Data property, data governance and Common European Data Spaces

Thomas Margoni,[*] Charlotte Ducuing,[**] Luca Schirru,[***] April 2023, v. 0.3

Abstract

The Data Act proposal of February 2022 constitutes a central element of a broader and ambitious initiative of the European Commission (EC) to regulate the data economy through the erection of a new general regulatory framework for data and digital markets. The resulting framework may be represented as a model of governance between a pure market-driven model and a fully regulated approach, thereby combining elements that traditionally belong to private law (e.g., property rights, contracts) and public law (e.g., regulatory authorities, limitation of contractual freedom). This article discusses the role of (intellectual) property rights as well as of other forms of rights allocation in data legislation with particular attention to the Data Act proposal. We argue that the proposed Data Act has the potential to play a key role in the way in which data, especially privately held data, may be accessed, used, and shared. Nevertheless, it is only by looking at the whole body of data (and data related) legislation that the broader plan for a data economy can be grasped in its entirety. Additionally, the Data Act proposal may also arguably reveal the elements for a transition from a property-based to a governance-based paradigm in the EU data strategy. Whereas elements of data governance abound, the stickiness of property rights and rhetoric seem however hard to overcome. The resulting regulatory framework, at least for now, is therefore an interesting but not always perfectly coordinated mix of both. Finally, this article suggests that the Data Act Proposal may have missed the chance to properly address the issue of data holders' power and related information asymmetries, as well as the need for coordination mechanisms.

[*] Corresponding author. Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven, Centre for IT & IP Law (CiTiP). Email: thomas.margoni@kuleuven.be.

[**] Co-author. Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; C2 interdisciplinary KU Leuven research project 'Datafication of the Circular Economy'.

[***] Co-author. Postdoctoral researcher at Centre for IT & IP Law (CiTiP), Faculty of Law and Criminology, University of Leuven (KU Leuven). His research is funded under the Skills4EOSC project. Skills4EOSC has received funding from the European Union's Horizon Europe research and innovation Programme under Grant Agreement No. 101058527.

1. Introduction

The Data Act proposal of February 2022 constitutes a central element of a broader and ambitious initiative of the European Commission (EC) to regulate the data economy.[1] As a matter of fact, the proposal can be seen as the most recent installment of a much broader plan. The other core elements completing this new regulatory landscape are the Data Governance Act (DGA[2]), the Open Data Directive (ODD[3]), and the Regulation on the Free Flow of Non-Personal Data (FFNPDR[4]), even though the latter two predate the European Data Strategy of 2020.[5] This body of laws has recently been referred to as EU data legislation or EU data law.[6] Moreover, there are additional and, at least to a certain degree, complementary legislative initiatives outside the field of data regulation properly understood that nevertheless intend to regulate data related fields, such as digital services (the Digital Services Act or DSA[7]), digital markets (Digital Markets Act or DMA[8]), Artificial Intelligence (AI Act[9]), the extraction of informational value from copyrighted works (Arts. 3&4 CSDM[10]), the processing of personal data (GDPR[11]), and most recently the liability for AI and IoT (AI Liability Directive[12] and Revised Product Liability Directive[13] proposals). Crucially, most these data and data-related legislation may be seen as the manifestation of a rising interest of the

[1] Commission, '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 ('Data Act proposal').

[2] 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) [2022], OJ L 152/1.

[3] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive) [2019], OJ L 172/56.

[4] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2019], OJ L 303/59.

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data (the European Data Strategy), COM/2020/66 final [2020].

[6] On the emergence of an EU 'data law', see T Streinz, 'The Evolution of European Data Law (Chapter 29)', in Paul Craig, and Gráinne de Búrca (eds), The Evolution of EU Law (3rd Edn, Oxford University Press, 2021).

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

[8] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1.

[9] Commission, 'Proposal from the European Commission for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act or AI Act) and amending certain union legislative acts' [2021], COM/2021/206 final.

[10] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Directive on Copyright in the Digital Single Market) [2019], OJ L 130.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016], OJ L 119/1.

[12] Proposal from the European Commission for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM(2022) 496 final, 28.9.2022 ('AI Liability Directive proposal').

[13] Proposal from the European Commission for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final, 28.9.2022 ('Revised product Liability Directive proposal').

EU legislator in a comprehensive regulation of digital and data-intensive markets, or in other words, in an EU Data Strategy.[14]

Accordingly, the EU legislator embarked in a rather ambitious enterprise dedicated to the erection of a new general regulatory framework for data and digital markets. On the one hand, this framework attempts to regulate certain players with an established market dominance (such as in the case of VLOPs and Gate Keepers[15]), while, on the other hand, it arguably attempts to create the conditions for an alternative EU based entrepreneurial ecosystem to blossom.[16] The EU lawmaker appears to have centered this figurative construction around a set of "EU core values" which include a competitive and functioning single market as well as fairness, proportionality, accountability, and transparency, all elements that can be clearly identified in the cited legislation.[17] The centrality of EU core values denotes another important characteristic of EU data and digital legislation: it explicitly embodies in the regulatory structure designed for data markets some of the key Charter's fundamental rights, including personal data protection and the privacy of communications, intellectual property rights, consumer protection, the right to use and dispose of lawfully acquired possessions, freedom to conduct a business and freedom of contract.[18] The resulting framework may be represented as a model of governance between a pure market-driven model and a fully regulated approach, thereby combining elements that traditionally belong to private law (e.g., property rights, contracts) and public law (e.g., regulatory authorities, limitation of contractual freedom) domains. The ultimate objective may very well be the creation of the market conditions for EU digital and data "champions", embedding and further promoting European core values, to thrive and compete with – usually non-EU – platforms and digital service providers.

