IN2DREAMS

Contract No. 777596

INtelligent solutions 2ward the Development of Railway Energy and Asset Management Systems in Europe

D4.5 – Legal aspect for smart contract adoption

DUE DATE OF DELIVERABLE: 31/12/2018

ACTUAL SUBMISSION DATE: 20/12/2018

Leader/Responsible of this Deliverable: KU Leuven (Charlotte Ducuing)

Reviewed: Y

Document status		
Revision	Date	Description
0.1	22-11-2018	First issue – KUL Writer: Charlotte Ducuing Internal reviewers: Ivo Emanuilov; Marie-Christine Janssens
0.2	22-11-2018 to 05-12-2018	Comments and review from CEFRIEL, UNIGE, UKON.
1	12-12-2018	Second issue – KUL
2	20-12-2018	Final version after TMT approval and quality check

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/09/2017 Duration: 24 Months

Executive Summary

Scenarios of WP 4 and 5 all imply data exchanges between various actors in the railways, which is more generally illustrative of the growing economic importance of data when fueling data-driven technologies in the big data context, particularly here in the “brick and mortar” industry. As a matter of fact, data and especially industrial data are considered by market players as a commodity. This is all the more true when they are traded in their own right, as well illustrated by the cross-scenario “marketplace of data and data monetization”.

Although data undeniably have economic value, their legal status - and in particular whether and under which conditions they could be subject to a form of ownership – remains far from clear. The lawmakers - and sometimes the judiciary authorities – at both EU and national levels attempt to clarify the legal status of data and where appropriate to find new ways for regulating data. This deliverable intends to clarify the legal status of data which is a core issue for all scenarios contemplated in WS2. The first chapter presents what “data” is from the legal perspective as well as the basics of property law. The second chapter outlines the status of data and digital objects under property law and more specifically attempts to show the difficulty for property law to deal with data as a subject matter. It concludes that data as such are poor candidate to ownership as an object. However, a digital update of property law is undoubtedly needed in order to find appropriate equivalence for ownership to be recognized on digital objects – rather than on data as such.

While data would often not be vested with ownership rights as such, they are however regulated by various legal regimes, which are presented in the third chapter with a specific focus on the railways as well as on the cross-scenario “marketplace of data and data monetization”. Data are found to be subject to a patchwork of rights and obligations, which sometimes conflict one against the other. Indeed, one data (operation) may simultaneously be impacted by several legal regimes. Besides, although data are impacted by regulations, they are usually not the regulatory focus as such which brings legal uncertainty as for what rights and obligations are related to data (operations) in a specific case. This issue is particularly striking when trading data in their own right within a data-marketplace.

This deliverable also provides for a legal analysis of some of the interactions between big data and the blockchain technology regarding property in the digital environment, in line with the general objective of WS2 to merge big data analytics and DLT. This analysis builds upon deliverable D4.1 and particularly upon the legal section (section 4), which analyses the challenges posed by blockchain-based smart contracts to contract law on the one hand and the interplay between the blockchain infrastructure and safety and (cyber-)security regulation in the railways on the other hand. While section 4 of Deliverable D4.1 addresses legal issues which are common to all scenarios contemplated in WS2, the present deliverable further focusses on specific legal challenges that the use of blockchain technology may pose to property law. Firstly, the deliverable finds that the blockchain technology shall be generally interpreted as a signal that property law needs a digital update, by virtues of its groundbreaking ability

to create digital scarcity, which is discussed as part of chapter 2 on the application of property law to data and digital objects. Secondly, the fourth and last chapter is entirely dedicated to the analysis of the impact of leveraging the blockchain technology to trade data. Such challenges are concretely illustrated in the study for the cross-scenario “marketplace of data and data monetization”, which is for this reason further analyzed here although this ambitious scenario will eventually not be technically implemented. Specific focus is placed on the concept of smart property. This chapter finds that “tokenization” of data (sources) in a blockchain can raise legal issues: the blockchain could indeed be leveraged to design “technological ownership” on data, therein circumventing the (perceived as) lack of ownership rights in data, which raises fundamental questions related to the (absence of) legal status of data. However, designing such technological ownership appears not to be feasible solely with the blockchain technology, as the later does not reach the data as such – as “offchain asset” – but only reaches the blockchain token representing them.

Abbreviations and Acronyms

Abbreviation	Description
CESL	Draft Common European Sales Law
CJEU	Court of Justice of the European Union
Computer Program Directive	Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), OJ L 111, 5.5.2009, p. 16–22.
Consumer Rights Directive	Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88.
Database Directive	Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.
DRM	Digital Rights Management
ECI Directive	Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), OJ L 345, 23.12.2008, p. 75–82.
Environmental Information Directive	Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, 1OJ L 41, 14.2.2003, p. 26–32.
EU	European Union
GA	Grant Agreement
GDPR or General Data Protection Regulation	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, OJ L 119, 4.5.2016, p. 1–88.
H2020	Horizon 2020 framework programme
InfoSoc Directive	Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.
JU	Shift2Rail Joint Undertaking

NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.
PSI Directive	Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, 1OJ L 345, 31.12.2003, p. 90–96.
Railway Safety Directive	Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (Text with EEA relevance), OJ L 138, 26.5.2016, p. 102–149.
Trade Secret Directive	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, OJ L 157, 15.6.2016, p. 1–18.
Utilities Directive	Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance, OJ L 94, 28.3.2014, p. 243–374.

Table of Contents

1. Introduction to the deliverable

Data analytics require (as the input) and produce (as the outcome) large amounts of data, which can flow easily among interested entities. As a result, data are gaining more and more value as we enter into what is now commonly referred to as the "data economy". As a matter of fact, data, and especially industrial data (or more generally data other than personal data within the meaning of data protection law), are considered by market players as a commodity. This is particularly the case where they are traded in their own right rather than considered as a "derivative" of the physical asset or person that they refer to content-wise. This has even materialized *de facto* in companies' contractual practices, as noted by legal scholars.(Wiebe 2017, 1; Zech 2016, 461) The IN2DREAMS "Marketplace of data and data monetization" scenario illustrates this trend towards treating data as a commodity.(Wiebe 2017, 63) The first section briefly presents the deliverable, including the scenario[1] that is discussed as well as the legal questions that will be examined (1). The second section will set the scene by describing "data" from a legal perspective and by laying down the core principles of property law (2).

1.1. Presentation of the deliverable

1.1.1. Presentation of the scenario "marketplace of data and data monetization"

The cross-scenario[2] consists of a data (sources) marketplace to which actors involved in the railway data business related to a railway infrastructure manager ("IM") would contribute. This involves at least the IM, its suppliers and "any entity that is involved in data creation and data utilization in this field".[3] All actors produce data in the course of their business activities and/or need data for the performance of their (data analytics) activities. The cross-scenario aims to bring together the data sources originating from the actors who can "trade" data with one another in an anonymous, or pseudonymous, manner. The "data market" is different from traditional markets in that it departs from the "customer-to-supplier" logic.[4] In this regard, the industrial customer of IT services – e.g. the railway IM – produces huge volume of data related to its infrastructure that for instance represent a needed input for its data analytics service provider or may otherwise have economic value for third parties. In that sense, every actor can simultaneously be a data producer and a data user which results in a lack

[1] For a technical presentation of the scenario, see the Deliverable D5.1, section 4.2 "cross-scenario 2: Marketplace of Data and Data monetization" and the Deliverable D.4.1, section 5.3 "Marketplace for monetization and servitisation".
[2] Deliverable D5.1.
[3] Deliverable D5.1, section 4.2.6 "scenario description".
[4] Deliverable D4.1, section 5.3 "Marketplace for monetization and servitisation".

of clarity of the market structure and a deemed lack of trust between the involved actors, especially with regard to the quality of the data produced.[5]

In order to take this economic reality into account, the cross-scenario contemplates placing the data marketplace on a blockchain as software infrastructure in order to structure the market without the "need of intermediary third party or centralized repository". [6] The blockchain also allows to "automat[e] governance logics in the digital ecosystem": the governance would indeed be enshrined in the protocol of the blockchain network to be set up. Based thereon, the actual exchanges of data would be performed by means of smart contracts that enable the actors involved to automate the exchanges while ensuring their completion. It can be accompanied with "direct reward mechanisms for the exchange of data sources" or, in other words, with a price. Finally, and with a specific view to incentivizing data trading on behalf of actors not professionally involved in the data economy field, the system would involve data analytics. They could enable the actors to easily see and even predict which of their data is or will be subject to high demand.

1.1.2. Overview of the legal questions

Fragmentation of the legal regime surrounding (operations on) data - Data marketplaces can be defined as "electronic marketplaces where data is traded as a commodity, an electronic marketplace being 'the concrete agency or infrastructure that allows participants to meet and perform the market transactions, translated into an electronic medium'"[7]. While typologies are being made according to the specificities of the respective cases, the trading of data "as a commodity" is core to a data marketplace. "As a commodity" would legally imply to be a thing eligible for ownership rights so that the thing can be sold and rented (or licensed). From a legal perspective, however, data do not have an overall legal status *as such*. In particular, the qualification of "data" under property law – in other words: can data be recognized as legal "thing"? – is debated in legal scholarship. Beyond the realms of property law, data are – directly or indirectly – subject to different rights and obligations(Drexl 2017) including as part of sector-specific regulation where relevant. The determination of who is entitled to

[5] In other domains, such as air traffic management, this has already proven problematic. Thus, for example, the planned rollout of the System Wide Information Management (SWIM) would similarly practically remove the strict lines between producers and users of data in the air traffic management domain. In turn, this gives rise to new concerns related to trust, safety and liability. For an overview of these issues, see Anna Masutti. 'Key Points and Proposals for a SWIM Regulatory Framework: The Way Ahead'. In: *Achieving the Single European Sky. Goals and Challenges*, edited by Pablo Mendes de Leon and Daniel Calleja Crespo, 201–19. Alphen aan den Rijn : Kluwer Law International, 2011.

