European Review of Private Law 5-2021 [807–830]

The Legal Regulation of Digital Wealth: Commerce, Ownership and Inheritance of Data*

José Antonio Castillo Parrilla**

Abstract: Digital wealth and its necessary regulation have gained prominence in recent years. The European Commission has published several documents and policy proposals relating, directly or indirectly, to the data economy. A data economy can be defined as an ecosystem of different types of market players collaborating to ensure that data is accessible and usable in order to extract value from data through, for example, creating a variety of applications with great potential to improve daily life. The value of data can increase from EUR 257 billion (1.85 of EU Gross Domestic Product (GDP)) to EUR 643 billion by 2020 (3.17% of EU GDP), according to the EU Commission. The legal implications of the increasing value of the data economy are clear; hence the need to address the challenges presented by its legal regulation.

These challenges are as follows: (1) the acceptance, especially from the perspective of personal data protection, that personal data serve as counter-performance in certain contracts; (2) an adequate conceptualization of the freedom of consent to avoid contradictions between the logic of contract law and that of personal data protection; (3) the qualification of data as goods and therefore possible objects of ownership, and the difficulties that this encounters; and (4) the transmission mortis causa of data as a property asset. We will try to outline the problems associated with each of these challenges and propose some solutions.

Zusammenfassung: Digitale Werte und ihre notwendige Regulierung sind in den letzten Jahren in den Vordergrund gerückt. Die Europäische Kommission hat mehrere Dokumente und politische Vorschläge veröffentlicht, die sich direkt oder indirekt auf die Datenwirtschaft beziehen. Eine Datenwirtschaft kann als ein Ökosystem aus verschiedenen Arten von Marktteilnehmern definiert werden, die zusammenarbeiten, um sicherzustellen, dass Daten zugänglich und nutzbar sind, um aus Daten einen Wert zu schöpfen, indem sie beispielsweise eine Vielzahl von Anwendungen mit großem Potenzial zur Verbesserung des täglichen Lebens schaffen. Der Wert von Daten kann laut EU-Kommission bis 2020 von 257 Mrd. EUR (1,85 des EU-BIP) auf 643 Mrd. EUR (3,17 % des EU-BIP) steigen. Die rechtlichen Implikationen des steigenden Wertes der Datenwirtschaft liegen auf der Hand; daher ist es notwendig, sich den Herausforderungen zu stellen, die sich aus ihrer rechtlichen Regulierung ergeben.

Diese Herausforderungen sind wie folgt: (1) die Akzeptanz, insbesondere aus Sicht des Datenschutzes, dass personenbezogene Daten als Gegenleistung in bestimmten Verträgen dienen; (2) eine adäquate Konzeptualisierung der Einwilligungsfreiheit, um Widersprüche zwischen der Logik des Vertragsrechts und der des Schutzes

* The final version of this article was submitted on July 28, 2021.

** Posdoc Researcher at University of Granada. Email: castillop@ugr.es.

personenbezogener Daten zu vermeiden; (3) die Qualifizierung von Daten als Waren und damit als mögliche Gegenstände des Eigentums und die Schwierigkeiten, die damit verbunden sind; und (4) die Übertragung mortis causa von Daten als Vermögenswert. Wir werden versuchen, die mit jeder dieser Herausforderungen verbundenen Probleme zu skizzieren und einige Lösungen vorzuschlagen.

Résumé: La richesse numérique et sa nécessaire réglementation ont pris de l'importance ces dernières années. La Commission européenne a publié plusieurs documents et propositions politiques concernant, directement ou indirectement, l'économie des données. Une économie des données peut être définie comme un écosystème composé de différents types d'acteurs du marché qui collaborent pour faire en sorte que les données soient accessibles et utilisables afin d'en extraire de la valeur en créant, par exemple, une variété d'applications à fort potentiel pour améliorer la vie quotidienne. La valeur des données peut passer de 257 milliards d'euros (1,85 % du PIB de l'UE) à 643 milliards d'euros d'ici à 2020 (3,17 % du PIB de l'UE), selon la Commission européenne. Les implications juridiques de la valeur croissante de l'économie des données sont claires; d'où la nécessité de relever les défis que présente sa réglementation juridique.

Ces défis sont les suivants: (1) l'acceptation, notamment du point de vue de la protection des données personnelles, que celles-ci servent de contre-prestation dans certains contrats; (2) une conceptualisation adéquate de la liberté de consentement pour éviter les contradictions entre la logique du droit des contrats et celle de la protection des données personnelles; (3) la qualification des données en tant que biens et donc objets possibles de propriété, et les difficultés que cela rencontre; et (4) la transmission mortis causa des données en tant qu'actif immobilier. Nous tenterons d'exposer les problèmes liés à chacun de ces défis et de proposer quelques solutions.

1. Data Marketplaces and the Data Economy

1. The data economy can be defined as an ecosystem where different market actors collaborate to ensure that data is accessible and usable, with the aim of extracting value from that data. An important part of the data economy takes place through data marketplaces, platforms where parties can exchange and/or monetise data sets (both raw data and processed data). The value of the data economy crossed the EUR 400bn threshold in 2019 for the EU27 plus the UK, up 7.6% year-on-year; while the value of the data marketplace reached EUR 75bn in 2019 for the EU27 plus the UK, up 5% year-on-year. Despite this, the rules currently available to us are insufficient to address this phenomenon.

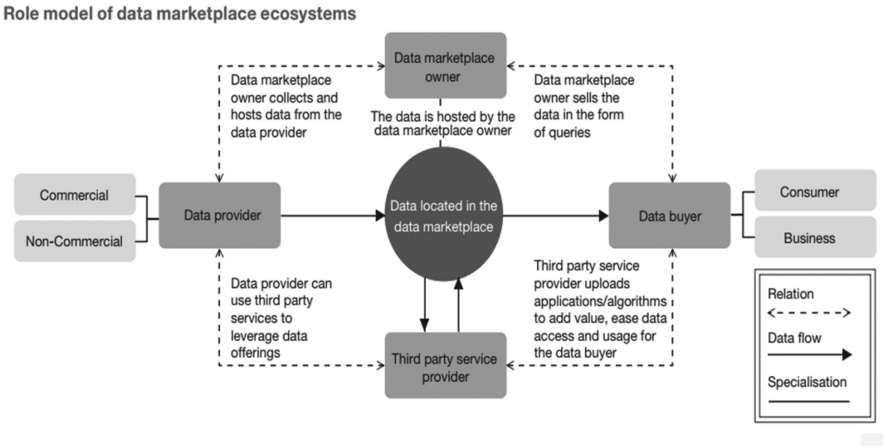
2. Data marketplaces are platforms that provide an infrastructure for the exchange or sharing of data, thus enabling the economic exploitation and monetization of data.[1] As platforms, data marketplaces act as neutral intermediaries and allow their customers to upload, sell or share data (understood as

1 Spiekermann defines data marketplaces as electronic marketplaces where data is traded as a commodity; and e-marketplaces as infrastructures that allow participants to meet and conduct

products) through access, usage or exchange contracts (e.g., purchase and sale contracts). The presence and development of data marketplaces can bring benefits to business activity, social creativity and technological momentum.[2]

3. Data marketplaces facilitate such an important activity for the data economy as data analytics, which requires constant storage and exchange of data.[3] In data marketplaces, data providers de facto act as owners of the data, offering it to others, as we can see in the following figure[4]:

Figure 1 Role Model of Data Marketplace Ecosystems (Spiekerman (n.1) p. 210).