Within this broader and ambitious context, the remainder of this article will discuss the role of (intellectual) property rights as well as of other forms of rights allocation in data legislation with particular attention to the Data Act proposal. This should prove particularly interesting given the relevance of IP and data rights in relation to one of the main mechanisms envisioned by the EU to achieve the stated policy objectives: the establishment of a single European market for data, or in the wording of the EC, of Common European Data Spaces (CEDS). At the time of writing, the Data Act proposal has not been adopted yet. The main text that has been used for this analysis is the EC proposal of February 2022. During

[14] This comprehensive approach can be identified not only in the *travaux préparatoires*, but also rather explicitly in the relevant EC policy documents. See, e.g., the European Data Strategy (n 5). See C Ducuing, T Margoni, L Schirru, D Spajic, T Lalova-Spinks, L Stähler, E Bayamlıoğlu, A Pétel, J Chu, B Peeters, A Christofi, J Baloup, M Avramidou, A Benmayor, T Gils, E Kun, E De Noyette, and E Biasin. 2022. White Paper on the Data Act Proposal. CiTiP Working Paper Series 11-12, <https://www.law.kuleuven.be/citip/en/news/item/old/white-paper-data-act> .

[15] See ex pluris, Quintais, João Pedro and Schwemer, Sebastian Felix, The Interplay between the Digital Services Act and Sector Regulation: How Special is Copyright? European Journal of Risk Regulation (2022), 13, 191–217.

[16] See, eg, the European Data Strategy (n 5).

[17] Illustratively, the Data Act proposal (n 1), in its art 8(1) on the 'conditions under which data holders make data available to data recipients' provides that: 'Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV'.

[18] See, eg, the Data Act explanatory memorandum, specifically the section on 'Fundamental Rights'. Data Act proposal (n 1).

the review process of this article (March 2023), the EU Council[19] and the European Parliament[20] have published their own texts with a view to complete the trialogue process indicatively during the Spring of 2023. While mainly focusing our analysis on the EC proposal, we endeavor to consider the most significant changes that may be introduced by the newly published texts. Readers should be warned however that there is necessary an aleatory element in discussing not yet adopted texts.

2. From data property to data governance via data portability. And back?

The way chosen to achieve a fair and efficient European market for data able to create value, while fostering innovation and reducing situations of data dominance, has remarkably not been a property-based approach. This was notwithstanding initial demands in the opposite direction.[21] In other words, the proposition to create *ex novo*, or to extend existing (intellectual-) property rights to data appears, at least from a formalistic perspective,[22] to have been rejected in EU data legislation.[23] This can be clearly seen for instance in Art. 35 Data Act proposal, but a similar property-skepticisms was arguably already present in "older" initiatives such as in the case of the ODD, both in relation to the general rule of reuse by default of Public Sector Bodies' (PSBs) documents, as well as in the specific cases of High-Value Datasets and research data.[24] This appears as a crucial element of discontinuity of the EU data strategy with past legislative initiatives such as the Database Directive. As a matter of fact, this change may be arguably interpreted as a rather explicit choice towards the abandonment of the traditional (intellectual) property arena as a regulatory device for data exchanges, in favor of a more granular data governance regime. Data governance, for present purposes, is broadly defined as a system of rights and responsibilities that determine who can take what actions with respect to data, with the focus being placed on the management of such rights and responsibilities.[25]

---

[19] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), 17 March 2023, 7413/23 ('compromise version of the Council').

[20] European Parliament, Amendments adopted on 14 March 2023 on the 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), P9_TA(2023)0069.

[21] As mentioned by Hungenholtz (2018, 1): "With the incessant growth of the 'data-driven economy' have come calls for the introduction of a novel property right in data. Apparently in response to demands from the automotive industry and encouraged by a number of German lawyers and scholars, the European Commission has in its 2017 Communication on 'Building a European data economy' tentatively advanced the idea of creating at EU level a 'data producer's right' that would protect industrial data against the world." PB Hugenholtz, 'Against "data property"' in H Ullrich, P Drahos, G Ghidini (eds), *Kritika: Essays on Intellectual Property* (Edward Elgar Publishing, 2018) <https://pure.uva.nl/ws/files/34981369/Data_property_Muenster.pdf>

[22] W Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version) (2022) GRUR International, 9.

[23] Hugenholtz (n 21).

[24] See, eg, Open Data Directive (n 3) arts 10, 13 and 14. European Commission, Directorate-General for Research and Innovation, Eechoud, M., Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2777/71619.

[25] see R Abraham, J Schneider, J vom Brocke, Data governance: A conceptual framework, structured review, and research agenda (2019) 49 International Journal of Information Management 424-426.

