IIC (2022) 53:917–949
https://doi.org/10.1007/s40319-022-01204-8

ARTICLE

Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data

Tommaso Fia

Accepted: 18 May 2022 / Published online: 23 June 2022

Abstract This article analyses how intellectual property rights (IPRs) affect access to non-personal data (NPD). In so doing, it homes in on a quasi-IPR, trade secrecy, and shows how applying it to NPD can lead to the overexpansion of IP protection. The risks of overprotection relate to the perpetuity of trade secret protection and the predominant interventions to correct market failure that scholars advance in order to restrict IPRs and quasi-IPRs. The paper then goes one step further to survey regulatory and interpretive solutions that could help to mitigate the risks of overprotection and make room for creating data access rules. Specifically, it explores two principles deriving from "physical" property theory that can be rejigged for the purpose: the *numerus clausus* of IPRs and the social function of intellectual property. Conceptualised in a novel fashion, these could steer legislatures and courts towards a restrictive understanding of IP forms and contain the propertisation of new intangibles, such as NPD aggregations.

Keywords Non-personal data · Trade secrets · Data governance · Data access · *Numerus clausus* of IPRs · Social function of IP

I would like to thank Janice Denoncourt, Peter Drahos, Jens Schovsbo and the two anonymous reviewers for their insightful comments on the earlier drafts of the paper. All errors are my own.

T. Fia (✉)
Ph.D. Researcher, Department of Law, European University Institute, Florence, Italy
e-mail: tommaso.fia@eui.eu

1 Introduction

Investigation of data and information ownership is no longer in its early infancy. Questions such as "Who is the data owner?" have attracted media coverage for some time now[1] and have raised major ethical dilemmas that academics struggle to face.[2] Moreover, the important issue of data ownership, being inherent to the growth of the digital economy, has caught the attention of policymakers and legal scholars. A laundry list of sub-questions, such as "What is data?", "What is ownership?", "What do we mean by property?", ensues.

The paper examines intellectual property rights (IPRs) in non-personal data (NPD) making up large-scale sets. "Big Data" is the conventional shorthand used here. Intellectual property rights impact both the collection and usage of datasets by "affect[ing] the ease of access to the data, despite its nonrivalrous nature".[3] To use the nomenclature with which economists are more familiar, they create barriers that curtail access to assets, determining "who can exploit a resource, who benefits and who loses".[4]

This analysis relies on several assumptions that circumscribe its scope. One first delimitation comes from how we conceptualise data. "Data" is a rather vague notion that should be treated carefully. For present purposes, it means any machine-readable syntactic digital element that is defined only by its representative characters (bits), regardless of its content.[5] Second, we need to understand what data is "non-personal". In this respect, the paper deals with data that does not fall under the GDPR definition of "personal data".[6] This limitation, albeit controversial,[7] is needed only to avoid investigating the intersections of intellectual property and data protection laws for present purposes. Third, the topic and the arguments presented here operate on the assumption that in the digital economy there is a need for

[1] Hern (2014), with regard to personal data.

[2] Most recently, in respect to personal data, Hummel et al. (2021).

[3] Rubinfeld and Gal (2017), p. 361.

[4] Drahos (1997), p. 201.

[5] *Cf.* Zech (2016a), p. 74. In this sense, *see* the legal definition of "data" that the Data Governance Act and the Data Act proposals adopt: "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording" (Commission "Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)" (Communication) COM (2020) 767 final, Art. 2(1); Commission "Proposal for a Regulation of the European Parliament and of the Council on European on harmonised rules on fair access to and use of data (Data Act)" (Communication) COM (2022) 68 final, Art. 2(1)).

[6] "Personal data" means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, Art. 4(1). Hereinafter the "GDPR".

[7] Purtova (2018); Graef et al. (2020).

opening up access to data and furthering data sharing practices.[8] Intellectual property rights, forming an access barrier, can stand in the way of these objectives. Data collectors can restrict access for "non-owners" that do not have access to data – e.g. a public authority, a small business, a researcher, etc. For a matter-of-fact illustration, let's imagine a digital company (a technology provider) and city authorities cooperating on a smart city project. The technology provider is commissioned to implement a smart waste management solution that harvests data of diverse typologies (e.g. bin load, bin location, and so forth). To protect the data it stores, it will most likely adopt technical and contractual measures. In the absence of a clear provision on the matter in their agreement, the digital company can deny the city authorities access to these datasets, claiming they are trade secrets.[9] The city authorities will then have little choice but to negotiate a new agreement. Otherwise, they will not be able to access data that they might intend to reuse for (other) public purposes. Likewise, competitors, unless they can replicate the data,[10] would not be able to access datasets that the provider collects, for example in order to repurpose the data and enter a secondary market (e.g. manufacturing of rubbish bin gears). By the same token, a national train operator can temporarily obtain a precautionary injunction blocking access to publicly available data on the train ride status, since it amounts to the extraction of "substantial parts of a database" under EU database rights.[11]

The article analyses how IPRs, and specifically a quasi-IPR (trade secrecy), affect access to NPD.[12] In so doing, it homes in on the specific case of trade secrecy and how applying it to NPD might lead to overprotection. The prevailing understanding of access-enhancing solutions pivots on competition law and policy interventions that aim to resolve specific market failures. The paper goes one step further to survey regulatory and interpretive solutions that could help to mitigate the risks of overprotection. The remainder of the paper continues over three sections. Section 2 sets the scene by outlining recent developments in the history of IPRs and quasi-

[8] *See*, *inter alia* and across diverse sectors and subjects, Drexl et al. (2016); Mayer-Schönberger and Ramge (2018); Atkinson (2019); Fia (2021). The most comprehensive and thorough contribution to date is German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos 2021).

[9] As shown below, that is exactly the case in *Lyft Inc v. City of Seattle*. If the former can prove making an investment to arrange data in databanks, it can gain the database *sui generis* right protection as well.

[10] Rubinfeld and Gal (2017), pp. 350–351.

[11] In July 2019, the Italian train operator Trenitalia sued the British company GoBright Media Ltd. to obtain a precautionary injunction in order to block access to real-time train status data available on the app that GoBright Media had developed. The app "scraped" off data made available by Trenitalia on the Viaggiatreno portal, despite there being no agreement between the two companies. The Rome District Court issued the injunction, blocking the app's access on the grounds that the app accessed the portal about 800,000 times per day, which qualified as a "substantial part" of the database (*see* Art. 7(1) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20). Later on, the same Court quashed the injunction, since the number of times the British business accessed the Viaggiotreno portal could not be considered as extracting a substantial part of the database (*see* Judgment of Rome District Court, 5 September 2019). Moreover, the Court underscored that any user could lawfully extract non-substantial amounts of data from the Viaggiatreno portal, since the maker of the database deliberately intended to make it accessible to the public. *See* Ciani Sciolla (2021), pp. 205–206.

[12] On what I mean by "quasi-IPRs", *see infra* note 36 and Sect. 3 below.

IPRs. It explains how and why IP can stretch all the way to massive sets of NPD. Proprietary overexpansion to NPD follows from the long-standing evolution of a highly protectionist legal system. Once the bigger picture has been drawn, I move on in Sect. 3 to scrutinise one instance of this overexpansion, i.e. the intersection between trade secrecy and NPD. As will be seen, trade secrecy is one of the most flexible forms of (quasi-)proprietary protection for data that actualises the issues of overprotection. The latter are worsened by the perpetuity of trade secrecy. To shape data governance across different actors, further interpretive and regulatory routes can reduce the impact of the IP system on NPD. Therefore, Sect. 4 explores how intellectual property rights can be "resisted" (i.e. restricted) in the light of the need to open up data access.[13] In doing so, it delineates two principles deriving from (physical) property theory: the *numerus clausus* ("fixed number") of IPRs, and the social function of intellectual property. The former, I argue, can restrict IP forms if it is construed as a fixed list of standards with fixed rationales and objectives. Thus conceptualised, it can steer legislatures and courts towards a restrictive understanding of IP forms and contain the propertisation of new intangibles, such as NPD aggregations. The social function doctrine construed as a meta-regulatory tool incorporating the interests of non-owners (e.g. small companies, consumers, researchers, and city authorities) in the balancing of opposing fundamental rights can also serve as an alternative to steer the judiciary and the legislature towards restricting IPRs in NPD. Making these more fit for the IP realm (and specifically for trade secret protection) in the data economy might mitigate proprietary overexpansion to NPD and leave more room for data access. Section 5 gives a conclusion.

2 Data: The Latest Direction of a Highly Protectionist Trend

There are similarities and differences between physical property and intangible intellectual property. What they have in common is that they both single out legal constructs governing the allocation of wealth in human societies.[14] They are "relations between individuals",[15] amounting to forms of private sovereignty[16] over things.[17] Typically, intellectual property laws confer monopolies on something

[13] *See supra* note 8.

[14] Gambaro (2009).

[15] Drahos (2016), p. 1.

[16] *Ibid*., pp. 171 *et seq*.

[17] In civil law systems, things as legal objects are frequently referred to as "goods". There are several definitions of "goods". Under Italian law, goods are "the things that can be objects of rights" (Italian Civil Code, Art. 810); in German law, the term "good" (*Sache*) only indicates material objects, which are part of the broad genus of *Rechtsobjekte*. In light of the traditional civilian distinction, goods can be tangible or intangible. The former encompass corporeal resources which are objects of property rights, being *erga omnes* (or rights *in rem*), that is "against the world" (*see* van Erp (2017), p. 236.). In common law systems, property rights are allocated to whoever has the "better title": "if a person in her relation with another person has the stronger right to an object" (*ibid*., p. 236.), then she has a property right in a thing. Intangibles as a conceptual object of property, on the other hand, were first theorised by the German jurist Josef Kohler and include intellectual creations, such as inventions, distinctive signs and creative works. Their legal protection mostly consists in monopolies for exploiting a good. *See*, further, Peukert (2021), pp. 126–128.

intangible that stems from human ingenuity ("abstract objects"). Real property and personal property laws, on the other hand, establish rights in material goods, such as chattels and land. The borderline between the two proprietary macrocosms has been nearly uncontested since time immemorial.[18]

Sorting out the objects of property and those of intellectual property is rather simple. What is more challenging, however, is to ascertain which intangibles attain legal protection. Intellectual property, quite unlike property, has been in a transient state with regard to its core areas for many years now, particularly since the advances in digital technologies dating back to the 1980s. Traditionally, the core areas of IP have been trade marks, patents, copyright, and design rights. More nebulous as to their proprietary nature are trade secrets[19] and unfair competition. In recent decades, the scope of intellectual property rights has increased dramatically, to stretch far beyond the original range of application.[20] Some have argued that IP has drifted into a highly protectionist regime,[21] leading to proprietary overprotection. Proprietorial expansion follows the process of hoarding immaterial resources that previously belonged to the public domain. Thus conceived, today's IP standards have largely become "the product of the global strategies of a relatively small number of companies and business organisations that realised the value of intellectual property sooner than anyone else".[22] Being formed this way, the IP legal framework frequently fails to provide the public with the results of innovative activities.[23]

The last chapter of IP, the hyper-protectionism story, concerns data. Data in digital format, unlike knowledge, is a good that can perfectly well be excluded according to economic theory. As Hess and Ostrom put it with respect to information, "[t]hese technologies have generated greater access […] while at the same time enabling profit-oriented firms to extract value from resources previously held in common and to establish property rights".[24]

Quite unlike in the 1990s and early 2000s, what is at stake here is intellectual property rights not in well-arranged databases,[25] but in unstructured aggregations of data. The success of technologies such as Big Data, the Internet of Things (IoT), and

[18] Smart gadgets, however, put property and intellectual property in conflict with each other in novel ways. *See*, *inter alia*, Fairfield (2017).