4. Data marketplaces can be classified according to several criteria. We will use two: (1) the number of actors on each side of the negotiation and (2) the type of data exchanged or shared. In terms of the number of actors, a first division can be made: bilateral markets and multilateral markets. In bilateral markets, data interaction (e.g., data exchange or sharing) takes place between two distinguishable user groups or market parties; whereas in multilateral

transactions in a secure electronic environment (M. Spiekermann, 'Data Marketplaces: Trends and Monetisation of Data Goods', 54. *Intereconomics* 2019, p 209).

2 Y. Demchenko, W. Los & C. de Laat, 'Data as Economic Goods: Definitions, Properties, Challenges, Enabling Technologies for Future Data Markets', 2. ITU (*Journal: ICT Discoveries*) 2018, p (3) at 4.

3 A. Pauer, L. Nagel, T. Fedkenhauser, Y. Fritzsche-Sterr & Resetko, *Data Exchange as a First Step Towards Data Economy* (Düsseldorf: PricewaterhouseCoopers GmbH Wirtschaftsprü fungsgesellschaft) 2018, p 11.

4 M. Spiekermann, 54. *Intereconomics*, p 210.

markets, interaction between market parties is facilitated by platforms that are not directly involved.[5]

5. Depending on the type of data being exchanged or shared, we can distinguish between (1) personal data marketplaces versus non-personal data marketplaces, or mixed data marketplaces; (2) specific data marketplaces for certain categories of data; (3) and, markets for raw data versus markets for secondary or processed data.

6. Non-personal data marketplaces are an emerging sector at present, as these data are not regulated by the General Data Protection Regulation (GDPR), but by EU Regulation 2018/1087 of 14 November 2018 on a framework for the free movement of non-personal data in the EU[6] . As far as personal data marketplaces are concerned, it should be stressed at the outset that they are a reality, however uncomfortable that may be. A personal data marketplace is not illegal per se; it must, however, comply with the requirements of the GDPR.

7. There is a wide range of data marketplaces which can be generic or specific depending on the type of data they focus on. Dawex or Qlik DataMarket are generic data marketplaces. Here are three examples of specific data marketplaces that present specific problems depending on the type of data traded through them[7]:

8. Climpact-Metnext focuses on the sale of weather data to farmers.[8] Climpact-Metnext does not only act as a marketplace: it provides operational tools and services to measure the impact of weather on economic activity and to model future activity based on weather forecasts, as well as tools and expertise to create and structure weather risk management products to brokers, banks, insurers and reinsurers.[9]

9. AAAData began as a marketplace specifically for auto number plate data sold to auto insurance brokers.[10] They have now expanded the categories of data, although it is still automobile data.[11] This is a good example of a 'quasi-personal' data marketplace: in principle, car-related data are non-personal data, but if it is

---

5 M. Spiekermann, 54. *Intereconomics*, p 209.

6 The European Data Strategy estimates that the value of non-personal data will reach 1.5 trillion by 2027 (EU Commission Communication: 'A European Strategy for Data', Brussels COM (2020) 66 final 19 Feb. 2020, p 26).

7 Other data marketplaces are: Advaneo (https://www.advaneo.de/en/#), Caruso (https://www.caruso-dataplace.com/), Qlik DataMarket (https://www.qlik.com/us/products/qlik-sense/data-sources) o Dawex (https://www.dawex.com/en/). A more extensive list can be found in M. Spiekermann, 54. *Intereconomics*, p 211.

8 EU Commission Staff Working Document: 'On the Free Flow of Data and Emerging Issues of the European Data Economy' Accompanying the document 'Communication Building a European Data Economy', Brussels SWD (2017) 2 final, p 13, fn. 43.

9 https://www.crunchbase.com/organization/climpact-metnext. Other meteorological data marketplaces are Api-Agro (https://api-agro.eu/en/) or Graniot (https://graniot.com/).

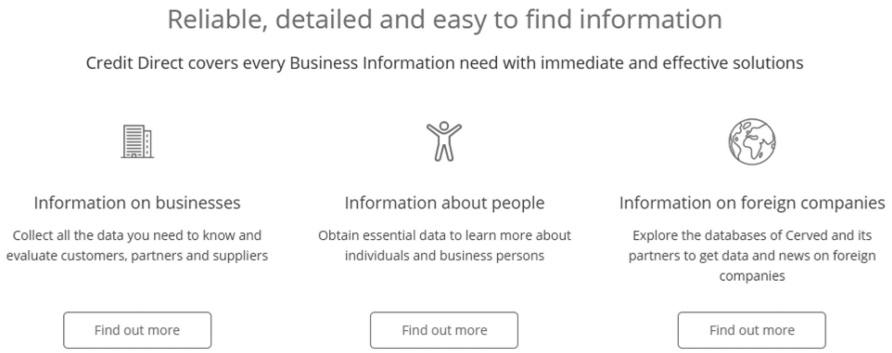
10 EU Commission Staff Working Document, supra n. 8, p 13, fn. 43.

11 https://www.aaa-data.fr/.

possible to find out the driver and/or the owner of the car, these data become personal data. It goes without saying that this is relatively easy to do.

10. Cerved has also expanded its business model. It started as a marketplace for credit rating data sold to banks.[12] It is a clear example of a specific data marketplace that works with both personal and non-personal data.[13]

Figure 2 Cerved Scheme of Information Available for Exchange



11. In practice, it is difficult to distinguish personal data from non-personal data unless it is data that in no way relates to individuals (e.g., weather data). This difficulty is increased by the fact that most data marketplaces are mixed markets.

12. At the moment, companies are not willing to share or exchange data as much as is desirable. As a result, the data marketplace has so far been dominated by privately managed commercial platforms operating in closed systems. However, the trend seems to be changing as legal certainty for data transactions increases.[14]

13. Nevertheless, the legal regulation of data as an economic asset faces certain challenges, such as the following: (1) the acceptance, especially from the perspective of personal data protection, that data serve as counter-performance in certain contracts; (2) an adequate conceptualization of the freedom of consent to avoid contradictions between the logic of contract law and that of personal data protection; (3) the qualification of data as goods and therefore possible objects of ownership, and the difficulties this encounters; and (4) the mortis causa transmission of data as an economic asset. We will try to outline the problems associated with each of these challenges and propose some solutions.

12 EU Commission Staff Working Document, supra n. 8, p 13, fn. 43.

13 https://www.cerved-online.com/credit-direct/?utm_campaign=2018_CervedOnline&utm_medium=Banner&utm_source=SitoCerved.