2.1. Art. 35 Data Act proposal: no to (some) data property

The EU has long been infatuated with the recognition of property or quasi-property rights in data. Illustrative is the (almost exclusively European) Sui Generis Database Right (SGDR) that, by protecting certain databases, indirectly offers a degree of property-based protection to the data therein contained.[26]

During the drafting phase of the Data Act, among the various options considered to incentivize the opening-up of privately held databases, an extension of the current SGDR to machine-generated data or the creation of a new property right in machine-generated data were taken into consideration, along with other non-property approaches (for example, a specific unfair competition remedy somehow similar to the one adopted in Japan).[27] The rejection of this proprietary approach – conceived as a market-based incentive to disclose and exchange data[28] – in favor of the creation of a set of access and portability rules, combined with provisions regulating B2B and B2G data exchanges, or in other words the adoption of a data governance strategy, can unquestionably be seen as a defining feature of the broader EU data policy.[29]

Art. 35 Data Act proposal is illustrative in this sense where it *clarifies* that the SGDR does not apply to IoT data. The approach of the legislator seems in line with the stated objective of clarifying the exclusion of IoT data, or perhaps more generally of machine generated data, from the SGDR. During the policy and scholarly debates leading to the Data Act proposal, evidence was presented to supporting the need to preserve a competitive environment and avoid monopolistic situations in information markets as well as the preservations of fundamental rights and therefore to counter the extension of proprietary claims to data. Arguments and evidence in the opposite direction have likewise been produced, but undoubtedly not to a degree sufficient to tilt the fundamental balance between property rules and the public interest in access to data.[30]

---

[26] PB Hugenholtz, 'Something Completely Different: Europe's Sui Generis Database Right' *in* S Frankel, D Gervais (eds) The Internet and the Emerging Importance of New Forms of Intellectual Property (Alphen aan den Rijn: Wolters Kluwer, 2016). E Derclaye, The legal protection of databases: a comparative analysis (Elgar, 2008). T Margoni & M Kretschmer, A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology (2022) 71(8) GRUR International, 689 <https://doi.org/10.1093/grurint/ikac054>.

[27] Tatsuhiro Ueno, 'Chapter 6: Big data in Japan: Copyright, trade secret and new regime in 2018' In Sharon K. Sandeen, Christoph Rademacher, and Ansgar Ohly (eds), Research Handbook on Information Law and Governance (Cheltenham, UK: Edward Elgar Publishing, 2021).

[28] J Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 257. H Zech, 'Data as a Tradeable Commodity – Implications for Contract Law' *in* J Drexl (ed), *Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition* (Edward Elgar 2017). A Wiebe, 'Protection of industrial data—a new property right for the digital economy' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil (GRUR Int) 877.

[29] Margoni & Kretschmer (n 26).

[30] See, eg, Ducuing and others (n 14). E Derclaye, M van Eechoud, M Husovec, M Senftleben, European Copyright Society, 'Opinion of the European Copyright Society on selected aspects of the proposed Data Act' (12 May 2022) < https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf> . J 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)' (2022) Max Planck Institute for Innovation and Competition Research Paper No. 22-05, 101. EDPB-EDPS. 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European

Accordingly, the proposition expressed in Art. 35 may be seen as a pro-competitive, pro-innovation, and pro-information markets rule. More specifically, the wording of the provision suitably focuses on the need to *clarify* the law in this area and not to change it, given the political, technical, and legal hurdles connected to the amendment or repeal of (intellectual) property rights.[31] Probably, an area where the current formulation could be further improved is the avoidance *tout court* of the slippery creation v obtaining dichotomy as a condition for SGDR existence. In other words, instead of stating that data generated or *obtained* from IoT is not covered by the SGDR, Art. 35 could enjoy an even wider acceptance if it simply stated that IoT data are considered created data (or better, data where the substantial investment, if any, is in the creation phase) within the meaning of Art. 7 Database Directive. Given the ongoing scholar and judicial uncertainty around the creation-(now generation?)-obtaining dichotomy, particularly evanescent in the case of data recorded from the surrounding environment,[32] Art. 35 would simply clarify, in what could be seen as an act of authentic interpretation, that IoT data have simply never qualified for SGDR protection.[33]

Whether simple sensors are included in the definition of IoT and thus also excluded from the SGDR is disputed.[34] In any case, beyond a plausible literal interpretation, it seems rather contradictory, to the point of absurdity, that such a revolutionary regulatory approach to IoT data excludes possibly the single largest source of the data (sensor data) thereby almost nullifying the useful effect of the norm.

Limiting proprietary claims over IoT data is certainly an important first step. Nevertheless, the question of how to reach and release the value contained in privately held databases is not thereby fully answered. In particular, it should be noted how data holders can still exert an almost absolute power over data deriving from their factual and technological control over the devices generating them. It could effectively be argued that this situation – while not formally qualifying as *property* from a legal point of view – often enables data holders to behave *as if* they were vested with such an entitlement. The solution adopted for public sector data is noteworthy, however, its extension to privately held data is not without hindrances. In fact, whereas the Open Data Directive (ODD) enacts a set of rules on the reusability of High-Value Datasets, of research data, and of documents held by Public Sector Bodies (PSBs), and whereas the DGA attempts to facilitate the voluntary sharing of data by individuals and businesses and harmonises conditions for the use of certain public sector data,[35] a similar approach would have been arguably difficult

---

Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 20 (2022). W Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version) (2022) GRUR International, 9. M Leistner and L Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (European Union, 2022) < https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266>.