[6] Deliverable 4.1, section 5.3.

[7] F. Stahl, F. Schomm, G. Vossen, & L Vomfell, A Classification Framework for Data Marketplaces, Vietnam J Comput Sci, 2016, p. 137, as quoted in the 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/2017/02 final), 17.

perform what activities on what data therefore becomes a difficult legal question in the context of "big data". This leads to legal uncertainty as to the legal nature and one's entitlement to access or use data[8] which has been said to be detrimental to the free flow of data among market players and therefore to the data economy. It has also been found to be detrimental, among others, to the assessment of the value of data, e.g. in case of damage.(Maeschaelck 2018, 39) The case of the railway sector is a good illustration of this. It is subject to specific rules as a utility (railway-specific regulation), in certain circumstances as a public authority (access and PSI legal regimes) and as (cyber)security-sensitive entity (NIS, critical infrastructure, public security law) which are sometimes contradictory (public security exceptions in access and PSI regimes).

Blockchain as a technological alternative to the absence of a clear legal status of data?- In the meantime, the blockchain technology and its smart contract applications have been put forward as technical enablers to manage and monetize the use of one's (physical or digital) asset by third parties based on the concept of "smart property". The blockchain-based smart property would consist of a technological alternative to legal property. This comes as a specific form of technical regulation of agreements between parties. In the case of a data marketplace, the use of the blockchain technology as a means to manage one's property would be seen as a potential technological solution to the (perceived) problem of lack of clarity and workability of the legal framework of "data" or even as an attempt to protect "one's data" in the absence of ownership rights.

1.1.3. Organization of the deliverable

This deliverable provides a legal study of the "marketplace of data and data monetization" scenario and more precisely, on property law. Unlike certain aspects of intellectual property law, 'classical' property law is not harmonized at EU level and is therefore mostly regulated by very different national legal regimes.(Storr and Storr 2017) In particular, a dividing line can be drawn between civil law and common law States. The analysis of the respective national law of all Member States goes beyond the ambit of this contribution. Especially, the aim is not to determine and compare the legal treatment of data with regard to property law in the respective national laws of the Member States.[9] This deliverable rather aims to present the main conceptual challenges in handling data as a commodity. National legislations and/or national court cases are therefore made to serve this purpose, but the deliverable does not aim to be exhaustive in this regard.

[8] (Graf von Westphalen and Westphalen 2017) (Sein 2017)

[9] See the tables in Document de B&B, p. 23: the authors compared the legislation of several Member States (namely, Belgium, France, Germany, Italy, Spain and the United Kingdom) and their case law on the existence of an ownership right in data. They also show whether there has been national case law in this matter. They limit the analysis to the ownership rights on data, and do not tackle or recall previous case law on similar questions with reference to software.

As part of the introductory first chapter, the next sections will (1) provide a basic presentation of data and data features from a legal perspective on the one hand, and of property law on the other hand. Then, (2) a general overview of the property law regime of data and digital assets is provided. Based on the conclusion that (at least raw) data are not the subject-matter of ownership rights, the third chapter displays the various legal regimes that could apply to (operations on) data in the railway sector (3). Finally, and with a view to providing a forward-looking legal perspective, the last chapter analyses (4) the legal impact of leveraging the blockchain technology to manage or "enforce" trading of data, based on the concept of smart property.

1.2. Setting the scene: presentation of data and property law

This chapter is divided into two sections: the first one presents data and the features of data from a legal taxonomy perspective (1). The second one presents the main concepts of property law (2).

1.2.1. Data as legal subject-matter: tentative definition

Although broadly used, paradoxically the term "data", as a subject-matter of this study, does not have a clear and commonly-agreed definition (Zech 2017, 3). Therefore, it should firstly be further delineated.

Data vs. computer data? – According to the Oxford English Dictionary, data (mass noun) are (definition 1.1) "the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media".[10] The Oxford English Dictionary limits the definition of "data" to the feature that operations can be performed on them by a computer. In this regard, this is narrower in scope than the definition given by ISO - and referred to by the European Commission in its Communication "Towards a thriving data-driven economy" [11] – which does not exclude non-computable data. According to ISO/IEC 2382-1, "data is 'a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing'. Data can be either created/authored by people or generated by machines/sensors, often as a "by-product". Examples: geospatial information, statistics, weather data, research data, etc." The computability of data – or their digital character – as a necessary criterion, is also discussed from the perspective of the process of data creation: the debate revolves around whether "data" only refer to machine-generated

[10] Oxford dictionary online, https://en.oxforddictionaries.com/definition/data, last visited 12th September 2018.

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a thriving data-driven economy", COM(2014) 442 final, 4.

data or does it also include human-generated ones. (Duch-Brown, Martens, and Mueller-Langer 2017, 8)

As for EU law, it seems to suggest that "data" includes both human- and computer-generated data: "personal data", within the meaning of the GDPR[12], are defined as any "information" enabling identification of a natural person without considering whether it is created or respectively processed by a machine or a computer. Besides, the Cybercrime Directive[13] applies to "computer data"[14], defined as "a representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function". Thereby, it implicitly admits that the general term "data" also applies to data not suitable for or created by computer. Obviously, the discussion on the ownership on data mostly concerns computer data, although the vocabulary used is sometimes unclear.[15] Finally, further taxonomies of (in particular computer) data exist, both for technical and respectively legal purposes.

Data vs. data carrier - A distinction should be made between the data and the data physical carrier. Data cannot exist on its own without an infrastructure and especially a carrier(van Erp 2017, 13) – such as a server, a chip, etc. However, they should be distinguished as the physical carrier would be subject to a specific legal regime in its own right. Identification of data as such is important from the perspective of discussing the existence of rights on data, as this questions typically arises where no other right can be claimed (e.g. rights attached to the physical carrier). Whether ownership can be claimed on data *based on rights in the physical data carrier* – among potential other triggers - is precisely one of the questions surrounding the debate on the ownership of data.

Data vs. information? **-** The dictionary definition describes data in light of their format and features: in other words, "data" refers to the carrier of a message regardless of the message itself (e.g. whether

[12] Article 4 (1) of the 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 ("General Data Protection Regulation", or "GDPR").
[13] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 3013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
[14] Article 2 (b) of the Cybercrime Directive.
[15] The Proposal of the Commission for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union of 13th September 2017 (COM(2017) 495 final) rather refers to "electronic data" (article 2 (1)) which however seems to amount to "computer data". The Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Towards a thriving data-driven economy' (/* COM/2014/0442 final */) refers also to "digital data" (see i.a. in section "global context and call to action"). The 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/2017/02 final) also refers to "machine-generated data" which also appear to amount to computer data.

the information carried is confidential, refers to a natural person, etc.). Drexl makes a distinction[16] between the "syntactic and the semantic levels"(Drexl 2017, 13): the syntactic level refers to "representation of the information" while the semantic level "relates to the meaning" (or: to the message). Technically speaking, data shall be understood from a syntactic level and shall therefore be distinguished from the information carried: this distinction is indeed made in the Cybercrime Directive with a reference to "computer data". However, the definition of "personal data", in that it makes a tie between personal data and information that allows to identify a natural person, mixes up the two levels. The case of personal data is a complex one as the trigger lies in the potential identification of a natural person, while both semantic and syntactic levels can be means to do so. For instance, an information consisting of the name of a natural person consists of "personal data" (semantic level). It can also qualify as "personal data", data stemming from the computer of a natural person where the information contained can be linked to this person (e.g. by means of the origin of the data such as the IP). This difference between the two legal texts can be explained by their underpinning rationales: while the Cybercrime Directive aims to criminalize certain activities in relation to information systems and the data that they contain, data protection law aims to protection the natural persons. The distinction between the message (the information) and the carrier (the data) is *de facto* not always clear-cut, which results in difficulties to account for a clear understanding of data in the law.[17] In particular, and as will be further discussed in chapter 4, the legal regime dealing with data is very often related to the semantic level, namely to the information that is carried by the data. Wiebe even adds a third level, namely "pragmatics", referring to "the goal that is pursued by the information.(Wiebe 2017) He considers that patent law and trademark law protect information according to their "pragmatic" level. The distinction between the different levels shall however be retained, at least theoretically, so as to understand how different legal regimes may simultaneously apply to a single dataset, according to their respective trigger point.(Wiebe 2017)

Features of data - Data are an intangible asset.[18] They are usually described as essentially ubiquitous and non-rivalrous. Although related and sometimes considered as analogous, these characteristics should be distinguished. Ubiquity of data refers to the fact that data are easily copied without any detrimental effects on the first (original) data, which makes them non-excludable. "(Non)rivalry of consumption describes the degree to which the consumption of a resource affects (or does not affect) the potential of the resource to meet the demands of others". The non-rivalry of data implies that their use "does not exclude another from using the same data"(Storr and Storr 2017) which makes them different from oil – to which data are sometimes compared – which is "a purely rivalrous good [and can therefore] only be consumed once".[19]

[16] The same distinction is also used in (Zech 2016, 462–63)
[17] (van Erp 2017, 10–11)
[18] OECD, Data Driven innovation: Big data for growth and well-being, OECD Publishing Paris, 2015, 197.
[19] OECD, Data Driven innovation: Big data for growth and well-being, OECD Publishing Paris, 2015, 180.