14 M. Spiekermann, 54. *Intereconomics*, p 210.

2. Data as Counter-performance and the GDPR

14. The first challenge we face in relation to the necessary legal regulation of digital wealth is to answer the question of whether or not data can function as counter-performance in certain contracts. We can see the importance of this question by looking at the evolution of EU Directive 770/2019 from its original EU Directive Proposal 634/2015 through European Data Protection Supervisor (EDPS) Opinion 4/2017.

15. In its first version, EU Directive Proposal 634/2015 states (1) that, in the digital economy, information about individuals is considered a value comparable to money, (2) and that digital content is not always exchanged for monetary counter-performance, but is also exchanged for other counter-performances than money, such as allowing access to personal or other data.[15] Recital 24 of EU Directive 770/2019 states, however, that data protection is a fundamental right and that personal data cannot be considered as a commodity, although it recognizes that consumers provide personal data to the entrepreneur when the latter provides them with certain digital content or services. It gives as an example those cases where the consumer opens an account on a social network and provides a name and email address, and these are used for purposes other than exclusively for the provision of the digital content or services, or other than to comply with legal requirements, or other cases where the consumer consents to any material constituting personal data, such as photographs or messages he uploads, being processed by the entrepreneur for commercial purposes. In addition to these changes, the term 'actively providing data', which was present in EU Directive Proposal 634/2015, disappears.

16. These are very significant changes, which originate from the EDPS Opinion 4/2017.[16] In this opinion, the EDPS advises against the use of the term 'data as counter-performance'[17] and expresses its opposition to the acceptance of personal data as a commodity.[18] The EDPS also recommends avoiding the term 'actively provides', as it contradicts existing and future data protection rules.[19] In short, the EDPS considers that any future rules should not alter the balance found by the GDPR as to the circumstances in which the processing of personal data in the digital marketplace can take place.[20]

---

15 Recital 13 EU Directive Proposal 634/2015. See also Recital 14 and Art. 3.1 EU Directive 634/2015.

16 EDPS Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Brussels 14 March 2017.

17 Ibid., p 10.

18 Ibid., p 3.

19 Ibid., p 21.

20 Ibid., p 9.

17. Both the original version of the EU Directive Proposal 634/2015 and the EDPS Opinion 4/2017 reflect the current debate around the acceptance (or not) that data (personal and non-personal) function as counter-performance in certain contracts. In our view, it is difficult to maintain for much longer a position such as the one defended by the EDPS in 2017 without outright denial of reality. We will devote the following lines to explaining the reasons behind this opinion, with the intention of encouraging a debate that will open up the position of personal data protection authorities on this issue.

18. Point 2. 3 of the abovementioned EDPS Opinion presents some arguments against the acceptance of data as counter-performance[21]: (1) the Proposal does not define what is meant by counter-performance, which could appear to oversimplify a variety of business models and uses of data into a single term; (2) the link that the Proposal makes between paying a price with money and actively providing data as counter-performance is misleading, because while the consumer is aware of what he/she is giving when paying with money, the same cannot be said for data insofar as standard contractual clauses and privacy policies do not make it easy for the consumer to understand what precisely is done with the data collected about him/her; and (3) if personal data can be compared to money to a certain extent, they are obviously not identical. As to the last argument, it should be recalled that, according to Recital 13 of EU Directive Proposal 634/2015, data is a value comparable to money, not identical.

19. The first two arguments seem to confuse the logic of data protection with that of the data economy. Mandatory compliance with the principles of Article 5 GDPR does not affirm or question the economic value of data or the possibility of its use as a commodity. In the case of a monetary counter-performance, the provider would not be obliged to report on the use of money, despite the fact that money (as well as data) can be used for a wide variety of purposes. If the consumer does not provide a monetary counter-performance, but consents to the processing of his data, the provider must comply with the requirements of Article 5 GDPR, but because this data is personal data regardless of whether or not it functions as a counter-performance. Mentioning that the supplier considers the consumer's personal data as a counter-performance also has nothing to do with compliance with the transparency principle of Article 5 GDPR, as this principle refers to information about the identity of the controller and the purposes of the processing (Rec. 39 GDPR).

20. The term 'actively provides' also seems to generate confusion. The EDPS now conflates the consent requirements for the processing of personal data (Article 4.11 GDPR) with the 'active provision' of data. According to the EDPS[22]: (1) the

21 Ibid., p 9.
22 Ibid., p 12.

distinction between actively and non-actively provided personal data does not exist in data protection law; (2) the notion of 'active provision of data' could generate an adverse effect if providers do not ask for data to be provided directly, but collect and process the same data provided passively by consumers; and (3) this notion could contradict e-privacy rules.

21. The first two arguments are striking. It is normal that the idea of 'active data delivery' is not present in data protection rules, as it is specific to the view of data as an economic asset and the GDPR does not understand data in this way.[23] The second argument concerns a possible breach of the rules, not an 'adverse effect'. Any rule, by definition, can be breached. Therefore, the risk of non-compliance with a future standard does not seem to be a very convincing argument against its introduction in an EU Regulation or Directive. As regards e-Privacy compliance, Article 5(3) of European Commission (EU) Directive 2002/58/EC requires that the data subject is provided with clear and comprehensive information about the purposes of the processing and is offered the right to refuse such processing by the controller.[24] This obligation connects with the principle of transparency in data processing in Article 5 GDPR. Again, compliance with the principle of transparency has nothing to do with the fact that an 'active provision of data' means that the data acts as a counter-performance.

22. What does 'active provision' of data mean? It means the voluntary and informed consent to the processing of one's own data, even if it is not required by law[25] or necessary for the proper performance of the contract. This does not affect compliance with the transparency principle of Articles 5(1)(a) GDPR and 5(3) Dir. 2002/58/EC.

23. In short, the current wording of EU Directive 2019/770 (Recital 24 and Article 3) does not call into question (1) that data function as counter-performance in practice, nor (2) that in order to act as payment it must be an active provision. However, the terms 'counter-performance', 'commodity' and 'active provision of data' are avoided and replaced by a detailed description of the reality to which they refer: the terms are deleted and their definitions are put in their place.[26]

---

23 See C. Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy', in Lohsse, R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p 353.

24 See Arts 6.2.c and 6.3.b of e-Privacy Regulation Proposal.

25 See A. de Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Napoli: Edizioni Scientifiche Italiane 2017), p 72. De Franceschi adds an interesting nuance with regard to the active provision of data: it is not decisive whether personal data is provided 'actively' or 'passively', but whether the consumer consciously 'pays' with his own personal data through it. With this in mind, the term 'active provision of data' could be rephrased as 'conscious payment with data'.

26 According to Metzger, despite all the changes, the essential approach of Art. 3 of the current EU Directive 770/2019 remains the same as in the 2015 Proposal insofar as the Directive continues to

24. Is the notion of 'actively providing data' (or conscious payment with data) incompatible with the consent requirements under the GDPR? In relation to this particular question, the answer should be in the negative. According to Article 4.11 GDPR, consent must be a specific, informed and unambiguous indication of the data subject's wishes through a clear affirmative action signifying agreement to the processing of personal data. What can be problematic, as we will see below, is the GDPR's idea of 'freedom of consent' when data is given in exchange for digital content or services.