[31] Various initiatives have been taken into consideration by the EC in relation to the SGDR, including its reform, repeal or abolition. These initiatives were supported by the two studies commissioned by the EC which in different ways have failed to identify a clear case for the maintenance of the SGDR. However, as it has been effectively pointed out, repealing legislation creating proprietary rights is not exempts from hardship; see generally Husovec, Martin, The Fundamental Right to Property and the Protection of Investment: How Difficult Is It to Repeal New Intellectual Property Rights? (May 21, 2019), in Christophe Geiger (eds), Research Handbook on Intellectual Property and Investment Law (Edward Elgar 2019).

[32] Derclaye (n 26).

[33] Ducuing and others (n 14).

[34] Drexl and others (n 30). Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector' (2022) Discussion Paper 2022–13.

[35] DGA, respectively Chapters III and IV and Chapter II.

to implement as a generalized solution for privately held databases. It would have necessarily taken the form of some sort of positive obligation to make available privately held data, with the potential to encroach upon property (including intellectual property), competition principles, and other fundamental rights such as the freedom to conduct a business. Additionally, an apprehension was voiced that such an approach could have resulted in distancing private actors from a too heavily regulated EU data market.

2.2. Regulating data markets: data portability and data spaces

The road chosen by the EU to reach privately held data seemingly takes the name of Common European Data Spaces (CEDS). In other words, the creation of a smi-regulated landscape for data featuring elements of interoperability, portability, trust, efficiency, and fairness should offer the incentives that private actors need to exchange data for economic and societal benefit.[36] This framework will ostensibly form the template for what has been termed the European single market for data. The policy objectives that the EC aims to achieve by fostering data sharing and re-use include economic growth, technological innovation, support for policymaking, and the preservation of European values such as the already mentioned privacy, property, competition, consumer protection and pluralisms. Whereas a specific definition of CEDS is not present in data legislation, and possibly rightly so given the fluidity of the concept at such an early stage, data portability, in its various manifestations, appears as a central tenet of data spaces.[37]

The data portability principle as applied to cloud and edge providers (Art. 29 Data Act proposal) is an interesting first manifestation of the broader general principle. It also reveals how some of the objectives expressed in the Data Act proposal can be traced back to older EU legislation (i.e., FFNPDR) confirming a vision of stable and expectable principles of the EU *acquis*. It is likewise noteworthy that this older EU legislation originally formulated the principle of data portability as a set of soft regulatory interventions, a sort of general normative goal that would have needed to be voluntary adopted by cloud providers. Given the failure of this self- or co-regulatory approach to deliver the expected policy objectives, the EU legislator appears to have intervened, in the Data Act proposal, with stronger and mandatory provisions to address issues such as vendor lock-in.[38] However, more generally, this also illustrates how the portability of data – which since its original delimitation to personal data in the GDPR appears to have developed into a general data portability principle – has become an accepted legal mechanism to deal with various instances of data-related 'market failures'. This is not only apparent in the case of cloud and

[36] While there is surprisingly enough – no definition of a 'data space' in the Data Act proposal, the Commission Staff Working Document on data spaces states that data spaces are designed to 'overcome legal and technical barriers to data sharing by combining the necessary tools and infrastructures and addressing issues of trust by way of common rules. A common European data space brings together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing', Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final, 2.

[37] Common European Data Spaces are based mainly on voluntary data sharing, however data legislation identifies a number of data sharing obligation.

[38] Commission, Commission Staff Working Document 'Impact Assessment Report' accompanying the document 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) SWD (2022) 34 final, Annex 9. See also Art. 1(4a) of the Council text.

edge computing as per Chapter VI,[39] but also in other situations, such as with IoT data (Chapter II Data Act proposal[40]), as well as with health data (Health Data Space Regulation proposal).[41]

2.3. Data rights, data portability and data access: IoT data and B2G obligations

Internet of Things (IoT) devices, i.e., common domestic or industrial devices such as fridges, toasters, cars, medical devices or industrial tractors, have become a paradigmatic example of the regulation of data. IoT products are physical devices with built-in components (e.g., sensors, software) which generate, obtain, collect, and communicate data about their performance, use and environment often to their manufacturer (see Rec. 14 Data Act proposal). IoT data may notably improve the devices' operation to the benefit of the user or be further aggregated and processed by the manufacturer to gain insights on users' activities and, hence, optimize products and services' offering. In the literature, questions about whom amongst the various actors involved in the generation of data, in particular the user of the device or its manufacturer, should be entitled to exert control over the data have been long debated.[42]

Although generated by the interactions of several stakeholders, data stemming from IoT products are often appropriated by IoT product manufacturers or providers of related services, given their material power to determine the hardware and software functions of the product. As noted above, manufacturer and service providers often reserve (contractually or technologically) the exclusive access to, and use of, such data to the detriment of users, whether consumers or businesses, but also of competitors in aftermarkets and consequently negatively affecting competition and innovation.

