devices with built-in sensors and software which generate, process and communicate data while in such, such as about their environment and use. They are also alternatively referred to as 'connected' or 'smart' products or devices, such as smart tractors, smart watches, fridges, smart cars, health devices, etc. Sensors may also alternatively be placed on equipment, such as railway tracks or farm soils to produce data on the operation and/or environment of the equipment.

(Especially IoT) data have gained the role as valuable economic resources in the data economy but their use and value is often appropriated by so-called 'de facto controllers', namely most often IoT products manufacturers or providers of related services. This is detrimental to consumers and/or businesses – whether product users, product aftermarket service providers or businesses engaged in unrelated activities -- who could either make profitable use of them or may require such data to conduct their own business. Relatedly, this is generally deemed sub-optimal compared to data-related innovations that could result from broader data reuse.

While (IoT) data have no legal status, especially under property law, the question how they should be regulated has been subject to an intense debate. Data are *sui generis* goods (whether should they be referred to as 'goods' in the first place is also debatable) in the economic taxonomy. Featured as 'public goods' and "most of the time" infrastructure resources[3] because of their ubiquity, non-rivalry and general-purpose character, they are also characterised as heterogeneous and contextual. This stands in the way of a generic classification, and thus seemingly of a universal legal status. In the data economy, data, and especially IoT data, are often created as a result of the interaction of many actors while many of such and other actors would greatly benefit from (re)using them, whether for economic or non-economic purposes. However, at the same time, the broad (re)use of data may sometimes happen to clash with objectives of general interest while also interfering with the rights or legitimate interests of the same or other actors, such as the freedom to conduct a business of, respectively and for entirely different reasons, manufacturers and IoT product business users and the rights to privacy and data protection of individuals.

The debate surrounding the regulation of the value arising from data, and in particular IoT data, crystalised in 2016-2017 with the option envisaged by the European Commission ('EC') to establish a 'data producer's right' on data, namely a form of data ownership,[4] with IoT data being the main focus.[5] Faced with strong and well-argued oppositions, the options was eventually abandoned. Against this background, many regulatory options have been considered, whether data-specific or not and from a

[2] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, 23.2.2022 ('Data Act proposal').

[3] OECD, 'Data-Driven Innovation - Big Data for Growth and Well-Being' (OECD 2015) ch 4 <https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en> accessed 7 April 2019.

[4] Data ownership should be understood as "an economic ownership right in data as intangible assets in the form of an exclusive right that enables the right holder to appropriate the economic benefits from the use of these data". Josef Drexl, 'The (Lack of) Coherence of Data Ownership with the Intellectual Property System' in Ansgar Ohly and others (eds), *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur* (Cambridge University Press 2021) s 16.2 Data Ownership as Intellectual Property.

[5] European Commission, 'Communication Building a European Data Economy' (2017); European Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy - Accompanying the Document "Communication Building a European Data Economy"' (2017).

variety of legal branches whether classically classified under private or public law. Schematically, they range from the legal endorsement of the status quo namely de facto exclusive control of data, to the creation of a universal ownership(-like) right, to a piecemeal approach with (mere) sector- or data-specific data (access) rights, through the allocation of 'sticks' in the bundle of property rights afforded to one or several actors deemed legitimate and to the design of (collective) data governance mechanisms. Some have pleaded for a data-specific revision of either competition law[6] or of the regulation of unfair commercial practices while some others oppose data-specific regulation and propose to regulate data indirectly via their technological environment. Eventually, the ALI and ELI Principles for a Data Economy propose a novel and *sui generis* approach with the creation of 'data rights' triggered and operationalised by mechanisms inspired from both private and public law.[7] The ALI-ELI Principles have already caught the attention of the EC as visible in the European Data Strategy of 2020[8] and constitute a source of inspiration for the regulation of IoT data under the Data Act – although with significant differences -, as further discussed in this paper.

The Data Act proposal – and particularly the regulation of IoT data under, mainly, Chapter II – can be viewed as mainly pragmatic. The EC establishes mechanisms to solve long-standing well-known issues observed with such data, while attempting to navigate the boundary parameters in place, such as, in addition to the specific features of data, the existence of legacy frameworks (i.e. IP rights, trade secrets protection, personal data protection) generally left unaffected, the perceived risk of disinvestment from manufacturers and the diversity of IoT products and services. It is also commonplace that the legislative interventions of the EU law-maker are often indifferent to the classical branches of the law under national legislations. Based on access and portability rights, IoT data regulation under the Data Act is at first glance quite alien to property law and in particular to 'ownership'.

This being, this paper investigates the following assumptions. First, IoT data regulation under the Data Act constitutes a property institution, in the broader sense of "institution for organising the use of [data] as resources in society", as put by Cohen[9] following T.W. Merrill.[10] Such functions are principally and classically assumed by the legal branch of property law,[11] although the classical mechanisms of property law are not fit for data as such. This is clearly suggested by the vocabulary. The very title of the Data Act reads "harmonised rules on fair access to and use of data" and a both strong and novel emphasis is placed on the act of "generating" data[12] and on the regulation of data "use". Secondly,

[6] For example, Germany has amended its national competition law to include data-specific provisions (and more generally provisions adapted to the digital environment), see 10th Amendment Act of 18 January 2021; Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen (GWB-Digitalisierungsgesetz).

[7] ALI-ELI, 'Principles for a Data Economy' (American Law Institute - European Law Institute, 2020) <https://www.europeanlawinstitute.eu/projects-publications/current-projects-feasibility-studies-and-other-activities/current-projects/data-economy/> accessed 8 April 2020.

[8] In its Data Strategy of 2020, the EC refers indirectly to the Principles for the Data Economy, by mentioning its intention to lay down "usage rights for co-generated IoT data", Communication 'A European strategy for data' 2020 (COM/2020/66 final) s 5.A.. The term "co-generated data" was coined by ALI-ELI Principles for the Data Economy, ibid.

[9] Julie E Cohen, 'Property as Institutions for Resources: Lessons from and for IP' (2015) 94 Texas Law Review 1, 3–4.

[10] Thomas W Merrill, 'The Property Strategy' (2012) 160 University of Pennsylvania Law Review 35, 2062.

[11] Property law is classically defined as the branch of law dealing with the "legal relations between a subject and a substantial and relevant group of other subjects regarding an object". Sjef van Erp, 'The Need for a Common Vocabulary on "Data Ownership"' (2019) 8 European Property Law Journal 1, 2.

[12] In contrast, the GDPR refers to the 'processing' of data, meaning, essentially, any operation or set of operations personal on personal data. The coming into existence of personal data is only referred to as the "collection" of personal data, see Regulation (EU) 2016/679 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 […] ('General Data Protection Regulation' or 'GDPR'), OJ L 119/1, Art. 4(2).

with data, the boundaries between the branches of law are necessarily getting increasingly connected which raises novel arduous questions. This is the main lesson learned from the aborted 'data producer's right' option contemplated by the EC in 2016, which notably made clear that ownership is not reconcilable with personal data protection. Instead of opposing the phenomenon, the ELI-ALI Principles for a Data Economy demonstrably embrace it, which seems to be also the path taken with the regulation of IoT data under the Data Act proposal. The paper investigates the hypothesis that, in order to do so, the regulation of IoT data is built on the interpenetration of property institutions with personal data protection law.

Against this background, the paper analyses the regulation of IoT data under the Data Act with property law lenses from a philosophy of law perspective. To be sure, the point is *not* to enquire whether the regulation of IoT data under the Data Act *falls under* a specific materialisation of property law that would be analysed with a technical legal plumbing perspective. Clearly, it does not, and many differences are obvious. In particular, the rights granted by the Data Act are neither *in rem* (but rather *ad personam*) nor *erga omnes* (but enforceable against specific persons). While property law is typically universal, the scope is limited *rationae personae.* I.e. the obligations incumbent on data holders are not applicable to micro and small enterprises, and online gatekeepers cannot benefit from the exercise of the data portability right.[13]

The objective pursued therewith is, generally, to enquire into both the extent to which property law constitutes a source, and the effects thereof, in order to conceptualise IoT data regulation. Similar enquires have long been made concerning the sources of personal data protection law.[14]

Analysing the regulation of IoT data through the lenses of property law also allows to identify possible loopholes in the regulation. As a well-established branch of law, property law has indeed developed mechanisms to serve a range of purposes enshrined in the general objective to organise the use of resources in society, which serve here as a yardstick.

The analysis conducted here helps conceptualize the nature of the regulation of IoT data, and especially its both intricate and thorny relationship to personal data protection. The GDPR constitutes indeed both a boundary parameter to the regulation of data for their economic value, but also seemingly a source of inspiration. 'Data control', namely the empowerment of individuals and businesses with respect to 'their' data, is becoming a pervasive objective of the EU law-maker. Expected to bridge the gap between personal data protection and the regulation of data as a source of economic value, 'data control' is demonstrably at work in the Data Act. This paper aims to understand this notion better and, more generally, to understand better the regulatory patterns at work in EU legislation concerning data. The coming together of many branches of law with data, particularly visible with the regulation of IoT data regulation in the Data Act, constitutes a methodological challenge for scholars, who traditionally develop a branch-specific expertise. On the flip side, it confirms the relevance of the research presented here.

[13] Data Act proposal, Art. 7(1) and Art. 5(2). These provisions – and in particular the former have been heavily criticised, see in particular Giuseppe Colangelo, 'European Proposal for a Data Act – A First Assessment' (2022) CERRE Evaluation Paper 15–16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4199565>.

[14] Concerning the GDPR, see *i.a*. Henry Pearce, 'Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law' (2018) 4 European Data Protection Law Review (EDPL) 190; Gianclaudio Malgieri, '"Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?' (2016) 20 Journal of Internet Law 3.

Finally and as further elaborated in this paper, the analysis informs the important question to what extent the goals traditionally served by property law - and in particular ownership as a parangon - can be achieved *without ownership,* in particular how to decouple tradability from ownership while taking into account the afore-said specificities of data, in a manner fair to the different legitimate stakeholders. Looking at the regulation of IoT data through the lenses of property law can help discern the elements stemming – or respectively *not stemming* – from property law. Both the vocabulary (i.e. 'control', 'use' being granted an all-encompassing meaning, 'data portability', etc.) and the legal mechanisms leveraged in the Data Act, are obviously quite alien to property law. They defiantly obscure the association with this branch of law, yet they do not constitute a valid reason to *not* compare IoT data regulation to property law.

The paper does not present a comprehensive account of the substantive rules applying to IoT data regulation. Reciprocally, it does not discuss all aspects of property law.[15] It begins with an analysis of the rationales, with a specific focus on data control which has a property law flavour. Then, the third section focuses on the question whether IoT are recognised as an object of rights or regulatory subject-matter, which is a prerequisite for property law. The fourth section outlines the allocation of rights in the triangle formed by the 'data holder', the 'user' and the 'third party' chosen by the user exerting her right to data portability. The fifth section enquires about a possible property law reading of 'FRAND terms' under which the data holder shall make data available as a use case. The sixth and last section concentrates on an important provision, namely the second part of Article 4(6) assumed to be particularly alien to a property law reading. The seventh section concludes and identifies avenue for further research.