Data are also characterized by their short lifecycle. They are quickly created but also quickly destroyed. Beyond their practical destruction, the data economy relies on real-time data so that data quickly lose their economic value. Not only do they constantly change, but data "derives value exactly for this reason". (Surblyte 2016, 5–6) Against this background, data are generally described as volatile and hardly definable, in the sense that the contours of what a "datum" is, are a moving target. Data are rarely referred as an isolated asset. In particular in the context of the so-called "big data economy", data make part of large datasets which grant them economic value.(Drexl 2017, 13) This feature makes it difficult to isolate concretely "datum" as a subject-matter in its own right.

1.2.2. Presentation of the main concepts in property law

Subject-matter of ownership rights - Ownership rights have been granted on tangible assets, divided up between movable and immovable ones. While the law does not explicitly include intangibles, it is debated in various jurisdictions whether and to what extent ownership rights extend to (specific?) intangibles, as will be further discussed below. Here, intangibles are generally referred to as assets "that cannot be transferred manually".('What Virtual Worlds Can Do for Property Law by Juliet M. Moringiello :: SSRN' n.d., 162) The subject-matters of ownership rights greatly differ amongst the national jurisdictions.[20] Whether intellectual property rights shall be considered as making part of ownership rights is also discussed. They are sometimes referred as "ownership-like rights"[21] in that they grant exclusive rights with respect to intangibles while being triggered by different criteria as property law precisely based on their non-rivalrous character.

General presentation of legal protection of ownership rights[22] - Ownership rights are usually described as a bundle of rights(Ishmaev 2017, 7) that a person has with relation to a delineated "thing", that entitle him to decide upon the use of the thing (*usus)*, to gain financial gains stemming from the exploitation of the thing (*usufructus*) and finally to dispose of the thing and especially to give or sell it wholly or in part (alienability).(Pearce n.d., 192) Ownership does not mean "sovereignty" or absolute disposition of the thing. The law indeed typically regulates in which circumstances the property can be seized – temporarily or definitely - among others, in the case of bankruptcy or expropriated, e.g. for reasons pertaining to public order. The determination of the owner of a thing is regulated explicitly in statutory although with great divergence amongst the jurisdictions.

[20] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 38.
[21] Whether "intellectual property rights" shall be referred to as "ownership rights" is debated in the scholarship. Some scholars refer to "entitlements" rather than "ownership rights", see (van Erp 2017, 1) In particular, copyright does not entirely fit in the definition of "ownership" in that it includes moral rights that cannot be transferred.
[22] The vocabulary of property law is not harmonized, especially in EU law. See on this matter E. Ramaekers, European Union Property law, From Fragments to a System, Intersentia 2013, chapter 4.

Ownership rights are also burdened with exceptions and tolerances, such as rights of way with regard to immovable property: the law indeed only protects the owner against "unlawful interferences" which implies that some interferences of lawful.[23] Again, the scope *rationae materiae* of ownership rights and of the exceptions that the owner shall endure, differ not only across jurisdictions but also depending upon the type of property. Further, the legal means at the disposal of the owner to defend their ownership rights are also subject to diverse regimes. While common law is generally credited to allow for some "self-help" conduct on behalf of the owner – e.g., to conduct repossession, civil law would be more reluctant: in case of unlawful interference, the owner would generally have to claim her rights to court unless vested with derogatory public authority.(Stănescu 2015)

Ownership rights on movables and immovables would also generally differ to a large extent[24]: for instance, property rights on immovable includes legal protection against interferences to the enjoyment of the thing which gives rise to rights against troubles caused by neighbors which obviously does not make sense with regard to movables. The core of ownership rights, however, fundamentally remains the right to exclude third parties from the right to perform certain activities in relation with the owned "thing". In that sense, the first right of the owner is to claim ownership (*rei vindicatio),* although the means by which to do so differ amongst the jurisdictions.

Property law does not operate in isolation and obviously interacts with other branches of law having an impact on a "thing", although the boundaries of property law as well as its interactions with other branches of law vastly differ amongst the different national jurisdictions. For illustration, ownership is often linked to liability for damages caused by means of the thing; it is also often related to the legal qualification of the trading of a thing in exchange for compensation ("sale contract"). Similarly, theft in criminal law is often related to the legal status of a thing, when materially characterized by the deprivation of the possession of the thing. Discussing the existence of ownership rights in a thing, in this case data, inevitably leads to discussing more generally the legal status of a thing.

The rationale of the legal creation and protection of ownership rights - The legal, economic and philosophical scholarship is divided on the determination of the rationale for the creation of ownership rights. According to Ishmaev(Ishmaev 2017, 11), referring to the work of Penner[25], the rationale for setting up property legal regimes derives from the interests of the owner in the use of things: "here use and exclusion are two sides of the same coin". This definition therefore considers property legal regimes as grounded in scarcity and rivalry of things, namely the fact that the use of the thing by A prevents B to use that same thing. This line of reasoning leads to a distinction between property rights and intellectual property rights, where the latter refers to non-scarce things. From a more macro-

[23] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 115.
[24] (Lehdonvirta and Virtanen 2010, 9) (Low and Teo 2017)
[25] Penner, James E. 1997. The Idea of Property in Law. Oxford: Oxford University Press

economic perspective, Fairfield notes that one of the functions of property law is to "guide incentives to use resources productively", thereby underlying the economic policy role of property law.(Fairfield 2005, 21)

Rights in rem vs. rights ad personam: the erga omnes effect - Ownership rights are described as making part of rights *in rem.* According to Van Erp, the classical distinction between rights *ad (*or *in) personam* and rights *in rem* more fundamentally drew a line between respectively "liability questions" and "questions of wealth". The former are "inter-personal"; they can be created either by statutory provisions or by contracts privately arranged by parties. They constitute "the rights of behavior of some particular person".(Ishmaev 2017, 7) As opposed to that, the rights *in rem* are directly attached to the thing: as a result, a transfer of ownership of a thing also results in a transfer of the whole bundle of rights related to that thing. For example, the sale of an immovable also results in a transfer of lease contract that could be attached to the immovable. Reciprocally, the "extinction of the things" results in the extinction of the right *in rem*.(Savelyev n.d., 4) The latter are "about a person and his assets or, […] legal relations between a subject vis-à-vis a substantial number of other subjects regarding an object".(van Erp 2017, 5) In that sense, ownership rights are rights to exclude third parties from activities in relation to the thing: they are enforceable against third parties (sometimes grandly referred to as "the rest of the world") - or in other words they have *erga omnes* effect. The *erga omnes* effect thereby grants the owner control over the thing. The distinction between *erga omnes* vs. *ad personam* effect perfectly reflects civil law systems while it should be qualified with regard to common law systems. The latter indeed also include property rights "if someone has the better title" or in other words, if a person in his relation with another person has the stronger right to an object".(van Erp 2017, 236)

The principle of numerus clausus **-** Because of their *erga omnes* effect, ownership rights are subject to the legal principle of *numerus clausus*, deemed the most important principle of property law.(van Erp 2017, 16) This principle implies that statutory law regulates the "number and content of property rights", on the one hand, and "the way in which these rights can be created, transferred or destroyed".[26] In other words, only statutory law can delineate the contours of the *subject-matter* of ownership rights ("thing-ness") as well as the contours of ownership rights.(van Erp 2017, 1–3)

Failing to rely on stronger ownership rights based on statutory law, parties can arrange - weaker - *ad personam* contractual rights.[27] The latter are potentially infinite as they can be freely created by the parties. Their weakness, however, lies in that *ad personam* rights are only enforceable against the

[26] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 65
[27] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 51

debtor – e.g. the contractual counterparty.[28] Besides, and set aside the *existence* of an ownership right, the owner within the meaning of property law can, to a certain extent, dispose contractually of the bundle of rights which constitutes the ownership rights. In particular, the owner can arrange personal servitudes, such as lease contracts with third parties. The distinction between rights *in rem* and rights *ad personam* (and in particular contract law) is in that sense not complete and both branches of private law obviously interact. To guarantee *erga omnes* effect of a sale contract (to the benefit of the new owner), especially for immovable and intellectual property rights, statutory law typically usually regulates the sale or other contracts relating to the thing. Notably, the law would typically regulate the relations between property law and contract law, e.g. in case of different persons claiming property rights in the same things based on different legal regimes. The respective boundaries of property law and contract law also varies according to the national legislation.

The principle of transparency - Again, related to their *erga omnes* effect, ownership rights are subject to the principle of transparency.[29] They are logically enforceable against third parties only provided third parties can be made aware of the existence of the right. Van Erp and Akkermans distinguish two components of transparency, namely specificity – or specialty – on the one hand, and publicity, on the other hand. The principle of specificity is sometimes referred to as inherently linked to this of certainty: the contours of the thing – as subject-matter of property rights - shall be clearly defined so that property rights can be attached to it.