[19] On the quasi-IP nature of trade secrets, *see* Sect. 3 below.

[20] Beckerman-Rodau (2010), p. 88. This is the case, for instance, of the audiovisual rights in sports events in some EU Member States (*e.g.* Italy) and the *sui generis* right in databases (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20 (Database Directive).

[21] Today's high level of protectionism stems from the process of globalisation of intellectual property on the basis of international agreements, such as TRIPS (1994). *See* Drahos (1997); Sell (2003).

[22] Drahos and Braithwaite (2002), p. ix. *See also*, in respect of the negative effects of IP on science, Drahos (2020).

[23] Zukerfeld (2017); Drahos (2020); Drahos (2021), p. 59. *See also* the thorough analysis in Boldrin and Levine (2008).

[24] Hess and Ostrom (2003), p. 112.

[25] The Database Directive defines a database as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Art. 1(2)).

artificial intelligence (AI) hinges on harnessing large-scale datasets (such as those stored in non-relational databases)[26] from which programmers extract valuable information through powerful algorithms. Data that makes up massive digital aggregations is typically a raw meaningless component when it is produced. Therefore, not only is it a by-product of other activities, but it has also become a basic "recorded abstraction of the world" resulting from the transformation of all aspects of reality into data ("datafication").[27] In most applications, it has become an infrastructure that makes any kind of activity, good or service possible.[28] Data dependency then goes through processes of data appropriation[29] and propertisation, making reliance on massive datasets a matter of survival in global markets. IP standards contribute to this cause, for they form the basis of and formalise the relationship between individuals and social aggregations in their proprietorial endeavours. By taking this to the extreme, Haggart argues that they open the door to a "'neo-feudal' global economy, with IP (and data) owners ensconced at the top".[30] Thus, novel challenges for intellectual property ensue in today's "datafied" world. If any component of reality is computable and convertible into data, then a widespread proprietary architecture is a plausible future. If we open the way for IPRs and quasi-IPRs in respect of data, it is striking how most data elements can virtually turn into something eligible for protection.[31]

Some empirical evidence can pinpoint the problems of a proprietorial data ecosystem. Today, a company can quite easily rely on trade secrecy or database rights to protect NPD by referring to such protection schemes within the terms and conditions of a given data-driven service. Even though the protection does not meet the legal requirements, it will usually take some time before a non-owner that does not have access to NPD (typically a smaller competitor, a newcomer, a public authority, or a weaker contractual counterparty) can obtain judicial redress. The actors with little or no bargaining power at all will most likely abstain from getting involved in costly and endless lawsuits. One may also think, for example, of data collected by smart agriculture machinery, which is routinely transferred to product manufacturers "using copyright and licensing agreements to control the data collected by their products' software".[32] Smart car data[33] and, more generally, IoT data[34] suffer a similar proprietorial fate. Similarly, "cleansing" or anonymising

[26] Unlike RDBMS databases (or "relational databases"), NoSQL databases (also known as "non-relational") can store large quantities of data that are not put in a structured and relational order. Gervais provides a thorough explanation in this respect. *See* Gervais (2019), pp. 8–9.

[27] Sadowski (2019), p. 2.

[28] Ducuing (2020); Fia (2021), pp. 201–204.

[29] In Hess's and Ostrom's wording, propertisation of data and information is an "intellectual land-grab" (Hess and Ostrom (2003), p. 112).

[30] Haggart (2018), p. 184.

[31] *See* Drexl (2021a, b), p. 222, arguing that "data ownership legislation would recognise ownership in any encoded information without any additional substantive requirements".

[32] Tusikov (2019), p. 127. *See also* Fairfield (2017).

[33] Perzanowski and Schultz (2016), pp. 146–148; Drexl (2018).

[34] Noto La Diega (2022).

research data may amount to imbuing that dataset with copyrightable expression,[35] and so preventing reuse by others.

After outlining the issues related to IP and quasi-IP overexpansion to NPD, the following section zooms in on the application of trade secrecy to NPD to show the status of data propertisation in practice.

3 Trade Secret Protection of Non-Personal Data in the EU: Features and Overprotection Issues

Thus far, numerous legal scholars have investigated whether and how IP and quasi-IP[36] rights (i.e. copyright, *sui generis* database rights, trade secrets, and patents) apply to NPD.[37] Other jurists have proposed creating a data producer's right in NPD to enhance the allocation of NPD as a tradeable commodity.[38] For present purposes, I will home in on the form of quasi-IP protection that can easily stretch to NPD, that is trade secrecy.[39] Not coincidentally, this has been deemed "the most important legal instrument for protecting data exclusivity".[40]

Litigation concerning trade secrecy and large-scale datasets is still in its infancy though. To date, no judgment has dealt precisely with the protection of massive data aggregations as a trade secret in the EU. In the US, *Lyft Inc v. City of Seattle*,[41] a case filed with the Washington Supreme Court, recently shed light on the challenges of using trade secret protection to prevent data access. By contrast, at great length secondary sources dwell on how trade secrecy can apply to large-scale datasets. In the following sub-section, I will draw on the doctrinal debate to determine to what extent trade secrecy extends to NPD. Subsequently, I will move on to analysing the problems of overprotection and provide some empirical evidence of these by expanding on *Lyft*.

[35] Mattioli (2018), p. 145.

[36] By "quasi-IP rights" – Ricolfi (2019) used this particularly fitting expression – I mean trade secrets and those forms of exclusivity whose proprietary nature is controversial. *See* Sect. 3 below.

[37] The literature on the topic is vast. The more significant contributions encompass, in chronological order of publication date, Drexl et al. (2016); Zech (2016a); Zech (2016b); Drexl (2017); Farkas (2017); Ottolia (2017), pp. 3–149; Wiebe (2017); Zimmer (2017); Boerding et al. (2018); Ciani (2018); Determann (2018); Hilty (2018); Hugenholtz (2018); Krönke (2018); Mattioli (2018); Ritter and Mayer (2018); Scassa (2018); Thouvenin et al. (2018); Tjong Tjin Tai (2018); Gervais (2019); Sappa (2019); Banterle (2020); Corrales Compagnucci (2020), pp. 19–49; Montagnani (2020); Weber and Eggen (2020); Drexl (2021a, b).

[38] This is the solution proposed by Zech (2016a) and considered by the Commission. Numerous authors have opposed his viewpoint: Drexl et al. (2016); Kerber (2016); Drexl (2017); Hugenholtz (2018). *See also* the thorough scrutiny in Yu (2019); Stepanov (2020).

[39] I am mindful of the fact that copyright and patent laws afford some degree of protection for NPD too, as multiple authors cited *supra* in note 37 have concluded. I nonetheless leave them aside, as the analysis, albeit informative, would not add any more substance to the following sections.

[40] Zech (2021), p. 72.

[41] *Lyft Inc. v. City of Seattle* 94026-6 (WA 2018).

3.1 Trade Secrecy and Non-Personal Data: A Closer Look

The traditional role of trade secret protection is to complement other IPRs,[42] since it aims to safeguard business integrity from the misappropriation of valuable confidential information, rather than encourage information holders to keep it secret.[43] At the international level, trade secret protection is established by Art. 39 of the TRIPS Agreement. In the EU, it has recently been harmonised under the Trade Secrets Directive (TSD).[44] The majority of legal scholars posit that it does not confer a property-like exclusive right (such as the "formal" intellectual property standards), but is more akin to unfair competition or tort law.[45] Other scholars, however, disagree with this conceptualisation, making it clear that trade secrets are instead (or should be viewed as) a genuine IP right, underscoring the advantages[46] and the disadvantages[47] of this approach. Other commentators rightly maintain that trade secrecy is "quasi-IP", meaning that it is an atypical mesh of liability rules and property rules,[48] making it akin to both typical IP standard forms and unfair competition. The TSD embraces the latter regime by providing both injunctions and compensatory mechanisms to preserve trade secrecy.[49]

Leaving the nature of trade secrecy aside, we should see whether it can easily stretch to NPD gathered in large-scale sets. To ascertain this, we need to determine (i) whether NPD gathered in large-scale sets falls within the definition of "trade secret" under Art. 2(1) TSD, and (ii) who is the "trade secret holder" under Art. 2(2) TSD.

3.1.1 Definition of "Trade Secret" and Non-Personal Data

The TSD refers to trade secrets as "information". This wording might suggest that "data", being something "less" than information, is left out. Some legal scholars, in fact, have employed the distinction between the semantic layers (i.e. data as information conveying a meaning) and the syntactic layers (i.e. data as sequences of zeros and ones) to ascertain whether data falls within the purview of the TSD. Zech and Drexl maintain that the legal definition applies to the semantic level.[50] Data aggregations as a syntactic whole, especially if they are not organised or processed

[42] Arcidiacono (2016), p. 1074.

[43] Determann (2018), p. 15.

[44] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (Trade Secrets Directive).

[45] Sappa (2019), p. 410; Determann (2018), p. 15; Schovsbo et al. (2020), p. 17. Some jurists maintain that a trade secret is rather similar to the notion of possession in private law (Zech (2016a), p. 63; Banterle (2020), p. 211).

[46] Among the US law scholars, *see* Graves (2007); Lemley (2008).

[47] Ghidini (2010), pp. 57–59, focusing on Italian law before the harmonised legislation under the Trade Secrets Directive.

[48] Ottolia (2017), pp. 47–51; Ricolfi (2017), p. 223.

[49] Ottolia (2017), pp. 49–51.

[50] Zech (2016b), p. 465; Drexl (2018), p. 92.

in any way, may seem to fall outside the scope of the EU legislation.[51] In many cases, however, the data masses embody information that doubtless qualifies as a trade secret, since the threshold for information to be considered eligible for trade secret protection is virtually non-existent.[52] Thus, keeping data and information apart would be a rather difficult and artificial task,[53] as the Commission appears to acknowledge as well.[54] Not only must information within the scope of trade secrecy be related to business activities, but also pretty much any kind of information that a firm can produce in the course of its corporate activities falls within the ambit, including connected device data and data resulting from analytics processes.[55] Moreover, as Noto La Diega and Sappa maintain in respect of IoT data, "[e]ven if the Trade Secrets Directive does not expressly refer to data resulting from a machine-to-machine process, an extensive interpretation of this text, which includes them in the protectable subject matter together with data generated in other and more traditional ways, has to be followed".[56]

In sum, pretty much all data aggregates that contain and represent (semantic) information fall within the scope of the TSD. That said, we now need to see if NPD amounts to protectable "information" according to the definitional specifics of the TSD. Trade secrecy protects information that meets three prerequisites: (i) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (ii) it has commercial value because it is secret; and (iii) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[57]

Secrecy is not an absolute criterion, but a relative and functional one.[58] This means that parties can share information without destroying its secret status, as long as they do not publicly disclose it but only transfer it from one storage system to another. For instance, this is the case for confidentiality agreements that bind cloud service providers.[59] Similarly, according to Ottolia, the following events do not destroy secrecy: (i) releasing portions of information that do not provide knowledge advantages; (ii) structuring and arranging a dataset in a different fashion, where the structure and arrangement have economic value; or (iii) unlawfully opening up access to datasets for which secrecy can be restored by means of injunctions.[60] Other legal authors maintain that the secrecy criterion depends on how a holder

[51] In this sense, Nordberg (2020), p. 202. More specifically, she distinguishes between pre-processed raw data, which is eligible for trade secret protection, and unprocessed data, which is not.

[52] Drexl (2018), p. 92.

[53] Surblytė-Namavičienė (2020), pp. 60–61.

[54] Commission (2017b), p. 20.

[55] Zech (2016b), p. 465; Drexl (2018), pp. 92–93.

[56] Noto La Diega and Sappa (2020), p. 440.