Where appropriate, the analysis compares the regulation of IoT data under the Data Act proposal with the ALI-ELI Principles for a Data Economy. The latter has indeed undoudbtedly influenced the former, although major differences can also be identified.

The object of the analysis consists in a legislative proposal from the EC, which will thus inevitably change in the legislative process so the analysis developed here may no longer hold true for later versions. Also, the Data Act proposal has been the object of different – and even sometimes contradictory interpretations. This is clearly caused by inconsistencies and unclarities which could be clarified throughout the legislative process. We make the assumption that this is also a result of its "engineering" regulatory character ("puzzle" character, on a more critical account), whereby a particularly large amount of scattered elements are to be combined, depending on contextual parameters, in order to settle the question who is entitled to what. While elaborating on this assumption, the paper does not aim to discuss inconsistencies and unclarities in the first place. Finally, the paper does not directly discuss the expected effectiveness of the rules.[16]

[15] For instance, securities are entirely absent from the legislative proposal and therefore not discussed here.

[16] On whether the Data Act is likely to deliver on the expectations, see in particular Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (Max Planck Institute for Innovation and Competition 2022) Max Planck Institute for Innovation & Competition Research Paper 22–05; Erik Habich, 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard Essential Patents for the Data Act Proposal and the Digital Markets Act' (2022) Forthcoming International Review of Intellectual Property and Competition Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119834>; Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law' (Max Planck Institute for Innovation and Competition 2022) Research Paper 22–12; Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector' (2022) Discussion Paper 2022–13; Inge Graef and Martin Husovec, 'Seven Things to Improve

2. The rationales for IoT data regulation: focus on data control

Before delving into the analysis of the legal regime in the following sections, the present section enquires into the rationales for the regulation of IoT data in the Data Act with the question to what extent they can – or respectively cannot - be associated with property law.

Under the general goal to foster a fair data economy, the rationales can be clustered as follows. First, to "empower users" and grant them "data control"[17] in the context where the data holder often enjoys *de facto* control of data; second, to foster data reuse for innovative and other public policy purposes such as the protection of the environment, the transition to the circular economy and a better health protection.[18] Third, although the distinction with the second objective is not entirely clear-cut, the public law objective to solve data-related competition issues, such as vendor lock-in.[19] Broader access to data by aftermarket independent actors is thereby simultaneously viewed as both a competition fix and an avenue for further data-driven innovation.[20] At the same time, the regulation of IoT data – and especially data access rights - should not undermine the investment incentive of manufacturers.[21]

Although with many occurrences, the Data Act does define neither the notion of 'user empowerment' nor this of 'data control'.[22] User empowerment and data control are referred to interchangeably as, generally, the ability for users to "meaningfully control how the data generated by their use of the product or related service is used and enabling innovation by more market players", in contrast to the situation where the manufacturer has "exclusive control over the use of data […]".[23] This section focusses on the data control rationale, most closely related to private law and property law, and on the justifications directly associated with it. The protection of the manufacturer's incentive to produce data can also typically be associated with intellectual property law justifications and is further

in the Data Act' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793>; Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives (Second Version)' (18 July 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436>; Colangelo (n 13); Zohar Efroni and others, 'Position Paper Regarding Data Act (Proposal of the European Commission, 23.02.22)' (Weizenbaum Institute for the Networked Society - The German Internet Institute 2022) Weizenbaum Policy Paper, 2 <https://www.ssoar.info/ssoar/handle/document/79542>.

[17] Data Act proposal, Rec. 25.

[18] "[…] such data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular [through?] facilitating the maintenance and repair of the products in question", Rec. 14 (see also Rec. 19); "The aim of this Regulation [is] to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services […]", Data Act proposal, Rec. 28.

[19] The Impact Assessment clarifies that the Data Act proposal aims to tackle the issue of the exclusive position of IoT products manufacturer over the data, which is viewed as problematic for aftermarket services providers (in contrast to, i.a. online services-related data, European Commission, 'SWD, Impact Assessment Report Acompanying the Data Act Proposal' (23 February 2022) 68. See also Rec. 28.

[20] On the confusion between competition and innovation in data sharing legal regimes, see Charlotte Ducuing, 'Data as Infrastructure? A Study of Data Sharing Legal Regimes' [2019] Competition and Regulation in Network Industries <https://doi.org/10.1177/1783591719895390>. For a detailed analysis of this confusion, see also Drexl and others (n 16) paras 15–18.

[21] "It is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product", Rec. 28.

[22] The notion of 'data control' is not new with the Data Act proposal. It can be traced back to the EC Communication 'A European Data Protection Framework for the 21st Century' of 2012, and it is literally visible, for example, in the GDPR (Rec. 7 and 68) and in the EC Communication 'Building a European Data Economy' and its Staff Working Document of 2017 (see for example, SWD, p. 33).

[23] Data Act proposal, Explanatory Memorandum, point 3. See also Data Act proposal, Rec. 25.

discussed throughout the paper. The relationship with the other objectives is also further discussed throughout the paper and in the conclusion.

The objective to grant users 'data control' can be directly associated with four main justifications, or otherwise said four connecting points to data, put forward in the proposal for being granted rights: (a) The need for clarification on what users can do with data;[24] (b) A general call for fairness especially because, as purchasers or long-terms users, they bear the risks and benefits of using such products;[25] (c) The contribution of users to the generation of data, alongside (at least) manufacturers and/or related service providers ("data generation is the result of the actions of at least two actors, the […] manufacturer […] and the user of th[e] product");[26] finally, (d) the link between the user and data, namely the fact that data represent the digitalisation of users actions and events.[27] The remainder of this section discusses the conceptual sources of these justifications, with the exception of justification (a) which is of a general nature.

Justification (b) – the fact that users bear the risks and benefits of using the IoT products - would seem to point to a property law rationale, although not explicitly recognised as 'generative of data' in the proposal (the 'generation of data' is discussed further in this section).[28] It could be viewed as a sign that IoT data are considered as either inherent parts or accessories to IoT products (see section 3). Although such notions are distinct one from the other, and fragmented across national legislations, the legal fiction of recognising a thing as an inherent part or as an accessory to another thing would generally lead to the legal regime of the former following this of the latter. It is debatable – and maybe context-dependant - whether, as a matter of fact and pursuant to property law tradition, IoT data are indeed either structurally or functionally related to IoT products.[29]

This stands in sharp contrast to "digital content or digital services" incorporated in or interconnected with a tangible movable item, regulated under the Consumer Sales of Goods *Directive after the (contract) legal regime of the sales of goods,* precisely because their absence "would prevent the goods from performing their functions" ("goods with digital elements").[30] In any event, the legal regime of IoT data in the Data Act does contrariwise not follow this of IoT products. This may be easily associated, first, with the specific features of data – and especially their technological artefact nature and thus reliance on their physical generation source. Second, it shall be associated with the objectives of the Data Act proposal to *distribute* rather than *centralise* rights.[31] The rights related to IoT data do simply not follow rights on IoT products. In conclusion, the Data Act does not view data as either an inherent part or as an accessory of IoT product. The argument based on the economic act of owning (or leasing)

[24] Users (whether consumers or SMEs) are confronted with the question of "what [they] can expect in terms of who can use the data when they buy such products", European Commission, 'SWD, Impact Assessment Report Acompanying the Data Act Proposal' (n 19) 9.
[25] Data Act proposal, Rec. 6 and 18.
[26] Data Act proposal, Rec. 6.
[27] Data Act proposal, Rec. 14.
[28] This can be compared to the ALI-ELI Principles for a Data Economy, see ALI-ELI (n 7) s 18(1)(b).
[29] Sjef van Erp and Koen Swinnen, 'The Legal Status of Co-Generated Data: With Particular Focus on the ALI-ELI Principles for a Data Economy and the Rules on Accession, Commingling and Specification' (2022) 2022 Technology and Regulation 61, 65.
[30] Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods […], OJ L 136/28 ('Consumer Sales of Goods Directive'), Art. 2(5).
[31] Data Act proposal, Rec. 6.

the IoT product generating data plays a more mundane role as a connecting point to data as part of a general idea of 'fairness', cumulatively to other justifications ('one of').

Justification (c) recognises the "action" of the user through the use of the product as 'co-generative' of data, in the parlance of the ALI-ELI Principles for a Data Economy which coined the term,[32] for the first time in EU legislation.[33] The 'action' of the user may differ depending on the product or service at stake and may consist in 'only' having their behaviour passively monitored.[34] The manufacturer is recognised at the same time as (co-)generator of data. Although not clarifying the concrete action generating data on the side of the manufacturer,[35] the Data Act proposal points most likely to the design of the product, including the software producing data, and possibly to the operation of such product and software.[36] The action of the manufacturer points directly to the Lockean labour justification of property, whereby the mixing of objects of the world with her own labour justifies the extension of ownership to the fruits of that work.[37] Putting the 'action' of the user on equal footing endorses the legal fiction, proposed by Fezer et al., that 'being monitored' should be deemed to constitute labour, in the Lockean sense of being generative of new goods.[38]

In contrast to both justifications (b) and (c), the link between the user and data put forward in justification (d) seems alien to property law justifications, and conceptually closer to personal data protection ones. As a reminder, justification (d) relates to the link between the user and data, namely the fact that data represent the digitalisation of users actions and events. Personal data, the existence of which triggers the application of the GDPR, is precisely defined as information *relating to* a natural person.[39] The well-known justification for personal data protection is that the processing of personal data by a third party has the potential to harm the data subject. As demonstrated by Purtova, the *relational* character of personal data means that the resource at stake is not merely data viewed as a standalone good, but the individual(s) in question (Facebook platform users, in her use case) whom she refers to as "user livestock".[40] The protection of individuals under personal data protection law should thereby be viewed as essentially dignitarian, following the Kantian distinction between things

[32] ALI-ELI (n 7) s 3(1)(h) and 18.

[33] To compare, the Communication 'Building a European Data Economy' refers solely to the "machines or processes" of manufacturers and service providers as generative of data, see European Commission, 'Communication Building a European Data Economy' (n 5) s 3.4.

[34] Data Act proposal, Rec. 17.

[35] Data Act proposal, Rec. 6.

[36] Both justifications are comparable to factors that can be recognised as co-generative of data according to the ALI-ELI Principles, see ALI-ELI (n 7) s 18(1)(b) and (d).