The Data Act proposal grants *access rights* to the users as 'co-generators' of data. It further establishes the rules and obligations for the three categories of actors at stake, namely the data holder, the users and the 'third party' that the users can entrust with their data. Beyond access rights, the proposal also regulates the use of data by the parties in this trilateral relationship (see below Fig. 1) and attempts to find an understandably delicate ridgeline between the empowerment of users (through the affordance of specific access and use rights), the protection of data holders' investments (through the protection of trade secrets and other intellectual property rights) and the promotion of competition (through the transferability of data to third parties and the possibility of third parties to develop aftermarket products or services).

---

[39] See C Ducuing, 'Chapter VI of the Data Act – The 'right to switching' *in* Ducuing and others (n 14).

[40] See C Ducuing, 'Chapter II of the Data Act – Data Control of users' *in* Ducuing and others (n 14). D Spajic and T Lalova-Spinks, 'The broadening of the right to data portability for IoT products: Who does the Act *actually* empower?' *in* Ducuing and others (n 14).

[41] See D Spajic and T Lalova-Spinks, 'The broadening of the right to data portability for IoT products: Who does the Act *actually* empower?' *in* Ducuing and others (n 14). Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM/2022/197 final (EHDS proposal).

[42] N Cohen and C Wendehorst, American Law Institute and European Law Institute, ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights. ELI Final Council Draft < https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf>

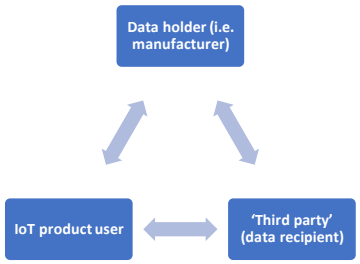

Figure 1 – Trilateral relationship

As habitual in EU secondary legislation, also in the case of data legislation, most of the provisions are "without prejudice" to certain rights, including personal data protection and intellectual property rights (with the explicit exception in the latter case of the SGDR).[43] With regards to Trade Secrets (TS) the situation appears more nuanced, given the specific attention that they receive in the Data Act proposal.[44]

It suffices here to observe that the relationship between TS and IoT data regulation in the Data Act is complex, especially in relation to the often too abstract distinction between raw data (frequently devoid of trade secrecy and the core of the Data Act provisions) and derived information (a much more familiar category for TS but excluded from the scope of these provisions). More generally, given the way in which TS operate and chiefly the fact that their subsistence is often a function of an *ex-post* judicial assessment, combined with the insertion of conditions of confidentiality (Art. 4(3)) or even strict necessity (Art. 5(8)) in the data portability rules, there seem to be a realistic possibility that data holders acquire a *de facto* position of, essentially, regulatory agents for the identification and protection of their own trade secrets, with the ensuing risk of trumping their own data sharing obligations.[45] As it will be argued below, this is an illustrative example of an area where a better integration of the Data Act proposal with the DGA could have produced interesting synergies. Both the Council and EP texts have proposed quite substantial amendments to data portability obligations, either suspending or allowing data holders to exceptionally refuse to share data which is identified, by the data holder, as TS.[46] In both cases there is a duty to notify the competent authority established at Art. 31, but only in the EP text there seem to be a clear indication that this authority will be effectively in a position to decide about the *prima facie* existence of a trade secret and thus, arguably, of the legitimacy of a refusal to share data by data holders.

Another pertinent argument to substantiate the claim hereby proposed of a transition from a data property to data governance model is the introduction, in the Data Act proposal, of the concept of 'exceptional need' under which Public Sector Bodies (PSBs) can request access to private sector data, albeit under clear and somehow strict conditions. On this basis, chapter V provides for a general and ambitious B2G data sharing legal framework, which, whereas certainly limited to situations of emergency (the preamble illustratively lists health emergencies, emergencies resulting from environmental degradation and major natural disasters including those aggravated by climate change, as well as human-induced major disasters, such as major cybersecurity[47]), introduces a specific obligation for data holders to share their data with the requesting PSB. The data obtained by the PSB seem to be subject to a limited disclosure obligation. On the one hand, in fact, there is no general requirement for the PSB to keep the data private, but a list of conditions, including obligations to respect the rights of individuals in case of

[43] See Data Act proposal (n 1) fn 20, rec 28.
[44] See for a more detailed analysis, Radauer, A, Bader, M, Aplin, T & Searle, N 2022, *Study on the legal protection of trade secrets in the context of the data economy: final report*. Publications Office of the European Union. https://doi.org/https://data.europa.eu/doi/10.2826/021443; Josef Drexl and others (n 30); M Leistner and L Antoine (n 30); E De Noyette & T Margoni, 'The Data Act and the 2016 Trade Secrets Directive' *in* Ducuing and others (n 14).
[45] See Josef Drexl and others (n 30). M Leistner and L Antoine (n 30). E De Noyette & T Margoni (n 44)
[46] See e.g., Art. 4(3) EP text and Art. 4(3a) Council text.
[47] See Data act proposal (n 1) rec 57.

personal data, necessity and confidentiality obligations in case of TS, a general obligation to destroy the data as soon as it is no longer necessary, as well as a prohibition for the PSB to use the data in a manner incompatible with the purpose for which they were requested (Art. 19 and Rec 65). On the other hand, the PSB are given specifically the right to share those data with individuals or organizations for scientific research or analytics in a way that is compatible with the purpose for which the data was requested (and subject to similar conditions, Art. 21). This provision will for instance enable the sharing of data by a governmental department (e.g., the Minister of Health) with a University for the purpose of scientific research provided that the use limitations established in the chapter, and in particular in Art. 21, are met.