[57] Trade Secrets Directive, Art. 2(1).

[58] Ottolia (2017), p. 53; Surblytė-Namavičienė (2020), pp. 73–74.

[59] Sandeen (2014); Surblytė-Namavičienė (2020), p. 75.

[60] Ottolia (2017), pp. 53–54.

collects data. Determann and Drexl argue that data produced by sensors in IoT environments (e.g. cars, tractors, thermostats) is not secret, since smart devices collect and store data that is "generated and displayed in plain sight, depriving such information of secrecy".[61] Similarly, data harvested by a smart car on a freely accessible road can be collected by cars of diverse manufacturers, and thus cannot meet the secrecy prerequisite.[62] This interpretation, however, revolves around the fact that (semantic) information in the public domain is not secret and is out there, "up for grabs", so to speak. Secrecy of data, being a recorded abstraction of this information, is nevertheless another thing. As shown in the foregoing, data can be kept secret by means of contractual and technical measures. Hence, it can meet the requirements of Art. 2(1) TSD even if its source is information "in full sight".

The second prerequisite is the commercial value that is connected with keeping information secret. Recital 14 of the TSD stipulates that commercial (or economic) value can be either actual or potential. Protecting potential economic value establishes quite a high protection threshold that is built not on the (positive) effect that another actor (e.g. a competitor) can gain from information misappropriation, but on the "likelihood of harm that could be suffered by a trade secret holder".[63] In short, the TSD construes the economic value requirement through the lens of the trade secret holders themselves. Thus defined, it turns into the competitive advantage that stems from keeping information secret.[64] In Big Data applications, any dataset can virtually amount to a competitive advantage for an information holder. Even unstructured NPD may have potential commercial value and therefore can meet the requirement. This seems to downplay the fact that single data elements[65] or raw data[66] are left out of the subject matter since they amount to "trivial information".[67] It is very unlikely that an individual item of data interests the data stakeholders of the data value chain. Moreover, it is not clear what constitutes an individual (syntactic) item of data in practice. This depends on what one considers to form a data element, but there is no common agreement on this. For example, a data element can be just a zero-one sequence. But how long should the zero-one sequence be to qualify as a single data element? It is then problematic to ascertain what a data element is. More importantly, the scope of the trade secret definition does not preclude data combinations and aggregations from protection.

The third requirement concerns the reasonable steps a holder must take to keep information secret. As for massive datasets, holders routinely rely on contractual

[61] Determann (2018), p. 16. *See also* Drexl et al. (2016), p. 7; Drexl (2017), p. 269; Farkas (2017), p. 23; *cf.* Ottolia (2017), pp. 52 *et seq.*; Sappa (2019), p. 415.

[62] Drexl (2017), p. 269.

[63] Surblytė-Namavičienė (2020), p. 84.

[64] *Ibid.*, p. 84.

[65] Drexl (2017), p. 269; Surblytė-Namavičienė (2020), pp. 61–62. *See also* Noto La Diega and Sappa (2020), p. 440. *cf.* Wiebe (2017), p. 65; Zech (2016a), p. 63.

[66] Nordberg (2020), p. 202.

[67] Trade Secrets Directive, Recital 14 reads: "[t]he definition of trade secret excludes *trivial information* and the experience and skills gained by employees in the normal course of their employment, and also excludes information which is generally known among, or is readily accessible to, persons within the circles that normally deal with the kind of information in question" (emphasis added).

agreements and technical measures (e.g. encryption) to avoid data diffusion. Trade secrets can thus safeguard data and information against unfair practices of employees, contractors, and any other market player with which companies are involved (e.g. unauthorised copy of an entire dataset).[68] As stated above, erecting contractual and technical barriers amounts to taking "reasonable steps," making trade secrecy easy to gain in respect of NPD aggregations.

3.1.2 Trade Secret Holders in Data-Driven Applications

A substantial part of the legal scholarship has underscored the issue of identifying the trade secret holder under Art. 2(2) TSD when it comes to large-scale datasets. It is virtually impossible to single out one rightholder when data is generated and exchanged by networks of companies.[69] Specifically, identifying one holder results in considerable uncertainty in data pools and interconnected smart devices (for example, manufacturers and users of a smart device or machine; or contractors, providers and users of an AI system).[70] As Drexl puts it, "it is not necessarily clear whether the manufacturer exercising de facto control over the data or the user of the device, physically possessing and operating the device, is controlling the trade secret in this sense. Yet another possibility would be to consider both persons as co-holders of the trade secret".[71] Article 2(2) TSD, however, defines the trade secret holder as "any natural or legal person lawfully controlling a trade secret". Unlike a formulation such as the "trade secret owner", the "holder" notion can encompass not only the first entity protecting information as a secret, but also the subsequent persons that (lawfully) have access to the information (e.g. licensees). In the absence of specific case law on the matter, the broad notion seems to enable joint data control that is protected by trade secrecy and involves multiple contractual parties voluntarily sharing data. There can be issues nevertheless in respect to cases where contractual measures between the parties do not govern data-related rights and obligations (for example, which company can retain data, and which company must delete it).

3.1.3 Interim Conclusion

Trade secrecy is a flexible form of quasi-IP protection that can easily apply to NPD. The vast majority of data aggregations can qualify as trade secrets under Art. 2(1) TSD. Single data elements may be left out, but this does not prevent companies from accessing trade secrecy because it is difficult to determine what qualifies as a "data element". Moreover, it is very unlikely that they are interested in individual items of data. That said, singling out the trade secret holder presents a conundrum when contractual measures do not regulate the data-related rights and obligations in

[68] Sappa (2019), p. 414; Wiebe and Schur (2019), p. 819.

[69] Drexl (2017), p. 269.

[70] Leistner (2021), p. 234.

[71] Drexl (2018), p. 95.

networks of businesses. Multiple firms can then qualify as joint trade secret holders if they contribute to creating sets of NPD.

3.2 Problems of Overprotection: Theory and Practice

In the foregoing we have seen that trade secrecy is flexible and adaptive to ever-changing data-driven technologies. The previous section has shown that businesses can quite easily harness trade secrecy to protect large-scale datasets. That said, we should look into how trade secret protection of NPD impacts the data economy. The problems of overprotection concern the very ambit of trade secrecy.

One first set of issues associated with it concerns transparency and public oversight of corporate activities. A thorough study by Kapczynski has cast light on the transformation of US trade secret law into a significant driver for corporate power. Specifically, it enables firms to consider almost any information that they hold as a trade secret, "empower[ing] [them] to keep important information about their commercial products and services secret, and to obscure information about benefits that corporations receive from government".[72] In practice, US trade secret protection stretches to nearly any type of data aggregation, including (among NPD illustrations) data about the source and processing of toxic waste, information about water and energy use that Google needed to collect to build a novel data hub in North Carolina, and information held by Uber and Lyft about zip codes of drop-offs and pick-ups.[73] The extension of trade secrecy to all these settings may mean that "claims to property in information and data come into conflict with what the public needs to know to govern itself" if corporations' risky products and practices involving vast aggregations of data are kept secret. The same gamut of issues concerns EU trade secret legislation. Viewed through the lens of an activity designed to balance fundamental rights, the rights and interests of trade secret holders come into conflict with other actors' rights and interests when it comes to fostering algorithmic fairness, transparency, and accountability.[74]

A second source of problems impacts the dynamics of competition and, more generally, the position of weaker actors in the data markets. Trade secrecy may form the basis of exploitative conduct by businesses that prevents others from accessing data. In this case, the businesses are simply not willing to exchange data, in order to preserve a competitive advantage in the markets.[75] When there are "unique data access points" in data markets,[76] trade secrecy can thus amount to an insurmountable advantage that actors with limited bargaining power (most typically, small companies or local public entities) cannot overcome. This has motivated the EU Commission to propose the Data Act, which purports to open up data access while restricting the boundaries of trade secrecy.[77] Some key features of trade secrecy

[72] Kapczynski (2022), p. 1371.

[73] Kapczynski (2022), pp. 1372–1373.

[74] Scalzini (2022), pp. 351–352; Maggiolino (2018), pp. 199 *et seq.*

[75] Scalzini (2022), pp. 352–353, Kapczynski (2022), p. 1377 (footnote).

[76] Rubinfeld and Gal (2017), pp. 350–351.

[77] *See* Sect. 4.3 below.

compound the problems of overprotection. Unlike other IP standards, trade secret protection is perpetual.[78] The longer items of information are kept secret, the longer they are afforded with protection. Accordingly, a trade secret holder (or a few holders) can just retain datasets and avoid sharing without any time limit so long as "reasonable measures" to exclusively control data are put in place. Thus defined, trade secrecy stands in the way of access to data categories that lose value over time, such as real-time data, or cannot be easily replicated in future.

We have seen above that the TSD came into force in 2016. Unsurprisingly, there is no EU case-law regarding trade secrecy and its application to large-scale processing practices. A US case, *Lyft Inc v. City of Seattle*,[79] is a useful illustration of the aforementioned problems. Lyft Inc and Rasier LLC (an Uber subsidiary) carry out data-driven transportation services in Seattle.[80] In 2014, in the light of mediation amongst the city, Lyft, Rasier, and the taxi and for-hire stakeholders, Lyft and Rasier were supposed to submit quarterly standardised reports to Seattle encompassing various data categories (e.g. the total number of rides, the percentage of rides for each zip code, pick-up and drop-off zip codes, and so forth). Lyft and Rasier objected by raising confidentiality concerns connected with transferring data to the municipal authorities. The city administration had implemented appropriate technical and organisational measures to prevent data losses and unintentional disclosure. Lyft and Rasier nevertheless insisted that quarterly zip code reports consisted of trade secrets protected by the Uniform Trade Secrets Act (UTSA). In 2016, a Texan resident filed a request under the Public Records Act (PRA) to access reports made up of data from late 2015. The municipality of Seattle warned him that those reports were deemed confidential by Lyft and Rasier, while seeking an injunction under the PRA to obtain access to the requested reports. The King County Superior Court, however, issued a permanent injunction preventing said reports from being disclosed, maintaining that the zip code reports were trade secrets under the UTSA. Eventually, the Washington Supreme Court overturned this decision, granting access to the reports. According to the court, the latter qualified as "public records" even if they were trade secrets. Their disclosure can be prevented only if "disclosure would clearly not be in the public interest, and would substantially and irreparably damage a person or a vital government interest".[81]

Some lessons can be learnt from *Lyft* by checking the problems of overprotection against the case findings. First, even though the court eventually ruled in favour of the municipal authorities, it took a while before the latter could access datasets collected by the private providers. Trade secrecy perpetuity made it impossible for the city administration to access data. Time-sensitiveness, however, is essential to getting valuable insights out of datasets, e.g. elaborating urban policies based on data reuse. This suggests that regulatory tools other than *ex post* interventions such as antitrust law remedies (Art. 102 TFEU)[82] might complement the existing

[78] Noto La Diega (2022).

[79] *Lyft Inc. v. City of Seattle* 94026-6 (WA 2018).

[80] Malone (2020).

[81] *Lyft Inc. v. City of Seattle* 94026-6 (WA 2018).

[82] On the "essential facility doctrine" as a way of opening up access to NPD *see* Fia (2021), pp. 195–198.

framework by focusing on less time-consuming procedures, as we will see further below.[83] Access-restricting conduct, moreover, frustrated the municipality's attempts to pursue the public interest. This shows that reflecting on how to restrict IP and quasi-IP rights in issues connected to data governance involves going beyond considerations of competition law and policy. When it comes to governing data flows across different stakeholders of the data economy, there are multiple rights and interests involved that antitrust laws alone cannot encapsulate. For these very reasons, coupling competition policy with further regulatory and interpretive tools as explored below might offer novel grounds for discussion.