[37] John Locke, *Second Treatise of Government* (Princeton University Press 2018) ch V <http://www.jstor.org/stable/10.2307/j.ctv19fvzzk> accessed 4 July 2022. The commentaries are many. See in particular 'Two Treatises of Government | Background, Content, & Facts | Britannica' <https://www.britannica.com/topic/Two-Treatises-of-Government> accessed 4 July 2022; Jeremy Waldron, 'Property and Ownership' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Summer 2020, Metaphysics Research Lab, Stanford University 2020) <https://plato.stanford.edu/archives/sum2020/entries/property/> accessed 23 November 2021; Dan Wielsch, 'The Differentiation of Property - On the Development of a Foundational Legal Concept' (2016) 5 European Property Law Journal 77.

[38] Karl-Heinz Fezer, Hrsg Pencho Kuzev and Tobias Wangermann, 'Repräsentatives Dateneigentum' 49. This proposition is also discussed in Patrik Hummel, Matthias Braun and Peter Dabrock, 'Own Data? Ethical Reflections on Data Ownership' (2021) 34 Philosophy & Technology 545, 552–553.

[39] GDPR, Art. 4(1).

[40] Nadezhda Purtova, 'The Illusion of Personal Data as No One's Property' (2015) 7 Law, Innovation and Technology 83, 107.

(subject to quantification) and persons.[41] As data are inseparably linked to individuals, the legal protection extends to their downstream use (*i.e*. subsequent to transfer) in an unwaivable manner.

For the first time in EU legislation, the inseparability of 'non-personal data' to, *i.a*., businesses is recognised as a source of rights, similar to personal data protection law. Justification (d) seems therefore not only alien to property law but potentially contradictory to it. The remainder of this paper, and especially section 5 below, discusses more in details the rights deriving directly from this justification.

Analysing the traces of property law - and contrasting them with other sources - in the objectives and justifications of IoT data regulation inevitably takes us to the ALI-ELI Principles for a Data Economy. They play an obvious inspiring role, as all justifications discussed above can be traced back from them, even though the Data Act pursues its own logic. The recognition of *several different* justifications for the allocation of rights shares similarities with the approach of the ALI-ELI Principles. However, in contrast to the latter, the Data Act proposal assumes these justifications to be *cumulatively* present to the benefit of mainly one actor, namely the 'user'- with the manufacturer being also recognised as a co-generator of data. Such assumption – or legal fiction – is however not representative of reality. Defined as "a natural or legal person that owns, rents of leases a product or received a service",[42] the notion of 'user' is not strictly associated with the use (in the broader sense) of the product but with the property regime of the latter. As already underlined based on the analysis of the Data Act proposal for smart farming, a mere use (in the broader sense) of the product under a service control would not suffice for such customer to qualify as a 'user' within the meaning of the Data Act proposal.[43] In the latter case, however, the various justifications would not converge with the 'IoT product user' (as defined by the Data Act proposal). They would for instance be broken down between the latter who bears the risks and benefits of the product (justification b) and, temporarily, her customer whose actions would generate data (justification c), such data representing the digitalisation of her actions and events (justification d). Although based on the observation that IoT data are characterised by a large number of stakeholders and, thus, on the need to *distribute* rights between them, the Data Act proposal does not recognise all of them as direct beneficiaries of statutory rights.

In contrast to the ALI-ELI Principles[44] but also to most property law regimes,[45] the Data Act proposal does *not* apply a *de minimis* rule to the contribution of actors (and in particular users) in the (co-)generation of data, to the extent that a mere *passive* role of the user of *being monitored* is recognised as generative of data and therefore of rights. This can easily be associated with, first, the specific features of data and the ensuing aim to *distribute* rights – which is also visible in the ALI-ELI Principles,[46] rather than *centralise* them as ownership would typically do as per property law.[47] Second, property law is theoretically justified as universal and blind to power asymmetries while redistribution and the restoration of (market) balance are traditionally, and schematically, assumed by other policies and branches of law. In contrast, the Data Act proposal is pervasively concerned with power asymmetries

[41] Mark Verstraete, 'Inseparable Uses' (2021) 99 North Carolina Law Review 427. See also Václav Janeček, 'Ownership of Personal Data in the Internet of Things' (2018) 34 Computer Law & Security Review 1039, 1043.
[42] Data Act proposal, Art. 2(5).
[43] Atik (n 16) 9–10.
[44] ALI-ELI (n 7) para 18.
[45] Erp and Swinnen (n 29) s 3.
[46] ALI-ELI (n 7) pt III. Because they are intended to all to a broader range of data, the Principles include obviously other principles governing the conditions in which the granting of 'data rights' is triggered.
[47] Erp and Swinnen (n 29) 68.

and aims to restore balance in favour of the user (see also section 5 below). This explains the very low threshold for recognising rights to users, as a means to empower them.

The Data Act recognises a personal data protection law-like dignitarian justification for granting rights to users, alien - and logically contradictory - to property law. The ALI-ELI Principles bring all justifications (b to d) together as potential factors of (co-)generation of data, including such a 'privacy-like' (and thus property law-alien) one. In contrast, the Data Act proposal expressly recognises *'(co-)generation' of data* only concerning the action of the manufacturer and the use of the product by the user, whether knowingly sticking more strictly to property law theory or inadvertently. Against this background, sections 4 to 6 analyse the rights and obligations which detract from these justifications. Before that, the following section turns to the identification and recognition of IoT data as an object of rights as a prerequisite.

3. IoT data as a regulatory subject-matter

This section analyses whether the regulation of IoT data under the Data Act recognises 'data' as an object of rights or, in other words, as a legal thing. The recognition, including the identification and delineation, of a 'thing' as an object of rights is indeed the starting point for property law and it is of particular importance for ownership.[48] As the scholarly debate on the 'data producer's right' has demonstrated, the specificities of data in the data economy, in particular their volatility, dynamicity and unclear contours, make them a poor fit for being recognised as a legal thing.[49]

The Data Act does recognise IoT data as an object of rights - or as a regulatory subject-matter. IoT data is indeed the main object of rights to access and use. Two elements could be viewed, at first glance, as contradictory to this finding. They require thus further discussion and will be analysed in turn. First, the 'by design' compliance as per Article 3(1) and, second, the fact that the data *source* (namely the IoT product or related service) constitutes the main trigger for regulation. Then, I turn to the distinction between personal data and non-personal data, which is – again – present with the Data Act, and what this distinction means with property law lenses. I conclude on the recognition of data as a regulatory subject-matter as a broader pattern at work in EU law and on its likely impat on personal data protection law. Finally, I make on opening to question the relevance of the scope of data, with a view to the rationales for regulation as analysed in the previous section.

First, the by default obligation to provide access to data under Article 3 reads as a product- or service-related obligation, namely as the obligation for the data holder to design products and/or related services "*in such a manner that* data generated by their use are, by default, […] and where relevant

[48] On the notion of 'object of entitlement' as a prerequisite for data to be regulated as property, see Sjef van Erp, 'Data Protection in Hybrid Worlds' in Cristina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) s 12.4 <https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/data-protection-in-hybrid-worlds/A30C61B5E28CA068B2FE4A2243FCE639> accessed 6 July 2022.

[49] The features of data have generally been found to stand in the way of the principle of transparency under property law, which can be broken down into two main principles, namely identifiability and publicity, and which is also closely connected to the principle of legal certainty. Erp and Swinnen (n 29). P Bernt Hugenholtz, 'Data Property: Unwelcome Guest in the House of IP', *Paper presented at Trading Data in the Digital Economy: Legal Concepts and Tools* (2017) 12. Koen Swinnen, 'Ownership of Data: Four Recommendations for Future Research' (2020) 5 Journal of Law, Property, and Society 139. Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 JIPITEC 264–265.

and appropriate, directly accessible to the user" (emphasis added),[50] whereby data is seemingly regulated 'only' indirectly. This provision should read as a 'by design compliance' obligation. By design compliance has gained traction in the field of Law and Technology as a means to tame the embedded power of technology. The 'de facto control' of data by IoT product manufacturers and service providers is a well-known phenomenon and precisely viewed by the EC as a problem to fix with the Data Act. This being, the Data Act does not *genuinely* regulate the technological environment of IoT data, *i.e.* by mandating either a specific type of environment or its shared control by stakeholders to prevent the de facto control by the 'data holder', options which have been discussed concerning connected vehicles.[51] The focus remains with 'data', as visible throughout the rest of the Data Act and especially with Article 4 reading as a fall-back to Article 3. By design compliance as per Article 3 should thus logically be viewed as a *means to comply* with data-related obligations, rather than as pointing to IoT products and related services as the main object of rights and obligations.

Second, IoT data are not defined *per se* but with reference to their source, namely IoT product or related service ("data generated by [the] use [of IoT products and related services]"). This gives the impression that IoT data would neither be defined clearly nor regulated in their own right, both being analysed now in turn. That data are not clearly defined and delineated is true, and probably inevitable to some extent. The definition of data as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording"[52] is particularly broad and even confusing (especially the unclear notion of 'compilation') and it is not strictly linked to the classical definitions of data.[53] As a result, the notion of 'data' could confusingly extend beyond mere bits and bytes to 'things in a digital format' or digital content.[54] This also means that the Data Act is more likely to overlap with legacy frameworks, such as IPRs and trade secrets. To diminish the chances of overlap with legacy frameworks, the proposal applies only to "data in the form and format in which they are generated by the product" and not to derivate data,[55] although the distinction is likely to be hard to make in practice.

In terms of delineation, data are targeted based on their generation "by the use of" IoT products or services, so that the actual data (and especially their semantics) cannot be identified *ex ante.* This is known to property law, that applies to any type of things which are generated, provided they fall under the legislative buckets in force (*i.e*. the classical categories of tangible immovables or movables). The generation of data as a trigger for regulation can actually be viewed as a 'lesson learned' from prior discussions. As a means to identify data with a reasonable level of predictability despite their amount

[50] Data Act proposal, Art. 3(1). This is to the extent that the Position Statement of the Max Planck Institute rightly questions the relationship between Art. 3 of the Data Act proposal and the Sales of Goods Directive, essentially asking whether the 'by design compliance' requirement of Art. 3 shall be considered as a conformity criterion under Art. 7(1)(a) of the Sales of Goods Directive, Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods […], OJ L 136/28.

[51] Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data' (2018) 9 JIPITEC; Charlotte Ducuing, 'Beyond the Data Flow Paradigm: Governing Data Requires to Look beyond Data' (2020) Special Issue: Governing Data as a Resource Technology and Regulation 57, s 4.

[52] Data Act proposal, Art. 2(1).

[53] For an analysis of this same definition in the Data Governance Act proposal, see Julie Baloup and others, 'White Paper on the Data Governance Act' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3872703 9–10 <https://papers.ssrn.com/abstract=3872703> accessed 21 November 2021.

[54] Drexl and others (n 16) para 58.

[55] According to Rec. 17, data shall include "data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights".

and their being in constant motion, it aims to make it both feasible to regulate data as a thing[56] and appreciative of their very nature as technological artefacts. In short, defining data by reference to their generative source can simply help 'capture' data.[57] Paradoxically, it is by picturing data as flow that the Data Act regulates them as things.[58] Defining data by reference to the generation can also be associated with the property law rootings (see section 2 above).