3. Freedom of Consent and the GDPR When Personal Data are Given in Exchange of Digital Content or Digital Services

25. Freedom of consent is the cornerstone of both contract law and data protection law. Therefore, a common understanding of what 'freedom of consent' means would be crucial for a less problematic coexistence of personal data protection rules with data economy rules. This is not currently the case. While the other consent requirements of Article 4.11 GDPR are compatible with the idea of giving consent to the processing of data in exchange for goods or services, a strict interpretation of 'freedom of consent' according to Recitals 42 and 43 GDPR would exclude the possibility of giving consent to the processing of data in exchange for goods or services.

26. According to Article 4.11 GDPR, consent to data processing must be freely given. In assessing whether consent is freely given, account shall be taken to the greatest extent possible if, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that are not necessary for the performance of that contract (Article 7.4 GDPR). Article 7.4 does not specify whether this situation qualifies the consent as freely given or not. Recitals 42 and 43 clarify this question. According to Recitals 42 and 43 GDPR, consent shall not be considered freely given if (1) its withdrawal entails any detriment to the data subject, or (2) the processing of the data is not necessary, for technical, contractual or legal reasons, and the provision of services or content depends on the data subject's consent. If consent does not meet all the requirements of Articles 4 and 7, it will not be a valid basis for processing as contrary to the GDPR.[27]

27. In the following, we will set out an alternative interpretation of Recitals 42 and 43 GDPR. This is a somewhat strained interpretation, and contrary to the criteria expressed by both the EDPS and the European Data Protection Board (EDPB).

---

apply both to consumers who pay with money and to those who give personal data in exchange (A. Metzger, 'A Market Model for Personal Data: State of Play Under New Directive on Digital Content and Digital Services', in S. Lohsse, R. Schulze & D. Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (Baden-Baden: Nomos 2020), p 28.

27 EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Brussels 4 May 2020, pp 4–6.

However, it is of interest insofar as it would help to promote the coexistence between the logics of the data economy and the protection of personal data. Personal data protection rules should not become a dead letter to the extent that they end up being ignored de facto, nor should a restrictive interpretation of them act as a barrier to the economic development that the economic use of data (personal and non-personal) allows and that other regions of the world are already pursuing.

28. The first half of Recital 43 states that consent should not be considered a valid legal basis for data processing when there is a clear imbalance between the data subject and the controller, while the second half only states that consent shall be presumed not to have been freely given in other situations, but does not mention that these situations invalidate consent, merely that it is presumed not to have been freely given. It is not clear from this Recital whether this is an *iuris et de iure* presumption or an *iuris tantum* presumption. Among the situations mentioned in Recital 43, consent should be presumed not to have been freely given when the performance of a contract, including the provision of a service, is dependent on consent, even if consent is not necessary for such performance. A clear reference to the use of personal data for counter-performance can be observed here. If in the first half of the Recital it is stated that certain situations 'do not constitute a valid legal basis' and in the second half of the same Recital, on the other hand, it is referred to as 'presumptions', we might be inclined to argue that such presumptions are *iuris tantum*, otherwise such a terminological distinction would not have been necessary in such a short space. Continuing with the reasoning, we can affirm that the situations mentioned in the second half of Recital 43 should lead to a presumption (*iuris tantum*) that consent has not been freely given, but that this presumption can be dismantled. Finally, the set of presumptions does not in itself imply that consent to data processing is not a valid legal basis in the situations described in the second half of Recital 43.

29. Insofar as the EDPB does not support the alternative interpretation mentioned above, the question arises whether the situations referred to in Article 3(2) of Directive 770/2019 meet the requirements for valid consent under Article 4(11) of the GDPR, as interpreted by Articles 42 and 43 of the GDPR and the EDPB.

30. It is also important to clarify what detriment means. According to the EDPB, we should consider as detriment any clear cost or disadvantage to the data subject following the withdrawal of consent, such as intimidation, coercion or any other significant consequence. Therefore, detriment will be present if, after the data subject withdraws his or her consent to data processing, the performance of the service decreases to the prejudice of the user.[28] For the sake of clarity, some of the following situations should be considered as detriment according to the criteria just mentioned:

---

28 Ibid., p (11) at 12.

31. A data subject (customer or user from a contract law perspective) downloads an app and the app asks for consent to access data on the phone. This is not necessary for the app to work, but it is useful for the controller (provider) to know the behaviour of the data subject. When the user withdraws this consent, the application only works to a limited extent.[29]

32. A customer opens a 'zero-rated' bank account. The bank asks the customer for his consent to allow third parties to use his payment data for direct marketing purposes. If the customer refuses to consent to this data processing, the customer will be refused banking services or the 'zero-fee' bank account will be transformed into a '5-euro fee' bank account.[30] If the customer initially agrees, but later decides to withdraw consent to the data processing, the bank may terminate the customer's account or charge EUR 5 as an alternative payment (to the data).

33. According to the GDPR, the data subject must not suffer any negative consequences after withdrawing his or her consent to data processing. If negative consequences are possible or foreseen (e.g., in the general terms and conditions of the contract), it is assumed that the consent has not been freely given and is therefore invalid. For the EDPB, the above situations are examples of invalid consent under the GDPR.

34. But what if the same situations are looked at from a contract law perspective? If the parties have entered into a contract freely and with adequate information, the contract should normally be regarded as binding on them, unless they agree (also freely) to its modification or termination.[31]

35. Thus, from a contract law perspective, the idea of 'freely given consent' under the GDPR would jeopardize the stability of the contract due to the precariousness of consent, as it would grant the data subject a *sine die* right of unilateral termination *ad nutum*.[32] As a consequence, there would be a risk of unjust enrichment of the data subject as a user of the service. To avoid this worrying situation, a flexible interpretation of the notion of freely given consent under the GDPR seems desirable.[33]

---

29 Ibid., p 12.

30 Ibid., p 9, para, 33, as an example of conditional consent. This is an example based on a real case, https://www.elconfidencial.com/tecnologia/2019-02-13/bankia-cuenta-on-ley-proteccion-de-datos-infraccion_1821530/.

31 C. von Bar et al., *Principles, Definitions and Model Rules of European Private Law – Draft Common Frame of Reference (DCFR)* (München: Sellier –European law publishers 2009), p 74.

32 A. de Franceschi, *La circolazione dei dati personali tra privacy e contratto*, p (55) at 56, and (111) at 117.

33 C. Wendehorst, in *Trading Data in the Digital Economy: Legal Concepts and Tools*, p 354.

36. The flexible interpretation of the notion of 'freely given consent' under the GDPR that we propose should take into account the difference between 'freedom' and 'irresponsibility'. Consent will be considered free if the subject has not given consent under threat or coercion and can withdraw it at any time. Moreover, freedom entails responsibility. Therefore, if the data subject withdraws his or her consent to data processing, there must be consequences, in the same way as if he or she withdraws a monetary payment. These consequences should aim at restoring the economic balance of the parties (avoiding unjust enrichment of the user) and should be distinguished from the idea of 'detriment'. Therefore, the idea of detriment should be understood as going beyond the contractual consequences arising from the withdrawal of consent and aiming at avoiding the unjust enrichment of one of the parties.