4 Herding IPCats: Stemming the Tide of Intellectual Property Through Property Theory

Section 3 has shown that trade secrecy does provide some protection for NPD. As much as other access barriers, it can prevent different actors (e.g. public authorities, non-profit organisations, competitors, and so forth) from making use of datasets held by trade secret holders. In Sect. 2, we also saw that IP and quasi-IP expansion to NPD might curtail access to data.[84,85] An exploration of alternative solutions, therefore, ought to find regulatory and interpretive tools that make more room for data access. A viable strategy, I would argue, entails looking for solutions that restrict the ambit of IP and quasi-IP forms to a more circumscribed set of cases.

Hence, in the subsequent sub-sections I address a rather functional question: "Bearing in mind the risks of IP and quasi-IP overprotection of NPD, how can IP and quasi-IP forms be restricted for this purpose?". In this sense, looking into the IP exceptions and limitations to apply to our case is a well-trodden path in the legal literature.[86] These studies are certainly thought-provoking, but they neglect an element on which I intend to concentrate below: the regulatory and interpretive principles capable of informing lawmakers and judiciaries. Finding appropriate regulatory and interpretive impetus, I would argue, is much more vital in the data economy. The law just cannot keep pace with data-driven technologies. As Fairfield puts it, we need legal narratives that can increase the speed at which laws can be adopted[87] instead of rule-based and sector-specific approaches. Thus, narratives for different interpretations of existing laws[88] can play a more crucial role than targeted rules, which can quickly go awry and ultimately fail to resist proprietary overprotection. IP and quasi-IP laws need tools that make them sufficiently flexible with regard to ever-changing technologies.

[83] *See* Sect. 4.3.

[84] One of the best-known blogs on intellectual property law is called "The IPKat" http://ipkitten.blogspot.com accessed 23 January 2021. Hence the borrowing and use of the idiomatic phrase in the section title.

[85] *See supra* note 8.

[86] *See*, *inter alia*, Geiger et al. (2018); Gervais (2019), pp. 10–14.

[87] Fairfield (2021), pp. 82–83.

[88] *See* Mattei and Quarta (2018), p. 31, speaking of "counterhegemonic interpretations of existing property laws".

In the rest of the section, I delineate two regulatory principles that can help to restrict the IP and quasi-IP legal framework. One is the *numerus clausus* principle of IPRs. This posits a closed number of IP and quasi-IP standards. Its justiciability can prevent legislatures and courts from extending IP forms to intangibles that fall short of IP laws' rationales and fixed objectives. The second is the social function of intellectual property. Understanding it as a balance of rights that takes proper account of non-owners' interests can revitalise its salience. Its main addressees, we will see, would be the judiciary. The two principles are analysed in turn. Subsequently, I check their feasibility against EU trade secret protection.

4.1 *Numerus Clausus* Principle for IPRs (Pursuing Fixed Objectives and Rationales)

The ever-expanding nature of intellectual property reveals another difference with physical property. In civil law and (to a lesser degree) common law jurisdictions, property is systematised according to the *numerus clausus* ("closed number") principle. The origins of this date back to ancient history. In Roman law, it was never codified in the legislation, but was applied in practice as a way of ensuring legal certainty for third parties.[89] In doing so, it held a meta-regulatory[90] status because it restrained the *dominium* [ownership and control of property] as a powerful exclusionary protection applying to all third parties. Romans were concerned with the consequences of ownership on wider society.

In contemporary law, the *numerus clausus* means that property rights are confined to a closed inventory of allowable forms.[91] Historically, this "fixed list" has found at least three justifications.[92] First, in civil systems it stands as a bulwark against the dissolution of the unitary concept of ownership, whereby as a default rule property rights in things must be allotted to an individual owner rather than split into fractional rights shared among two or more people.[93] Second, some legal literature has seen the *numerus clausus* as a tool for "optimal standardisation" of property rights[94] by lowering the costs of investigating them. To put it concisely, a closed number of types standardises property burdens and drives down information costs for potential purchasers and tortfeasors, "who need to know which rights in relation to things are property rights, because of their potential tort liability for interfering with property rights".[95] Third, other commentators have cast light on the "democratic" dimension of the *numerus clausus* principle of property law. This has to do with the fact that "the inherently public quality of property rights justifies substantive and procedural limits on the creation of new property forms. New

[89] Akkermans (2008), p. 55.

[90] For a definition of meta-regulation *see* further below in this sub-section.

[91] Clarke (2020), p. 242. On the *numerus clausus* principle in property law, *see*, *inter alia*, Merrill and Smith (2000); Di Robilant (2014).

[92] Clarke (2020), pp. 251–253.

[93] Hansmann and Kraakman (2002), p. 375. *See also* Resta (2010), pp. 23–24.

[94] In this respect, *see* Merrill and Smith (2000).

[95] Clarke (2020), p. 252.

property forms must reflect values the collectivity approves of and must be ratified through democratic processes".[96]

Hence the conclusion that the *numerus clausus* does not prevent new property forms, such as the "common goods" (*beni comuni*) in Italy and the Community Land Trust (CLT) in the US, Australia, New Zealand, and Belgium,[97] from bourgeoning. It operates instead as a threshold for legitimising novel property standards according to the collectivity's input.

In the realm of intellectual property, the *numerus clausus* takes on a meaning that somewhat mirrors the "democratic" dimension of the *numerus clausus* of physical property, so to speak. It pertains to how IPRs breed artificially scarce environments. Patents and copyright are not things of the physical world, but legal creations (read: artificial monopolies) aimed to incentivise corporate innovation. Legislatures and courts across the world are aware of the distortive potential of legitimising monopolies in abstract concepts. Thus, the *numerus clausus* doctrine aims to confine intellectual property to a handful of fixed standards,[98] thus limiting the default rule of economic freedom in the form of free flow of ideas and knowledge.[99] It is the legislature's job to "put IP in order", directing its evolution in such a way as to prevent overexpansion at the expense of other constitutional rights and liberties.[100] The *numerus clausus* of intellectual property, therefore, ensues from the principle of separation of powers, whereby allocative choices are the responsibility of democratically elected legislatures.[101] Hence, not all practices for appropriating immaterial assets are worthy of protection – only those meeting the needs of market failures that legislatures redress by creating an IP standard.

In the area of intellectual property, however, the *numerus clausus* is "probably at its weakest"[102] or "essentially non-existent".[103] There are at least three reasons why the principle has not been seen at work in the realm of intangibles. First, it only applies to "primary" rights (the IP standards, such as copyright, trade marks, and patents), not to "economic" rights (i.e. pecuniary interests, or "fractioned" rights) in intangible entities.[104] Economic rights are routinely transferred by means of contractual agreements (e.g. licences), irrespective of whether an underlying primary right exists. Private arrangements form a texture of iterative social norms of data appropriation.[105] (Exclusive) licence agreements virtually turn into ownership gridlocks, for private autonomy has no real limits.[106]

[96] Di Robilant (2014), p. 400.

[97] On the CLT, *see* generally Vercellone (2020).

[98] Mezzanotte (2015), pp. 200–201.

[99] Ghidini (2010), p. 17.

[100] Mezzanotte (2015), p. 275.

[101] Resta (2010), pp. 25–26.

[102] Merrill and Smith (2000), p. 19.

[103] Mulligan (2013), p. 235.

[104] Ubertazzi (2014), pp. 187–188; Resta (2010), pp. 74–75; Mezzanotte (2015), pp. 191 *et seq.*

[105] Contractual arrangements form a *de facto* exclusive layer over data, which is somehow more worrying than IP protection. Factual exclusivity is analysed more thoroughly in Fia (2021). *See also* Fairfield (2017).

[106] Mezzanotte (2015), pp. 236–238.

Second, the courts and even (regulatory) private actors[107] restrain the formal rigour of the *numerus clausus* of IP forms as well. Today, legal systems are not limited to domestic legislation. Sources of international law, supranational law (such as EU law), transnational law (such as the *lex mercatoria*), and soft law (e.g. codes of conduct, commercial practices) tend to be in addition to, and even prevail over, national "law-as-command" instruments. This has particularly been the case since intellectual property entered the "global" era in the 1990s.[108] Hence, new forms of exclusive rights in abstract objects proliferate. Their recognition mostly involves the courts. The latter operate on the assumption that exclusivity is the optimal governance mode of any form of intangible. So, for example, they are prone in Italy to recognise IPRs in novel incorporeal goods, such as the depictions of other tangibles or intangibles.[109] At times, courts even endorse the customary propertising efforts of private (regulatory) bodies: one may think of the code of conduct of the advertising industry in Italy.[110] Overall, in both civil law and common law jurisdictions the judiciary has lost sight of the original meaning of the *numerus clausus* as a way of containing the consequences of ownership for society in general.

Third, the legislators less frequently transpose the entrenched hermeneutic routes of the courts into law. Legitimisation of new IPRs mostly occurs in a "disguised" fashion, that is by extending the scope of standard forms or lowering the threshold of proprietary protection.[111] IP extension to computer programmes, TV formats and domain names illustrates this.

Despite its original potential, the principle of *numerus clausus* of IPRs as it is understood today does not have sufficient force to counter the overexpansion of IP. A reconsideration of its role may nevertheless render it a well-functioning principle in today's data economy. First, there is a need for reinstating the original meta-regulatory significance of the *numerus clausus* as a component of the right of intellectual property (Art. 17(2) of the Charter of Fundamental Rights of the European Union, CFREU).[112] Meta-regulation means finding governance modes of other forms of regulation.[113] The *numerus clausus* pertains to how governance of intangibles ought to work. In this sense, a "fixed number" of IP and quasi-IP standards would encourage courts to adopt more restrictive approaches to

[107] I refer to actors' promulgation of codes of conduct, legal customs, private regulations and so forth.

[108] Drahos (1997).

[109] *See* the thorough analysis in respect to the case-law of the Italian Supreme Court (*Corte Suprema di Cassazione*) in Mezzanotte (2015), pp. 215–222.

[110] For instance, Art. 13 of the Italian Advertising Self-regulation Code (*Codice dell'Autodisciplina Pubblicitaria*), a private arrangement furnished with "legal personality" (*personalità giuridica*) under Italian law, protects advertising ideas from misappropriation. The Italian Supreme Court maintained that this provision amounted to unfair competition and could affect not only liability rules, but also property rules (Cass. civ., sez. I, 15 febbraio 1999, no. 1259). *See ibid*., pp. 211–213.

[111] Resta (2010), p. 31.

[112] Charter of Fundamental Rights of the European Union [2012] OJ C-326/391. Hereinafter, the "CFREU".