At first glance, data seem to not be regulated in their own right but, rather, as either inherent parts or accessories to IoT products and related services, which would imply that their legal regime follows this of IoT products and related services (on this, see also section 2 above). In property law terms, this implies that the object of rights would then not be *data* but the IoT products or related services. The 'user empowerment' objective could seem to back such reading, with both the justification (b) (discussed in section 2 above) and Recital 25 linking data to the act of purchasing the product.[59] However, the objectives served by IoT data regulation are not limited to 'user empowerment' in the strict sense of empowering users *with respect to the sole product* that they have purchased or leased. Nor is the Data Act proposal solely justified by the acquisition or long-term use of the product or service (on this, see section 2 above). Besides, the legal regime of IoT data does not align with this of products and services. Quite in contrast, it is specific to IoT data, as discussed in the following section. For illustration, the user shall suffer limitations to her right to use data to the benefit of the data holder[60] who also benefits rights on data, while she may otherwise use data for purposes unrelated to the products and services.

A remark should be made on the distinction between personal and non-personal data which is gaining traction in EU law[61] and which is notably at work in the Data Act. The literature has already unravelled many logical and feasibility issues deriving from the reference to 'non-personal data' in legislation[62] - which has clearly not prevented the EC from continuing in the same path. Our point here is rather of a conceptual nature. Personal and non-personal data are all the objects of the general access and use rights under Chapter II while subject to specificities. For example, Chapter II provides a(n exclusive) legal basis for the sole processing of *non-personal data* by data holders while laying down purpose limitations to the benefit of users (further discussed in section 6 below).[63] The assumption seems to be that the GDPR does already sufficiently regulate personal data, while the Data Act should provide counterparts for non-personal data where deemed appropriate. Personal data and non-personal data

[56] Whether it is effective is not discussed here. For a critical view, see Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law Max Planck Institute for Innovation & Competition Research Paper No. 22-12 - 43 Pages Posted: 20 Apr 2022 Last revised: 23 Jun 2022 Peter Georg Picht

[57] Erp and Swinnen (n 29) 62.

[58] On the notions of 'data as things' and 'data as flow', see Michael J Madison, 'Tools for Data Governance' [2020] Technology and Regulation 29.

[59] Data Act proposal, Rec. 25.

[60] Data Act proposal, Art. 4(4).

[61] The first occurrence in law (after policy documents) can be traced to Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59 ('Free-Flow of Non-Personal Data Regulation'). Then, the notion made its way to the Regulation (EU) 2022/868 of 30 May 2022 on European data governance, OJ L 152/1 ('Data Governance Act' or 'DGA').

[62] Josef Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' <https://ssrn.com/abstract=3274519> accessed 13 November 2018; Inge Graef, Raphaël Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation' (2019) 44 European Law Review 605; Charlotte Ducuing, Lidia Dutkiewicz and Yuliya Miadzvetskaya, 'Legal and Ethical Requirements (TRUSTS Trusted Secure Data Sharing Space)' (2020) 6.2 43–44.

[63] Data Act proposal, Art. 4(6).

are seemingly viewed as objective categories of data and subject-matters of – either the same or, where deemed appropriate, distinctive – rights. By 'objective categories of data', we mean categories of data which are to a significant extent (*deemed)* independent from the context. The Data Act appears to be based on the implicit assumption that there would be a *summa divisio* of (all?) data, composed of data being either personal or non-personal. The GDPR would constitute the 'law of personal data', as complemented *i.a*. by the Data Act which would additionally constitute the 'law of non-personal data' among other legal instruments.

To conclude, IoT data are regulated under the Data Act in their own right and recognised as a regulatory subject-matter. As a matter of fact, data constitute technological artefacts reliant on their technological environment (and especially the IoT product) rather than standalone objects, which is also logically accounted for (i.e. with the 'by design compliance' nature of Article 3(1)). This being, the Data Act does regulate IoT data *as such* rather than their technological environment, which is targeted only as a means to an end, in line with the 'by design compliance' trend in EU legislation.

The recognition of data as a regulatory subject-matter is not novel with the Data Act, which therein follows a recent but marked trend.[64] It is observable not only with property law-like legal regimes (*i.e*., control and/or access rights) but also in the recently-adopted Data Governance Act ('DGA'),[65] which is fundamentally based (more or less explicitly) on *the prior existence of entitlements on data*.[66] Strikingly, this trend is also visible in the field of 'personal data protection law' with the GDPR *i.e.* recognising data as the subject-matter of the portability right.[67] The recognition of data as a regulatory subject-matter may seem trivial, so much has it acquired the force of self-evidence. However, it is not quite in line with the original spirit and letter of the law whereby the presence of personal data constitutes a *trigger* for the application of the law, with the aim to *protect individuals* rather than 'data'.[68] From a Kantian perspective, the conception of data as a thing, and even more so as a legal thing, seems misaligned with the relational nature of personal data at the basis of personal data protection law (on this, see also section 6 below). The following hypothesis can be formulated, subject to further research. First, associated with the legislative attempts to regulate data in their quality as economic resources, this trend, by endorsing the abstraction of data,[69] is characterised by a proprietarist ethos. Second, and while the GDPR is already prone to it, the view of data as a regulatory

[64] Ducuing defines the 'data flow paradigm' by the reunion of the "regulatory objective to foster the flow of data […]" and data as a regulatory subject-matter where she focuses on the granting of control vs access rights, Ducuing, 'Beyond the Data Flow Paradigm: Governing Data Requires to Look beyond Data' (n 51) 59–60. Similarly, Streinz observes that European law lays down "data ownership and access to data laws [which] conceive of data as a regulatory object that can be 'owned' and 'accessed'", Thomas Streinz, 'The Evolution of European Data Law (Chapter 29)', *The evolution of EU law (3rd edition)* (Paul Craig and Gráinne de Búrca, Oxford University Press 2021) 20.

[65] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act or DGA), OJ L 152/1.

[66] Charlotte Ducuing, 'The Regulation of "Data": A New Trend in the Legislation of the European Union?' (*CITIP blog*, 6 April 2021) <https://www.law.kuleuven.be/citip/blog/the-regulation-of-data-a-new-trend-in-the-legislation-of-the-european-union/> accessed 19 November 2021. This materialises in legal issues with the definition of 'data holder', as discussed by Baloup et al. concerning the DGA proposal from the EC, Baloup and others (n 53) s 2.2.

[67] GDPR, Art. 20. See also the linguistic shift from "data relating to individuals" (Directive 95/54/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, OJ L 281/31 ('Data Protection Directive'), e.g. Rec. 14 and 27) in the former to "data owned" by them in the latter (GDPR, Rec. 7 and 68).

[68] On this, see Dara Hallinan and Raphaël Gellert, 'The Concept of "Information": An Invisible Problem in the GDPR' (2020) 17 SCRIPTed 269; Streinz (n 64); Ducuing, 'The Regulation of "Data"' (n 66).

[69] On the process of abstraction of data, see Herbert Zech, 'Information as Property' (2015) 6 Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 192.

subject-matter will further infuse privacy and personal data protection, either by means of their (re)interpretation through these pervasive lenses, or because of the interaction with, *i.a.*, the DGA and the Data Act.[70] Third, the view of data as a regulatory subject-matter is – or can be - expected to bridge the gap between, schematically, the nascent economic law of data and personal data protection and privacy regulation, however with the risk of denaturing the latter.

Finally, a last note should be made on the policy choice to regulate data generated by IoT products or related services, in light of the rationales discussed in the previous section. The notion of 'product' is narrow in the Data Act proposal.[71] However, and as already highlighted, the rationales for regulating IoT data are also present to a great extent concerning 'mere' sensors, entirely designed to generate, process and transmit data, such as sensors embedded in soils, animals,[72] railway tracks, etc. The rooting in the product manufacturer-product user relationship could also be questioned. Some of the rationales for the regulation of IoT data (as discussed in the previous section) are also present with other types of relationships, which do however not fall under the scope of the regulation of IoT data under the Data Act. For instance, data arising from the traffic management of trains and planes are co-generated by several actors at stake (such as railway infrastructure managers and railway undertakings and, respectively, airports, traffic managers and airlines) raise serious allocation issues.[73] In such cases, data represent also the digitalisation of the actors' activities and events. As digitisation progresses, such situations are likely to increase in numbers. This raises the question whether the scope should be limited to IoT *products* and to the *relationship* between, essentially, the manufacturer and the user. On the flip side, it is clear that the broader the scope of application, the more complex the regulation is likely to get to accommodate all specificities. The main reason for sticking to IoT products and to the relationship between the data holder (mainly the manufacturer) and the user appears to be the well-known presence of power asymmetries to the detriment of the latter and the aim to restore balance. The ambition of the EC with the Data Act is obviously *not* to allocate the use of *all* co-generated data.[74]

4. The allocation of rights in the triangle

This section looks into the question to what extent the rights and obligations concerning IoT data under the Data Act can be viewed through property law lenses, before the following section focusses on the

[70] This may apply as a result of the enforcement of the Data Act, as further discussed by Charlotte Ducuing and Aliki Benmayor in The White Paper on the Data Act, in the CiTiP Working Paper Series, edited by Charlotte Ducuing and Thomas Margoni, 2022 (forthcoming). Especially, the obligation for all enforcement authorities, *including data protection authorities* with respect to personal data protection-related provisions, to aim for a "consistent application" of the Data Act, together with enforcement authorities (Data Act proposal, Art. 31(4)) could nudge them to tip in favour of data sharing, potentially to the detriment of personal data protection and privacy.

[71] A product is defined as "a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data", Data Act proposal, Art. 2(2).

[72] Atik (n 16) 8–9.

[73] See Charlotte Ducuing, Orian Dheu and Aliki Benmayor, 'RNE Data Study - Consultancy Study for RNE' (CiTiP - KU Leuven 2022) <https://rne.eu/news/rne-non-personal-data-policy-progress/>; Charlotte Ducuing, 'Chapter 2 of the Data Act – New Wine in Old Bottles?' (*CITIP blog*, 12 May 2022) <https://www.law.kuleuven.be/citip/blog/chapter-2-of-the-data-act-new-wine-in-old-bottles/> accessed 19 September 2022.

[74] To compare, and while having clearly IoT data in mind, the ALI-ELI Principles for a Data Economy are designed to apply, more generally, to data as a resource (principle 2) especially in the context of co-generated data (principle 3), irrespective of the sector. This being, the Principles re flexible and do take additional criteria into account to grant rights, such as the context and the legitimate interests at stake, etc. As discussed in section 2, the ALI-ELI Principles for a Data Economy do also apply a rule *de minimis* for the recognition as one as 'co-generator' or data.

