Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Data : from "property" towards "commons"

Poullet, Yves

Published in:
Liber amicorum Serge Gutwirth

Publication date:
2024

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2024, Data : from "property" towards "commons". dans *Liber amicorum Serge Gutwirth.* VUB Press, Bruxelles, pp. 103-127.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 15. Jul. 2026

Data: from "property" towards "commons"

Yves Poullet[*]

I am honoured to participate, together with all his other friends, in the redaction of this book offered to Serge Gutwirth at the moment of his retirement. Serge and I have shared so many nice moments around one (and often more than one) beer, notably but not only to exchange common or contrasted reflections on privacy issues or on the still-increasing protection of intellectual property (IP); we have together created the CPDP as it is today which knows a marvelous success. This article below aims to go forth with our thriving discussions, and especially with the article that Serge and Gloria have redacted in my own *liber amicorum*. In this regard, dear Serge, I quote your conclusion: "*le droit de propriété et l'information (ou des données) semblent tout simplement juridiquement incompatibles : si on veut tout simplement faire du droit, c'est impossible*"[1]. I totally share this point of view, and this modest contribution intends to enlarge the debate.

Hence, the first part of this contribution consists in analyzing how the 'Property' approach is defended by both the protagonists of the intellectual property field, and the data protection advocates. This first part also intends to show how this approach is leading to contradictory outcomes, that are incompatible with the societal and economic needs, and their imperatives in favor of data sharing. Then, the second part of the contribution uses an example of data collected through a connected object (*in casu*, a smart fridge), to illustrate how the Internet of Things creates data that can be used for different purposes and by numerous actors. Finally, the third part of this contribution intends to show how the Data Act, presently in discussion between the EU authorities,[2]

---

* Honorary Rector of the University of Namur, member of NADI and of the Belgian Royal Academy. Thanks to Michael Lognoul for his quite useful and patient proofreading of the article. This article was submitted in February 2023 and has not been updated since this date..

1 Serge Gutwirth, Gloria González Fuster, 'L'éternel retour de la propriété des données: De l'insistance d'un mot d'ordre' in Cecile de Terwangne, Elise Degrave, Séverine Dusollier & Robert Queck (eds), *Laws, norms and freedoms in cyberspace*, *Liber Amicorum* Yves Poullet, (Larcier, 2019, pp. 117-141)..

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), Brussels 23 February 2022, COM(2022)68

considers the legal nature of data as giving birth to a kind of "bundle of rights", according to the concept of commons developed by Ostrom's doctrine[3], which is very dear to my friend Serge[4]. The argument made by the present contribution is that the Data Act Proposal might indeed be perceived as an illustration of the notion of commons, which serves the development of innovation, while remaining respectful of the legitimate interests of the different actors at stake, and of their equilibrium.

I. From the 'proprietary' approach to its questioning by recent EU regulatory texts[5]

The 'proprietary' approach

As mentioned in the introduction, the 'proprietary' approach towards data has been developed by certain privacy advocates, to offer a better protection to data subjects and to their liberties. According to these authors, the so-called data subject, under the General Data Protection Regulation (GDPR)[6] vocabulary, would be the owner of his (or her) personal data. More precisely, the relationships between the data subject and data would have to be considered as a "property" right or as a right similar to IP, meaning that it would include the right to limit the use of personal data by third parties, and even to forbid it. In this context, the consent (and the correlative right to withdraw consent) might be viewed as

final. The European Parliament Internal Market and Consumer Protection (IMCO) committee adopted its opinion report on the draft Data Act on 24 January 2023.

3 See notably, Elinor Ostrom. 'Private and common property rights' in B. Bouckaert & G. De Geest (eds), *Encyclopedia of law and economics*, (Edward Elgar, 2000, p. 343)

4 Serge Gutwirth & Isabelle Stengers, « Le droit à l'épreuve de la résurgence des commons" (2016) *Revue Juridique de l'environnement*, 306-343. Also from Gutwirth, see: "Les communs: avec, malgré ou contre le droit?" (2022), 69132022/33, *Journal des tribunaux,* 33. It should be noted that the *Journal des tribunaux* devoted a whole special edition to the commons phenomenon, which highlights the relevance and interest of this concept nowadays.

5 We do not develop here the arguments in favour or in disfavour of the proprietary approach. The reader might see more developments in Yves Poullet, 'La propriété des données – Balade au "pays des merveilles à l'heure *Big data'*, in *Mélanges en l'honneur de Michel Vivant* (pp 339-356).(Lexis-Nexis 2020).

6 Regulation 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), *OJ*. L. 119, 4/4/2016.

the right of the data subject to decide who is authorised to use their data.[7] The recent right established by the GDPR to require the portability of personal data is considered by these authors as supplementary evidence of the property of data subjects regarding their personal data. As Purtova has explained:

> Propertisation of personal data will respond to the individual preferences for Privacy as the individual has a chance to decide for himself to disclose data and benefit from it or to pay a higher price for e.g., mortgage in a more sensitive way than the current system does.[8]

Regarding now the collection of data and the exploitation of databases, the EU Directive on databases[9] created a *sui generis* right that benefits their makers by protecting the corresponding substantial investments made by these actors. Furthermore, the directive provides for the validity of technical and (to some extent) contractual means used by database-makers in order to protect their investments. Therefore, regarding databases and the individual elements that they contain, one might highlight that their "appropriation" can be eased by several protection schemes. This includes the protection offered by copyright and allied rights legislation (such as the *sui generis* right), but also by the contractual provisions imposed on users, or even the protections established through technical means, beyond the frontiers of the protection strictly offered by IP legislation. Therefore, contractual provisions might forbid or sanction any failure to comply with the limits placed on the use of protected works, while technical means (e.g., anticopying devices, watermarking technologies or digital rights management systems) are preventing "illicit" (or undesired) uses of protected works. On top of that, the circumvention of such technical protection measures is prohibited by the directive on copyright.[10] As demonstrated

---

7 On that aspect, among other authors, see Gutwirth & Fuster (n 1) pp. 136ff, which is denying any analysis of the consent as argument in favour of the property approach and, in the same sense, our articles on the same topic.