[113] Parker (2007), p. 211. Legal scholars have mostly explored meta-regulation as a governance mode that holds companies accountable for implementing corporate management processes ("self-regulation"). *See*, *inter alia*, Ayres and Braithwaite (1992); Grabosky (1995); Parker (2002); Parker et al. (2004), pp. 6–7. Here "meta-regulation" has a broader meaning stretching beyond corporate applications.

recognising IPRs, since the latter are just one of many ways of governing abstract objects. Hence, the judiciaries would have to consider data governance modes (such as shared and "open" management based on use rights)[114] that they frequently neglect by taking IPRs as the default rule.[115]

Second, regulators and courts should view the *numerus clausus* as an inventory of IP and quasi IP-forms attached to definite *rationales* and pursuing *objectives* for which those IP standards have been designed.[116] This stems from the fact that legal provisions are anchored in doctrines and rationales that give grounds for their existence and functioning in empirical and pragmatic terms. By contrast, the very normative foundations of intellectual property seem to have an identity crisis when it comes to protecting data in the data economy. Today, the strength of the typical IP rationales, such as the "fairness", "personhood" and "welfare" theories of intellectual property,[117] seems to be faltering under the pressure of features of the data economy. IP fairness doctrines are based on the natural law consideration that individuals have a natural right to the fruits of their creations and discoveries. Personhood theories of IP are grounded in the fact that intellectual assets display and express authors' personalities. Welfare theories see IPRs as legal constructs that address the underproduction of public goods by offering an incentive for their creation. All such theories have lost their traction in data-intensive environments to some extent. It is problematic to argue along Lockean lines[118] that natural law can justify data production as property, as the same data routinely stems from different producers. Similarly, the assumptions and implications of personhood theories, that is the strong link between creative works and their author's personality, simply fades away in data production contexts as there is no such connection. The utilitarian arguments of the welfare theories (i.e. the creation incentive) do not apply to IP in today's world, where informational assets (such as data) are produced at near-zero marginal cost.[119] More practically, the proposed rendition of the IP "closed number" would thus require explaining the application of IP forms according to rationales that show the objectives that their protection pursues. As Fairfield notes, the most effective rules governing technology should be "humble", "tak[ing] one case at a time, one issue at a time", since

> … rules divorced from lived experience or the actual context that caused humans to think those rules were a good idea turn bad quickly … In fact, keeping a rule humble, tied to its origins and context, without immediately

[114] Drahos (2006).

[115] Mezzanotte (2015), p. 214.

[116] Such a consideration was already clear to Ricketson (1992) in the Nineties. *See also* Drahos (2016), pp. 260 *et seq*., arguing in favour of an "instrumentalist" approach to intellectual property anchored in the original objectives rationalising IP standards.

[117] *See* generally Fisher (2001), pp. 168 *et seq*.; Drahos (2016), and Fisher's detailed overview at http://ccb.ff6.mwp.accessdomain.com/Maps/IPTheories.html. Accessed 14 March 2021.

[118] *See* generally Attas (2008).

[119] Lemley (2015); Ricolfi (2021).

generalizing it, may enable us to act quickly without destabilizing other areas of law.[120]

Thus conceptualised, the novel *numerus clausus* of IPRs could have two practical implications. First, allocating property rights in abstract things would become the primary job of legislatures.[121] Hence the conclusion that any novel proprietary form should undergo a legislative process and be backed up only by definite rationales and objectives. Legislatures would encompass national and supranational legislators such as the EU, which gathers different stakeholders in the decision-making process through public consultations.[122] Forging exclusive rights by means of international trade agreements, therefore, may also increase the bottom-up participation of consumers, end users, and activists. Second, being circumscribed within their rationales and objectives, IP standards cannot stretch to new intangibles by means of judicial interpretations solely grasping at exclusivity as the default rule. Moreover, legal analogical reasoning would need to be linked to a given IP rationale and objective for granting protection. In doing so, the *numerus clausus* could steer courts towards denying protection to new intangibles that do not meet the prerequisites of the IPR fixed list, such as NPD.

I will now summarise the proposed understanding of the *numerus clausus* principle of IPRs with fixed objectives and rationales. The "closed number" of IP forms has a democratic core. In the data economy, it could be used to ratchet down the trend to consider property as the "natural" governance mode of intangibles. To do so, the *numerus clausus* of IPRs should be designed as a fixed number of IP and quasi-IP forms attached to rationales and pursuing fixed objectives. Thus articulated, a closed number could prevent exclusive rights from stretching to data and other immaterial assets that do not meet the original IP protection goals. So, on the one hand, the main regulatory forum for allocating new incorporeal rights would be the legislature. On the other hand, courts and other non-legislative actors would have to refrain from creating or recognising proprietary iterations, unless they could account for an underlying objective and rationale for which the IP form was designed.[123] They would be required to fall in line with the meta-regulatory nucleus of the *numerus clausus* of IPRs.

[120] Fairfield (2021), p. 77. Fairfield does not refer to IP laws; more generally, he argues that the law must be human, humble, experimental, iterative, diverse, and viral to keep up with technology.

[121] Conversely, Noto La Diega and Sappa maintain that the principle of non-discrimination calls for extensive interpretations of the Trade Secrets Directive. Accordingly, trade secrets may stretch to machine-generated data. *See* Noto La Diega and Sappa (2020), p. 440, and, more generally, Peukert (2015).

[122] In fact, the results of the public consultation on the Commission Communication "Building the European Data Economy" COM (2017) 9 final, which had been held between 10 January 2017 and 26 April 2017, showed that most respondents rejected the proposal for a new data producer's right on non-personal data. *See* Commission (2017a).

[123] *Cf.* Mezzanotte (2015), p. 224, maintaining that the application of IP forms should be grounded on specific constitutional principles and liberties.

4.2 Bringing the Social Function of Intellectual Property Back to Life

A second force for restricting intellectual property lies in valuing its social function. The social function of law conjures up philosophical ideas dating back to Thomas Aquinas.[124] In the early 1900s, legal scholars with diverse backgrounds, such as Josserand, Duguit, Kohler and von Gierke, applied the social function principle to property rights.[125] Their scholarship shared a critical view of private property as a bourgeois absolute right, with no limitations on owners' sole and despotic dominion over their assets. These scholars maintain that property rights should, on the contrary "have their share of social responsibility"[126] and entailed obligations for owners. The principle then served as a foundational basis to constitutionalise the limitations, "for the public good", on the right to property, especially in Germany and Italy,[127] as well as in the European Convention on Human Rights (ECHR).[128] Within the EU secondary legislation, the social function doctrine has stretched even beyond the field of property rights and turned into an essential component of how different fundamental rights are balanced.[129] Some legal scholars have recently turned their attention to delineating the principle in the realm of intellectual property.[130]

The social function doctrine of property law revolves around the consideration that rights can clash with one another. Thus, there is a need for a fair balance of opposing rights and interests. As Geiger puts it,

> [b]alance is the key concept that lies behind the social function. If law is a question of balance, there cannot be an "absolute" right that can be exercised in a totally selfish manner with no consideration for the consequences that this exercise involves, but only rights that are "relativised" by the rights of others and the wellbeing of the community.[131]

The key to weighing and balancing rights is to draw boundary lines for how they are laid out in the legislation. This turns into considering the general interest as the lodestar for exercising property rights. Overall, the rights of property and intellectual property

[124] Geiger (2013), p. 157.

[125] *Ibid*., pp. 159–162; Mattei (2015), p. 111.

[126] Mattei (2000), p. 31.

[127] Sganga (2018), pp. 195–209. *See*, employing diverse wordings, Art. 14(2) of the *Grundgesetz* (German Basic Law) and Art. 42(2) of the Italian Constitution. *See also* other domestic Constitutions, such as Art. 48(2) of the Croatian Constitution, Art. 30(1)(2) of the Macedonian Constitution, and Arts. 33(2) and 128(1) of the Spanish Constitution.

[128] First Protocol, Art. 1(2).

[129] *Inter alia*, Recital 4 of the GDPR reads: "[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its *function in society* and be balanced against other fundamental rights, in accordance with the principle of proportionality" (emphasis added by the author).

[130] Geiger (2013); Sganga (2018), pp. 191–232. Ottolia argues against employing the social function as a legal means to include public interest considerations in the balancing of IPRs against other rights and interests: Ottolia (2010), pp. 143–146.

[131] Geiger (2013), pp. 157–158.

"can be restricted in order to safeguard the public interest"[132] according to the "principle of proportionality" of Art. 52(1) of the CFREU.[133] In this sense, the CJEU has, since the 1970s, employed the social function doctrine to limit property rights, in order to build up the European single market.[134] More recently, the social function has turned into a "general clause" limitation to deal with general interest issues that Member States and the EU as a whole address as public policy matters, such as security, public health and environmental protection.[135] In *Sky Österreich*, the CJEU went even further, seeing the social function as a limitation on freedom to conduct business, in order to counterbalance freedom of the press.[136] Thus defined, the social function is a flexible concept that not only serves a market-correcting function, but can also redress any imbalance in proprietary and non-proprietary interests.[137]

Influenced by European Court of Human Rights (ECtHR) jurisprudence, the CJEU has used fair balancing to offset the author's exclusive rights (copyright) against users' rights in the digital realm. In the judgments *Scarlet Extended v. SABAM*[138] and *SABAM v. Netlog*,[139] the Court viewed the (opposing) fundamental rights (specifically, freedom of expression and information as established by Art. 11 CFREU) as the lodestar for this balancing act. The prevailing understanding of the social function of IPRs has more recently come to encapsulate fair balancing in the exceptions and limitations established by national and EU secondary legislation. The CJEU cases *Pelham*,[140] *Funke Medien*[141] and *Spiegel Online*[142] are illustrations of this tendency. In these decisions, the CJEU emphasised that the domestic courts of EU Member States could not rely on the rights established in the CFREU to derogate from an author's exclusive rights when an exception or a limitation did not apply. In short, the exceptions and limitations of copyright "internalise" the balancing act between different rights and interests.[143] By contrast, fundamental rights cannot serve as an external limitation of copyright protection. Thus conceptualised, the Court's view seems to reiterate the leading position of "rights

[132] Geiger C, *Reconceptualizing the Constitutional Dimension of Intellectual Property – An Update*, Center for International Intellectual Property Studies Research Paper No. 2019-11, 2019, p. 28.

[133] In the CFREU (Art. 17(1)(2)) and ECHR (Protocol 1, Art. 1) formulations, however, the social function is not mentioned as a limitation of the owner's prerogatives and rights. *See* Quarta (2016), p. 102.

[134] Marella (2013), p. 561.

[135] *Ibid*., pp. 561–562, mentioning Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v. Council and Commission* [2008] ECR I-06351; Joined Cases C-379/08 and C-380/08 *ERG and Others* [2010] ECR I-02007; Case C-504/04 *Agrarproduktion Staebelow GmbH v. Landrat des Landkreises Bad Doberan* [2006] ECR I-00679.

[136] Case C-283/11 *Sky Österreich GmbH v. Österreichischer Rundfunk* [2013] ECLI:EU:C:2013:28, para. 45.

[137] *See*, in respect of real property (particularly the CLT), Vercellone (2020), pp. 77–78.

[138] Case C-70/10, *Scarlet Extended v. SABAM*, ECLI:EU:C:2011:771.

[139] Case C-360/10, *SABAM v. Netlog*, ECLI:EU:C:2012:85.

[140] Case C-476/17, *Pelham GmbH and Others v. Ralf Hütter and Florian Schneider-Esleben*, ECLI:EU:C:2019:624.

[141] Case C-469/17, *Funke Medien NRW GmbH v. Bundesrepublik Deutschland*, ECLI:EU:C:2019:623.

[142] Case C-516/17, *Spiegel Online GmbH v. Volker Beck*, ECLI:EU:C:2019:625.

[143] Schwemer and Schovsbo (2020), p. 385.

holders at the top and users' interest below".[144] As Schwemer and Schovsbo assert, "even though the Court apparently accepts that sometimes conflicts between IPR and fundamental rights may occur, one should – when within the copyright system – assume that priority has been given to the exclusionary powers of rights holders at the immediate expense of users".[145] Hence the conclusion that pre-emptively excluding external limits of copyright law may well pose challenges when the internal limitations (read: the exceptions and limitations stipulated by EU secondary legislation) fall short of "ensuring full compliance with the European [freedom of expression] standards".[146] This is a likely scenario when it comes to technological developments that make certain exceptions or limitations obsolete.