4. Data as Goods and Data Ownership

37. If data function in practice as counter-performance (whatever terms the rules ultimately use), it means that data are 'delivered'. If data are 'delivered', then they function as goods. If data function as goods, then data can be owned.[34] And finally, if data can be owned, then the powers that the right of ownership of the data confers on the owner of the data, and who owns the data,[35] must be spelled out. But, to begin with, can data be considered as goods?

38. First, we need to clarify what we mean by 'data' or, rather, what types of 'data' are relevant for the purpose of reflecting on a possible right of ownership of data. The term 'datum' is defined as 'an item of information' according to the Oxford English Dictionary, so that 'data' is usually used as a synonym for information. In this article we use the term 'data' to refer to so-called 'digital data', according to International Standard Organisation (ISO) 10782-1:1998, which defines 'data' as 'a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing'. From a syntactic point of view,[36] data can be either structured or unstructured data. Structured data has a considerably higher economic value than unstructured data. Within the latter, processed data and, among processed data, personal profiles, are particularly attractive economically. Although our reflections will mainly focus on structured data, we understand that the legal consideration of

34 K. Swinnen refers to this situation as 'de facto ownership', and describes very clearly: 'in a day-to-day commercial and economic life people treat them as if they are goods or, in other words, as if they are owned' (K. Swinnen, 'Ownership of data: Four Recommendations for Future Research', 5. *Journal of Law, Property, and Society* 2020, p (143) at 144).

35 This question was already outlined by Angela Merkel in her speech at the 2018 World Economic Forum (K. Swinnen, 5. *Journal of Law, Property, and Society*, p 143).

36 H. Zech, 'Data as a Tradeable Commodity', in A. de Franceschi (ed.), *European Contract Law and the Digital Single Market – The Implication of the Digital Revolution* (Cambridge: Intersentia 2016), p 53.

unstructured data should not be neglected insofar as they can also be of use and thus have legal relevance.

39. We can ask whether it is possible to commodify a fundamental right and turn it into a commodity.[37] This debate arose more than a century ago and was resolved in favour of being able to commodify (and therefore commercialize) certain fundamental rights related to personality (honour, privacy, personal image).[38] To the extent that the right to data protection is also a fundamental right close to those mentioned above, the same arguments can be used by analogy to respond also favourably to the possibility of commercializing one's own personal data. If one fully accepts the economic use of fundamental rights such as privacy or one's own image (e.g., the use of one's own image for advertising campaigns), what would be the problem in admitting a similar use of one's own personal data, (e.g., using them as counter-performance)? It would be desirable to concentrate efforts on analysing the characteristics of data as goods in order to protect, as far as possible, the potential economic use powers of the data subject.[39] However, adapting the category of goods to data poses some difficulties from a legal point of view.

40. To address the question of data as goods, we propose to use a functional concept of goods that accommodates the new forms of wealth arising from the Digital Revolution. Thus, 'goods' can be understood as static meta-legal entities, with potential economic utility and legal relevance.[40] They are entities because they are individualisable, e.g., they can be named and certain characteristics can be attributed to them. They are meta-legal because they designate realities that are outside the world of law,[41] regardless of whether they are corporeal, incorporeal, material or immaterial.[42] They are static entities, because their existence does not depend on their being exchanged.[43] Finally, they are useful[44]; and this justifies their legal relevance.[45]

---

37 A synthesis of the positions for and against and the advocates of each can be found at K. Swinnen, 5. *Journal of Law, Property, and Society*, p (169) at 170.

38 S. D. Warren & L. D. Brandeis, 'The Right to Privacy', 4. *Harvard Law Review* 1890, p (193) at 220.

39 K. Swinnen, 5. *Journal of Law, Property, and Society*, p 146.

40 J. A. Castillo Parrilla, *Bienes digitales. Una necesidad europea* (Madrid: Dykinson 2018), p 282.

41 In contrast to concepts such as 'law' or 'contract', which are purely legal.

42 Data are material entities, but not corporeal insofar as they are mere electrical impulses.

43 Unlike services, which only exist as long as they are provided by the debtor.

44 B. Biondi, *I beni* (Torino: Editrice Torinese 1956), p (6) at 9. The author uses the term 'useful' in a broad sense. This broad sense can fit for data, since data processing enables companies, for instance, to optimize their production processes, to improve their products, to pick up on trends, to send personalized offers to customers, etc (K. Swinnen, 5. *Journal of Law, Property, and Society*, p 143).

45 Not all 'objects' are 'things' according to § 90 BGB, nor are all 'things' 'goods' according to Art. 810 of the *Codice civile*. Only those objects/things with legal relevance (due to their potential

41. With regard to the materiality/corporeality of the data, it must first of all be observed that there are two main models in the theory of goods. The Germanic model does not use the term 'goods' but 'things' and restricts it to corporeal objects (§ 90 Bürgerliches Gesetzbuch (BGB)). The French model uses the term 'goods', and admits as such both corporeal and incorporeal things (Article 810 *Codice civile*). The Germanic model has influenced EU law (Article 1.2.b Directive 1999/44/EC; Article 2.3 EU Directive 2011/83/EU; Article 2.5 EU Directive 771/2019), but this does not mean that both models have blurred in the legal systems of the respective EU Member States. The Germanic model is used by Austria, Belgium or the Netherlands, among others; the French model is used by Italy or Spain. For practical purposes and as far as data ownership is concerned, the Germanic model does not accept the right of ownership over immaterial or incorporeal goods, while the French model does. In fact, we can see how even Article 814 of the *Codice civile* regulates electricity understood as a good.

42. Do data, understood as an economic asset, fit into the concept of digital goods that we have just proposed[46]?

43. The first difficulty concerns the individuality of data. We always speak of data in the plural.[47] Data, in the singular, has no value, neither economic nor legal. Moreover, data are encoded and machine-readable information.[48] Any information can be eternally divided. Where can we set the minimum limit that allows us to speak of a data and not of several data[49]?

44. Data acquire value as a set: each piece of data belonging to a set of data will have more value the more data the set has and the more interrelated they are. In contrast, physical goods are governed by the paradox of scarcity: a good will have more value the

---

utility, in the broad sense in which Biondi uses the term) are to be considered as things/goods in a legal sense.

46 See D. Quah, *Digital Goods and the New Economy,* https://www.researchgate.net/publication/4808107_Digital_Goods_and_the_New_Economy for a similar concept of digital goods which also encompasses data.

47 It could be said that the GDPR considers data packages as movable property insofar as it regulates the right to data portability (Art. 20 GDPR).

48 EU Commission Communication: 'Towards a Thriving Data-Driven Economy', Brussels SWD (2014) 214 final 2 July 2014, p (4) at 5: 'According to ISO/IEC 2382-1, data is a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing'; G. Sartor, *L´informatica giuridica e le tecnologie dell´informazione*, 2nd edition (Torino: Giapichelli Editore 2012), p 141; H. Zech, in *European Contract Law and the Digital Single Market*, p 53.