8 Nadezha Purtova, Nadezhda, '*Property rights in personal data European perspective*' (Doctoral dissertation, University of Tilburg), Box Press.. In the same sense, notably: Corien Priens,, 'Property and privacy – European perspectives and the commodification of our identity', in L Guilbault & P. B Hugenholtz (eds), *The future of public domain*, (pp. 223-257) (Kluwer, 2006). For the rejection of the proprietary approach, see notably: Yann Padova,, 'Entre patrimonialité et injonction au partage', (2019) 155(1) & 156(2), *Lamy Droit de l'Immatériel* ; Thomas Hoeren , 'A new approach to data property?'(2019) *AMI*, 58 et 59

9 Directive 96/9 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ. L. 77, 27 March 1996.

10 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on of certain aspects of copyright and related rights in the information society, *OJ. L.*

by Strowel,[11] rightsholders might jointly use three methods to reinforce the appropriation of works – and, in this way, of "data": IP legislation, technical protection devices or measures and contractual provisions.

Questioning of the "proprietary" approach

I am definitely not subscribing to that proprietary approach, for several reasons. In particular, regarding protected works and databases, it should be stressed that their appropriation through multiple ways (as described above) might go beyond the bounds of the protection strictly afforded by the intellectual property legislation. For instance, technical measures might hinder access to the content of a non-protected work or the use of a non-original piece of a generally original work. Such measures might also restrict access to and the use of a work by its legitimate users: for instance, in the case of a quotation or use for pedagogical purposes. Yet, on that point, it must be highlighted that the EU legislator has recently introduced a "correcting" principle in the Copyright in the Digital Single Market Directive.[12] In order to ensure a fair balance between rightsholders and legitimate users and to guarantee access to protected works for the latter, the directive clarifies that rightsholders should ensure "that the use of technological measures does not prevent the enjoyment of the exceptions and limitations" to copyright.[13] Furthermore, certain new exceptions to copyright

---

167, 22 June 2001, p. 10. See, particularly, the recitals 47 and 48: "(47) Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorized by the rightholders of any copyright, rights related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

(48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorized by the rightholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development …."

11 Alain Strowel, 'Les communs numériques modelés par les outils du droit privé'. (2022) 6913 *Journal des tribunaux*, 627.

12 Directive 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, *OJ* L 130, 17/5/2019.

13 Directive 2019/790, Recital 7. The entire recital reads: "The protection of technological measures established in Directive 2001 remains essential to ensure the protection and the effective exercise of the rights granted to authors and to other rightsholders

have been enacted, notably for research institutions, regarding data-mining.[14] In similar fashion, the European Court of Justice (ECJ) has recently decided that the *sui generis* right to a database could be used only in cases where there is a threat to the likelihood of amortisation of the investment that triggers the protection.[15] Finally, the Data Act Proposal, in its section 35, seeks to introduce a new limitation regarding the legal protection of databases:

> In order not to impede the exercise of the right of users to access and use data in accordance with Article 4 of this Regulation or the right to share such data with third parties in accordance with Article 5 of this Regulation, the *sui generis* right provided for in Article 7 of Directive 96/9/EC shall not apply to databases containing data obtained or generated through the use of a linked product or service.

All these advances are clearly denying the "absolute" character of IP (and allied rights) and point to the need to take other interests into account.

Regarding the assimilation of data protection to a type of property right, at least three main arguments against this approach should be stated precisely.[16] First, one might ask questions such as: "How to justify a property on data built outside of me, or even without me, and often unknown or incomprehensible to me, like certain medical analysis? Who is the author of these data?" Secondly, the extensive use of consent as a legal basis for processing personal data is counter-productive in respect of the protection of our liberties. This legitimises a "market" of personal data, characterised by an informational dissymmetry and libertarian capitalism, which increases the risk of discriminations and abuses, in particular due to the vulnerability of certain populations. Thirdly, this approach leaves aside the fact that data protection is only a mean, a tool, and not an end

---

under Union law. Such protection should be maintained while ensuring that the use of technological measures does not prevent the enjoyment of the exceptions and limitations provided for in this Directive. Rightsholders should have the opportunity to ensure that through voluntary measures. They should remain free to choose the appropriate means of enabling the beneficiaries of the exceptions and limitations provided for in this Directive to benefit from them. In the absence of voluntary measures, Member States should take appropriate measures in accordance with the first subparagraph of Article 6(4) of Directive 2001/29/EC, including where works and other subject matter are made available to the public through on-demand services."

14 Directive 2019/790, article 3.

15 ECJ, 3 June 2021, *CV-Online Latvia SIA vs. Melons SIA*, C-672/19.

16 For more developments on this topic, see Yves Poullet, ',La « propriété » des données – Balade au « pays des merveilles » à l'heure du Big Data.' in *Mélanges en l'honneur de Michel Vivant* (pp. 339-356).(Lexis-Nexis 2020), and the authors quoted there.

in itself. In other words, the purpose of Acts such as the GDPR is to protect individuals' privacy – considered as the free development of each individual in a given society – in order to ensure their free and original expression, which is a necessary condition of a democratic society. Hence, data protection requires there to be a balance between different liberties and a need to consider, to a certain extent, the general interests of society.