A novel understanding of the social function of IPRs can redress the imbalances in IP owners' and non-owners' interests and rights. Being adaptable, the social function can be a suitable tool for driving down the *dominium* of IP owners over non-personal data. As with the *numerus clausus*, its meta-regulatory capability is promising. Under this perspective, the social function of intellectual property would require courts and legislatures not only to balance rights against one another, but also to consider the interests of non-owners as the lodestar for this balancing act. This stems from the fact that (intellectual) property rights can be envisaged to be "non-equal rights". IP allocation is not a neutral choice, but rather a distributive equity matter[147] that has to consider the needs of those whose rights and interests are left aside.[148] Hence, control over data by means of IPRs can be re-decentralised[149] by restricting the ambit of intellectual property itself. To illustrate this, it is from this perspective that a farmer, a small company or a researcher can seek judicial redress for an agreement that allocates IPRs in data to a conglomerate with stronger bargaining power. On a similar note, city authorities can see proprietary protection of urban mobility data collected by private providers restricted.[150]

We can summarise our conceptualisation of the social function of intellectual property as follows. Fostering the social function of IPRs amounts to making them fit for the interests not only of rightholders, but also of a wide number of beneficiaries that have limited bargaining power and are interested in keeping data out of IP enclosures (e.g. small companies, researchers, public authorities, non-profit organisations). In this sense, the lodestar for balancing rights against one another is constituted by the interests and rights of non-owners. Thus, putting the social function doctrine to work can contain the rights of IP owners in NPD. An effective restricting exercise lies in the way in which IPRs are balanced against other fundamental rights in the light of the interests of non-owners. Yet it remains to

[144] *Ibid*., p. 386.

[145] *Ibid*., p. 386.

[146] Geiger and Izyumenko (2020), p. 302.

[147] *See*, *inter alia*, Bracha and Syed (2014), pp. 287 *et seq.*; Drahos (2016), p. 199.

[148] *Cf.* Quarta (2016), p. 281.

[149] *Cf.* Ricolfi (2021).

[150] Frosio (2020); Priora and Sganga (2020).

be examined which other fundamental rights of non-owners can offset IPRs in both judicial and legislative contexts.

The most obvious one may be freedom of expression and information (Art. 10 ECHR; Art. 11 CFREU). Data, we have seen, is nothing but a tiny piece of information. As Hugenholtz notes, freedom of expression and information stands in the way of recognising property rights in data, for the notion of information encompasses syntactic data and commercial speech as well. In his words,

> [f]rom this perspective, data and information must flow freely, uninhibited by property rights or other state-created restrictions, unless a compelling societal need for protection ("necessary in a democratic society") can be established. Freedom of expression and information, in other words, makes IP rights in data the exception to the default rule of freedom.[151]

Freedom of information can serve the needs of multiple categories, such as journalists, urban communities, and researchers, as well as municipal authorities and small companies – individuals and organisations interested in seeing IP protection driven down. It is noteworthy that the TSD provides for an exception to the trade secret protection where the "use or disclosure of the trade secret was carried out […] (a) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media".[152] Access to the "intangible components" of a smart device, such as the data produced, can therefore be placed on such a legal footing.[153]

Second, freedom of scientific research is another force to counterbalance intellectual property rights. NPD is the raw material of research activities; however, companies and public bodies routinely refuse to provide access to their stored datasets to research institutions. There is a burgeoning literature exploring the relationship between science, human rights, and intellectual property.[154] In the EU, Art. 13 CFREU requires that academic research be "free of constraint". Restrictions to freedom of research activities are possible, but, under Art. 52(1) CFREU, are "subject to a strict standard of review".[155] Now, there is no denying that intellectual property is included in these restrictions, but "hard questions can be asked regarding whether the balance struck by existing [IPRs] does justice to the values of academic and research freedom".[156] Today's data-intensive research environments call for restricting intellectual property laws that apply to data to make full use of data-mining techniques.[157] *A fortiori*, IPRs in NPD hardly prevail over freedom of

[151] Hugenholtz (2018), pp. 66–67.

[152] Trade Secrets Directive, Art. 5(a).

[153] Noto La Diega (2022).

[154] Drahos (2020), pp. 336 *et seq*.; Geiger (2013).

[155] Lock (2019), Article 13, p. 2141.

[156] Barendt (2010), p. 215.

[157] Reichman and Okediji (2012), pp. 1368 *et seq*. The proposed Digital Services Act moves towards creating researcher rights of access to data held by very large online platforms (*see* Commission "Proposal for a Regulation of the European and Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (Communication) COM (2020) 825 final, Art. 31(2)).

academic research. Such a line of reasoning filters through the text and data mining (TDM) exception in the DSM Directive.[158] The latter nevertheless ends up creating a secondary market for TDM practices that fall into the hands of private publishers, which are "well aware that their publishing portfolios have informational value beyond the published articles they have aggregated".[159] By contrast, a hermeneutical tool such as the social function can reverse the trend by empowering researchers to restrict IPRs in data held by large publishers in judicial proceedings and by directing the national and EU legislatures towards recognising freedom of academic research as prevailing over IPRs.

Third, freedom of services as established in the Treaties can counterbalance the overexpansion of IPRs in NPD.[160] In its 2017 Communication, the European Commission has construed this freedom as a "principle of free movement of data within the EU",[161] as already established in respect of personal data.[162]

4.3 Practical Consequences of the Proposed Theories for EU Trade Secret Law and Interplay with EU Secondary Legislation

At this stage of the analysis, one question arises: How can we relate the theoretical framework that has been sketched out to the central theme of this paper, i.e. EU legal protection of trade secrets? Both the *numerus clausus* of IPRs and the social function of intellectual property as conceptualised above can prove useful.

The *numerus clausus* of IPRs can be seen in action in restricting the extension of trade secrecy to NPD. Trade secrets have been designed to safeguard valuable business and workplace information, giving a competitive advantage and protection from misappropriation. Thus conceived, they relate to the know-how type of information in the TRIPS Agreement formulation (Art. 39) and the TSD. The latter explicitly enumerates clear examples in this respect.[163] One can think of customer lists, information on suppliers, business plans, formulas for products and market research and strategies. However, one may retort that NPD aggregations, in contrast, fall outside the rationales and goals that motivated the EU legislator to promulgate the TSD. Syntactic data does not amount to valuable information taking on a straightforward meaning, unless one synthesises and analyses it by means of complex analytics processes.[164] Non-processed and raw NPD, therefore, would be excluded from trade secret protection in the light of the *numerus clausus* principle.

[158] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 (DSM Directive), Arts. 3 and 4.

[159] Hugenholtz (2019).

[160] Hugenholtz (2018), p. 68.

[161] COM (2017) 9 final, 7. The same reflections permeate the proposal for a Data Governance Act.

[162] GDPR, Art. 1(3).

[163] Trade Secrets Directive, Recital 2.

[164] *Cf.* COM (2020) 767 final, 12, stating that "the re-use of data, which *may* contain trade secrets, should take place without prejudice to Directive (EU) 2016/943" (Recital 7 of the proposed Data Governance Act; emphasis added by the author). Hence the conclusion that data does not always meet the trade secrecy prerequisites.

In seeking to elaborate an answer in respect of the social function of intellectual property, two caveats are worth noting before proceeding. First, the TSD establishes a suite of exceptions to trade secrecy, aiming to offset opposing rights and interests, pretty much as the social function sets out to do. Specifically, Art. 5 reads:

> Member States shall ensure that an application for the measures, procedures and remedies provided for in this Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases: (a) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media; (b) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest; (c) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise; (d) for the purpose of protecting a legitimate interest recognised by Union or national law.

As Schovsbo maintains, this provision does not, strictly speaking, refer to predetermined "exceptions", but to obligations for EU Member States to "ensure that an application for the measures, procedures and remedies provided for in the [TSD] is dismissed in any of the listed cases".[165] Aplin argues that the wording of Art. 5 may be an "instruction to judicial authorities of Member States to interpret existing provisions in the light of article 5"[166] instead. To transpose this provision into domestic law, Member States have nevertheless been given much leeway. Different approaches have thus been adopted,[167] the consequence being that the national legislations have followed highly divergent paths of implementation, and the associated risk of legal uncertainty with regard to EU legal systems has arisen.[168] Moreover, some specific challenges concern the exceptions of Art. 5 that might come in handy to counter overprotection. The exception for freedom of expression or information (Art. 5(a)) might require an "unjustified" restriction of the rights in question, if viewed through the lens of ECtHR case law.[169] By the same token, the legitimate interest exception (Art. 5(d)) may leave unresolved the question of what a legitimate interest is and how the balancing act would operate in such settings.[170]

Second, nothing prevents the CJEU from extending the internalisation processes of the balancing act that we have seen above in respect of copyright law cases to other IPRs and quasi-IPRs, such as trade secrets.[171] The detrimental effects of internalisation may specifically circumscribe the balancing act to the realm of

[165] Schovsbo (2020), p. 18.

[166] Aplin (2021), p. 188.

[167] Aplin (2021), pp. 188–189.

[168] Scalzini (2022), p. 350.

[169] Aplin (2021), p. 190.

[170] Aplin (2021), pp. 192–193.

[171] Noto La Diega (2022).

freedom of expression and information (Art 5(a)). This would mean that the TSD provides a major limitation to offsetting other fundamental rights. However, Recital 21 bodes fairly well as it opens the way to a broader balancing act:

> [i]n line with the principle of proportionality, measures, procedures and remedies intended to protect trade secrets should be tailored to meet the objective of a smooth-functioning internal market for research and innovation, in particular by deterring the unlawful acquisition, use and disclosure of a trade secret. Such tailoring of measures, procedures and remedies should not jeopardise or undermine fundamental rights and freedoms or the public interest, such as public safety, consumer protection, public health and environmental protection, and should be without prejudice to the mobility of workers.

The proposed view of the social function of intellectual property may offer guidance in filling in the blanks of the TSD seen above. Viewing the interests and rights of non-owners as the lodestar for the balancing act may well help to flesh out the exceptions enshrined in Art. 5 and bridge the legislative gaps, with specific regard to the exceptions of Art. 5(a) and (d) and the wording of Recital 21. A broader assortment of fundamental rights and interests, such as those mentioned in the previous sub-section, would strengthen the position of non-owners as opposed to the trade secret holders in the balancing act. Moreover, the social function of IP would provide a fresher set of tools to provide a basis for data access where competition law and policy are of little help, and redistributive equity needs to be restored. To be sure, antitrust aims to find effective *ex post* remedies to economic dominance that can help in the data economy. It deals with the market effects of an undertaking's (or several undertakings') conduct. Such considerations are nevertheless less helpful when we look at the data life-cycle as an ecosystem gathering actors that pursue interests other than business optimisation and welfare maximisation. One may take public institutions and non-profit organisations as examples of actors that do not necessarily pursue these objectives. For example, with regard to Art. 102 TFEU, Drexl points out that

> [i]t is to be noted that the new-product rule would also exclude application of competition law to public entities that seek access to data in the public interest where these entities do not engage in any economic activity in the sense of the concept of an undertaking under EU competition law.[172]

Reflections of competition policy and law thus provide a basis for data governance in the form of a set of remedies that resolve well-defined market failures. To cite Drexl again, "[a]s regards data access regimes, the question will therefore be what market failures and what interests will justify a deviation from exclusivity".[173] By looking at non-owners' fundamental rights and interests, the legislature and the judiciary can in fact even more effectively limit the overexpansion of trade secrecy when it comes to issues such as data-driven

[172] Drexl (2017), p. 284.