The B2G obligations, albeit very limited in scope, represent a fundamental advancement in the recognition of the public utility of data, and sets proportionate – yet narrow – conditions under which this public utility takes precedence over the private interest. Unsurprisingly, these provisions have been further refined and in certain cases narrowed in the EP and Council texts, however, the overall mechanism seem to remain in place.

2.4 Other non-property based instance of data control: technology

When "data" is object of proprietary claims, usually via intellectual property rights, an authorization is needed for third parties to enjoy any of the reserved rights. The authorization can be contractual (e.g., a license), or statutory (exceptions and limitations). Control over data, however, can take other forms. Technological applications, such as Digital Rights Management (DRM) and Technological Protection Measures (TPMs), as well as contractual provisions have proven very effective in exerting control over data, sometimes proving even more effective in absence of any underlying proprietary claims.[48] At other times, license agreements and terms of use often rely on an underlying proprietary claim (e.g., copyright) to expand their effect to third-parties.[49] The use of TPMs and DRMs to control the access and use of protected content has been praised for their effectiveness, but also criticized due to their ability to prevent the enjoyment of certain exception and limitation as established in Art 6(4), ISD).[50]

Interestingly, technological empowered access- and use-control measures are also seen in the governance-based approach embraced by the proposed Data Act. In this case, rather sensibly, they seem to have been drafted to operate independently from any underlying copyright or related right. The Data Act proposal addresses the use of 'Technical protection measures' (TPMs) deployed by data holders, essentially by recognizing them so long as they don't interfere with the data rights provided to users and, as recently added by the version of the Council, "shall not be used as a means to discriminate between data recipients".[51] Whether legal rights and entitlements on the one hand, and TPMs on the other, are fully aligned remains uncertain. However, the general recognition of a power to technologically control access and use to (necessarily unowned) data is a relevant element that further substantiates the argument that the Data Act proposal, despite a formal rejection of property in data, may let slip through its threads an enduring proprietary rhetoric that may legitimize a *de facto* appropriation of data by data

[48] Case C-30/14 *Ryanair Ltd v PR Aviation BV* [2015] ECLI:EU:C:2015:10

[49] See T Margoni. The protection of sports events in the EU: Property, intellectual property, unfair competition and special forms of protection (2016) 47(4) IIC - International Review of Intellectual Property and Competition Law, 386 (discussing access rights in sports events and the use property and contracts to boost third-party effects).

[50] Margoni & Kretschmer (n 26).

[51] Data act proposal (n 1) art 11(1).

holders. This appropriation is enabled by the mentioned combination of physical control of the product, the recognized faculty to engineer technological locks, and the general dominance of data holders in their relationship with users and data recipients.[52] This view appears reinforced by the use of ambiguous expressions such as 'unauthorized access to the data', which the TPMs are designed to prevent. Given the general absence of underlying (IP)Rs in data, it is indeed unclear what 'authorization' implies, and in particular whether it could allow data holders to unduly expand the scope of their TPMs to prevent, essentially, access to data beyond mere contractual authorizations. The Council and EP texts do not clarify this point. Yet, it is noticeable that the compromise version of the Council is especially concerned with the relationship between data holders, users, and the data recipients, as can be seen not only from art 11 but also from the addition of the new Recital 50(a). Art. 11 seems to substantially reinforce the position of data holders employing TPM to regulate the use of *their* (!) data thanks to the addition of new obligations (prohibition to alter or remove TPMs), or remedies (compensation), in a way that is logically incompatible with the recognition of users' access and portability rights in *their* (?) data. The plausible conclusion that, particularly in the Council text, a property-based approach resurfaces disguised under the reassuring label of technological protection measures is only partially mitigated by the ending provision of new Art. 2a which could be read both as expanding its effects to third parties, or as limiting third party effects only to violations of art. 4(4).[53]

Finally, *Technical* Protections Measures under Article 11 of the Data Act may or may not overlap with *Technological* Protection Measures in EU Copyright *acquis*, either with the same scope or not, and either with the same right holders or not. More clarity in this area seems essential given the purported relevance of technological solutions in the realization of European Data Spaces.[54] In particular, for both the copyright *acquis* and for the Data Act proposal, it seems timely to add a clarification that the altering or removal of an illegitimate TPM, i.e., a TPM that unlawfully restricts users' rights, is not subject to penalizing provisions. Alternatively, if there is a desire not to incentives TPM tinkering, it should be clarified that the application of a similarly defined illegitimate TPM affords specific compensatory remedies to users who see their rights harmed. It seems incompatible with the EU constitutional order a provision that discriminates in terms of remedies and effective judicial restore between data holders' and data users' rights.

2.5 Data allocation through contract regulation

The Data Act proposal dedicates significant attention to contracts and, interestingly, to contract regulation, especially in cases of B2B data transactions. Due to the limited availability of (intellectual) property rights on data, contract regulation is leveraged by the proposal as a significant means to allocate data rights indirectly. We hereby discuss two examples of this instance.