Beyond these intrinsic defaults of the "property" approach in both fields (i.e., IP and data protection), the approach ought to emphasise that the concurrent application of these two approaches would lead to contradictions which might be prejudicial to the interests of all parties. For instance, the exercise of IP rights by the collector of personal data might limit the opportunities for third parties to benefit from the data collected in accordance with the legal protection of databases. In the same vein, the use of IP rights by the collector of personal data could to some extent prevent data subjects from accessing information regarding the "logic" behind the algorithmic processes and uses of their data. Conversely, the data subjects might oppose the lack (or withdrawal) of consent from the data collector to refuse (or stop) the use of their data. Therefore, it is important to harmonise the different interests at stake in the exploitation of data, in particular when it is collected autonomously by devices such as those developed in the context of the Internet of Things. But the two proprietary approaches discussed above cannot be reconciled when they are applied to data collected in a digital environment as they are going in contradictory directions: one is in favour of the data subject and the other benefits the collector of data. This observation highlights the need to find a balance between the two types of right; or, better still, to find an approach to these rights in which each considers the other. This equilibrium is all the more necessary due to the fact that developing the data market is in itself a necessity, which makes the data-sharing between actors present in data markets particularly important. That is the main aim of the Data Act, as I demonstrate later in this contribution, based on the second part of this article – which intends to illustrate, using the example of a smart fridge, the eco-system of data in the context of the Internet of Things, and to analyse the position of the different actors concerned with such data.

II. Eco-system of data: example of a smart fridge

From data to their usages

To discuss the eco-system of data, I propose the following use case: someone purchases the latest version of a smart fridge, sold by company A. Naturally, this smart fridge includes an operating system and the offering of (smart) services for this fridge requires the data that are collected through its use to be managed and exploited. Multiple scenarios might be imagined on this basis, implying different actors in each case. For instance, company A might perform all the tasks described, such as manufacturing and selling the product, developing the software, and managing the services associated with the fridge through data exploitation. Another contrary scenario would be that while undertaking A manufactures and sells the fridge, undertaking B develops its software, while undertaking C offers the services related to the exploitation of data collected by the fridge, based on appropriate contractual terms. A third scenario could be that while undertaking A manufactures and sells the fridge, undertaking B takes care of developing the software and managing the smart services based on data exploitation. In the result, the exploitation of the data collected by the fridge might be carried out by undertaking A, B or C. Furthermore, these three companies might either be subsidiaries or not. If this use case is analysed by using the legal categories proposed by the Data Act Proposal, the following developments could pertain.

The intelligent fridge is a "product", as defined by the article 2(2) of the Proposal:

> "product" means 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.

Regarding the software managing the functioning of the intelligent fridge, this element would qualify as a "related service" under article 2(3) of the Proposal:

> "related service" means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions.

Finally, turning to the notion of "data-holder", article 2(6) of the Data Act defines this concept as follows:

> "data holder" means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data.

In the above use case, and based on the three scenarios considered, the undertakings A, B and C could in turn qualify.

As regards, more precisely, the data that could be collected through the use of a smart fridge, one might consider the following elements: a camera records images of the content of the fridge systematically and regularly; a system of automated recognition determines the nature and potentially the brand of the food (or pharmaceuticals) placed in the fridge (e.g., using tags on the products and/or automated analysis of the images from the camera). Turning back to the legal categories proposed by the Data Act Proposal, these features of the smart fridge might qualify as a "virtual assistant". This concept is defined by article 2(4) as follows:

> "virtual assistants" means software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices.

As a complementary remark, it should be noted that the user of the smart fridge might be either a natural or a legal person. For instance, this could be the case if a company offers the use of a smart fridge to its employees. In this regard, article 2(5) of the Data Act Proposal defines the notion of "user" as follows: "user" means a natural or legal person that owns, rents or leases a product or receives a service.

All the types of data discussed so far might be stored for some time if the final user wants to monitor the evolution of their consumption of the items contained in the smart fridge (e.g., to determine whether the weekly consumption of milk increases or is even). Furthermore, certain data about the functioning of the fridge might be kept automatically. For instance, this could be the case with the electricity consumption of the fridge, alongside the temperature inside and outside the fridge, to determine the optimal cooling intensity according to the

temperature of the room where the fridge is installed. Logs regarding remote access to and the use of "related services" offered with the fridge through a mobile app and a communication network, or the geo-location of the persons accessing it (and the precise moment of this access), might also be kept automatically by the fridge operating system.

On top of the operations of data collection and retention described above, one might also consider the processes of data related to the automated ordering of products. This type of ordering might be operated either by the fridge itself (e.g., by checking the imminent lack of certain products based on its programming by the purchaser of the fridge) or by a human intervention (e.g., through an order placed on the fridge's mobile app). In both cases, the orders are automatically transferred to a supermarket, which will pack the goods ordered and provide delivery details to the user of the fridge. This type of operation obviously implies the recording of traces regarding the orders, such as "What was ordered? Which customer is behind the order? When and where did the delivery take place? What was the amount of the order?".

Such a scenario definitively is not pure fiction, as this kind of "use case" regarding the Internet of Things already appears, and much more of these will quickly be taken to market. Based on the above description of the personal data potentially exploited in relation to the use of a smart fridge, I now analyse its ecosystem and potential uses. However, I must at the outset note that several uses of such data could be based on pseudonymised or even anonymised data.

Ecosystem and its stakeholders

On the one hand, it is quite clear that a great deal of the data collected will be of interest to the final user of the smart fridge. One might consider, from this perspective, the possibility of the user having a clear view of the contents of their fridge, the monitoring of electrical consumption and the corresponding environmental impact, and the related energy costs, the ease of ordering products and the control on the related expenses, etc. From this perspective, the possibility offered to final users of having a unique grocery supplier for most of the products automatically ordered by the smart fridge might be of interest, since it will be possible to negotiate discounts or other advantages with that supplier. On the other hand, all or part of the complementary services that make the fridge "smart" might be presented by the fridge supplier (or by any other service-provider) as separate services. In this case, all the additional services would probably have to be paid for in addition to the primary purchase of the fridge at a price that includes only the basic functionalities of a "regular" fridge. In this hypothesis, according to the terminology adopted by article 2(7) of the

Data Act Proposal, the provider of the additional services might be considered a "data recipient":

> "data recipient" means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law.