[173] Drexl (2021b), p. 21.

exploitative and exclusionary practices and algorithmic fairness. On the legislative front, the proposed Data Act is moving in this direction by mandating the disclosure of trade secrets when a smart device user requests access to data generated by the product, as long as "all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties".[174]

5 Conclusion

This article has examined the intersection between IP and quasi-IP rights and NPD by homing in on the most important legal means for protecting data exclusivity, i.e. trade secrecy.[175] It then explored the regulatory and interpretive tools that may help to overcome issues of overprotection when it comes to imposing limitations on access to NPD, with specific regard to those associated with trade secrecy. Section 2 showed that the path towards IP overprotection of novel intangibles such as NPD has been followed for quite some time. The overexpansion of IP is the linchpin of a highly protectionist system. Because of the "datafication" of reality, IPRs and quasi-IPRs can virtually stretch to any data aggregation. Section 3 then examined how EU trade secrecy legislation applies to NPD. Specifically, businesses can easily apply trade secrecy to protect troves of NPD by implementing confidentiality agreements and technical measures (e.g. encryption). As *Lyft* demonstrates, applying trade secrecy to NPD combinations can create issues of overprotection, related mainly to data-driven exclusionary conduct in the data markets and lack of algorithm transparency. The perpetuity of trade secret protection exacerbates these issues even further.

Against this background, I have delineated ways of resisting IPRs in respect of data. Such a reflection, we have seen, amounts to coming up with regulatory and interpretive solutions that can complement competition policy. Accordingly, Sect. 4 delineated two meta-regulatory principles that, mostly drawing on physical property theory, could restrict the ambit of IPRs and thus mitigate proprietary "spill-over" into NPD. First, clawing back a *numerus clausus* of IPRs could steer courts and legislatures towards a more restrictive understanding of IP forms and contain the propertisation of new intangibles, such as NPD aggregations. IP and quasi-IP forms would amount to a fixed list of standards explained by clear rationales and pursuing fixed original objectives. Extending and allocating IPRs and quasi-IPRs would require national legislators and supranational regulators to identify those rationales and objectives. By contrast, courts would be left out of the legitimisation of new IP forms unless they could demonstrate that a rationale and objective for protection applied. Second, the social function doctrine, construed as a meta-regulatory tool focusing on the interests of non-owners (e.g. small companies, researchers, journalists, public authorities, and non-profit organisations) within the balancing act between opposing fundamental rights, could serve as an alternative, to direct the judiciary and the legislature towards restricting IPRs in respect of NPD. For this

[174] Proposal for a Data Act, Art. 4(3). *See* similarly Arts. 5(8) and 19(2).

[175] Zech (2021), p. 72.

purpose, fundamental rights such as freedom of information and expression, freedom of academic research, freedom to conduct business and freedom of services are the most suitable principles to offset IPRs. I then checked the proposed theories against the issue of the overexpansion of trade secrecy. Specifically, a *numerus clausus* of IPRs with fixed objectives and rationales might stem the tide of the trade secret protection of syntactic data aggregations. Even more fundamentally, the social function of IP would help to interpret the exceptions enshrined in Art. 5 TSD so as to consider a broad assortment of non-owner fundamental rights and interests as a counterbalance to trade secrecy. This would complement competition law and policy tools, which may well leave public entities and non-profit organisations aside when weighing and balancing the interests of data stakeholders.

The paper has aimed to investigate the premises of an intellectual property system fit for data access rules. Further research should now move on to study how to make access rules a reality. The proposed Data Act is a promising starting point in this respect, as we have seen. Overall, the framework that I have explored here is in its early stages. The next steps in this direction will of course be even more challenging.

Funding Open access funding provided by European University Institute - Fiesole within the CRUI-CARE Agreement.

References

Akkermans B (2008) The principle of numerus clausus in european property law. DPhil thesis, Maastricht University 2008. https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/1386614/guid-9388e80c-c577-4c74-a99b-0e27439bd792-ASSET1.0.pdf. Accessed 13 Feb 2022

Aplin T (2021) The limits of EU trade secret protection. In: Sandeen S, Rademacher C, Ohly A (eds) Research handbook on information law and governance. Edward Elgar, Cheltenham

Arcidiacono D (2016) The trade secrets directive in the international legal framework. Eur Pap 1:1073–1085. https://doi.org/10.15166/2499-8249/83

Atkinson, RD (2019) IP protection in the data economy: getting the balance right on 13 critical issues. Information Technology & Innovation Foundation (ITIF) Report. https://www2.itif.org/2019-ip-protection-data-economy.pdf. Accessed 13 Feb 2022

Attas D (2008) Lockean justifications of intellectual property. In: Gosseries A, Marciano A, Strowel A (eds) Intellectual property and theories of justice. Palgrave Macmillan, London, pp 29–56

Ayres I, Braithwaite J (1992) Responsive regulation: transcending the deregulation debate. Oxford University Press, Oxford

Banterle F (2020) Data ownership in the data economy: a European dilemma. In: Synodinou T-E, Jougleux P, Markou C, Prastitou T (eds) EU internet law in the digital era regulation: regulation and enforcement. Springer, Berlin

Barendt E (2010) Academic freedom and the law: a comparative study. Hart, Oxford

Beckerman-Rodau A (2010) The problem with intellectual property rights: subject matter expansion. Yale J Law Technol 13:35–89
Boerding A, Culik N, Doepke C et al (2018) Data ownership – a property rights approach from a European perspective. J Civ Law Stud 11:323–370
Boldrin M, Levine DK (2008) Against intellectual monopoly. Cambridge University Press, Cambridge
Bracha O, Syed T (2014) Beyond efficiency: consequence-sensitive theories of copyright. Berkeley Technol Law J 29:229–315
Ciani J (2018) Governing data trade in intelligent environments: taxonomy of possible regulatory regimes between property and access rights. In: Chatzigiannakis I, Tobe Y, Novais P, Amft O (eds) Intelligent environments 2018: workshop proceedings of the 14th International conference on intelligent environments. IOS Press, Amsterdam
Ciani Sciolla J (2021) Il pubblico dominio nella società della conoscenza: L'interesse generale al libero utilizzo del capitale intellettuale comune. Giappichelli, Turin
Clarke AC (2020) Principles of property law. Cambridge University Press, Cambridge
Commission (2017a) Summary report of the public consultation on building a european data economy. https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy. Accessed 13 Feb 2022
Commission (2017b) 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. SWD (2017b) 2 final
Corrales Compagnucci M (2020) Big data, databases and "ownership" rights in the cloud. Springer, Berlin
Determann L (2018) No one owns data. Hast Law Rev 70:1–44
Di Robilant A (2014) Property and democratic deliberation: the numerus clausus principle and democratic experimentalism in property law. Am J Comp Law 62:367–416
Drahos P (1997) Thinking strategically about intellectual property rights. Telecomm Policy 21:201–211. https://doi.org/10.1016/S0308-5961(97)00002-5
Drahos P (2020) Responsive science. Annu Rev Law Soc Sci 16:327–342. https://doi.org/10.1146/annurev-lawsocsci-040220-065454
Drahos P (2021) Survival governance: energy and climate in the Chinese century. Oxford University Press
Drahos P, Braithwaite J (2002) Information feudalism: who owns the knowledge economy? Earthscan Publications, London
Drahos P (2006) Freedom and diversity – a defence of the intellectual commons. Australas Intellect Prop Law Resour 1. http://www.austlii.edu.au/au/other/AIPLRes/2006/1.html. Accessed 13 Feb 2022
Drahos P (2016) A philosophy of intellectual property. 2nd edn, ANU eText
Drexl J (2017) Designing competitive markets for industrial data – between propertisation and access. J Intellect Prop Inf Technol E-Commerce Law 8:257–292. https://doi.org/10.2139/ssrn.2862975
Drexl J (2021) The (lack of) coherence of data ownership with the intellectual property system. In: Bruun N, Dinwoodie GB, Levin M, Ohly A (eds) Transition and coherence in intellectual property law: essays in honour of Annette Kur. Cambridge University Press, Cambridge, pp 213–223
Drexl J, Hilty RM, Desaunettes L et al (2016) Data ownership and access to data: position statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the current European debate. Max Planck Institute for Innovation and Competition Research Paper No. 16-10, 2016. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf. Accessed 13 Feb 2022
Drexl J (2018) Data access and control in the era of connected devices. study on behalf of the European Consumer Organisation BEUC. https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf. Accessed 13 Feb 2022
Drexl J (2021b) Data access as a means to promote consumer interests and public welfare – an introduction. In: German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds) Data access, consumer interests and public welfare. Nomos, pp 11–23
Ducuing C (2020) Data as infrastructure? A study of data sharing legal regimes. Compet Regul Netw Ind 21:124–142. https://doi.org/10.1177/1783591719895390
Fairfield JAT (2017) Owned: property, privacy, and the new digital serfdom. Cambridge University Press, Cambridge
Fairfield JAT (2021) Runaway technology: can law keep up? Cambridge University Press, Cambridge

Farkas TJ (2017) Data created by the internet of things: the new gold without ownership? Rev La Prop Inmater 23:5–17. https://doi.org/10.18601/16571959.n23.01
Fia T (2021) An alternative to data ownership: managing access to non-personal data through the commons. Glob Jurist 21:181–210. https://doi.org/10.1515/gj-2020-0034
Fisher W (2001) Theories of intellectual property. In: Munzer SR (ed) New essays in the legal and political theory of property. Cambridge University Press, Cambridge, p 168
Frosio G (2020) Sharing or platform urban mobility? Propertization from mass to MaaS. In: Finck M, Lamping M, Moscon V, Richter H (eds) Smart urban mobility: law, regulation, and policy. Springer, Berlin, pp 163–189
Gambaro A (2009) Dai Beni Immobili Ai Beni Virtuali. In: Enciclopedia Treccani www.treccani.it/enciclopedia/dai-beni-immobili-ai-beni-virtuali_%28XXI-Secolo%29/. Accessed 13 Feb 2022
Geiger C (2019) Reconceptualizing the constitutional dimension of intellectual property – an update. Cen Int Intellect Property Stud Res Pap No. 2019-11, p. 28
Geiger C (2013) The social function of intellectual property rights, or how ethics can influence the shape and use of IP law. In: Dinwoodie GB (ed) Methods and perspectives in intellectual property. Edward Elgar, Cheltenham, pp 153–176
Geiger C, Izyumenko E (2020) The constitutionalization of intellectual property law in the EU and the Funke Medien, Pelham and Spiegel Online decisions of the CJEU: progress, but still some way to go! IIC Int Rev Intellect Prop Compet Law 51:282–306. https://doi.org/10.1007/s40319-019-00901-1
Geiger C, Frosio G, Bulayenko O (2018) Text and data mining in the proposed copyright reform: making the EU ready for an age of big data? IIC Int Rev Intellect Prop Compet Law 49:814–844. https://doi.org/10.1007/s40319-018-0722-2
Gervais DJ (2019) Exploring the interfaces between big data and intellectual property law. J Intellect Prop Inf Technol E-Commerce Law 10:3–19. https://doi.org/10.2139/ssrn.3360344
Ghidini G (2010) Innovation, competition and consumer welfare in intellectual property law. Edward Elgar, Cheltenham
Grabosky PN (1995) Using non-governmental resources to foster regulatory compliance. Gov An Int J Policy Adm 8:527–550. https://doi.org/10.1111/j.1468-0491.1995.tb00226.x
Graef I, Gellert R, Husovec M (2020) Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation. Eur Law Rev 44:605–621
Graves CT (2007) Trade secrets as property: theory and consequences. J Intellect Prop Law 15:39–90
Haggart B (2018) New economic models, new forms of state: the emergence of the 'info-imperium' state. In: Ullrich H, Drahos P, Ghidini G (eds) Kritika: essays on intellectual property. Edward Elgar, Cheltenham, pp 159–188
Hansmann H, Kraakman R (2002) Property, contract, and verification: the numerus clausus problem and the divisibility of rights. J Legal Stud 31:373–420
Hern A (2014) Sir Tim Berners-Lee speaks out on data ownership. The Guardian. www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership. Accessed 13 Feb 2022
Hess C, Ostrom E (2003) Ideas, artifacts and facilities: information as a common-pool resource. Law Contemp Probl 66:111–146
Hilty RM (2018) Big data: ownership and use in the digital age. In: Martinez C (ed) Intellectual property and digital trade in the age of artificial intelligence and big data. CEIPI-ICTSD, p 85
Hugenholtz PB (2018) Against 'data property'. In: Ullrich H, Drahos P, Ghidini G (eds) Kritika: essays on intellectual property, Volume III. Edward Elgar, Cheltenham, pp 48–71
Hugenholtz PB (2019), The new Copyright Directive: text and data mining (Articles 3 and 4). Kluwer Copyright Blog. http://copyrightblog.kluweriplaw.com/2019/07/24/the-new-copyright-directive-text-and-data-mining-articles-3-and-4/. Accessed 10 Mar 2021
Hummel P, Braun M, Dabrock P (2021) Own data? ethical reflections on data ownership. Philos Technol 34:545–572. https://doi.org/10.1007/s13347-020-00404-9
Kapczynski A (2022) The public history of trade secrets. UC Davis L Rev 55:1367–1443
Kerber W (2016 A new (intellectual) property right for non-personal data? An economic analysis. MAGKS Joint Discussion Paper Series in Economics, No. 37-2016, Philipps-University Marburg, School of Business and Economics, Marburg. https://www.econstor.eu/bitstream/10419/155649/1/870294326.pdf. Accessed 13 Feb 2022
Krönke C (2018) Data regulation in the internet of things. Front Law China 13:367–379. https://doi.org/10.3868/s050-007-018-0028-9