First, the Data Act proposal takes the effective control of data by the data holder as 'the starting point',[55] which, according to Rec. 5, should in any event 'not be interpreted as recognizing or creating any legal

[52] On this, see Ducuing, "An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses" (2022) CiTiP Working Paper, 18–19.
[53] Art. 11(2a) last sentence: The same shall apply to any other party having received the data from user violating the obligation in Article 4(4)".
[54] For a more elaborate analysis of the TPMs in the Data Act proposal, see LS Stähler, 'Article 11 of the Data Act – The regulation of unauthorized 11 access to data' *in* Ducuing and others (n 14). Ducuing and others (n 14) 19.
[55] Data act proposal (n 1) rec 5.

basis for the data holder to hold [such] data, or as conferring any new right on the data holder to use data […]'. This statement seems of difficult reconciliation however not only with the legal recognition of TPMs (previous section) but also with the conditions that the data holder may agree with a data recipient to make data available pursuant to Chapter III. When compelled to make data available to a data recipient, either on the basis of Chapter II of the Data Act or on forthcoming (i.e., data space specific) legislation, the data holder may indeed levy a 'fair compensation'.[56] What is exactly covered by the fair compensation is however unclear, especially whether the compensation is connected to the value of the data themselves or is simply intended to cover the technical arrangements and costs necessary to make data available. This does not only represent an important conceptual distinction but may also be interpreted as an indirect legal endorsement of the *de facto* control of data by the data holder as well as, importantly, of the legitimacy of such *de facto* control.[57] The Council text notably clarifies that the compensation shall take into account the investments in data collection and production, and especially whether other parties contributed to the obtaining, generating or collecting the data in question, echoing again a property law rhetoric.[58]

Second, Chapter IV of the Data Act proposal regulates unfair terms related to data access and use between enterprises, namely between an enterprise and an SME. It is based on a threefold structure for establishing the unfairness of contractual terms: First, a 'black list' of terms irrefutably deemed unfair,[59] second, a 'grey list' of terms subject to a rebuttable presumption of unfairness,[60] and, third, a general definition of unfair terms.[61] Therein inspired by the Unfair Terms Directive regulating business-to-consumer contracts,[62] the Data Act refers to the principle of good faith in contracting as a yardstick, and provides that unfair terms shall be deemed non-binding on the beneficiary (i.e. the SME).[63] Striking differences can however be identified between the two legal frameworks. While the Unfair Terms Directive applies to any contractual term which has not been individually negotiated (boilerplate or terms and conditions),[64] the scope of Chapter IV of the Data Act applies only when the SME has attempted to influence the content of the contractual term in vain.[65] Besides, and in contrast to the Unfair Terms Directive which applies in principle to all business-to-consumer contracts irrespective of the contractual object,[66] Chapter IV of the Data Act applies solely to contractual terms having as object the access to and use of data as well as the related liability and remedies provisions and only to the benefit of SMEs.[67] Finally, a significant limitation to the reach of Chapter IV of the Data Act is the subjective reference to the

[56] Data Act proposal (n 1) arts 8-9.
[57] On this, see also Ducuing, "An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses" (n 52) sec 5.
[58] Compromise version of the Council (n 19) Art. 9(1a)(b).
[59] Data Act proposal (n 1) art 13(3).
[60] Data Act proposal (n 1) art 13(4).
[61] Data Act proposal (n 1) art 13(2).
[62] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29 ('Unfair Terms Directive').
[63] Data Act proposal (n 1) art 13(1).
[64] Unfair Terms Directive (n 62) art 3.
[65] Data Act proposal (n 1) Rec. 52.
[66] Unfair Terms Directive (n 62) art 1(1).
[67] Data Act proposal (n 1) art 13(1).

'gross[…] deviat[ion] from good commercial practice' as a constitutive element of the definition of an unfair contractual term.[68]

This being, a particularly interesting provision for the purpose of this paper is the presumption of unfairness of contractual terms that 'prevent the [SME] from using the data *contributed or generated by that party* during the period of the contract, or […] limit the use of such data to the extent that [the SME] is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner' (emphasis added).[69] This provision establishes that a party that has contributed to the coming into existence of data should enjoy what, from a property theory point of view, essentially could be seen as *usus* and *fructus* entitlements. In other words, the proposal, through the indirect regulatory lever of contractual fairness, appears to attain a situation of right allocation in data that mimics the effects of property rights. The compromise version of the Council reinforces the breadth of this data allocation rule by extending the benefit of Chapter IV to all enterprises (i.e. not only SMEs) onto which contractual terms are 'unilaterally imposed' by another enterprise.[70]

3) Conclusions

The analysis developed in the preceding sections attempts firstly to highlight the role of data legislation in the achievement of a set of well identified policy and regulatory objectives for a single market for data via the tool of Common European Data Spaces. Secondly, it shows both the often inadequate but enduring role of (intellectual) property rights in regulating data as well as the recent efforts by a new data governance paradigm to emerge. The proposed Data Act has the potential to play a key role in the way in which data, especially privately held data, may be accessed, used, and shared. Nevertheless, as we argued, it is only by looking at the whole body of data (and data related) legislation that the broader plan for a data economy can be grasped in its entirety. The transition from a property-based to a governance-based paradigm emerges as a key characteristic of the EU data strategy. However, we have identified instances, where the "stickiness" of property rights – if not in a strict legal sense, certainly in the form of legacy legal mechanism and rhetoric – is still present, especially in the Council text of the Data Act proposal. Other legislation, such as the DGA, which does not expressly regulate data property matters, may arguably possess the potential to develop clearer governance opportunities that are expected to naturally complement the Data Act. It is therefore surprising to notice how this last connection has often not been made explicit. In extreme synthesis, the DGA provides for a trust infrastructure on which actors can rely when exchanging data. In contrast, the Data Act consists mainly of obligations to make data available in different scenarios, often based on fairness considerations. Logically, there should be well delineated interfaces between these two complementary spheres. Yet, this complementary is often purely putative.