'FRAND terms' for the data holder to make data available to the third party. The specific case of the second sentence of Article 4(6) is discussed in section 6, as a defensive right for the user. We do not discuss the effect of legacy legal frameworks as regulated under the Data Act, such as personal data protection, IP rights and the Trade Secret Directive, although their impact on the legal regime is recognised.

The user enjoys a by default freedom to use data for "any lawful purpose",[75] without any requirement to state reasons.[76] This may possibly include data monetisation (or commercialisation), for instance by exerting her data portability right with a data intermediary, although the proposal is not quite explicit on that question[77] (on this, see also section 5 below). Although the Data Act proposal does not expressly grants 'exclusive rights' to the user,[78] rights to use data by the data holder or by 'third parties' proceed from her.[79] On paper at least, the user would thus seem to be granted a form of right to exclusive use. Strangely enough, personal data may be processed by the data holder without the prior consent of users qualifying, in this respect, as data subjects, pursuant to the (conditions of the) GDPR.[80] In this case, then, the right to process personal data does not necessarily proceed from the user qualifying as a data subject. In contrast, the data holder "shall only use any *non-personal data* generated by the use of a product or related service on the basis of a contractual agreement with the user […]" (emphasis added),[81] which seems to recognise the prior existence of (property) rights on data to the user. We analyse the data holder and the third party in turn, which will also enable us to conclude on the rights of the user.

Depriving the data holder of the by default right to use data appears contradictory to the recognition of the manufacturer as a co-generator of such data (see section 2 above) as well as internally inconsistent. Because the term 'use' is not defined (i.e. whether it implies mere technical processing of data or processing for one own purposes), the consequences of the absence of such an agreement of the user are unclear.[82] This being, the remainder of the Data Act inconsistently appears to assume the existence of such an agreement.[83]

This is to the extent that the data holder – and not the user - is granted extraordinary enforcement rights under Article 11. First, (i.) the right to apply technical protection measures ('TPMs'), a form of

[75] Data Act proposal, Rec. 28.

[76] In its Position Paper on the Data Act proposal, the Max Planck Institute criticises this regulatory option and recommends that the use of data by the user shall be "further clarified and better delineat[ed]". The Max Planck Institute essentially advocated for a permitted use approach (or purpose-based approach), which could exclude commercial use (or be limited to enabling added value uses and services), Drexl and others (n 16) paras 10–11. Similarly, see also the ALI-ELI Principles for a Data Economy, according to which a co-generator of data is entitled to claim certain 'data rights' to the data controller for certain grounds, *i.e.* the right to access or have data ported should be based on the necessity of such data for maintenance or re-sale purposes or to monitor the quality of the product, ALI-ELI (n 7) s 20.

[77] For an analysis of this question, see Drexl and others (n 16) paras 15–16. See also Kerber (n 16) 10.

[78] As noted by Drexl et al., the wording of rec. 6 suggests the opposite, Drexl and others (n 16) paras 46–48.

[79] ibid 44–55.

[80] The Data Act proposal does indeed *not* provide for constraints in this respect, in addition to the exhaustive list of legal bases for the processing of personal data as per the GDPR, Art. 6. Personal data could therefore be processed on Art. 6(1)(b) GDPR (the processing is necessary for the performance of the contract) or 6(1)(f) (the processing is necessary for the purposes of the legitimate interests of the controller […]). The processing of personal data is then purpose-bound.

[81] Data Act proposal, Art. 4(6).

[82] This topic is further discussed by Charlotte Ducuing, in the White Paper on the Data Act, CiTiP Working Paper, edited by Charlotte Ducuing and Thomas Margoni, 2022 (forthcoming).

[83] Kerber (n 16) 21–22.

technological self-help well-known to copyright although with notable differences.[84] They consist in "appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and compliance with [IoT data regulation as per the Data Act] as well as with the agreed contractual terms for making data available [while they] shall not be used as a means to hinder the user's right to effectively provide data to third parties […]".[85] Second and relatedly, (ii.) the right to require from a data recipient not only the destruction of "infringing data" but also of deriving "infringing" goods, services or data[86] under the conditions laid down under Article 11(2), including when the data recipient has "abused evident gaps in the technical infrastructure of the data holder designed to protect the data",[87] which would logically include the TPMs as per Article 11(1).

As they read in the proposal, such provisions are unclear, especially in terms of their respective scope *rationae materiae*,[88] which seriously hinders the analysis. In particular, a striking question relates, generally, to the existence of underlying substantive statutory rights. In short, are TPMs allowed (and legally protected based on Article 11(2)) as technological enforcement of underlying rights, or, alternatively, as technological *alternatives* to rights? It is also unclear whether TPMs are allowed (under Article 11(1)) *erga omnes,* while the specific enforcement rights granted under Article 11(2) are clearly targeted at the 'data recipient' (*i.e.* the 'third party' chosen by the user to exercise her data portability right). In this context, we do not engage into a comprehensive analysis here but merely identify a few pointers.

Article 11 raises the obvious question whether it amounts to a legal endorsement of the *de facto* control of data by the data holder, through the protection of the technical environment. It would then constitute an alternative (potentially, much more efficient) to a direct and straightforward granting of entitlements on data to the data holder. At first glance, it would seem that the data holder benefits from a *by default right to reserve data technically*, and make use of related special enforcement rights, with obligations to provide access to data as per the Data Act being the exception. Although not directly akin to (intellectual) property law (i.e. not *erga omnes,* but seemingly limited to the data recipient), the enforcement rights as per Article 11(2) are noticeably far-reaching. First, their scope *rationae materiae* extends beyond data directly subject to substantive rights and obligations as per the Data Act, namely to things *deriving* from such data, although subject to either a balancing or a proportionality test,[89] and, second, from a procedural perspective, they seem to amount to injunctions that data holders can require courts – or competent authorities - to decide "without undue delay".

This seems to stand in contradiction with Recital 5 that states that the Data Act should "not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service. Instead, it takes as a starting point the control that the data holder

[84] See Leander Samuel Stähler, in CiTiP White Paper on the Data Act proposal, CiTiP Working Paper Series, ed. Charlotte Ducuing and Thomas Margoni, 2022 (*forthcoming).*

[85] Data Act proposal, Art. 11(1).

[86] The data holder is also allowed to use, essentially, technological self-help, known as technical (or technological) protection measures, as per Art. 11(1). The Data Act is however unclear both on the scope of such provision and on its legal consequences. On this, see Leander Stähler, 'Article 11 of the Data Act: Avenues of Interpretation in the Regulation of TPMs for Data' (*CITIP blog*, 28 July 2022) <https://www.law.kuleuven.be/citip/blog/article-11-of-the-data-act-avenues-of-interpretation-in-the-regulation-of-tpms-for-data/> accessed 23 August 2022.

[87] Data Act proposal, Art. 11(2).

[88] For a synthetic analysis of the – highly diverging – interpretations, see Stähler (n 87).

[89] Data Act proposal, Art. 11(3).

effectively enjoys, *de facto* or *de jure*, over data generated by products or related services". Recital 5 (in combination with Article 11) should thus be read as distinguishing *positive rights of access and use* (that the Data Act does, indeed, *not* grant to the data holder) from *defensive rights* to protect data from detrimental use by third parties, that Article 11 *does* provide. The objective is then to keep incentives for the data holder to invest in further data generation,[90] as such incentives are presumed to be weakened by the rights of access and use granted to other parties.[91] This leads to the paradoxical finding that the granting of access and use rights to other parties goes hand in hand with a certain legal endorsement of *de facto* control of data (the extent of which is debatable, as discussed above).

This looks like an attenuated form of the data producer's right 'defensive right' option contemplated by the EC in 2017, designed to incentivise voluntary data sharing.[92] Symptomatically, the question whether there is indeed a need to protect the investment of data holders based on Article 11 shares interesting similarities with earlier debates on the 'data producer's right'. The question was then whether the creation of such data ownership would be justified by the need to incentivise data production and/or exchange, which constitute typical rationales for the creation of exclusive intellectual property rights for intangibles.

This, in turn, calls obviously into question the boundary line between 'defensive' vs 'positive rights', both *de jure* and *de facto.* Should the Data Act indeed protect the "data-generating infrastructure"[93] of data holders, it would indeed enable the later to engage decidedly and calmly into value-generating data activities (data sharing, etc.). In the following section on 'FRAND terms', we further discuss whether the Data Act also endorses the *de facto* control of data by the data holder in a *positive manner.* The question how the Data Act proposal aims to empower users for the use of 'their' data invites us to take a closer look at the regulation of third parties chosen by user to exercise her data portability right, in the remainder of this sub-section.

While the data holder may, under the aforementioned circumstances, use data for their own purposes, 'third parties' may use data only "for the purposes and under the conditions agreed with the user",[94] particularly following the exercise by the user of a right to 'data portability'.[95] More generally, the possibility for third parties to use data is entirely subjugated to the users' agreement and bound to the related purpose(s). It is thereby clear that Articles 5 and 6 grant the user *more than a (mere) data portability right*. Their reach extends indeed beyond data access, namely to the regulation of the *use* of data – both positively (what the third party *shall do)* and negatively (what the third party *shall not do),* with the obvious aim to empower users. This raises two questions.

[90] The granting of defensive rights to the data holder seems to detract also from the fear that the access to her data by users and third parties could weaken her technological environment, albeit already protected under the so-called Budapest Convention (Council of Europe 2001 Convention on Cybercrime), referred to in Rec. 10, and the Cybercrime Directive (Directive 2013/40).

[91] The economist Kerber argues that there is no such need, Kerber (n 16) s 4.3. In contrast, the Position Statement of the Max Planck Institute argues that the endorsement of the *de facto* control of data by data holders would "allow[her] to charge a price for the sharing of data which, in turn, can be used for improving the quality of data […]", Drexl and others (n 16) para 116.

[92] European Commission, 'Communication Building a European Data Economy' (n 5); Staff Working Document 'On the free flow of data and emerging issues of the European data economy accompanying the Communication 'Building a European data economy' 2017 (SWD/2017/02 final) s 7.2.

[93] Angelina Fisher and Thomas Streinz, 'Confronting Data Inequality' (2022) 60 Columbia Journal of Transnational Law 829, 833.

[94] Data Act proposal, Art. 6(1).

[95] Data Act proposal, Art. 5.