On the other hand, the principle of publicity is practically implemented by different measures, which notably depend upon the type of things. Therein, legal value would typically be attached to the possession of movable things (e.g. by bringing presumption of property): it can for example bring presumption of ownership in French law;[30] in a different fashion, possession can bring property rights in case no stronger ownership claim is made by a third party in English law. Publicity can be granted by legal registration with regard to immovable things or movables of high value such as aircrafts, trains or cars.[31] Similarly, patent law and trademark law also provide for respective registries. The legal value to be attached to respectively possession and registration in this regard greatly differs amongst the jurisdictions and especially whether these measures of publicity also grant presumption or proof of ownership.[32]

[28] For a more detailed analysis of contract law, see Deliverable D4.1 section 4 "introduction to the legal aspects of DLTs, smart contracts and related safety and security considerations in the railway sector".
[29] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 75.
[30] France Civ 3ème 11 juin 1992.
[31] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 87.
[32] Van Erp and Akkermans, Cases, materials and text on property law, 2012, 131.

2. Data as a subject matter of ownership rights?

The economic value of data as fuel of the digital economy questions their legal status, as illustrated by the data marketplace scenario that is being discussed in this deliverable. In other words: does one (and if so, who) have ownership rights in data, just like in a car or a table? The legal answers may vary according to the national jurisdictions and, in particular, not all jurisdictions explicitly regulate whether ownership rights can be vested in intangibles. Even when statutory law includes (or does not prevent) ownership rights in intangibles, questions arise as to the "thing-ness" of data, given their specific features as will be presented hereafter.(Fairfield 2014, 850) The question of whether there is or should be ownership rights in raw data was recently reactivated on the occasion of the Communication of the Commission "Building the data economy".[33] The Commission contemplates the opportunity to create an exclusive right – such as a new intellectual property right - on "raw machine-generated data", in order to legally back a genuine data market and thereby enhance the data economy.[34]

The debate surrounding ownership rights in data and digital objects is however far from new and has in fact already been put on the table on and off. Discussions on the existence of ownership rights in "data" appears to have taken different forms which logically derives from the progressive digitization of human activities. It always boils down to the following questioning: can data, as intangibles, be subject-matter of ownership rights *in their own right* similarly to tangible things? Data ownership has therein been discussed in the context of criminal law, and especially in situations of employees "siphoning" data from the servers of their (former) employer. The emergence of cloud computing also triggered discussions with reference to the data that a customer entrusts a cloud computing provider with but also to the cloud computing virtual environment.(Bartolini, Santos, and Ullrich 2017) With the grow of online social networks, the notion of "virtual property" has emerged, specifically with regard to the property of the data featuring the activity of an online player's "avatar" – which will be further analyzed in the section 3 of this chapter.[35] With the emergence of the IoT, the legal regime of "digital content" of connected things (e.g. "digital books" in an e-book reader) provided for by the trader to consumer has been questioned too, especially its situation in the traditional "good / service"

[33] Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions "building a European Data Economy", COM/2017/09 final.

[34] The contours of such idea is further described in the 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(2017) 2 final.

[35] See for instance, Stanislaw Tosza, « AIDP global report. Online social networks and violations committed using I.T. – identity fraud and theft of virtual property », Revue internationale de droit pénal 2013/1 (Vol. 84), p. 115-139. DOI 10.3917/ridp.841.0115.

dichotomy.[36] In the specific field of data protection law, the legal nature of the entitlements of data subjects vis-à-vis personal data has also been discussed. The EU legal scholarship – following the US pattern - has notably been questioning the rationale for protecting personal data and whether data subjects would "own" the personal data relating to them.[37] The ability of the blockchain technology to create and manage "crypto-tokens" or digital coins used as money (e.g. Bitcoins) also raised questions as for their property regime. Besides, the discussion on the existence of ownership rights in data mirrors to a certain extent the questioning in relation to software ("computer programs") and databases, in particular before intellectual property rights were instituted specifically concerning them,[38] although the property regime of these objects remains controversial in some respects. (Yu 2018)

In order to rightly set the terms of the debate on the existence of ownership rights in (raw) data and for the sake of legal consistency, this chapter will take into account the broader discussion on the property of digital objects. Indeed, questioning whether "data" – as information carrier in the digital environment - as such would qualify as subject-matter of ownership rights may result in more nuanced answers, depending upon the characteristics of the data. In other words, the "on-or-off" question of whether data are or should be vested with ownership rights on data may prove to need a subtler rewriting, such as: (under which conditions) are or should ownership rights be vested in data? In that sense, the analysis performed in this deliverable meets (and relies on) a more general questioning around the fitness of property law to adapt to the digital environment, known as "digital property rights" although this expression is often followed by a question mark.(van Erp 2017, 23) The first section will look into how EU law has tackled ownership - or ownership-related – rights in data (1). The second section will then present some judicial and/or scholarly answers to the question of ownership in data or in digital objects according to national legislations (2). The last section will conclude the chapter by presenting the conceptual grounds which prevent (at least raw) data from being vested with ownership rights (3).

[36] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 9th December 2015, COM(2015) 634 final, as critically discussed in particular in (Hojnik 2017; Sein 2017).

[37] S. Gutwirth & G. Gonzalez Fuster, « L'éternel retour de la propriété des données : de l'insistance d'un mot d'ordre », in E. Degrave, C. de Terwangne, S. Dusollier & R. Queck (dir.) Law, norms and freedoms in cyberspace. Droit, normes et libertés dans le cybermonde. Liber amicorum Yves Poullet, Larcier, Collection du CRIDS, 2018, 1717-140, 8. (Pearce n.d.)

[38] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs and priorly Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs.

2.1. (How) does EU law regulate the property regime of data or digital objects?

This section does not deal with intellectual property rights. Where appropriate, intellectual property rights in (operations on) data will be touched upon in the next chapter with reference to the legal regimes applying to the data marketplace scenario. This section looks at whether and how EU law has dealt with property law – or property law-related concepts with regard to data and digital objects. While the competence of the EU to regulate property law *as such* is debated,[39] EU law has undoubtedly had an impact on property law in various fashions. The discrepancies between the national legislations of the Member States are said to have a detrimental effect on the internal market, which is all the more important in the digital environment.

2.1.1. Digital exhaustion: towards an EU concept of digital sale and of digital ownership?

The concept of "sale" has been clarified by the Court of Justice of the European Union (CJEU) with regard to an intangible software in the *UsedSoft* case in 2012.[40] The Court was requested to clarify the exhaustion of the distribution right granted by the Computer Program Directive[41] in the situation of an authorized downloading of a software copy online, *without any tangible support*. In casu, the holder of the exclusive right on the computer program – Oracle – distributed copies of its software mostly by means of internet-enabled downloading, without a tangible support. The operation was qualified by Oracle – within the meaning of the supporting contract – as a "license" contract. The license was granted for unlimited period upon payment, by which the user was notably entitled to store a permanent copy of the software. The practice of Oracle was to market licenses as part of "group licenses", which as a matter of fact could therefore remain partly unused by the customer. While Oracle license stipulated that the license provides for "non-transferable user rights", the company UsedSoft acquired un-used Oracle user licenses from Oracle customers[42], which led to legal disputes between Oracle and Usedsoft.

The question referred to the CJEU was therefore whether exhaustion of distribution rights extends to purely online downloading of a software. In other words: does the concept of "sale" within the

[39] E. Ramaekers, European Union Property Law, From Fragments to a System, Intersentia, 2013, 127-141.
[40] Case C-128/11 UsedSoft GmbH v Oracle International Corp, 3 July 2012, ECLI:EU:C:2012:407 (hereafter, UsedSoft case)
[41] Article 4 (2) of the Computer Program Directive: "the first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof".
[42] UsedSoft case, para 25 to 25.

meaning of the first sale doctrine apply to intangible software? The CJEU answered positively to this question and considered that the situation at stake qualifies as a sale, *despite the absence of tangible support of the software*. In other words, the CJEU applied a functional equivalence to the sale of tangible and intangible copies of software while the doctrine of exhaustion – linked to the concept of sale – was traditionally "developed to cover the resale of physical / tangible objects".(Mezei 2015, 24)

The *UsedSoft* case has been heavily discussed in literature.[43] The discussion revolved around the reach of the case: does it provide for guidance for qualification of *any* "sale" of intangible works? By recognizing digital sale, would the Court have attempted to recognize the existence of digital property rights?[44] Alternatively, conversely, is its reach contrarily limited to software - or even more restrictively to digital exhaustion of software *within the meaning of the Computer Programs Directive*? The CJEU is requested to clarify whether digital exhaustion also exists within the meaning of the InfoSoc Directive in a pending case related to the resale of e-books.[45] Until this clarification and in our opinion, the UsedSoft case jurisprudence shall be interpreted as applying only to digital exhaustion of software within the meaning of the Computer Program Directive.[46] The Court made indeed clear that the term "sale" shall be considered as an "autonomous concept of European Union law"[47] with regard to the "subject-matter and purpose of the directive"[48] which therefore prevents from interpreting the case as guidance on "digital sale" at large. The Court notices that the directive[49] "makes no distinction according to the tangible or intangible form of the copy [of a program] in question"[50] (article 4(2)) and further hints to the *lex specialis* character of the directive vis-à-vis copyright protection as harmonized mainly by InfoSoc Directive. This interpretation of the case appears to be confirmed by the Art & All Posters case in 2015[51] on the exhaustion of the distribution right as part of copyright protection, in which the Court insisted on the tangible character of the object onto which the protected work is incorporated.[52]

---

[43] See in particular (Hilty 2015)
[44] On the link between the UsedSoft case and digital property law, see the critical paper (Geiregat 2017) The author notably argue that, in the UsedSoft case, the Court would have confused intellectual property law and "material-object contracts" and would have attempted to create digital property rights.
[45] C-263/18, request for a preliminary ruling from the Rechtbank Den Haag (The Netherlands), in the Nederlands Uitgeversverbond (NUV)/Groep Algemene Uitgevers (GAU) v. Tom Kabinet (pending case).
[46] This position is also held in i.a. (Drexl 2017, 28)
[47] UsedSoft case, para 40.
[48] UsedSoft case, para 41.
[49] UsedSoft case, para 56.
[50] UsedSoft case, para 55.
[51] Case C- 419/13 Art & Allposters International BV v Stichting Pictoright, 22 January 2015, ECLI:EU:C:2015:27 (hereafter, Art & Allposters case).
[52] Art & Allposters case, para 40.