A major objective of data governance is precisely to support the reconciliation of conflicting interests between different data stakeholders.[71] Because data are often at the crossroads of multiple, concurrent, and possibly conflicting interests in a rather dynamic context, the added value of data governance, with

[68] Data Act proposal (n 1) art 13(2).
[69] Data Act proposal (n 1) art 13(4)(c).
[70] Compromise version of the Council (n 19) art 13(1).
[71] M Grafenstein, "Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as Well as the GDPR (2022) HIIG Discussion Paper Series No. 2022-02, 5

its inherent flexibility and ability to adjust to specific situations, has long been recognized in the literature as a means to carry out the required balancing exercise.[72]

An example of these coordination issues emerges, for example, in the necessity to reconciliate the data holders' interest in protecting their trade secrets (and in their power to determine *ex ante* what a trade secret is, see Sec 2.3. *supra*) and the legitimate interests of, respectively, the user and the chosen third party in accessing and using the data. In these situations, data holders indeed benefit from the cumulative advantages of factual control over the data and the ability to determine *ex ante* (i.e., prior to data sharing) trade secrecy, also thanks to the power asymmetries that often characterize these relationships. Accordingly, there is, once again, a risk that the data holder, by *de facto* acquiring a quasi-regulatory role, pre-empts the (usually judicial) determination of which data should be shared and how, in an arguable conflict of interest position.

In such a scenario, the facilitating and trust-bringing role of a neutral data intermediary, such as those regulated under the DGA, could theoretically be useful, if not necessary, to ensure that the Data Act delivers on its promise to allocate data fairly. Data intermediaries, as per the DGA, are providers of services that aim to establish commercial relationships for the purposes of data sharing between an indefinite number of data holders and users.[73] Data intermediaries are subjected to stringent rules, which aim to guarantee their independence and neutrality vis-à-vis the data, the data providers, and the data users, especially from players with a significant degree of market power.[74] The DGA even goes as far as noting that data intermediaries could support both voluntary data sharing but also 'facilitat[e] data sharing in the context of obligations set by Union […] law'.[75]

The Data Act proposal, and in particular IoT data provisions, appear to constitute a natural application of this preordained DGA scheme. It is therefore a remarkable omission that the connection to data intermediaries as per the DGA has not been formally established therein. It would seem a logical, yet necessary, provision that data holders, when making data available pursuant to their Data Act obligations, should be asked to choose a data intermediary, within the meaning of the DGA, which would operationalize the making available of data. Taking this crucial activity away from the data holder would help rebalance an otherwise asymmetric relationship, which is precisely the objective of the Data Act proposal. The extent to which the data intermediary would be involved, as well as the conditions under which they shall provide such services, remain to be further defined. Yet, by allocating to data intermediaries such tasks, the Data Act would not only address the issue of data holders' power and information asymmetries, but it would simultaneously contribute to solving the issue, voiced in the literature, that the stringent rules designed for data intermediaries may prevent a vibrant data

[72] Grafenstein n (71). MJ Madison, Tools for Data Governance (2020) 2020 Technology and Regulation 29, < https://scholarship.law.pitt.edu/fac_articles/394>. C Ducuing, 'Beyond the data flow paradigm: governing data requires to look beyond data' *In* Technology and Regulation (Vol. 2020, Issue Special Issue: Governing Data as a Ressource, pp. 57–64) <https://doi.org/10.26116/techreg.2020.006> . C Ducuing and RH Reich, 'Data governance: Digital product passports as a case study' *In* Competition and Regulation in Network Industries (Vol. 24, Issue 1, pp. 3–23). SAGE Publications.

[73] Data Governance Act (n 1) art 2(11).

[74] Data Governance Act (n 1) ch III.

[75] Data Governance Act (n 1) rec 27.

intermediaries' market from emerging.[76] Otherwise said, it would increase the alignment between the services provided by data intermediaries and the delivering of public value through data sharing.

The compromise texts of the EP and the Council do not explore this option. Instead, and as a result of the increased protection for the trade secrets of data holders who may in exceptional circumstances refuse to share IoT data pursuant to Chapter II, the amended texts propose to call upon the supervisory authority as a neutral third party.[77] Whether the involvement of the supervisory authority can prevent data holders from abusing trade secret protection in such circumstances remains to be further evaluated.

[76] See L von Ditfurth & G Lienemann. The Data Governance Act: – Promoting or Restricting Data Intermediaries? (2022) 23 (4) Competition and Regulation in Network Industries, 270-295.
[77] Compromise version of the Council (n 19) art 4(3a), art 5(8a).