49 These difficulties relate to data as raw information (e.g., of no interest in itself). It has nothing to do with the value of the particular information i.e., of interest for whatever reason. See EU Commission Staff Working Document, supra n. 8, p 13: 'For centuries, information has been traded. However, with the availability of information stored in a digital form, data trading has drastically increased'.

scarcer it is, to the extent that for this reason it is likely to generate more problems of rivalry of use.[50] Data are neither scarce nor rivalrous: they can be multiplied in an unlimited way at zero cost and can be exploited at the same time by an indeterminate number of subjects. Moreover, the impossibility of individualizing data makes it difficult to directly transfer the legal fictions protecting immaterial goods to data.

45. On the other hand, we can say that data are experiential goods. This characteristic makes their monetary valuation difficult. However, the difficulties in valuing data in monetary terms should not call into question their qualification as goods from a legal point of view.

46. The difficulties that we have just pointed out about the fitting of the data in the category of goods (difficult to individualize, and neither scarce nor subject to the paradox of scarcity) could be solved if we use as a standard that of fluid goods (gas, water, electricity).

47. Finally, we should not make the mistake of identifying the economic exploitation and commercialization of data with a violation of privacy.

48. The possibility of developing a right of ownership of data has given rise to a heated debate in the doctrine. The arguments against developing a right of data ownership are, in summary, the following[51]:

1. There are insufficient economic arguments (e.g., market failures) to support the need for a data property right. A hypothetical data ownership right could even diminish the possibilities for economic and social progress offered by big data and hinder the exercise of fundamental freedoms such as competition, provision of services, research or information.[52]
2. It is not clear that a future right of data ownership would lead to better access to data and to a smoother flow of data traffic, as it currently occurs spontaneously.[53]

---

50 M. Allara, *Dei beni* (Milano: Giuffrè Editore 1984), p 29; F. Galgano, *Trattato di Diritto civile, Vol. 1*, 3rd Edition (Padova: CEDAM 2015), p 356; C. Spanga, 'Dei beni in generale', in P. Schlesinger (Dir.), *Il Codice Civile Commentario – Art. 810–821* (Milano: Giuffrè Editore 2015), p 61.

51 EU Commission Staff Working Document, supra n. 8.

52 H. Zech, in *European Contract Law and the Digital Single Market*, p 76, nota 72; P. B. Hugenholtz, 'Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?', in S. Lohsse, R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p 71.

53 S. Lohsse, R. Schulze & D. Staudenmayer, 'Trading Data in the Digital Economy: Legal Concepts and Tools', in S. Lohsse, R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p 19.

3. On the other hand, it would be very difficult to establish the powers associated with a data property right, as data are non-rivalrous goods and have an unlimited capacity to multiply.[54]
4. The opportunities and challenges of the data economy are sufficiently well regulated with the current rules on trade secrets, intellectual property and databases.[55]
5. Finally, one should be cautious, as experience shows that once a law is developed at European level, it is very difficult to go back and make it disappear.

49. The first two arguments are of an economic nature and, in any case, are inferences about the future consequences of a right (data ownership) whose content is unknown. It is said that there are no market failures that justify the development of this right. A market failure is a situation in which the market is not able to allocate resources efficiently. It is true that propertization would restrict competition and raise barriers to entry in this market sector.[56] But, on the other hand, it does not seem reasonable to differentiate between digital contracts depending on the type of counter-performance.[57]

50. Data ownership would not be limited to B2C relationships, to which Directive 770/2019 is limited. Is an entrepreneur who pays another with data entering into a contract for consideration or free of charge?[58] Would it be advisable to apply the

---

54 H. Zech, in *European Contract Law and the Digital Single Market*, p (59) at 60.

55 See M. Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential Reform', in Lohsse, R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p 54; J. Reda, 'Learning from Past Mistakes: Similarities in the European Commission´s Justifications of the Sui Generis Database Right and the Data Producers´ Right', in Lohsse, R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p 303; y T. Aplin, 'Trading data in the Digital Economy: Trade Secrets Perspective', in R. Schulze & D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018), p (59) at 72.

56 M. J. Radin, 'A Comment on Information Propertization and Its Legal Milieu', 54. *Cleveland State Law Review* 2020, p 28.

57 Let us accept, for the purposes of this question, that the data function as counter-performance despite the reluctance noted above to call a spade a spade.

58 Facebook has been fined EUR 3.6 million by the Hungarian Competition Authority in Dec. 2019, https://www.gvh.hu/en/press_room/press_releases/press_releases_2019/gvh-imposed-a-fine-of-eur-3.6-m-on-facebook and by the Italian Council of State with EUR 7 million in Mar. 2021, https://www.wired.it/economia/business/2021/04/02/facebook-dati-utenti-gratis-consiglio-stato/?refresh_ce=. In both cases, the main argument of the sanctions is that Facebook advertised itself as free without being free (because it makes money from the processing of its users' personal data), and that therefore the slogan on its homepage ('It's free and always will be') is misleading. In other words, in the opinion of these two national institutions, payment with one's own personal data

rules of Directive 770/2019 beyond B2C relationships? The answer to these questions will determine the protection of entrepreneurs entering into digital contracts where they provide data as counter-performance. It is important to preserve legal certainty for actors involved in this emerging sector of the economy. The wealth-generating potential of each technological revolution requires an adequate social and legal framework for its proper development for the benefit of all.[59]

51. Could a future right of data ownership boost or slow down data traffic? To begin with, data traffic is likely to continue to grow regardless of the rules that regulate it. The right question would be whether the wealth generated by data traffic is adequately distributed among those who produce it, e.g., between the individuals who produce data through their digital behaviour and the companies that have the technology to economically exploit this data. At present, only the companies that process the data benefit from the economic potential of the data,[60] while data subjects are constantly giving up their data in exchange for certain products and services that are wrongly advertised as 'free' (e.g., without monetary counter-performance on the part of the customer).[61] If data is the oil of the 21st century, all persons or entities involved in its production process should benefit from such participation.[62]

52. In terms of the development of data ownership, five options have been considered[63]: (1) ad hoc data ownership law, (2) data ownership law as a sub-category of intellectual property law, (3) data ownership law as something similar to sui generis database law, (4) using trade secret law, and (5) relying on the protection offered by contracts signed between the parties.[64] It has also been

---

exists (ergo, the data are used as counter-performance), and a company's denial of this (by advertising itself as free when it is not) justifies the imposition of substantial fines for misleading advertising or infringement of competition rules.

59 C. Pérez, *Revoluciones tecnológicas y capital financiero. La dinámica de las grandes burbujas financieras y las épocas de bonanza* (Buenos Aires: Siglo XXI Editores 2004), p 20.

60 K. Swinnen, 5. *Journal of Law, Property, and Society*, p 143.

61 A. de Franceschi, *La circolazione dei dati personali tra privacy e contratto*, p 85. The author laments that, despite the steady growth in the value of data, data subjects are not fully aware of this value, and act as if the digital contracts in which they give their data were actually free of charge (and not contracts with a counter-performance in the form of personal data or consent to the processing of personal data, which is the same thing).