2.1.2. Digital content: towards Europeanisation of digital property?

Although limited in scope to B2C (Business-to-Consumer) relations and therefore not directly related to the data marketplace scenario, the concept of "digital content" needs to be briefly outlined here as the first attempt to legally categorize "digital goods" in EU law. Digital content is defined in the Consumer Rights Directive[53] as "data which are produced and supplied in digital form".[54] Recital 19 further clarifies that this encompasses "computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means". The recital further distinguishes between digital content "supplied on a tangible medium, such as a CD or a DVD [which] should be considered as goods within the meaning of this directive". On the contrary, digital content which is not supplied on a tangible medium "should be classified, for the purpose of this directive, neither as sales contracts nor as service contracts". As a result of this distinction, digital content not supplied on a tangible medium is not subject to regulation of sales contracts (namely article 18 to 20 of the Consumer Rights Directive). [55] While the Consumer Rights Directive is the first legal recognition of the "commercial use of data in sales law"(Franceschi and Lehmann, n.d., 55), it also illustrates the difficulty to design a functional equivalence of the concept of "thing" or "good" – not to mention ownership - for intangible objects, namely digital content and to ascertain the legal importance of the presence of a tangible medium.

The European Commission tried to provide an optional[56] harmonization of sales law across the EU by proposing a "Draft Common European Sales Law" (CESL). While ruling out the possibility for intangibles to be qualified as goods [57] subject to a sales contract [58], the proposal for a CESL provided for harmonization of the contractual legal regime of the "supply of digital content" mostly inspired from the legal regime of sales of goods. The concept of "digital content" was therefore envisaged as a third concept bridging the traditional "goods" vs. "service" dichotomy. Also, and importantly, the CESL proposal provided for a functional equivalence in the legal regime of the supply of digital content irrespective of it being supplied on a tangible medium or not. While never formally rejected, the proposal has *de facto* been abandoned.

---

[53] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88 (hereafter the Consumer Rights Directive).
[54] Article 2 (11) of the Consumer Rights Directive.
[55] Article 17 (1) of the Consumer Rights Directive. The Directive further provides for specific measures regarding digital content supplied to consumers.
[56] Article 3 of the Annex of the proposal for a CESL.
[57] Article 2 (h) of the CESL defined a "good" as "any *tangible* movable item […]" (emphasis added).
[58] Article 2 (k) of the CESL defined a "sales contract" as "any contract under which the trader transfers or undertakes to transfer the ownership of the goods to another person […]".

Following the abandonment of CESL, in 2015 the European Commission proposed two directives focusing more specifically on the consumer protection in contracts related to, respectively, "online and other distance sales of goods"[59] and "contracts for the supply of digital content".[60] The concept of "digital content", as it is being discussed here, is, however, noticeably limited to the regulation of contractual relations: it did not extend to the regulation of a legal status of "digital content". It does not solve whether digital content is protected by ownership rights. Precisely, while the definition of "sales contracts" in the proposed directive on online and other distance sales of goods explicitly refers to the "transfer [of] the ownership of the goods"[61], the proposed directive on contracts for the supply of digital content defines "supply" of digital content as "means providing access to digital content or making digital content available"[62] and remains silent of potential ownership rights in digital content.

2.1.3. Communication "Building the Data Economy": ideas contemplated by the Commission to foster the sharing of industrial data

Following its Communication of 2015 "A digital Single Market Strategy for Europe"[63], in 2016 the Commission issued a Communication "Building a European data economy" in which it observed that no "comprehensive policy frameworks […] currently exist at national or Union level in relation to raw machine-generated data […] or to the conditions of their economic exploitation and tradability". While raw machine-generated data are credited to have the potential to fuel the data economy to the benefit of the economy at large, the Commission considers that "machine-generated data" are insufficiently shared.[64] Among other reasons, the unbalance of bargaining power between contracting parties – such as the manufacturer of a connected device as opposed to a customer – was found to *de facto* enable the data holder to control data just like a legal "owner" would. The uncertainty surrounding the legal framework of data and operations on data was also found to be detrimental, while the Commission questioned the impact of legal fragmentation not only between the national law of the Member States

[59] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM/2015/0635 final - 2015/0288 (COD) and Amended proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, amending Regulation (EC) No 2006/2004 of the European Parliament and of the Council and Directive 2009/22/EC of the European Parliament and of the Council and repealing Directive 1999/44/EC of the European Parliament and of the Council, COM(2017) 637 final 2015/0288(COD).

[60] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final 2015/0287 (COD).

[61] In the proposal for CESL (article 2 (k)) but also in the proposal for a Directive […] on certain aspects concerning contracts for the online and other distance sales of goods, article 2 (a).

[62] Proposal for a directive on […] contracts for the supply of digital content, article 2 (10).

[63] Communication of the Commission of 6 May 2015 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—A Digital Single Market Strategy for Europe, COM(2015) 192 final.

[64] Communication of the Commission "Building a European Data economy", Para 3.2 (p. 9).

but also amongst (sector-)specific regulations. The Commission contemplates several measures aiming to foster data sharing. Among them, the potential creation of a "data producer's right"[65] on the other hand could, according to the design, amount to ownership rights in raw data (1). Complementarily or alternatively, the Commission contemplates an enhanced obligation to share or otherwise give access to data (2).

A data producer's right? - The creation of a "data producer's right" was not maintained in the proposal of the Commission for a regulation on the free-flow of non-personal data[66] so that it remains to be seen whether such a legal regime will ever be in place. The "data producer's right" was conceived as a means to enhance the trading of data.[67] The scope *rationae materia* would extend to "non-personal or anonymized machine-generated data not yet structured in a protected database", the Commission having in particular in mind the case of industrial data (marketplaces). The scope would also extend to the "metadata on the data" in relation to the latter. The protection would relate to the syntactical level of data, rather than on the semantic level – which could be protected by other legal regimes. The Commission contemplated different forms of rights. The most achieved option would consist of an ownership right-like legal regime providing *in rem* protection to the right holder and enabling him to prevent use of data by third parties without prior authorization. A more nuanced option would consist of creating a "purely defensive right" according to which the right holder would be granted legal tools (e.g. injunction) to prevent "illicit misappropriation of data" (which should be further laid down) and claim consequential damages. Several options could also be contemplated as for who could be the right holder: while "account [shall therein be taken] of the investment done and the resources put into the creation of the data", the Commission reckons that this could result in joint ownership in the complex environment of big data. In case a 'mere' purely defensive right would be created, the (lawful) data holder could be appointed as right holder. Several exceptions to the right are then laid down, such as the possible creation of an obligation to share data.

Concretely, with regard to the data marketplace scenario, the data captured by sensors placed on railway infrastructure assets would qualify as "non-personal or anonymized machine-generated data not yet structured in a protected database". Should such a data producer's right be created, they would therefore be affected.

---

[65] This measure is further discussed in the Commission staff document accompanying the communication.
[66] Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 13th September 2017, COM(2017) 495 final 2017/0228 (COD).
[67] This paragraph is based on the 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/2017/02 final, 33-36.

Obligations to share – or otherwise give access to – data? - In a different fashion, but with the same aim to enhance sharing or trading of data, the Commission also contemplates[68] additional data sharing obligations (some of them being outlined in Chapter 2). The Commission Staff Working document however mostly consists of preliminary reflections on this matter and does not lay down regulatory options.

Inspired from a French Act passed in 2016[69] and from the OECD research works on the notion of "data commons" [70], the Commission reflects upon the concept of "public interest data" which would constitute a "specific class of data which are neither 'open data' nor entirely private data". Data labelled as "public interest data" would trigger licensing obligations falling onto the data holder. Data could be considered as vested with "public interest" according to various criteria, which could result in private actors holding such "public interest data". Conceptually, such a regime could be similar to PSI regime (further outlined in Chapter 2), which makes it compulsory for public sector bodies to allow re-use of certain data that they hold, under fair 'licensing' conditions. However, PSI regime can be considered as an illustration of "open data" in the sense that any third party could re-use the data; as opposed to that, the legal regime of "public interest data" could be designed so that only certain categories of actors would be eligible to get access to – or even to get a right to re-use – the public interest data, or only for certain purposes.

To sum up, EU law is obviously confronted with the challenge of the absence of legal status of data, and in particular of its property law regime. However, EU law does not provide answers in this regard, although legislative initiatives are on-going. We will now turn to national legislation and case law.