The final user might also be a company, as shown above in the example of the company offering an opportunity for its employees to use smart fridges. In this case, the company might operate a certain surveillance of its employees through their use of their key access to the fridge (the products entered, the time of use of the fridge, the persons meeting around the fridge). It is quite clear that the employees have to be considered, in this context, as data subjects and must be protected under GDPR provisions. Their consent to see their data processed will not be considered as a valid legal basis because between employees and employer, consent is not considered as free, and it is not obvious that the "necessity of the contractual relationships" would legitimate that processing.

Regarding the stakeholders involved in the value chain of a smart fridge who might qualify as data recipients, numerous actors may obviously fall into this category. For instance, where the flow of data originating from the smart fridge is collected and processed by its supplier, the supplier will have to communicate (part of) this data to the supplier of the service that consists of the automatic ordering (and payment) of products that are missing in the fridge. Similarly, the supermarket that will take care of packaging the order, editing bills and delivering the products ordered will act as a data recipient that needs to interact with the upstream actors in the value chain. Incidentally, I note that the supermarket might also have an interest in using the dataflows and contractual relationships between the actors of the value chain to send advertisements to the final user of the smart fridge regarding specific products, based on their knowledge of the final user's consumption habits.

Turning back to the potential uses of the data by its collector, it is quite clear that the gathering of such diverse and abundant data and its potential aggregation with data from similar or related services create an opportunity to define the individual and/or collective profiles of the final users. For example, data collection and aggregation might lead to identifying any evolution in users' consumptions and tastes and the appearance or evolution of a medical situation such as an allergy to lactose or to seafood. Similarly, access to data regarding

food habits may lead to deductions about a final user's religion, membership of a specific ethnic group, etc. The socio-economic status of the final user (and its evolution through time) can also be easily deduced automatically by the fridge from the quality and price of the items ordered, as well as from the number of orders and their frequency. Furthermore, the evolution of the household can be deduced in the same way. Ultimately, data such as the location of the final user when they order via a mobile app, the moment when the user orders or even the frequency of the manual orders are all types of data that reveal the personal characteristics of the final user's identity and behaviour. Hence, it is quite clear that the collection of "trivial" data (as in the examples mentioned so far) has the potential to easily become "sensitive" data in the context of the services provided by the data collector or the data recipients – with all the attendant risks to individuals that come with the processing of their personal and sensitive data.

All such data, collected on a large scale, also give information to the supplier of the smart fridge (and potentially to all other service-providers) about the dynamics of the market and the relative power of its actors. For instance, the evolution of the market shares could be deduced from information consisting of the number of consumers placing orders in one supermarket or another; or ordering one specific product or another. In addition, the evolution of the market could also be foreseen, to some extent, through final user profiling, notably based on a similarity assessment between consumers, on the potential evolution of their tastes or on their responsiveness to targeted advertising. The use of these types of information is obviously important for the companies that can access and analyse them. Furthermore, in the hypothesis where these types of information would be communicated to rating agencies (in charge of the evaluation of the creditworthiness of market actors), the consequences could be severe. For example, such data processes might lead to accelerated bankruptcy or at least to a loss of confidence by the creditors of market actors.

Of course, to have the ability to infer all (or part of) the knowledge about final users or market players discussed above, both huge amounts of data and powerful data-processing technologies – such as machine learning – are needed. Regarding the provision of data-processing technologies and computing power, article 2(12) of the Data Act Proposal defines precisely the notion of "data processing service" as

> a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralized, distributed or highly distributed nature.

In the light of this definition, another actor in the ecosystem should be pointed to: cloud service-providers. Indeed, cloud services might be of interest for storing the collected data and making it available to its users or to any other actors who are authorised to access it.

Finally, I need to highlight the role of one last type of actor: public authorities. Public-sector bodies, in the case of public emergencies,[17] might benefit from the data collected and stored to deal with these emergencies. For instance, in the case where certain edible goods or pharmaceutical drugs would be subject to withdrawal from the market, public-sector bodies might send an alert to the users who have such problematic products in their intelligent fridges, or require the data-holders to do so.

To summarise, I wish to underline the following elements:

- Even if certain companies would undoubtedly prefer to develop and offer, on their own, all of the potential services related to the products that they manufacture (i.e., vertical integration) as regards the Internet of Things, in most cases there would still be room for numerous actors to be involved in the ecosystems at stake and interactions between them would be necessary.
- The protections arising from IP could make this interaction difficult (or costly) for certain actors. On the one hand, the primary data-holder might consider that the data collected constitutes a database, protected (at least) by a *sui generis* right. Therefore, the data-holder might exclude all other actors from the benefits linked to the exploitation of data. On the other hand, it is quite easy for service-providers to invoke the incompatibility, or the proprietary nature, of their hardware and/or software systems to deny (or at least make it more difficult) final users the opportunity to switch to different service-providers (i.e., competitors). For instance, the supplier of the smart fridge software and associated services might exclude certain competing applications, arguing that they are not compatible with the operating system.
- The lack of technical and functional interoperability and the quasi-absence of standards in this sector create a high risk of making final users (and

17 These two concepts are defined by the Data Act as follows: "'public sector body' means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies" (article 2(9)) and "'public emergency' means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s)'. It is quite clear that the problem will be the inclination of the public authorities to extend the scope of these notions and to minimise the procedure for getting the proclamation of a state of emergency, as we discuss in Part III.

data recipients) prisoners of the product suppliers and the original service-providers. For instance, if the final user of a service consisting of the automatic ordering of food items seeks to switch to another service-provider, doing so might be difficult in the case where the original provider of the service refuses their competitor access to their platform (and therefore to the necessary data).