The first question relates to the extent – and therefore efficacy - of the 'third party mechanism' both in time and *rationae personae.* Property law, and in particular ownership, is indeed impactful because of the *in rem* and *erga omnes* nature of rights. In turn, the user can use the 'third party mechanism' only *vis-à-vis* such third party, with little downstream effect. It applies only to a specific *moment* in the data value chain, irrespective of what happens *then* with the said data, in which the user retains no further rights on data (no *in rem* rights). It is true that the third party is in principle prohibited from transferring the data to a second line third party, irrespective of the data form (whether raw, aggregated or derived), unless necessary to provide the service requested by the user.[96] However, the user is granted with neither a direct right and action enforceable against downstream infringers nor legal protection for TPMs, in contrast to the data holder.[97] It is commonplace that the features of data, and especially their dynamicity, ubiquity and large amount, make it difficult to keep genuine 'control' of data, especially downstream the value chain. This consideration lied at the heart of the data ownership debate.[98] It was then further investigated by the engineering scholars community and promoted in EU-funded research and innovation projects, under the heading of 'data sovereignty',[99] in turn closely related to the original idea of 'data spaces'.[100] This stands notably in contrast to the ALI-ELI Principles for a Data Economy, which propose diverse mechanisms to take into account the downstream effect of various rights and entitlements weighing data downstream the value chain.[101]

This being, and although not explicitly mentioned in the text,[102] the third party mechanism does not seem to be subject to exhaustion. In other words, and subject to welcome clarification from the legislator, it seems possible for the user to exert her data portability right concerning the same or other data, several times, with several different third parties, and for different purposes. In short, the downstream effect of the user's rights is limited, *i.e.* her rights are enforceable solely against the

[96] Data Act proposal, Art. 6(2)(c).

[97] Article 11(2) grants the user with the possibility to "instruct" the third party concerning the processing of data, which could prevent the data holder from exerting her special enforcement rights. This, however, is unclear and raises numerous questions, see Leander Samuel Stähler, in CiTiP White Paper on the Data Act proposal, CiTiP Working Paper Series, ed. Charlotte Ducuing and Thomas Margoni, 2022 (*forthcoming).*

[98] Hummel et al. discuss the growing focus on claims relating to the actual controllability of data (albeit mainly in the field of personal data protection), namely the "*effective* means for data subjects to exercise control over her data" (emphasis added), Hummel, Braun and Dabrock (n 38) 554.

[99] Some of them have joined forces within the movement 'Data Sovereignty Now', constituted by the following members (at the time of writing): aNewGovernance, Freedomlab, Innopay, IDSA, i-Share, Meeco, MyData, Sitra, TheChainNeverStops and TNO.

There is not one single definition of 'data sovereignty' amongst research and industry organizations. Some lean straightforwardly towards full control of one over their 'own data' such as this of IDSA: "IDSA enables you to self-determine how, when and at what price others may use ['your' data] across the value chain", see https://internationaldataspaces.org/why/data-sovereignty/. Data sovereignty is often associated with the use of electronic ledger-based smart contracts, as part of the broader technology mix.

[100] *Designing Data Spaces* <https://link.springer.com/book/10.1007/978-3-030-93975-5> accessed 24 August 2022.

[101] ALI-ELI (n 7) pts IV, Chapter B (Effects of Onward Supply on the Protection of Others). See in particular the original propositions laid down in, respectively, Principle 33 with a direct action against a downstream data recipient, and Principle 34 dealing with 'data thieves'. The Principles also deal with the arduous question of the responsibility of a person processing data for her own purpose ('data controller') when such data constitute derived data compared to original data weighed with certain rights or entitlements. To do so, Principle 35 is based on risk-based approach. Interestingly, the Principles for a Data Economy go therein *beyond* the reach of the GDPR, which is unclear on the responsibility of a controller in the data value chain (i.e. vis-à-vis other controllers). On this, see Christiane Wendehorst, 'Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?', *Data as Counter-Performance - Contract Law 2.0?* (Lohsse, S; Schulze, R; Staudenmayer D, Nomos 2020)..

[102] Art. 8(4) reads "A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II." It could be indirectly read as a confirmation of the interpretation that there is indeed no exhaustion of the rights granted to the user under Articles 5 and 6.

chosen third party(ies) [103] and, respectively, the data holder, [104] to the exclusion of infringers downstream the value chain. However, while users' rights are thus not *erga omnes,* the non-exhaustible character of the third party mechanism (should it be confirmed) constitutes an interesting alternative for data, given their non-rivalry and ubiquity and the willingness of the EC to foster data reuse.

The relationship between the user and the chosen third party can be conceptualised as a compulsory license or as a "limited proprietary right" in the parlance of the Draft Common Frame of Reference ('DCFR'),[105] although the regulation of this triangular mechanism is very obscure (on this, see also the following section). The creation of limited proprietary rights is precisely one of the rights typically afforded to the owner of a thing,[106] as a supporting tool for her to enjoy the fruits of her thing (such as with IP or immovables). The data holder therein acts *on behalf of* the user as a data processor and arranges the technical conditions with the third party by means of a derivative contract.[107] While the data may concretely flow from the data holder to the third party, the user does indeed decide upon both the transfer of data to the third party and the purpose(s) of use,[108] based on explicit statutory rights while the data holder has no such rights.

To conclude, granting the user a by default - rather than purpose-limited - right to use data for *any lawful purpose* based on the rationales discussed in section 2 does find sources in property law. In terms of substance, the Data Act walks a ridgeline. On the one hand, it provides the user with *positive rights to use* data out of fairness considerations while, on the other, providing the data holder with *defensive rights* that protect – and to some extent endorse – her *de facto* control of data to incentivise her in further data production investments. This results in an unclear legislative allocation direction and, quite obviously, in a highly complex construct which questions its future 'reality test'. The following section takes a closer look at the condition under which the data holder shall make data available to the third party chosen by the user.

5. Conditions under which the data holder shall make data available to the chosen third party

This section looks into the regulation of the conditions under which the data holder shall make data available to the third party chosen by the user (chapters III and IV). By doing so, the aim is to continue the exploration of the extent to which the Data Act endorses the *de facto* control of data by the data

[103] See Data Act proposal, Art. 5.

[104] See Data Act proposal, Art. 4(6), discussed further below in section 6.

[105] Study Group on a European Civil Code and Research Group on EC Private Law (Acquis Group), *Principles, Definitions and Model Rules of European Private Law Draft Common Frame of Reference ('DCFR')* (Eds Christian von Bar, Eric Clive and Hans Schulte-Nölke, and Hugh Beale, Johnny Herre, Jérôme Huet, Matthias Storme, Stephen Swann, Paul Varul, Anna Veneziano and Fryderyk Zol, 2009).

[106] ibid Comments under VIII.–1:202: Ownership.

[107] Such a type of contractual construct, with many possible variants (i.e. whether with a mandate granted to the professional or not, for instance) can particularly be observed where the holder of rights (in this case, the user) is not a professional, see for instance the data controller – data processor relationship under the GDPR (GDPR, see in particular Art. 28) or, outside the 'data' environment, in railway law whereby the 'applicant' may acquire capacity rights from the railway infrastructure manager but the train can only be operated by a railway undertaking, subject to a separate contractual relationship with the infrastructure manager, see Directive 2012/34, Art. 10, 28, 38 and 41.

[108] Kerber gives another interpretation. He argues that there is a compulsory licensing agreement between *the data holder* and the third party. Kerber (n 16) 6–7.

holder. However, Chapters III and IV pursue also other objectives, and especially market ordering, which complicates the reading.

Where a data holder is obliged to make data available to a data recipient, Article 8 mandates, first, the conclusion of a contract concerning the terms for making the data available.[109] Such contract shall not include unfair terms as regulated under Article 13 (Chapter IV). Article 13 reads as data-specific regulation of unfair contract terms. It applies to contractual terms "concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations […]".[110] Unfair terms shall not be binding on the party to whom it has been unilaterally imposed. Similar to the Consumer Unfair Terms Directive,[111] Article 13 consists in three layers. First, a 'black list' of unfair terms; second, a 'grey list' of terms presumed unfair; and third, a general definition of 'unfair terms'. In other words, the data holder is under an obligation to 'be kind' under a regulation of B2B unfair commercial practices.

Second, the data holder shall make data available to the chosen third party under 'FRAND' (Fair, Reasonable and Non-Discriminatory) terms.[112] According to Article 9, any "compensation for making data available" shall be "reasonable" and Recital 42 clarifies that the compensation should "not be understood as paying for the data itself". In the case where the data recipient (the chosen third party) is an SME, the compensation shall not exceed the costs directly related to making the data available.[113] Recital 46 explains that such rule does not apply in case of making data available to other data recipients (non-SMEs): "in such cases, the companies are considered capable of negotiating any compensation if it is reasonable, taking into account factors such as *the volume, format, nature or supply of and demand for the data* as well as the costs for collecting and making the data available […]" (emphasis added).[114] FRAND terms constitute a well-known tool stemming from competition law. They have been laid down in competition law-inspired regulations such as mandatory licenses in IP and in the long-lasting regulation of liberalised network industries.[115] FRAND terms are generally expected to constitute a middle ground between rule-based regulation and the freedom to conduct a business. Under the Data Act, the European Commission views FRAND terms as a fall-back for competition law.[116] In other words, the data holder is under an obligation to 'be kind' under a legal regime closely inspired by competition law and aiming to restore fair markets.

---

[109] Data Act proposal, Art. 8(2).

[110] Data Act proposal, Art. 13(1). Chapter III applies only to the benefit of SMEs, but the wording of Art. 8(2) suggests that Chapter III shall be deemed applicable to the relationship between the data holder and the third party chosen by a user pursuant to Chapter II.

[111] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29 ('Consumer Unfair Terms Directive').

[112] Chapter III applies to the making available of IoT data by the data holder to the third party chosen by the user pursuant to Chapter II, but also to other future obligations to make data available, i.e. based on data space-specific regulations, see Art. 12.

[113] Data Act proposal, Art. 9(2).

[114] Rec. 46 seems to assume that data recipients are always businesses, whether SMEs or large ones. However, third parties chosen by users under Art. 5(1) may also be other types of entities, such as research organisations or not-for-profit organisations (see Rec. 29). This is also confirmed by the definition of a data recipient, see Data Act proposal, Art. 2(7). Where chosen third parties are non-businesses, a literal reading of Art. 9 would seem to suggest that the data holder may levy a 'reasonable' compensation but the wording of Rec. 46 seems equivocal in that respect.

[115] The latter are surprisingly often overlooked in review on FRAND terms. However, they constitute a major tool in the regulatory toolbox and, therefore, an interesting source of inspiration.

[116] Commission Staff Working Document, Impact Assessment Report Accompanying [the Data Act proposal], SWD(2022) 34 final, 23.2.2022, 6-7.

The interpretation of the FRAND terms is not easy,[117] starting with the simple question of the object of the contract, or in other words the counter-performance for the 'compensation'. The overall picture – and the comparison with earlier materialisations of FRAND - gives the impression that Chapter III mandates and regulates the 'sale' (or 'transfer') of data from the data holder to the third party.[118] The derogatory regime to the benefit of SMEs does not raise much issue. The 'compensation' would constitute the price, thereby seemingly endorsing the view that data is an object of trade. This would also mean the Data Act endorses the *de facto* control of data by the data holder, which could futher support the interpretation that the data holder may legitimately engage in other data transactions (namely, voluntary ones) that the data holder engages into. Recital 46 seems to suggest that the data holder could adapt the 'compensation' depending on both the nature of data and the market conditions (i.e. supply and demand), which further reinforces this interpretation. However, in contrast, the statement of Recital 42 that the compensation should "not be understood as paying for the data itself" seems to suggest that data should be made available for free. The compensation – and in particular the 'reasonability' requirement - would relate to other 'objects' of the contract, such as royalties for IPRs potentially at stake and to the respective activities involved in the making available of data,[119] with unclear consequences on the nature and interpretation of the contract.