2.2. Ownership rights in data? Conceptual challenges illustrated by national legislations and case law

Whether and how ownership rights are or should be reckoned in data has been discussed in the Member States, and mainly in Germany(Wiebe 2017, 66), The Netherlands, The United Kingdom, Italy(Franceschi and Lehmann, n.d., 3), Belgium(Gutwirth and Fuster n.d., 4) and France. This chapter does not aim to provide an (exhaustive) overview of how property law of the various Member States

[68] This paragraph is based on the 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/2017/02 final, 36-39.

[69] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JO République Française n°0235 of 8 October 2016, section 2. The legal regime of such « données d'intérêt général » however requires further implementing regulation.

[70] See in particular OECD, Data Driven innovation: Big data for growth and well-being, OECD Publishing Paris, 2015, 189.

has been tackling data and digital objects, but it leverages national legislation, case law and doctrinal discussions to present an overview of the conceptual challenges at stake. Based on the discrepancies between the national laws and on the consideration of ownership rights as a bundle of rights, the first section shows that some legal protection of (operations on) data can exist without the full bundle of ownership rights (1). The second section analyzes, through examples drawn from national law, the conceptual challenges that arise from the application of property law to data. In particular, this section outlines various criteria which trigger – or should trigger – the application of property law to data or more generally to digital objects which leads to differentiate amongst the data (2).

2.2.1. Unbundling the bundle of ownership rights: legal protection of (operations on) data without ownership

Actio revendicatio without ownership - Ownership rights have been described above as a bundle of rights. As a result, some of the rights may also be granted separately. For instance, Luxembourg passed a law designed to enable parties entrusting (cloud computing) service providers with their data ("incorporeal, non-fungible movables" in the law[71]) to have a right to claim (*action revendicatio*) the latter in case of insolvency of the service provider. The law refers to the "owner" but also alternatively to the "person who entrusted the service provider", thereby circumventing the absence of ownership rights on data. Although this law does not grant as such a legal status of property to data as such, a specific right – usually part of the bundle of rights granted by ownership rights – is created.

Sale without ownership - The owner of a thing in particular and typically has the right to alienate the thing, by means of selling or giving it (see chapter 1). Trading data as a commodity within a data marketplace legally questions this aspect of ownership rights. Is trading of data a "sale"?

While a thing subject-matter of ownership rights obviously triggers the applicable of the legal regime on sale contract, the opposite may not be true. For instance, German law on sale allows not only for "things" (within the meaning of property law) but also for "other subjects" to be sold(Franceschi and Lehmann, n.d., 55): this category of "other subjects" allows for the sale of objects that hardly fit the traditional category as "things" for lack of corporeality, such as electricity and software.(Franceschi and Lehmann, n.d., 55) Therefore, *theoretically* at least, it cannot be excluded that, under certain conditions, the law allows for the "sale" of data; this does not imply, however, that such data would be legally vested with ownership rights. It remains to be seen what legal regime would result from the qualification as "sale of data". English law in that it protects economic value, as part of equity law – aside property law – should also make part of this category, as discussed in the following subsection.

[71] Loi du 9 juillet 2013 portant modification de l'article 567 du Code de commerce [Law of 9 July 2013 Amending Article 567 of the Commercial Code] (Lux.), as quoted in (van Erp 2017, 253)

These examples obviously illustrate the discrepancies amongst the national regulatory frameworks but also highlight the flexibility of the law to accommodate new realities. While the legal status of data is unclear, ownership rights should be understood from an instrumental perspective. In other words, while ownership rights may entail a great array of legal consequences, the question should be rather: what legal consequences are found desirable and what are the tools that the law provides to attain such goals?

2.2.2. Application of national property law to data: in search for the digital equivalence to physical property

This section analyzes conceptual justifications and criteria that have been put forward to advocate the existence of ownership rights in (certain) data. Attempts have notably been made to shift the focus from "data" as subject-matter to "digital objects".

Legal value granted to the economic value of data? - One of the legal challenges lies in the gap between the undisputed *economic value* of data – or software before they were granted specific legal protection under Computer Program Directive – and the ubiquitous character of data. The question arose in relation to criminal offenses and in particular to the legal qualification of "theft". Can the economic value of data suffice to consider that they are a "thing", subject to theft? This question reciprocally leads to questioning whether *possession* of the thing is a determining criterion to qualifying a theft, namely depriving the owner of the possession of a thing. The Court of Appeal of Antwerp ruled positively to this question in 1984[72] with regard to software. It considered that copying software amounted to a theft within the meaning of Belgian criminal law in that it deprived the "owners" of the software of the economic value they derive from the software. Nonetheless, the Court recognized that they were not deprived of the "possession" of it, yet explicit legal condition for a theft.[73] The economic value (of software *in casu*) was therefore ascribed legal value as such in that it would make part of the wealth of the "owner" affected by the "theft".[74]

Although in a very different fashion, the economic value of data has also been ascribed legal value in English law where, according to Van Erp, the "duplex ordo of Common Law and Equity"(van Erp 2017, 8) enabled the "legal protection [of] economic interests" based on equity law aside from the property law regime provided for by common law. In this case, the recognition of economic value of data is

[72] Antwerpen, 13 december 1984, R.W., 1985-86, 244-246, obs. R. Verstraete, quoted in (Gutwirth and Fuster n.d., 3)
[73] Article 461 of the Belgian Criminal code.
[74] On the confusion between "property" and "wealth", see (Low and Teo 2017, 242) The authors note that confusion of property with the broader (and less legal) term "wealth" leads to artificially broadening the scope of property e.g. to any rights that one would hold (entitlements).

facilitated by the disconnect between ownership and theft: the absence of ownership right (on data) does not ban the recognition of a (data) theft. This disconnect between ownership and theft prevails also in US law which, according to Tosza(Tosza 2013, 136), recognizes theft not based on the existence of property rights in an asset but based on the fact that it has *de facto* some value. In this regard, English law, in that it protects economic interests beside property law, could be categorized in the above category of legal protection of (operations on) data without ownership.

The discrepancies amongst national jurisdictions aside, fundamentally the problem lies in the application of the concept of "possession" - core to property law in tangible assets – to intangibles[75] being essentially ubiquitous.[76] Some proponents of an (implicit) extension of ownership rights to data have argued that possession (and deprivation of possession, as in the case of theft) would be "analog-related". It would not fit the reality of the digital environment and would therefore artificially restrict the scope of "things" to physical ones. Against this background, the deprivation of an economic value deriving from the software "theft" considered as determining criterion of theft in the Antwerp case of 1984 could be interpreted, in our view, as an attempt to find a potential digital equivalent[77], although it raises many questions. In particular, it is commonly agreed that the economic value of data rise from the use that is made of them and in particular from the possibility to merge large amounts of data and have them computed by powerful IT tools. Given the requirement to precisely delineate the contours of a thing subject to ownership rights according to the principle of specialty, the economic value as determining criterion for recognizing ownership rights in data appears to be problematic.

Copying data as theft: digital property broader than property of physical goods? - In France, the Cour de Cassation (supreme judicial authority) took a radical position by ruling on two occasions[78] - namely in 2015 and in 2017 - that downloading data against the will of the data holder constituted a theft. While a theft is described in French criminal law as the fraudulent *deprivation* of someone else's property[79] (emphasis added), the Court considered that copying data - without affecting the original data – does qualify as theft. In these cases, the Court *did not (attempt to) identify* a digital functional alternative for rivalry of physical objects. The Court simply disregarded the possession of the data as a relevant criterion. In the case of 20th May 2015, also worth noting is the disregard of the Court for potential specific (conflicting) regulation of the data at stake, and notably their potential character as

[75] (Wiebe 2017).
[76] As Wiebe analyses, "the analogy to civil law property, where possession is a central concept of property in rem, cannot be upheld in a world of information that is detached from carriers and does not show the publicity function attached to bodily things", in (Wiebe 2017)
[77] Similar observation is made with regard to the law of Quebec, in (GIDROL-MISTRAL 2016, 71–100)
[78] Cour de Cassation, ch. Crim., 20th May 2015 No 14-81336 and Cour de Cassation, ch. Crim., 28th June 2017 No 16-81113.
[79] Free translation (from French) from the article 311-1 of the French Criminal Code: "Le vol est la soustraction frauduleuse de la chose d'autrui".

"administrative document"(Berger 2015, 6–8) subject to access rights and even rights of re-use by third party within the meaning of public law (PSI regime as presented in Chapter 3).