- The data collected by a smart fridge about its final users may seem trivial at first sight. But the variety and quantity of such data, together with the profiling capabilities offered by artificial intelligence (AI) technologies, imply that the data processes at stake will be quite sensitive to final users and companies. Even if natural persons are already protected by the GDPR, companies do not benefit from any similar protection, apart from competition law.
- Regarding the Internet of Things, the products and services offered are numerous and will keep on evolving, based on the needs and desires of final users and considering technical progress. Yet the complexity and opacity of the eco-systems surrounding such products and services are definitively problematic.

These elements demonstrate the absolute need for a regulatory framework that is able to manage the balance between the different actors discussed above in order to protect their respective legitimate interests but also to ensure the development of innovative services. This was precisely the main aim of the European Commission in its Data Act Proposal. The commission developed this proposal in response to the risks highlighted above, which were raised using data generated by the Internet of Things.

In the third part of this contribution, the concept of the "commons" is proposed as an explanation of the solution provided by the Data Act Proposal. This concept, launched by Ostrom[18] and since used by many other authors, might be useful to understanding the Data Act solution. This approach deviates from the model advocated by the proprietary approach proponents; it conceives of the legal nature of data as a "bundle of rights", as I explain below. Then I analyse the parallelism between this concept of commons and the framework sketched by the European Commission's Proposal.

18 Ostrom (n 3).

III.. About Data Act and commons

From commons …

As Isabelle Stengers and Serge wrote:

> C'est en 1990 qu'Elinor Ostrom publie son désormais célèbre: 'Governing the Commons'.[19] … Le titre même est un démenti au modèle du propriétaire de Hardin.[20] Les commons, contrairement à son pré, ne définissaient pas la ressource commune comme d' « accès libre » ni les commoners, comme un ensemble d'individus répondant à la norme idéale de l'homo oeconomicus, chacun animé par le souci exclusif de tirer le maximum de ce à quoi il a accès. La gouvernance, en effet, implique une « entente » et un souci partagé – ne pas détruire la ressource dont chacun dépend.[21] Il n'y a pas de « dilemme du prisonnier », qui vaille, les commoners agissent ensemble, organisent et produisent du droit vernaculaire qui exprime cette entente de façon contraignante.[22]

Definitively, Serge and Isabelle's approach considers the commons as a "bottom-up" alliance of individuals, driven by an altruistic will (or at least by a collective interest). In their view, these individuals self-regulate and define themselves the governance needed to achieve a common goal, considering their different interests. In my opinion, the original approach proposed by Ostrom seems to be more "open", since she not only discusses the rules established privately, on their own, by limited collectivities, but also the governance and adoption of rules by public entities such as states. What is important in her approach is the fact that these rules, whether issued by private or public entities, are defining institutional arrangements applicable to "rival resources" which are difficult to exclude. As Strowel points out, "l'intervention du législateur peut s'avérer décisive pour leur éclosion et développement."[23] Some authors, probably

19 Elinor Ostrom , *La gouvernance des biens communs: Pour une nouvelle approche des ressources naturelles*. (De Boeck,2010); see also, Erika Schlager & Elinor Ostrom, 'Property rights and natural resources: A conceptual analysis' (1992) 68 *Law and Economics*, 249-269; Elina Ostrom& Hess, Private and common property rights', (*Workshop in Political Theory and Policy Analysis*, 2008, 11 Indiana University).

20 GarettHardin, , 'The tragedy of commons' (1968) 162 *Science*, 1243-1248.

21 Peter Linebaugh, P.(2009), *The Magna Carta manifesto – liberties and commons for all*, (University of California Press, 2009).

22 Serge Gutwirth, & Isabelle Stengers, 'Le droit à l'épreuve de la résurgence des commons ' (2016), 2, *Revue Juridique de l'environnement* 315.

23 Strowel (n 11) p. 628. Strowel's reflection is even more justified in the case of the Data

including Serge, will regret the broadness of Ostrom's approach, to the extent that "mandatory commons" originating with public actors might not have the same "soul" and capacity to evolve as their private (i.e., voluntary) counterparts.

In any case, the essence of the commons doctrine is precisely the refusal of the property approach. A resource qualified as a common – in the context of this contribution, the data generated by the Internet of Things devices and services – belongs to nobody or, to be more accurate, it does not belong to a unique owner. Instead, such a resource constitutes a "bundle of rights" in the hands of different actors. The partition of different rights between different actors by their private or public enactments aims, on the one hand, to ensure a legitimate balance of the different interests claimed by each actor; on the other hand, this partition of rights also aims to maximise the value of the commons. The main idea behind the concept of commons is to attribute to different interrelated actors different rights to a common pool resource[24] such as the data collected. The principle is to recognise different rights that pertain to the same "good" (i.e., the data). In her work, Ostrom distinguishes five different types of right that pertain to commons:

- of access;
- to use and to subtract certain resources from the good;
- to manage the use of the good and to forbid certain uses;
- to exclude specific actors; and, finally,
- to alienate the good, either totally or partially, either temporarily or definitively.

Hence, contrary to the proprietary approach, there is no unique person who owns all the rights to a particular resource. In the case of data, the commons approach would imply that data-holders ought to consider fully the different rights afforded to other actors in the ecosystem. To achieve this, the commons require the adoption and governance of rules to be enacted by a collective discussion or, as in the case of the Data Act Proposal, in the context of a legislative framework.

Act Proposal, which arose after the failure of an attempt to self-regulate data sharing (e.g., with the so-called SWIPO (Switching Cloud Providers and Porting Data) code of conduct).

24 Regarding "common-pool resources", Ostrom evokes other examples linked with the environment, like drills, pastures, irrigation systems or fishing grounds. Creative commons is also invoked for explaining the way by which the exploitation of a work might be shared by different actors, in full respect of the authors' right. See, about "creative commons", the following articles: Gutwirth & Stengers (n 22); Strowel (n 11); and Séverine Dusollier, 'The master's house: Creative Commons v. Copyright' (2006) *Columbia Journal of Law and the Arts*, 271, 293.