62 J. Puyol Montero, *Aproximación jurídica y económica al Big Data* (Valencia: Tirant lo Blanch 2015), p 352; H. Zech, in *European Contract Law and the Digital Single Market*, p 76.

63 H. Zech, 'Building a European Data Economy – The European Commission´s Proposal for a Data Producer´s Right, 9. ZGE/IPJ (*Zeitschrift für Geistiges Eigentum – Intellectual Property Journal*) 2017, p (319) at 321; M. Becker, 'Rights in Data – Industry 4.0 and the IP Rights of the Future', 9. ZGE/IPJ (*Zeitschrift für Geistiges Eigentum – Intellectual Property Journal*) 2017, p (256) at 257.

64 S. Lohsse, R. Schulze & D. Staudenmayer, in *Trading Data in the Digital Economy: Legal Concepts and Tools*, p 20.

argued by some scholars that the rights conferred by the GDPR on the data subject constitute a set of rights similar to property law in that they combine traditional elements of property and intellectual property law.[65]

53. Starting from the general property law regime would have advantages and disadvantages. As advantages, it can be highlighted that it is based on a set of already known rules. As disadvantages, that this set of rules has important nuances in each legal system or group of legal systems; and that the already known set may not work equally well with new economic realities, as in the case of data. Generally speaking, the following default rules in favour of the right holder can be noted: (1) he can defend it erga omnes; (2) he can claim the object of ownership from whoever has it; (3) his right is not limited in time; (4) he can generate limited rights in rem at will; and (5) his creditors can attack the object on which the right of ownership rests.[66]

54. It does not seem reasonable to argue that data ownership should be considered as a new form of intellectual property.[67] It is true that data are information assets in the same way as immaterial goods. However, data do not have the component of creativity that is fundamental to any intellectual property work,[68] nor are they individualisable as we have already seen.

55. As far as protection through database law is concerned, data and databases are different realities, and must be regulated by different rights. The sui generis right of databases protects the investment and effort in the development of a database (classification criteria, search tools ...), whereas when we talk about data ownership, we do not necessarily refer to the data that are part of a database. Even in these cases, it is necessary to distinguish between the protection of the container that organizes the data (sui generis right of databases) and the data itself.[69]

56. Nor does trade secret law seem to be easily applicable to data. Most data are not secret and need not to be secret (even if they are not public data). The Trade Secrets Directive would only be partially applicable considering that (1) machine-generated data would hardly be considered a trade secret due to its low value as individual data and (2) that it is an implicit requirement of the Trade Secrets Directive to identify the information, which is difficult to fulfil in a big data context.[70] But above all, the fundamental reason for protecting a secret is precisely

65 See K. Swinnen, 5. *Journal of Law, Property, and Society*, p (147) at 148.

66 K. Swinnen, 5. *Journal of Law, Property, and Society*, p (149) at 150.

67 See also K. Swinnen, 5. *Journal of Law, Property, and Society*, p 151.

68 C. Wendehorst, 'The ALI-ELI Principles for a Data Economy', in A. de Franceschi & R. Schulze (eds), *Digital Revolution – New Challenges for Law* (München: C.H. Beck & Nomos 2019), p 50.

69 Leistner stresses that not all situations of 'proprietary use' of data involve heavy financial investment (M. Leistner, in *Trading Data in the Digital Economy: Legal Concepts and Tools*, p 27).

70 T. Aplin, in *Trading Data in the Digital Economy: Legal Concepts and Tools*, p (65) at 67.

that its secrecy is directly related to its potential economic value.[71] This is not the case for data understood as an economic asset.

57. Finally, there remains the option of developing an ad hoc data ownership right. This is, in our view, the most reasonable alternative since it allows to focus on the goals to be achieved rather than on the problems of adapting a previous regime.[72] It presents from the outset two challenges common to the ex novo development of any right: the delimitation of the powers and the identification of its owner(s). In the case of data ownership, we should add that it is not easy to select a prior paradigm to serve as a basis. In our view, the powers should respond to the current reality[73]: data is an economic asset that circulates both in specific markets (cooperation, sharing or exchange contracts) and through digital data exchange contracts, and where data serves as counter-performance in certain digital contracts.

58. Perhaps, if we take into account that data are electrical impulses (encoded machine-readable information) and that their characteristics do not allow for individualization, we could take electricity or fluid goods in general (water, natural gas, and electricity itself) as a base paradigm for a future development of data property law.

59. As regards the designation of a data owner, it is important to note a fact that gives rise to the right of ownership. For data ownership, one can argue for (1) the data owner's own behaviour,[74] (2) the use of certain data processing tools,[75] or (3) the interaction between the two facts (which would give rise to a situation of joint ownership) as a fact giving rise to the ownership. The latter option seems the most reasonable, as there is a clear interdependence between the data subject, who produces the data through his or her behaviour, and the developers of big data technology, who are responsible for making the raw data generated by these subjects available for processing and economic exploitation.

60. It is worth noting the difference between provided data, inferred data and observed data.[76] In all cases, these are personal data insofar as they relate to

---

71 Article 2.1.b Dir. 943/2016.

72 K. Swinnen, 5. *Journal of Law, Property, and Society*, p 152.

73 When taking into account the reality of how data work, the need for lawyers and policymakers to work closely with Information Technology (IT) specialists should not be forgotten (K. Swinnen, 5. *Journal of Law, Property, and Society*, p 165).

74 Not all data is generated from human behaviour on the internet. A clear example are machine-generated data, data created without the direct intervention of humans (K. Swinnen, 5. *Journal of Law, Property, and Society*, p 151).

75 In relation to this option, it should be noted that big data technology tools and IoT devices already have legal instruments to protect the investment in their development. In addition, the product obtained with the use of these tools should not be confused.

76 S. Cámara Lapuente, 'Resolución contractual y destino de los datos y contenidos generados por los usuarios de servicios digitales', in E. Arroyo Amayuelas & S. Cámara Lapuente (dirs.), *El derecho*

an identified or identifiable person (Article 4.1 GDPR). However, the rights of the data subject may differ slightly from one category to another. This issue should be taken into account in a possible development of the right to data ownership. For the time being, the differences between the data provided, observed and processed have had an impact on the right to data portability. According to the Working Party (WP2)9, the right to portability covers (1) data provided and created by the user and (2) data observed and collected by the service provider, but not (3) data subject to further processing that adds value to them (e.g., inferred data and personal profiling).[77]

61. In any case, the development of a data ownership right that responds to today's reality would have three important advantages: (1) it would promote legal certainty for the parties involved in the data economy, thus facilitating investments; (2) it would be a true reflection of the reality of the data economy (where data act de facto as goods in a property law sense); and (3) it would clearly determine who and to what extent benefits economically from the use of data, thus promoting a culture of transparency.