Leistner M (2021) The existing European IP rights system and the data economy – an overview with particular focus on data access and portability. In: German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds) data access, consumer interests and public welfare. Nomos, pp 209–251
Lemley MA (2008) The surprising virtues of treating trade secrets as IP rights. Stanf Law Rev 61:311–353
Lemley MA (2015) IP in a world without scarcity. N Y Univ Law Rev 90:460–515. https://doi.org/10.2139/ssrn.2413974
Lock T (2019) Article 13 CFR. In: Kellerbauer M, Klamert M, Tomkin J (eds) The EU treaties and the charter of fundamental rights: a commentary. Oxford University Press, Oxford
Maggiolino M (2018) EU Trade secrets law and algorithmic transparency. Annali Italiani di Diritto D'Autore, della Cultura e dello Spettacolo 27:199–217
Malone M (2020) Trade secrets, big data, and the future of public interest litigation over artificial intelligence in Canada. Canada Intellect Prop Rev 35:6–9
Marella MR (2013) La funzione sociale oltre la proprietà. Riv Crit del Dirit Priv 31:551–568
Mattei U, Quarta A (2018) The turning point in private law: ecology, technology and the commons. Edward Elgar, Cheltenham
Mattei U (2000) Basic principles of property law: a comparative legal and economic introduction. Greenwood
Mattei U (2015) La proprietà. 2nd edn, Utet
Mattioli M (2018) Data and intellectual property law. In: Mak V, Tai ETT, Berlee A (eds) Research handbook in data science and law. Edward Elgar, Cheltenham, pp 133–152
Mayer-Schönberger V, Ramge T (2018) A big choice for big tech. Foreign Aff 97:48–54
Merrill TW, Smith HE (2000) Optimal standardization in the law of property: the numerus clausus principle. Yale Law J 110:1–70. https://doi.org/10.2307/797586
Mezzanotte F (2015) La conformazione negoziale delle situazioni di appartenenza: numerus clausus, autonomia privata e diritti sui beni. Jovene Editore
Montagnani ML (2020) Dati e proprietà intellettuale in Europa: dalla 'proprietà' all'accesso. Dirit dell'economia 101:539–569
Mulligan C (2013) A numerus clausus principle for intellectual property. Tenn Law Rev 80:235–290. https://doi.org/10.2139/ssrn.2017023
Nordberg A (2020) Trade secrets, big data and artificial intelligence innovation: a legal oxymoron? In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive. Edward Elgar, Cheltenham, pp 192–218
Noto La Diega G (2022) Internet of things and the law. Routledge, Milton Park
Noto La Diega G, Sappa C (2020) The internet of things (IoT) at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers. Eur J Consum Law 3:419–458
Ottolia A (2010) The public interest and intellectual property models. Giappichelli, Turin
Ottolia A (2017) Big Data e innovazione computazionale. Giappichelli, Turin
Parker C (2002) The open corporation: effective self-regulation and democracy. Cambridge University Press, Cambridge
Parker C (2007) Meta-regulation: legal accountability for corporate social responsibility. In: Mcbarnet D, Voiculescu A, Campbell T (eds) The new corporate accountability: corporate social responsibility and the law. Cambridge University Press, Cambridge, pp 207–237
Parker C, Scott C, Lacey N, Braithwaite J (2004) Introduction. In: Parker C, Scott C, Lacey N, Braithwaite J (eds) Regulating law. Cambridge University Press, Cambridge, pp 1–12
Perzanowski A, Schultz J (2016) The end of ownership: personal property in the digital economy. MIT Press, Cambridge
Peukert A (2015) The fundamental right to (intellectual) property and the discretion of the legislature. In: Geiger G (ed) Research handbook on human rights and intellectual property. Edward Elgar, Cheltenham, pp 132–148
Peukert A (2021) A Critique of the ontology of intellectual property law. Cambridge University Press, Cambridge
Priora G, Sganga C (2020) Smart urban mobility: a positive or negative ip space? A case study to test the role of IP in fostering digital data-driven innovation. In: Finck M, Lamping M, Moscon V, Richter H (eds) Smart urban mobility: law, regulation, and policy. Springer, Berlin, pp 143–162

Purtova N (2018) The law of everything. Broad concept of personal data and future of EU data protection law. Law Innov Technol 10:40–81
Quarta A (2016) Non-proprietà: teoria e prassi dell'Accesso ai beni. Edizioni Scientifiche Italiane, Naples
Reichman JH, Okediji RL (2012) When copyright law and science collide: empowering digitally integrated research methods on a global scale. Minn Law Rev 96:1362–1480
Resta G (2010) Nuovi beni immateriali e numerus clausus dei diritti esclusivi. In: Resta G (ed) Diritti esclusivi e nuovi beni immateriali. Utet
Ricketson S (1992) New wine into old bottles: technological change and intellectual property rights. Prometheus 10:53–82. https://doi.org/10.1080/08109029208629514
Ricolfi M (2017) IoT and the ages of antitrust. Concorrenza e Mercato 1:215–232
Ricolfi M (2019) Il futuro della proprietà intellettuale nella società algoritmica. Giurisprudenza Italiana 10
Ricolfi M (2021) Multiple and overlapping transitions in IP. In: Bruun N, Dinwoodie GB, Levin M, Ohly A (eds) Transition and coherence in intellectual property law: essays in honour of Annette Kur. Cambridge University Press, Cambridge, pp 121–132
Ritter J, Mayer A (2018) Regulating data as property: a new construct for moving forward. Duke Law Technol Rev 16:220–277
Rubinfeld DL, Gal MS (2017) Access barriers to big data. Ariz Law Rev 59:339. https://doi.org/10.3868/s050-004-015-0003-8
Sadowski J (2019) When data is capital: datafication, accumulation, and extraction. Big Data Soc 6:1–12. https://doi.org/10.1177/2053951718820549
Sandeen SK (2014) Lost in the cloud: information flows and the implications of cloud computing for trade secret protection. Virginia J Law Technol 19:1–103
Sappa C (2019) How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. J Intellect Prop Law Pract 14:407–418
Scalzini S (2022) Trade secrets and data-driven innovation in the EU. In: Comandè G (ed) Elgar Encyclopedia of law and data science. Edward Elgar, Cheltenham, pp 347–353
Scassa T (2018), Data ownership. Centre for International Governance Innovation Paper No. 187/2018. https://www.cigionline.org/static/documents/documents/Paper%20no.187_2.pdf. Accessed 15 Feb 2022
Schovsbo J (2020) The directive on trade secrets and its background. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU Directive. Edward Elgar, Cheltenham, pp 7–21
Schovsbo J, Minssen T, Riis T et al (2020) An appraisal of the EU Directive on trade secrets. In: Schovsbo J, Minssen T, Riis T (eds) The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive. Edward Elgar, Cheltenham, pp 1–6
Schwemer SF, Schovsbo J (2020) What is left of user rights? Algorithmic copyright enforcement and free speech in the light of the Article 17 regime. In: Torremans PLC (ed) Intellectual property law and human rights, 4th edn. Wolters Kluwer, Alphen aan den Rijn
Sell SK (2003) Private power, public law: the globalization of intellectual property rights. Cambridge University Press, Cambridge
Sganga C (2018) Propertizing European copyright: history, challenges and opportunities. Edward Elgar, Cheltenham
Stepanov I (2020) Introducing a property right over data in the EU: the data producer's right – an evaluation. Int Rev Law, Comput Technol 34:65–86. https://doi.org/10.1080/13600869.2019.1631621
Surblytė-Namavičienė G (2020) Competition and regulation in the data economy: does artificial intelligence demand a new balance? Edward Elgar, Cheltenham
Thouvenin F, Weber RH, Früh A (2018) Data ownership: taking stock and mapping the issues. In: Dehmer M, Emmert-Streib F (eds) Frontiers in data science. CRC Press, Boca Raton
Tjong Tjin Tai E (2018) Data ownership and consumer protection. J Eur Consum Mark Law 7:136–140
Tusikov N (2019) Precarious ownership of the internet of things in the age of data. In: Haggart B, Henne K, Tusikov N (eds) Information, technology and control in a changing world: understanding power structures in the 21st century. Palgrave Macmillan, London
Ubertazzi LC (2014) Numerus clausus dei diritti esclusivi di proprietà intellettuale? IURISMAT 4:187–194
van Erp S (2017) Ownership of data: the numerus clausus of legal objects. Brigham-Kanner Prop Rights Conf J 6:235–258

Vercellone A (2020) Il community land trust: autonomia privata, conformazione della proprietà, distribuzione della rendita urbana. Giuffrè Francis Lefebvre, Milan
Weber RH, Eggen M (2020) Data ownership and data access in the internet of things (IoT). Eur J Consum Law 3:459–480
Wiebe A (2017) Protection of industrial data – a new property right for the digital economy? J Intellect Prop Law Pract 12:62–71. https://doi.org/10.1093/jiplp/jpw175
Wiebe A, Schur N (2019) Protection of trade secrets in a data-driven, networked environment – is the update already out-dated? J Intellect Prop Law Pract 14:814–821. https://doi.org/10.1093/jiplp/jpz119
Yu PK (2019) Data producer's right and the protection of machine-generated data. Tulane Law Rev 93:859–929
Zech H (2016) Data as a tradeable commodity. In: De Franceschi A (ed) European contract law and the digital single market: the implications of the digital revolution. Intersentia, Cambridge, pp 51–80
Zech H (2016) A legal framework for a data economy in the European digital single market: rights to use data. J Intellect Prop Law Pract 11:460–470. https://doi.org/10.1093/jiplp/jpw049
Zech H (2021) Exclusivity in data: how to best combine the patchwork of applicable European legal instruments. In: Sandeen S, Rademacher C, Ohly A (eds) Research handbook on information law and governance. Edward Elgar, Cheltenham
Zimmer D (2017) Property rights regarding data? In: Lohsse S, Schulze R, Staudenmayer D (eds) Trading data in the digital economy: legal concepts and tools. Münster Colloquia on EU Law and the Digital Economy III. Nomos
Zukerfeld M (2017) The tale of the snake and the elephant: intellectual property expansion under informational capitalism. Inf Soc 33:243–260. https://doi.org/10.1080/01972243.2017.1354107