The question is, then: to what extent could the provisions of the Data Act Proposal be interpreted as consecrating as commons, at least to a certain extent, data collected through Internet of Things technologies? To answer this complex question, I return to the use case developed in the second part of this contribution. But first I turn to the objectives of the Data Act Proposal as enunciated in the explanatory memorandum of the text:

> The proposal will help achieve the broader policy goals of ensuring EU businesses across all sectors are in a position to innovate and compete, effectively empowering individuals with respect to their data, and better equipping businesses and public sector bodies with a proportionate and predictable mechanism to tackle major policy and societal challenges, including public emergencies and other exceptional situations. Businesses will be able to easily switch their data and other digital assets between competing providers of cloud and other data processing services. Data sharing within and between sectors of the economy requires an interoperability framework of procedural and legislative measures to enhance trust and improve efficiency.[25] In this context, the Commission puts forward the proposed Data Act with the aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data.[26]

This quotation of the European Commission constitutes a clear assertion of its will to foster data-sharing as a way of permitting, at the same time, the exploitation of the value of the data collected and the creation of innovative services by companies using the data collected or evolving into the ecosystem of the Internet of Things. It is also an assertion of the commission's will to protect the rights and interests of data subjects, consumers and companies from the risks they are incurring due to the information dissymmetry between them and data-holders.[27] The solution proposed in the Data Act Proposal intends to define and impose governance rules which allocate certain limited rights to different

25 Explanatory memorandum of the Proposal, p. 1

26 Explanatory memorandum of the Proposal (n 25).

27 This wish to ensure a balance between the development of economy and the protection of the interests listed in the text is also asserted by the President of the European Commission: 'L'Europe doit «équilibrer le flux et l'utilisation des données tout en préservant un haut degré de protection de la vie privée, de sécurité, de sûreté et d'éthique'. See Ursula von der Leyen, *Une Union plus ambitieuse – Mon programme pour l'Europe, Orientations politiques pour la prochaine Commission européenne 2019-2024* (2019).

actors. That partition is deemed to ensure that the different interests at stake are respected, even if they might lead to conflicts between actors:[28]

> In this context, the Commission puts forward the proposed Data Act with the aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data. … Ensuring greater balance in the distribution of the value from data in step with the new wave of non-personal industrial data and the proliferation of products connected to the Internet of Things means there is enormous potential for boosting a sustainable data economy in Europe ... For this reason, the Data Act is a key pillar … in the data strategy. ... In particular, it contributes to the creation of a cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors.[29]

The economic development objectives, as they are highlighted by the European Commission itself, may be achieved only by creating a legal framework that fosters and allows for data-sharing. This the framework should do in a way that is respectful of the legitimate interests of each of the actors in the ecosystem and, therefore, by balancing their respective rights. In other words, the Data Act asserts the nature of the commons of data – at least, that is, regarding the scope of the Proposal, which is limited to the data collected through connected devices. In order to achieve its goals, the European Commission does not hesitate to limit certain actors' prerogatives or to create other new rights, as clearly asserted in the Proposal, as it describes the need to give new rights to the consumer in order to ensure their freedom of choice. At the same time, it asserts the need to limit certain rights of the data-holder or of the manufacturer:

---

28 See in this sense, the following recitals of the Data Act Proposal: 'In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonized framework specifying who, other than the manufacturer or other data holder is entitled to access the data generated by products or related services, under which conditions and on what basis' (Recital 4); and: 'Data generation is the result of the actions of at least two actors, the designer or manufacturer of a product and the user of that product. It gives rise to questions of fairness in the digital economy, because the data recorded by such products or related services are an important input for aftermarket, ancillary and other services. In order to realise the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use' (Recital 6).

29 Explanatory memorandum of the Proposal (n 25) pp. 1 and 2.

> The Internet of Things data access right for third parties upon the user's request limits the freedom to conduct a business and the freedom of contract of the manufacturer or designer of a product or related service. The limitation is justified in order to enhance consumer protection, in particular to promote consumer's economic interests. The manufacturer or designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service, which contributes to lock-in effects and hinders market entry for players offering aftermarket services. The Internet of Things data access right addresses this situation by further empowering consumers using products or related services 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. Consumers can therefore benefit from a wider choice in aftermarket services, such as repair and maintenance, and no longer depend on only the manufacturer's services. The proposal facilitates the portability of the user's data to third parties and thereby allows for a competitive offer of aftermarket services, as well as broader data-based innovation and the development of products or services unrelated to those initially purchased or subscribed to by the user.[30]

… to the Data Act

I now analyse the provisions of the Proposal in the light of the commons approach. The first provision to be mentioned definitively is the section 35 already quoted:

> In order not to impede the exercise of the right of users to access and use data in accordance with Article 4 of this Regulation or the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC shall not apply to databases containing data obtained or generated through the use of a linked product or service.

30 Explanatory memorandum of the Proposal (n 25) p. 13. See, in the same sense, the following paragraph: "The limitation of the manufacturer's or designer's freedom to contract and conduct a business is proportionate and mitigated by the unaffected ability of the manufacturer or designer to also use the data, insofar it is in line with the applicable legislation and the agreement with the user. Furthermore, the manufacturer or designer will also benefit from the right to require compensation for enabling third party access. The access right is without prejudice to the existing access and portability rights for data subjects under the GDPR. Additional safeguards ensure a proportionate use of the data by the third party" (Explanatory memorandum of the Proposal (n 25) p. 13).

This provision is essential. It denies any "proprietary" rights to the data-holder that would have been deduced from the reference to the "*sui generis*" right established by the 1996 Directive on Databases; and it explains how the user will have the right to control and impose certain uses on the databases.