Two related issues can be identified. First, property questions are intertwined with public law rules classically designed to restore fair competition (FRAND), which makes it hard to distinguish the 'property law layer' therein. Second, the reason why they are intertwined is that property questions are actually not genuinely tackled, but rather circumvented. The term 'compensation' and the mention that compensation shall not amount to a price for data can be viewed as a sign that the Data Act proposal *shies away* from clarifying whether data is an object of trade and whether the data holder may trade data, albeit not having a property title. The question is then tackled indirectly by laying down 'be kind' obligations (Chapter III and Chapter IV) which are seemingly expected to fluidify data transactions, irrespective of the legal qualification of the transaction – and potentially of the private law consequences. Subject to further research, a similar trend seems to be at work with the Data Governance Act, especially with the regulation of data intermediaries which aims to foster data sharing for commercial purposes, thereby shying away from mentioning 'sale', 'purchaser' or 'seller'.[120]

Only the future will tell whether – and to what extent - the circumvention of property problems by such a 'legal pragmatic engineering' will come back as a boomerang. On the one hand, it is true that private law – and especially property law and contract law – is mainly regulated by member States, so that the Data Act can therein be viewed as protected their prerogatives. On the other hand, the whole regulation of IoT data has profound consequences on private law while there is often unclearity as for the legal status of data. Additionally, the Data Act, as a Regulation, will apply directly between private entities without room for transposition. This means that "competent authorities", in charge of the

[117] For both competition and practical reasons, the Max Planck Institute recommends to delete the link between Chapter II and Chapter III, so that the data holder would not be able to claim a compensation, Drexl and others (n 16) paras 71–72.

[118] On the question how the 'reasonable compensation' under Art. 9 shall be interpreted, see also Graef and Husovec (n 16) s 4.

[119] This could for example consist in aligning the data available (*i.e*. the data generated by the use of a product) and the data that the chosen third party needs. On this see, Kerber (n 16) s 4.2.1. and Charlotte Ducuing, in the CiTiP White Paper on the Data Act proposal, CiTiP Working Paper Series, Ed. Charlotte Ducuing and Thomas Margoni, 2022 (*forthcoming*).

[120] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152/1, Chapter III.
See also the discussion on the definition of 'data holder' as proposed by the EC, Baloup and others (n 53) s 2.2.

enforcement of the Data Act according to Chapter IX, will be tasked with this thorny interpretation. Another simple reason can be found in the difficulty in achieving goals classically operationalised with property law *without* a genuine property law regime. This raises again the burning question whether the recognition of data (and more generally of things) by property law is a necessary prerequisite to the smooth operation of other branches of law, and especially contract law.[121]

6. Traces of personal data protection law: focus on the second sentence of Article 4(6)

The Data Act includes a number of limitations to the use of data by the respect actors in the triangle. They generally serve the purpose either to interface with legacy frameworks (such as IP rights, trade secrets or personal data protection law) and/or to accommodate the legitimate interests of several actors with respect to the data, either internally (within the triangle) or externally (to the benefit of other parties). This section focusses on the second sentence of Article 4(6), which is particularly alien to a property law reading. In turn, it shares stricking similarities with personal data protection law fundamentals. The analysis of this provision helps understand the notion of 'data control' better, as increasingly sought for by the EC. The section ends with a note on the vocabulary used in the Data Act, which takes occasional inspiration from personal data protection law.

The second sentence of Article 4(6) reads as follows: "the data holder shall not use such [i.e. non-personal] data generated by the use of the product or related service to derive insights about the economic situation, assets and product methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active". This provision follows long-lasting demands from business users of IoT products, under the general and misleading heading of 'data ownership',[122] to have more agency concerning 'their' data. The example of smart farming has been particularly discussed and is expressly referred to in the Data Act.[123] For instance, as IoT product manufacturers become the *de facto* 'owners' of data, farmers fear that, although innocuous on an individual level, IoT data could end up producing sensitive information on their farm. A study for the European Parliament notes that the aggregation and further processing of many such data from different data sources could result in "private information about crop yields and soil fertility […]" being created, which could otherwise qualify as trade secrets since they could be "used for pricing purposes".[124] As Recital 25 notes, this phenomenon is associated with the economic concentration in this – as well as other – sector so that "contractual agreements may be insufficient to achieve the *objective of user empowerment*. The data tends to remain under the control of the manufacturers […]" (emphasis added).[125] This is against this background that the Data Act proposal provides users not only with rights positively enabling them to make use of 'their' data (as discussed in section 4 above), but also defensive rights to restrict data use by, i.e. the data holder.[126] While in principle to the benefit of

[121] Ferenc Szilágyi, 'The necessity of data allocation: A plea for a private law (property law) perspective' (2021) 10 European Property Law Journal 180.

[122] See the work of Hummel et al. on the different claims and meanings conveyed with the term 'data ownership', albeit they discuss mainly personal data, Hummel, Braun and Dabrock (n 38).

[123] Data Act proposal, Rec. 14, 25

[124] Mihalis Kritikos, 'Precision Agriculture in Europe:Legal, Social and Ethical Considerations - Think Tank' (Scientific Foresight Unit (STOA), DG for Parliamentary Research Services 2017) 16–17 <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2017)603207> accessed 21 February 2020.

[125] Data Act proposal, Rec. 25.

[126] Data Act proposal, Rec. 25.

both individuals and businesses acting as users, the second sentence of Article 4(6) protects economic interests and is obviously targeted at businesses in the first place.

The problem at stake *could have been tackled* from many different angles, i.e. from a decisive competition law perspective or as part of Chapter IV on the regulation of unfair commercial terms. As it reads, the second sentence of Article 4(6) settles with a statutory prohibition of a data-specific commercial practice deemed unfair. The relative dominance of the data holder over the user is irrefutably presumed. Substantively, it can also be viewed as an 'add on' to trade secret protection, whereby the legal protection is extraordinarily extended to (the prohibition of) reverse engineering.[127] Applicable *solely* to non-personal data, the legal sources of Article 4(6) can also be found in personal data protection law. It is indeed the existence of an inseparable link between the data and the user and/or its assets and product methods (or in other words, the thing(s) that the data relate to) that constitutes the cause why the user could suffer detrimental effects from the use of data by the data holder.

Article 4(6) can directly be associated with the justification (d) (discussed in section 2 above) as it relates to the relational nature of some data. With obvious similarities to the GDPR, this results in a form of unwaivable purpose-limitation. Even though the user contractually agrees to the use of data by the data holder (e.g. 'sales' her data) pursuant to the first sentence of Article 4(6), the data holder does then not acquire an *absolute* right on such data but has to suffer limitations. However, the reading suggests that the prohibition of Article 4(6) applies 'weakly', namely solely to the data holder and not to any person happening to 'control' such data downstream the data value chain.[128] The nature of the harm, namely economic, that Article 4(6) aims to prevent, is also more narrow than in the GDPR.

By recognizing the inseparability between certain data and the user (or the user's economic equipment) and by weighting the use of data by the data holder, however consecutive to contractual agreement, to the benefit of the user, the second sentence of Article 4(6) shares little with property law. The provision compares to the broader 'right to desistance' proposed by the ALI-ELI Principles for a Data Economy (Principles 21) whereby a co-generator of data may require that the data controller desists from data activities which could harm her under certain conditions.[129] The ALI-ELI Principles give the example of manufacturers in the position to make more informed commercial decisions based on the knowledge acquired from farm data, which typically applies to the smart farming scenario described above.[130] The ALI-ELI reckon the GDPR as one of the sources for this right. They consider that the right to desistance fulfils a function similar to the right to reclaim a physical good.[131]

---

[127] See the clarification in Rec. 16 that the Trade Secret Directive does not prevent the "independent discovery of the same know-how or information […]. Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed […]", Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure ('Trade Secret Directive'), OJ L 157/1.

The trade secret inspiration is also acknowledged in Drexl and others (n 16) para 50.

[128] To compare, the rights and obligations laid down by the GDPR are most of the time enforceable against the controller, namely the person deciding upon the 'why and how' of personal data processing (see the definition in the GDPR, Art. 4(7). Any processing activity is therefore under the 'control' of at least one controller, whether the original controller or a downstream controller. This being, the relationships between independent controllers constitutes a blind spot of the GDPR. On this, see Wendehorst (n 102).

[129] See the other conditions that should be fulfilled, ALI-ELI (n 7) s 21.

[130] ibid 158.

[131] See comments from the rapporteurs under, respectively, Principles 21 and 17, ibid 21;17.

As claimed by the very Data Act, the second sentence of Article 4(6) can be associated with the objective to grant users with 'data control' namely, as a reminder, the ability for users to "meaningfully control how the data generated by their use of the product or related service is used […]".[132] The Data Act follows a user-centric 'data control' objective viewed as a two-facetted concept. On the one hand, users are positively enabled to make active use of 'their' data. On the other hand, the data holder as a powerful counterpart is prevented from using the said data for purposes detrimental to users (defensive facet). 'Data control' is also literally present in the GDPR (in contrast to the earlier Data Protection Directive)[133] and, increasingly, in recent policy documents dealing with both individuals - with respect to personal data - and businesses with respect to non-personal data.[134] The definition and role of 'data control' in EU legislation should be further elucidated, including the question whether it corresponds to the concept of informational self-determination.[135]

Section 3 described the recognition of data as a regulatory subject-matter as marked by a proprietarist ethos and poised with overflowing personal data protection law. In turn, this section describes the reciprocal phenomenon, whereby the dignitarian approach of personal data protection law extends to the protection of businesses with respect to 'their' non-personal data. We posit the hypothesis that the increasingly present notion of 'data control' is expected to constitute the conceptual bridge between the two. We make the assumption that this nascent development could be compared to the calls for the recognition of a right to 'informational self-determination' of businesses after – and as an alleged counterpart to - individuals'.[136] To the extreme, informational self-determination - or, alternatively, data control - could be operationalised by both economic rights and moral rights, similar to copyright legislation, with specificities for personal vs non-personal data.

Finally, the influence of personal data protection law can also be observed in the vocabulary and concepts, which should be further analysed. In particular, the term 'purpose' is used on several occasions and in particular concerning the conditions under which the third party shall process the

---

[132] Data Act proposal, Explanatory Memorandum, point 3. See also Data Act proposal, Rec. 25.

[133] GDPR, Rec. 7 and 68.

[134] Staff Working Document 'On the free flow of data and emerging issues of the European data economy accompanying the Communication 'Building a European data economy' 30; 33; Communication 'A European strategy for data' 10;20.