5. Data Inheritance

62. The term digital heritage has been used to describe different realities[78]: (1) the post mortem management of digital identity; (2) the criteria for the post mortem allocation of rights to digital goods and services[79]; and (3) the inheritance of data. The first of these meanings does not strictly correspond to the idea of inheritance, but is a sort of digital version of the post mortem protection of certain personality rights that may be affected when the subject's digital identity remains on the network after death.[80] The second meaning corresponds to the attribution of rights in respect of digital content and digital services contracted by a person who has died. Some countries have made specific provisions in this respect.

---

privado en el nuevo paradigma digital (Marcial Pons: Barcelona 2020), p (158) at 159; G. Malgieri, 'Property and (Intellectual) Ownership of Consumers´ Information: A New Taxonomy of Personal Data', 4. *PinG* (*Privacy in Germany*), 2016, p (133) at 149.

77 According to WP29, the latter category of data shall not be considered as having been provided by the data subject and therefore not falling within the scope of the right to data portability (WP29 'Guidelines on the right to data portability', Brussels 13 December 2016, p 10).

78 G. Resta, 'Digital Inheritance', in A. de Franceschi & R. Schulze (eds), *Digital Revolution – New Challenges for Law* (München: C.H. Beck & Nomos 2019), p (88) at 95; S. van Erp, 'Ownership of Digital Assets?', 5. *EPLJ* (*European Property Law Journal*) 2016, p (73) at 76.

79 J. C. Buitelaar, 'Post-mortem Privacy and Informational Self-Determination', 129. *Ethics Inf. Tecnol.* 2017, p (129) at 142.

80 In this regard, in Spain, G. Minero Alejandre, *La protección post mortem de los derechos al honor, intimidad y propia imagen y la tutela frente al uso de datos de carácter personal tras el fallecimiento* (Navarra: Aranzadi 2018).

63. The third meaning is the one that is of interest for the purposes of this article: is it possible to include specific provisions on data in the will, and can (or should) the data of a deceased person form part of his or her estate? If not, to whom does the data belong and what can be done with it?

64. These questions have to be supported by the above reflections: the ownership of data depends on the legal characteristics attributed to the data as property, and their transmission mortis causa depends on the characteristics of the right of ownership of the data. For example, data inheritance will have different characteristics depending on whether the data owner is (1) the data subject, (2) the developer of the big data technology, or (3) both together.[81]

65. The type of data involved (personal vs. non-personal; ordinary personal vs. special categories of data; genetic vs. other special data) will condition the possibilities for use of the data after the data subject's death. The latter assessment falls within the scope of personal data protection. In this regard, it should be noted that for the purposes of the GDPR, data of deceased persons are not personal data (as they are not persons), and this is recalled in Recital 27 of the GDPR when it states that the GDPR 'does not apply to personal data of deceased persons'.

66. Data of deceased persons can be very attractive in terms of economic use, especially as long as the attribution of rights to the data of deceased persons is not clear. As they are not personal data, the GDPR and national data protection rules do not apply to them. Only specific rules developed by states on data of deceased persons or other rules that are applicable on a case-by-case basis for different reasons are applicable to them. The economic potential of such data is almost similar to that of personal data (e.g., online consumer behaviour data by age and gender), but the compliance costs would be considerably lower. There are certain types of data whose characteristics complicate the problem somewhat more, such as health-related data, and especially genetic data. In these cases, it is more difficult to say that the data of a deceased person are no longer personal data to the extent that his (living) relatives may have identical genetic or health information.

67. It is important to distinguish between the criteria of post mortem transfer of rights to digital goods and services and data inheritance. There are multiple points of connection between the two aspects, which makes this point enormously complex. To this common complexity must be added the complexity arising from the different positions taken by EU Member States on Recital 27 of the GDPR and its national implementation.[82] This is an area that can only be described as

81 *Cfr.* G. Resta, in *Digital Revolution – New Challenges for Law*, p 89.

82 A complete overview of this problem can be found in K. Nemeth & J. Morais Carvalho, 'Digital Inheritance in the European Union', *EUCML (Journal of European Consumer and Market Law)* 2017, p 253; E. Harbinja, 'Digital Inheritance in the United Kingdom', *EUCML* 2017, p (253) at

problematic and will require in-depth discussion in the coming years. According to Öhman & Watson, between 1.4 and 4.9 billion Facebook users will die out by 2100, and those users will be from several countries. The authors stress that a purely commercial approach to data preservation poses significant ethical and political risks that require urgent reflection.[83] It should be added that personal profiles on social networks should be seen as rights to digital content and services, but are also directly related to post-mortem data processing.

6. Conclusions

68. As we have seen throughout these pages, the growth in the value of the data economy raises certain legal challenges that need to be addressed. Data (of any kind: personal or non-personal, raw data, inferred data or processed data) can and do function as commodities. However, regulating the 'economic asset' or commodity status of data in a standard can present certain difficulties.

69. First, if personal data are involved, one argument against considering data as commodities is that the protection of personal data is a fundamental right and that it is therefore not acceptable to qualify data as commodities. We have responded to this argument by pointing out that the acceptance of this reality (data function in practice as a commodity and as a counter-performance) does not question or endanger per se the protection of personal data; likewise, the economic use of privacy or one's own image does not question or endanger the protection of privacy or one's own image as a fundamental right.

70. On the other hand, certain personal data protection rules (Article 7 and Recitals 42 and 43 GDPR) and the way they are interpreted by data protection authorities (e.g., EDPS Opinion 4/2017 and EPDB Guidelines 5/2020) make it difficult or outright impossible to accept the economic flow of data, at least from a strictly normative point of view. In these pages we have proposed an alternative interpretation of Recitals 42 and 43 GDPR that would facilitate a coordination in this aspect of the logics of personal data protection and data economics.

71. Finally, the characteristics of data make it very difficult to qualify them as goods, which also makes it difficult to develop a right of ownership of data. The difficulties in developing a property right over data condition the possibilities of their transmission mortis causa as part of the estate, although in some countries there is already specific legislation on the post mortem processing of data.

256; A. Berlee, 'Digital inheritance in the Netherlands', *EUCML* 2017, p (256) at 260; M. O. Mackenrodt, 'Digital Inheritance in Germany', 1. *EUCML* 2018, p (41) at 48; B. Maeschaldaelck, 'Digital Inheritance in Belgium', *EUCML* 2018, p (37) at 41.

83 C. J. Öhman & D. Watson, 'Are the Dead Taking Over Facebook? A Big Data Approach to the Future of Death Online', BD&Soc (*Big Data & Society*) 2019, p (1) at 13.

72. It is true that the debate on the data economy is complex and that it will be difficult to develop a right to data ownership and to delimit its competences. Therefore, any call for caution is pertinent. However, caution should not be confused with inaction or lack of debate for fear of being wrong. The challenges discussed here need to be addressed in order to avoid two very dangerous situations from a legal point of view: (1) that personal data protection rules slow down the development of the data economy, or (2) that the development of the data economy forces certain obligations of data protection law to be ignored in practice.

This work was supported by PANELFIT, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

This article was first published in the EUROPEAN REVIEW OF PRIVATE LAW (Vol.29, Nr.5-2021, [807 – 830], 2021 © Kluwer Law International BV, The Netherlands).