In casu, the data at stake were considered by the Court as property within the meaning of French criminal law, thereby implying that civil law shall be interpreted as including ownership rights in mere data. The Court, however, has not clarified the practical repercussions of these rulings. Based on the consideration that all data would be "things" within the meaning of civil law, should inaccurate data be subject to liability regime of vicarious goods just like physical ones? Should intangible goods – as a subject-matter of property rights - be subject to securities law? Should they be taken into account in case of bankruptcy? Although the development of internet raised numerous issues in that area, acknowledging that *mere – or all - data* would be property also questions the taxation regime that would apply to them.[80] Further, as outlined also in Chapter 1, the nature of the thing vested with property rights has – or rather shall have - an impact on the legal property regime, as the needs are different. Property law, in particular, would typically include specific provisions for immovable as opposed to movable things. To sum up, where ownership rights would be implicitly recognized in mere or all data by a court of law, this would only be the first part of the legal problem. The second one would be to design a specific legal regime able to take into account – if possible at all (see the following section) – their specificities.[81]

Data as by-product: cyberproperty - Another line of reasoning to recognize ownership of data has been – quite paradoxically – to deny them any existence and legal recognition in their own right. Data would be a "by-product" or a part of another physical thing to which the legal regime of data would therefore be ancillary. As an illustration thereof, the Higher Regional Court of Karlsruhe in Germany recognized in 1995 that the ownership right of the data carrier – where the data were physically stored – also extended to the data.[82] Such an attempt of deriving the legal status of data from this of their physical carrier has been described as "cyberproperty"(Fairfield 2014, 839) whose theoretical limitations have already been underlined by legal scholarship: in particular, the ownership of the data carrier (i.e. the servers) may not be related to the data stored which has become obvious with the emergence of cloud computing.

The remainder of this section aims to outline attempts made to distinguish amongst the data the ones that form digital objects likely to be subject to ownership rights. It does not present an exhaustive legal analysis but aims to highlight the importance and difficult of delineating a digital "thing" within the meaning of property law.

---

[80] (Erlank 2015, 19)
[81] (Low and Teo 2017).
[82] OLG Karlsruhe, Urt. v. 07.11.1995 – 3 U 15/95 – Haftung für Zerstörung von Computerdaten, as referred to in (Wiebe 2017).

Rival digital objects: virtual property as legal property? - The emergence of virtual online worlds has given rise to a new approach to property in data or, more generally, in digital objects. Virtual worlds are "online environment in which [many] people interact with one another on a persistent basis through their online personae known as avatars".('What Virtual Worlds Can Do for Property Law by Juliet M. Moringiello :: SSRN' n.d., 160) In the case of virtual game worlds (e.g., World of Warcraft), the participants play through virtual world account that they create and spend "time and effort, or money" on to develop. While (black) markets have developed to "sell" the avatars, avatars' have also been hacked which questioned the value of the avatar (beyond the possible qualification as cybercrime). Are the avatars and/or the virtual items traded in the game protected by ownership rights to the benefit of the player having paid to be able to uniquely use them? In other words: does "virtual property" amount to actual legal property? (Erlank 2015, 3)

The American scholar Fairfield defined virtual property as "code that mimics the properties of real-space objects; it is rivalrous, connected and persistent" which would allow for the legal recognition of property. Persistency therein refers to the fact that the data does not "normally fade, decay, wear, or disappear through persistent use". [83] Against this background, the mere fact that virtual property has economic value would not *per se* be sufficient. Rather core to the reasoning is the fact that the virtual goods – the avatar and its "property" - are made unique within the operation of the game. It is in this respect crucial that the "virtual world" is common to a community of players so that there is not only a relation between a game publisher and a player but also with third parties, namely the other players.[84] This is in sharp contrast with digital content provided bilaterally to consumers, such as, for instance, e-books.

This line of reasoning has been recognized also by courts in the Netherlands. A siphoning of "virtual property" was qualified as theft with violence committed by a group of boys in the virtual community game Runescape, in a case ruled by a Dutch Court in 2009.[85] As highlighted by Erlank,(Erlank 2015, 2546) the fact that the thieves used violence is of utmost importance, as it offered the Court an opportunity to circumvent the complex issue of "virtual property" and convict the boys based on the criminal offence of assault. However, the Court took the "virtual property" case and considered that

[83] (Fairfield 2005, 20) This definition of property is very similar to the famous *Ainsworth* test in English law: in his speech in National Provincial Bank Ltd v Ainsworth, Lord Wilberforce gives the following criteria for legal recognition of property: "Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability" ([1965] AC 1175, 1247-1248).

[84] This point is also observed in (Erlank 2015, 8)

[85] LJN: BG0939, Rechtbank Leeuwarden, 17/676123-07 VEV, as referred to in (Lehdonvirta and Virtanen 2010, 8) For a study of Asian court cases related to virtual property, and especially of China and South Korea, see (Erlank 2015, 2543)

virtual items indeed qualified as immaterial property within the meaning of the law based on the following consideration: it had value for the possessor but also for the accused boys. In order to qualify as theft, the Court noted that there had been an actual transfer of control of the virtual items from the initial possessor to the accused boys. Based on national statutory law, which recognizes property in immaterial goods, the Court denied immateriality of the goods as element preventing them from potential ownership rights. Similarly, the Court did not require physical transfer of the item but transfer of the control over it,(Erlank 2015, 2547) thereby functionally adapting the definition of theft to the immaterial nature of the item.

The unique character of the avatars was made possible only based on the technical operation of the game publisher who creates rivalry (or exclusivity), within the framework of the specific "virtual world". Based on the concept of virtual property that virtual games only helped uncover, Fairfield argued that ownership rights exist on other digital objects, such as "domain names, URLs, websites, email accounts, etc.",(Fairfield 2005, 5) based on the same consideration that they are rivalrous, persistent and interconnected – meaning that all internet users are confronted with them.(Fairfield 2005, 14) A US Federal Court Circuit ruled that a domain name is an "intangible property right".[86] Some authors go a step further by suggesting that "e-books, digital music, movies and apps"(Storr and Storr 2017) could be considered as forms of "virtual property" although sometimes supplied in a purely bilateral contractual way, without third parties being involved or affected as would for instance be the case of a community of users in virtual games worlds.

To sum up, the discussion on "virtual property" invites to break the tangible vs. intangible dichotomy by reconsidering the deemed ubiquity and non-rivalry of data or more generally digital objects. Firstly, it equates "possession" of tangible things with "control" (van Erp 2017, 243–46) of intangible ones. Secondly, it further distinguishes amongst the "data" the ones that are made rival and can therefore be controlled. Such a position anyway bars the existence of ownership rights on raw data, such as railway infrastructure data in the data marketplace scenario.

Blockchain crypto-tokens: how to define the digital "thing"? - The emergence of cryptocurrencies created by means of the blockchain technology can be seen as an academic opportunity to further think about digital property besides the obvious practical and societal importance of deciding whether crypto-tokens are or should be vested with ownership rights. To name but a few, siphoning of crypto-tokens has already happened.[87] Setting aside the interests of crypto-tokens holders, other parties, such

[86] Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003), as reported by ('What Virtual Worlds Can Do for Property Law by Juliet M. Moringiello :: SSRN' n.d., 664)

[87] (Low and Teo 2017). Some authors have also contemplated the issue of property from the perspective of inheritage, see (Conway and Hickey 2017, 104)

as public authorities, have an obvious interest in qualifying transactions for various purposes – particularly for tax purposes.

Among other legal challenges, the following is of notable importance for our study on the existence of ownership rights in raw data. Deciding whether ownership rights exist in or around crypto-tokens requires that we firstly identify the "thing" at stake pursuant to the principle of specialty in property law. While this task may prove evident in the case of physical goods that can be sensed directly, a clear identification of digital objects proves more difficult. Although the common belief would be that blockchain users own e.g. Bitcoin, how do we concretely define Bitcoin? As reported by McGrath, Bitcoins are described by their pseudonymous creator Nakamoto as "a chain of digital signatures",(McGrath 2016, 20) or, in other words, "there is no such thing as a Bitcoin".[88] The blockchain system is designed to trace the *value* of the coin; however, the *actual data* used for doing so obviously do not *remain* over the course of transactions: they are modified at every transaction, precisely to transfer and maintain the *value* of the cryptocurrency. Concretely, the transaction consists of inserting *new* information on a block, including a reference to the previous transaction.[89]

This difficulty in finding criteria to identify and delineate the "thing-ness" of a digital object within the technicalities of the blockchain operation has led to very different legal conclusions as for the delineation of a "thing" suitable for ascription of ownership rights,[90] independently from the obvious observation that studies have been conducted on the basis of different legal regimes. While some argue in favour of following the transfer of value, it has otherwise been argued that property law cannot be applied for lack of an identifiable subject-matter[91] or that ownership rights can be applied only to the private keys that the users transfer by transacting cryptocurrencies or in other words to the means by which the bitcoin value is transferred.(McGrath 2016, 20) It has also been argued that the holders of bitcoins would only have "the legal right to have their bitcoins locked to their chosen public bitcoin address on the blockchain".[92] These diverging conclusions illustrate the fact that the legal analysis is based on ownership rights in tangibles and attempts to find criteria to ascribe "thing-ness" to intangibles. The legal problem lies (sometimes implicitly) in the determination of the level of technical details that should be taken into account to decide upon digital equivalence. As described by

[88] (Low and Teo 2017).
[89] For a more thorough explanation of the operation of Bitcoin transactions, ('Cryptocurrencies in the Common Law of Property by David Fox :: SSRN' n.d., 7)
As reported by Szelagyi, Murck assets that "Bitcoins are constantly mutating entities that are remade each time they are worked upon", (Szilagyi 2018, 11)
[90] On this matter, see the analysis of philosophical justification for property in (Szilagyi 2018).
[91] (Low and Teo 2017).
[92] (Low and Teo 2017).

Fairfield, blockchain invites lawyers to further refine the concepts of property law and in particular, the concept of a thing ("thing-ness")[93] which will be further discussed in chapter 3.