As regards the user specifically, the text establishes new rights for them. Article 3.1 requires that products and related services (e.g., the possibility linked to a smart fridge of ordering goods automatically) must be designed and manufactured "in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user".[31] In addition, article 3.2 adds to the list of information to be delivered to the user, under articles 13 and 14 of the GDPR, additional details that are quite important considering the opacity of the functioning of the Internet of Things products and services and their ecosystems.[32] At this stage, I note that this obligation to provide information not only benefits individuals, as in the case of the GDPR, but also legal persons. This increase in information beneficiaries, vis-à-vis the GDPR, can be explained by the risks incurred (especially by SMEs) that are discussed above and as spelt out in article 4.6:

> The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production 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.

31 See, however, the Explanatory memorandum of the Proposal (n 25) p. 16, which discusses the following restrictions regarding data to be made accessible to the user: "Data, which represent the digitization of the user's actions and events concerning the user's use of the product, should therefore be accessible to the user, while information obtained or inferred from such data, where lawfully held, should not be considered to fall within the scope of this Regulation'.

32 'Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format: (a) the nature and volume of the data likely to be generated by the use of the product or related service; (b) whether the data is likely to be generated continuously and in real-time; (c) how the user may access those data; (d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used; (e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established; (f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently; (g) how the user may request that the data are shared with a third-party; …'.

I agree with this inclusion of legal persons in the group of beneficiaries of information, although it should be noted that the protection of legal persons is justified by different grounds and reasons than those that apply to the protection of individuals (freedom to conduct a business vs. privacy and personal data protection). Yet this reasoning does not exclude the interest of considering that certain rights, as enacted by the data-protection legislation (such as the right of access or the right to oppose), might be extended to legal persons when there is a dissymmetry between the companies at stake. This dissymmetry creates a (likely) risk linked to the disequilibrium of information – for instance, in case of SMEs being confronted by large platforms, banks or insurance companies.

Precisely on that point, I note that article 4 affords users, be they physical or legal persons, the right to access their data generated by using the product, without undue delay, free of charge, of the same quality as that available to the data-holder and, where applicable, continuously and in real time. This right of access is to be combined, to a certain extent, with the right to use the data:

> The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so.[33]

Regarding these user's rights, additional elements have to be mentioned: first, in relation to the data that can be accessed, Recital 17 excludes the "derivative data" that result from any software process. It is quite clear that the Proposal seeks to protect the added-value processes that data-holders might use to infer new information based on the data originally collected. The same concern justifies the wording of article 4.4:

> The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate.

Secondly, trade secrets cannot be used as an argument to prevent a user from exercising their right of access. Thirdly, when the user is a legal person, the right of access to data related to natural persons is limited to cases in which a legal basis permits the processing of the data, based on the rules imposed by the GDPR.

33 Recital 28.

The Proposal contains other limitations on the prerogatives of the data-holders and data-recipients, to the benefit of users. For instance, article 5 imposes an obligation on data-holders (with the exception of micro or small enterprises) to share data with designated third parties at the request of users "without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time". The same article correspondingly forbids data-holders to share such data without a legal basis under article 6. 1 GDPR (consent, necessity of the contract or legitimate interest).[34] Furthermore, as regards the communication of data to third parties, the Proposal elaborates on several safeguards in order not to harm the respective interests of other actors. For instance, the Data Act excludes the so called "gatekeepers" (the very large platforms as defined by the Digital Markets Act[35]) from the potential beneficiaries of data. These gatekeepers are forbidden to solicit users or data-holders to make the data collected available to them. In addition, pursuant article 6.1, any

> third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned and shall delete the data when they are no longer necessary for the agreed purpose.

In addition, based on article 6.2(*c*) and (*f*), third parties cannot use the data to compete with the products which generate the data accessed (i.e., in this way protecting the manufacturer or the first data-holder); nor can they make available the data received to another third party. Finally, under articles 8.3 and 8.4, no discrimination may take place between comparable categories of data-recipient, and hence a data-holder must not make data available exclusively to a data-recipient, unless the user requests them to do so. In the use case of the smart fridge, this means that the data-holder is not allowed to give an exclusive advantage to one supermarket over another where automated orders are placed by the fridge itself.

Over and above all these provisions, two more essential requirements imposed by the text to ensure data sharing should be discussed briefly. The first has already been touched upon. According to article 35 of the Proposal, there should be a limitation of the *sui generis* right consecrated by Directive 96/9 on the protection of databases …

34 Article 5.6 of the proposal.

35 Regulation 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), OJ L265, 12/10/2022.

> in order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service claim the *sui generis* right under Article 7 … and in so doing hinder the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation.

The second one is even more important, pursuing as it does the same objective. Article 23 reads:

> Providers of a data processing service shall take the measures provided for in Articles 24, 25 and 26 to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider. In particular, providers of data processing service shall remove commercial, technical, contractual and organizational obstacles, which inhibit customers from terminating their contracts, concluding new agreements with other providers of comparable data-processing services (including cloud services) and porting data, applications or other digital assets. These operations require what the Proposal calls "functional interoperability".

This type of interoperability is defined in article 2(19) as "the ability of two or more data spaces or communication networks, systems, products, applications, or components to exchange and use data in order to perform their functions". It is interesting to note that an entire chapter of the Proposal, including articles 28 and those following it, is dedicated to different aspects of the concept of functional interoperability. As Recital 72 states:

> This Regulation aims to facilitate switching between data processing services, which encompasses all conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets, including data, to the concerned other providers and to continue to use them in the new environment while benefitting from functional equivalence.[36]

36 The functional interoperability required by the Data Act Proposal is broader than the portability right created by Article 20 of the GDPR, which is limited to the sole data "provided" by the data subject. The interoperability concept developed by the Data Act encompasses all elements needed for the good functioning of the system: according to Recital 72, 'Digital assets refer to elements in digital format for which the customer has the right of use, including data, applications, virtual machines and other manifestations

In order to facilitate this set of provisions and ensure that they are respected, the text creates the possibility for the EU to define "essential requirements" and "common specifications" and to promote the voluntary (and even mandatory)[37] adoption of standards.[38]