[135] For an analysis of informational self-determination as a rationale of personal data protection law, see Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021) 12 JIPITEC <http://www.jipitec.eu/issues/jipitec-12-4-2021/5409>.

[136] The German Data Ethics Commission advised for a "right to digital self-determination [to be recognised for businesses, which, according to the German Constitution,] cannot invoke the concept of human dignity […]", 'Opinion of the Data Ethics Commission' 238, 44. See the definition of both self-determination and *digital* self-determination that they provide, ibid 14. For its part, the Austrian data protection authority ('Datenschutz behörde' or 'DSB') held in a dispute in 2020 that a legal person has the constitutional right to data protection under the Austrian Data Protection Act ('Datenschutzgesetz' or DSG') and is entitled to lodge a complaint before the DSB (DSB - 2020-0.191.240, the decision can be found on the DSB website: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20200525_2020_0_191_240_00/DSBT_20200525_2020_0_191_240_00.html, last visited 31st August 2022). The DSB recognised that, going beyond the GDPR which protects only natural persons, the scope of Austrian data protection law extends to "every person" (Art. 1 of the DSG: "Every person shall have the right to secrecy of the personal data concerning that person […]"). The DSB offers an English translation of the relevant legislative provisions (see https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html , last visited 31st August 2022). See also the previous decision of the DSB, DSB-D216.713/0006-DSB/2018 (to be found on the DSB website: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f11d9943-2022-46a8-ad53-7c5cf9d59c22&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=18.03.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=EinerWoche&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20180913_DSB_D216_713_0006_DSB_2018_00 , last visited 31st August 2022).

data, namely solely for the purpose agreed with the user (purpose-bound).[137] The purpose for processing data plays also a role concerning the use of data by the data holder. Article 3(2)(d) lays down transparency obligations incumbent on the data holder, who shall state the purpose(s) for which she intends to use the data. Although an unclear construct, a possible interpretation of the first sentence of Article 4(6) is, then, to combine it with Article 3(2)(d). The user would then have the possibility to agree contractually to the use of data by the data holder for the purpose(s) stated by the data holder. This would read as another limitation to the use of data by the data holder, which would then be purpose-bound. This confirms the aim of the EC to turn the user into a 'controller' of the processing of 'her' data. The concept of 'purpose' plays also a predominant role in the other chapters of the Data Act, in particular in Chapter V on business-to-government data sharing obligations.[138]

7. Conclusion

The regulation of IoT data under the Data Act may generally be viewed as a property institution, in the sense that it lays down a form of initial allocation of the use of data between the main actors. It constitutes an original form of property institution, closely intertwined with other objectives pertaining traditionally to other branches of the law, such as competition law, the regulation of unfair commercial practices, personal data protection law and contract law. Departing one from the other is rendered arduous by the close imbrication and by the non-conventional means by which the property law objectives are pursued. The aim is obviously to empower the user by giving her a by default right to use data, in addition to concrete supporting mechanisms, such as the 'third party mechanism' based on the data portability right. However, two major limitations are visible. First, the Data Act simultaneously grants legal protection to the data holder with respect to her technological infrastructure, seemingly for fear that the empowerment of users with their data would desincentivise her to keep producing data. This results in an unclear legislative allocation choice and in a complex construct. Second, the analysis of the text with property law lenses enables to identify that the rights granted to the user have limited effects in time and *rationae personae.* They do not apply downstream the value chain, which weakens them, although the 'third party mechanism', if genuinely non-exhaustible – could partly compensate.

The regulation of IoT data confirm the thesis of Streinz that a 'European data law' is emerging,[139] whereby the initial personal data protection law is complemented with the economic law of data. This paper identified two reciprocal interplays in this respect. First, the Data Act illustrates a broader trend at work in EU law, namely the endorsement of the abstraction of data and the recognition of data, whether 'personal data' or 'non-personal data', as a regulatory subject-matter. Characterised by a proprietarist ethos, this are likely to infuse personal data protection law. Second, users are granted rights justified, *i.a.*, on the recognition that data *relate to* users(' equipments), which shares conceptual

[137] Data Act proposal, Rec. 33 and 34 and Art. 6(1).

[138] Data Act proposal, Rec. 60-68.

The concept of 'purpose' was also proposed to be used in the Data Governance Act proposed by the EC, in the Data Altruism Chapter, concerning non-personal data. Art. 19(2) entrusted data altruism organisations with the task to "ensure that the data is not to be used *for other purposes than those of general interest for which it permits* the processing" (emphasis added). On this see, Baloup and others (n 53) 41–42. Among other changes, the final version of the provision does not retain the term 'purpose' which is replaced with 'objective'. The final provision reads: "the recognised data altruism organisation shall not use the data for other *objectives* than those of general interest for which the data subject or data holder allows the processing. […]" (Data Governance Act, Art. 21(2)). In the final version of the text, the term 'purpose' applies only with respect to the processing of personal data.

[139] Streinz (n 64).

similarities with the notion of personal data as data related to an individual. One of such rights - the defensive purpose-limitation right enforceable against the data holder of Article 4(6) – has a striking personal data protection law flavour. Although very different, the 'data portability' mechanism is obviously inspired by Article 20 of the GDPR. Originating from personal data protection law, the concept of 'purpose' plays an interesting role. This follows the statement of Van Erp that, with data, ownership should be reconceptualised as "the power to access, control, delete, port and transfer",[140] an which has been followed by the ALI-ELI Principles for a Data Economy.

Against this background, we posit the hypothesis that 'data control' constitutes – or is expected to constitute – a conceptual bridge between the regulation of personal vs non-personal data, and between the economic law vs the personality rights approach to data. Data control seems indeed to be based on both economic concerns that data are exchanged on markets and the ambition to provide individuals and businesses with agency and autonomy concerning 'their' data.[141] As operationalised in the Data Act proposal, data control has both an active facet, namely the provision of rights expected to enable the user to use 'her' data, and a negative facet, namely the prohibition of data use by others when likely to interfere with the user autonomy. Whether data control could play the role as a functional equivalent to ownership for data, given both the specific features of data and the inherent imbrication of many branches of law, remains to be further examined.

The regulation of IoT data in the Data Act appears to be based on a private law ordering, namely on the decentralised actions by actors on markets. New to data, the constitution of such a 'private law infrastructure' for the operation of markets is quite illustrative of a property law approach. This is also expected, indirectly, to deliver on the public policy objectives to foster innovation and to fix market failures, while specific provisions are also included for such purposes. The EC could have chosen to solve market failures and foster innovation more directly by granting actors in the value chain with a direct right to access specific data for a specific purpose (*i.e.* aftermarket service providers for the purpose of their respective business).[142] While the Data Act constitutes the horizontal layer, (data spaces-) specific legislations could lay down such provisions.[143] This is for example the case with the Ecodesign Regulation proposal from the EC. As part of the circular economy agenda, the proposal creates the framework for granting data access rights to aftermarket businesses, as part of the establishment of 'digital product passports' which could virtually concern all products (groups), including IoT products.[144]

---

[140] Sjef van Erp, 'The Covid-19 App: What Data "Ownership" Really Means' (2020) 9 European Property Law Journal 1, 2. See also Sjef van Erp, 'Management as Ownership of Data', *Data as Counter-Performance - Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy*.

[141] Richter links informational self-determination to autonomy, seeing this principle as "an information-specific principle of autonomy that empowers individuals", Heiko Richter, 'The Power Paradigm in Private Law' in Mor Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (Springer Berlin Heidelberg 2018) 5.3.1 <https://doi.org/10.1007/978-3-662-57646-5_19> accessed 22 July 2019. On the liberal foundations of property law, see i.a. Hanoch Dagan, *A Liberal Theory of Property* (1st edn, Cambridge University Press 2021).

[142] The position statement of the Max Planck Institute is indeed critical of the non purpose-bound data access rights granted to users, for which there would be no justification – and in particular no *economic* and/or market failure-based justification. Drexl and others (n 16) paras 32–43.

[143] Data Act proposal, Art. 40(2).

[144] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC, 30.3.2022, 2022/0095 (COD), Chapter III.

As visible in both the Data Governance Act and the regulation of IoT data under the Data Act, the EC appears to shy away from regulating clearly core underlying property questions, such as whether data may be traded in exchange for a price. Instead, the EC proposes what was qualified here as a 'pragmatic legal engineering' to lay down the conditions for such trading to take place, i.e. with the imposition and regulation of contracts(' terms) and the regulation of intermediaries. It seems clear that the EC aims to deliver on fundamental property objectives – such as enabling the trading of data – without ownership.

Finally, a last note should be made on the need for governance mechanisms, again informed by property law. Ownership is characterised by a centralisation of rights with the owner, namely – to some extent caricaturally - the individualistic authority of the owner on 'her' thing. In contrast, the nature of data and the policy expectation that data are used by several stakeholders, imply a distribution of rights. This raises the logical question whether governance mechanisms are required to organise and/or operationalise such rights.[145] Governance mechanisms are defined here as the decision-making system and institutions for managing organisations. From a policy and regulatory perspective, data governance has been defined as a system of rights and responsibilities that determine who can take what actions wit what data.[146] The analysis of a concrete proposal for a data property institution, shows again the relevance of this question, subject to further research. The regulation of IoT data under the Data Act proposal displays many interfaces with legacy legal frameworks (mainly trade secrets protection, IP rights and personal data protection), which can understandably not be settled in the abstract in statutory legislation. Additionally, the whole legal regime relies on contractual negotiations between the actors in the triangle, with unpredictable outcomes.[147] This raises the question whether statutory rights should be completed with facilitating governance mechanisms, such as data intermediaries within the meaning of the Data Governance Act.[148]

[145] Erp, 'Management as Ownership of Data' (n 141). Van Erp looks to the construct of trusts under Québec law which is based on "ownerless property".

[146] Such definition is based on Rene Abraham, Johannes Schneider and Jan vom Brocke, 'Data Governance: A Conceptual Framework, Structured Review, and Research Agenda' (2019) 49 International Journal of Information Management 424. e the definition of 'governance' in the Cambridge online Dictionary, GOVERNANCE, https://dictionary.cambridge.org/dictionary/english/gov-ernance accessed 11 February 2020, and in the Oxford online Dictionary: GOVERNANCE https://www.oxfordlearnersdictionaries.com/definition/en-glish/governance?q=governance accessed 11 February 2020. See also Ducuing, 'Beyond the Data Flow Paradigm: Governing Data Requires to Look beyond Data' (n 51) 59.

[147] Kerber (n 16) s 4.2.1.

[148] The critique that the role of data intermediaries in facilitating and/or implementing the regulation of IoT data was raised by Picht (n 16). See also CiTiP White Paper on the Data Act proposal, CiTiP Working Paper Series, ed. Charlotte Ducuing and Thomas Margoni, 2022 (*forthcoming*).