Finally, according to the "commons" doctrine, the public interest must be taken into account. This consideration leads the European Commission to foresee the possibility of public authorities' requiring data-holders and data-recipients to make the data collected available to the public sector.[39] Nonetheless, the commission clearly requires such a prerogative to be limited in its Proposal. In this respect, Recital 61 provides that

> [a] proportionate, limited and predictable framework at Union level is necessary for the making available of data by data holders, in cases of exceptional needs, to public sector bodies and to Union institution, agencies or bodies both to ensure legal certainty and to minimize the administrative burdens placed on

---

of virtualisation technologies, such as containers. Functional equivalence means the maintenance of a minimum level of functionality of a service after switching and, should be deemed technically feasible whenever both the originating and the destination data processing services cover (in part or in whole) the same service type. Meta-data, generated by the customer's use of a service, should also be portable pursuant to this regulation's provisions on switching'. Regarding the automated orders of products in the smart fridge use case, Recital 80 reads: 'To promote the interoperability of smart contracts in data sharing applications, it is necessary to lay down essential requirements for smart contracts for professionals who create smart contracts for others or integrate such smart contracts in applications that support the implementation of agreements for sharing data. In order to facilitate the conformity of such smart contracts with those essential requirements, …'.

37 By requiring, in a first step, the intervention of the EU standardisation organisations; and by adopting binding delegated acts on that basis in a second step.

38 See Recital 80 and article 30(4) regarding the advantages granted to the actors who are respecting the standards: 'it is necessary to provide for a presumption of conformity for smart contracts that meet harmonised standards or parts thereof in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council'.

39 This trend to see the public authorities not only as provider of data at the benefit of the economy according with the Open data directive (last version in 2019) but, henceforth, as beneficiary of data held by private sector, what the European Commission qualifies as "reverse PSI" (Public Sector Information), is pursued. The Data Governance Act recently adopted (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) contains provisions about what is qualified as "data altruism". Data altruism is about individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used in the public interest. Such data has enormous potential to advance research and develop better products and services, including in the fields of public health, environment and mobility.

> businesses. To this end, data requests by public sector bodies and by Union institution, agencies and bodies to data holders should be transparent and proportionate in terms of their scope of content and their granularity. The purpose of the request and the intended use of the data requested should be specific and clearly explained, while allowing appropriate flexibility for the requesting entity to perform its tasks in the public interest. The request should also respect the legitimate interests of the businesses to whom the request is made. The burden on data holders should be minimised by obliging requesting entities to respect the once-only principle, which prevents the same data from being requested more than once by more than one public sector body or Union institution, agency or body where those data are needed to respond to a public emergency. To ensure transparency, data requests made by public sector bodies and by Union institutions, agencies or bodies should be made public without undue delay by the entity requesting the data and online public availability of all requests justified by a public emergency should be ensured.[40]

On this topic, I note, however, that the EDPS and the EDPB[41] have drawn attention to the fact that the conditions foreseen by the Data Act Proposal regarding access to data by public bodies are not sufficient, considering the GDPR requirements. In this regard, the EDPB and the EDPS recommended, among other things, that the legal basis for processing personal data should be "adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope".[42] In particular, the concepts "emergency" and "exceptional" should be defined more narrowly. Similarly, the scope and manner of the exercise of the power to request access to data by the public sector should be more clearly defined so as to protect individuals against arbitrary interference. In the smart fridge use case, for instance, it would be very difficult for public authorities to have access to the data generated by the fridge, owing to the lack of proportionality of the public health justification advanced.

Conclusions

The Data Act Proposal clearly demonstrates how the EU intends to foreclose on the individualistic proprietary approach defended by several actors, such as

40 Recital 61.

41 EDPB/EDPS, *Joint opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, (2022).

42 EDPB/EDPS (n 41) p. 3.

some data-collectors and privacy advocates, at least regarding the Internet of Things ecosystems. But this text also demonstrates how the EU seeks to impose, by regulation, a design (or eco-functioning) that takes into account the dangers of unregulated uses of data and the legitimate interests (including economic) of the actors in the ecosystems at stake. This approach justifies the substitution of a right of ownership with rights of access, of limited use and of control and to allow or refuse the communication of data to third parties. Each of these rights might be exercised by one or more of the different actors involved in the functioning of the ecosystem of the Internet of Things: users, data-holders, data-recipients and public authorities. To explain and justify that partition of rights – or, rather, that "bundle of rights" – commons' doctrine indeed seems to be[43] an adequate way, one that recognises the added value of data to our economy, our individual liberties and our society.[44] "Data-sharing" or, rather, "sharing the data", is the natural consequence of commons' doctrine. On this point, it is quite clear that the techno-legal approach proposed by the text is necessary in order to offer functional interoperability between actors' systems and devices. This techno-legal approach is also needed to ensure, as far as possible, data subjects' direct and user-friendly access to data generated by the functioning of their "products".

Furthermore, to achieve that goal, it is noticeable that only a transverse legal approach which goes beyond the traditional division between branches of law is possible. The Data Act Proposal might not be analysed from one sole branch of law or point of view. It mixes not only contract law, IP law, administrative law and human rights law, but also competition law and legislation aimed at standardisation. It also suggests that distinctions such as those traditionally made between personal and non-personal data, between data related to individuals and data related to legal persons or between data held by public and private actors must be re-evaluated. And that this re-evaluation should be made in the context of an increasingly unbalanced informational power with risks linked to the technical dependency of users vis-à-vis the technical devices offered to them by the Internet of Things.

---

43 ECJ (n 15). Compare with the text of the Explanatory Memorandum of the Data Act Proposal: 'In order to realise the considerable economic benefits that data, as a 'non-rival good', brings to the economy and society, a general approach to the allocation of data access and use rights is preferable to the granting of exclusive access and use rights' (§ 6).

44 See ECJ (n 15). See also the Recital 6 of the Data Act Proposal: 'In order to realise the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use'.