With regard to the data marketplace scenario, the line of reasoning presented here leads to the following conclusions. Firstly, by shifting the focus from data to digital "something" as a subject-matter, it conceptually bars the existence of ownership rights in raw data as such. The latter are regarded more as an instrument to create digital objects potentially subject to property law than as an object in their own right and in isolation. Secondly, it questions the impact of the blockchain technology as supporting tool of the data marketplace: does it affect the property law regime of the data being traded? This question will be analyzed in Chapter 4.

2.3. Raw data as poor candidate to ownership rights

This section concludes the chapter by wrapping up the reasons why *raw data* are a poor candidate to ownership rights, be it by means of implicit extension of statutory law or by means of recognition of specific ownership rights in raw data depending upon the legal order at stake.

2.3.1. Data as *de facto* poor candidate to appropriation

The characteristics of data have been found to make them an inappropriate candidate to ownership rights. (Gutwirth and Fuster n.d., 13) Their volatility and relatively short lifecycle as well as their non-rivalry (or "non-excludability"[94]) make data practically impossible to delineate and to control and therefore inappropriable.[95] Storr and Storr further notice that data, taken as objects, "has no physical counter-part":(Storr and Storr 2017) they cannot qualify as "things" subject to appropriation. These features would make it equally difficult to determine who the owner of the data would be and whether should there be an ownership right. It is all the more true that data are precisely used as communication means or, in other words, "in motion". As Wiebe explained, based on the example of data stemming from "networked cars", many different actors indeed take part to some extent to the production of data: the car manufacturer, the owner of the car, the software manufacturer, etc. Should

[93] (Fairfield 2014) The author argues that the concept of a thing as subject-matter of property law should be defined as "information about the limit of rights" instead of the physical boundaries of the subject-matter. What ultimately matters is to be able to delineate – within the meaning of the law – what is subject to property law. Physical aspect of a thing is – even in pure tangibles – never fully relevant. In order for a car to be subject-matter of property law, legal delineation is needed. Mere physicality of the car is not enough as the car itself consists of various pieces that together form the carOn the delineation of the contours of a "thing" within the meaning of property law.

[94] In the parlance of (Grimmelmann 2010)

[95] (GIDROL-MISTRAL 2016)

an ownership right exist regarding such data, Storr and Storr have observed that this could lead to complex situations of joint ownership.

This should not be interpreted as banning the existence or recognition of ownership rights in *all data,* or rather in any *digital object*. To compare, atoms are not recognized as subject-matter of ownership rights, but this does not prevent *physical objects* constituted by atoms to be vested with ownership rights. This conclusion should be interpreted as an invitation to find a way to break the tangible/ intangible dichotomy in property law and to design principles according to which property law would adapt to intangible objects. As touched upon in this chapter and as further discussed in chapter 4, the blockchain technology has the capability of creating some form of rivalry in digital goods and thereby anew places this question on the agenda.

2.3.2. Specific legal regimes of intangibles

Ascription of ownership rights in data has been opposed on the ground of the existence of specific regimes related to intangibles, over the course of their creation and development. The argument goes that the lawmaker, by creating *lex specialis* regulations for intangibles, would have banned the extension of property law applying to tangible goods *mutatis mutandis* to intangible ones. In this regard, the lawmaker notably chose to set up intellectual property rights on intangibles, but also ownership rights on some intangible assets such as carbon credits or company shares.(Reed et al. 2017) A *contrario,* other intangibles shall be considered as not being covered by *implicit* extension of ownership rights. (Gutwirth and Fuster n.d., 5) This argument is based on the legal *numerus clausus* principle: it is only by exception, explicitly provided for in statutory law, that ownership rights exist are created, the principle being non-appropriation. This is essentially what the Court of Appeal of the United Kingdom ruled in 2014[96] regarding a database. The Court considered that the recognition of a database as a subject-matter of common law liens[97] would imply to recognize a database as a thing owned which requires an act of the Parliament.

The same could be said in relation to criminal law and especially to theft. The Budapest Convention on Cybercrime,[98] as implemented in EU law by the Cybercrime Directive, provides for specific criminal offences in relation to information systems and computer data, implying that these provisions constitute *lex specialis* regime, which bans the existence of "theft" in data. In particular, Article 5 of the Cybercrime Directive ("illegal data interference") makes it mandatory for Member States to punish as criminal offences the activities of "deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and

[96] Our Response Limited v Datateam Business Media Limited [2014] EWCA Civ 281, 14 March 2014.
[97] A specific form of security.
[98] International Convention on Cybercrime, ETS No 185.

without right, at least for cases which are not minor". The *lex specialis* would render the general prohibition of theft irrelevant.

This argument is reinforced by a classical legal argument of regulatory consistency. The implicit extension of ownership rights to data would actually result in paradoxical situations where data could turn out to be subject to higher legal protection than, among others, intangibles protected by intellectual property rights, subject to limitations such as limited duration, exhaustion, private use exception and others, although being protected by intellectual property rights requires specific conditions to be met.[99] The same could be said about digital or, more generally, intangible objects.

2.3.3. What rationale for the creation of an ownership right in data?

Based on the consideration that an implicit extension of statutory ownership rights to data would be in breach of substantial legal principles such as the *numerus clausus* principle, ownership rights in data would need, if found necessary, to be specifically created. One could reasonably ask, what the rationale for setting up such a legal regime would be.(Drexl 2017, 30–38) While various rationales may concurrently justify the creation of ownership rights, Storr and Storr(Storr and Storr 2017) note that the core rationale lies in the scarcity of goods. Ownership rights are in this regard a form of economic allocation of scarce resources.

Yet, data were precisely described as abundant and non-rivalrous. It has therefore been argued that, from an economic perspective, legal appropriation of data would not be advisable. Among others, the argument goes that data, contrary to physical goods, can be shared easily and with limited transactional costs. The study of data's lifecycle would show a link between, respectively, the production and the distribution phase: the more data are distributed, the more (other) data are created. Incentives to produce data would not stem from the perspective of exclusive rights on data but mostly from the perspective of *what can be done* together with the creation and distribution of data.(Grimmelmann 2010, 2811–14) In our opinion, this question again shows that property law generally struggles to deal with data and digital objects and to find a digital equivalence to property law on physical goods.

[99] This argument is applied by analogy to the argument developed with regard to parasitism in Belgian law in A. Puttemans (Ed.), Introduction générale, principes et interrogations - Réflexions autour de l'arrêt Noël Marquet de la Cour de cassation, Vol. 1. Propriété intellectuelle & concurrence déloyale – Les liaisons dangereuses ?. Bruxelles: Larcier.(Collection de l'Unité de droit économique de l'ULB).

2.3.4. Ownership rights in data: in breach of fundamental rights?

Some legal scholars have argued that ownership rights on mere data would result in violations of various fundamental rights.(Drexl 2017; Yu 2018) In particular, it has been argued that, by allowing for appropriation of information, ownership rights in data would be in breach of the freedom of expression [100], which includes, more specifically, the freedom to impart, access and receive information. In this regard, the existence of ownership rights on data have been denied by the New Zealand Court of Appeal based on the consideration that this would be in breach of the principles of freedom of expression and free flow of data – recognized as higher-ranking legal principles of law.[101] The law of New Zealand obviously has no legal effect on the law of the EU or of its Member States, but it serves nonetheless as an illustration of the global search for a legal status of data. This line of reasoning can be traced back to the statement that information carried by data has not only economic value, but equally so a social and political value. Serge Gutwirth and Gloria Gonzalez Fuster therein consider that information should, by default and save *lex specialis* regimes, be a "common good", namely arguing that it should remain free and non-appropriable.[102]

2.3.5. Conclusion

This chapter provided for a presentation of the conceptual legal challenges raised by the recognition of data as subject-matter of ownership rights. It is based on the analysis of EU law, where available, and examples from national legislations and case law as illustrations of the different points. Ownership of data should be analyzed in the broader long-standing questioning on the application of property law to the online environment. To conclude, recognition of ownership rights in data is generally dismissed, as 'data' do not appear to be an appropriate object for property law. This does not mean that property law should be restricted to physical objects and disregard the digital environment. Quite the opposite, a "digital update"(Drexl 2017, 26–27) of property law is definitely needed but it should attempt to find appropriate criteria for a "functional equivalence" of physical property by looking at digital objects rather than at data as such. Data (and operations on data) are anyway subject of various legal regimes, which will be discussed in the following chapter with a focus on the railways. Whether "data" has or should have a legal status *by default* is still an open question, which will be further referred to in chapter 4.

[100] Article 11 of the Charter of Fundamental Rights of the European Union (2000/C 364/01).
[101] Jonathan Dixon v. The Queen [2014] NZCA 329 (CA516/2013) at [31]–[35] (N.Z.), as quoted in (van Erp 2017, 246–49) The decision of the Court of Appeal was then quashed by the Supreme Court.
[102] (Gutwirth and Fuster n.d., 14) Similar views have been expressed in the US, see (Determann 2018)

3. Specific presentation of the rights related to data in the railway sector

This chapter will present the main regulatory frameworks that can be applicable in relation to data used in the railway sector. Many legal regimes are likely to apply to a data-marketplace taking place in the railway sector, and in particular on the basis of the activities of a railway infrastructure manager. In order to bring order into this patchwork, a classification is needed: this chapter classifies the legal frameworks according to their purpose. Firstly, applicable intellectual property rights are presented, as they can be considered the most legal powerful means for actors to control data (1). The second section signals other legal regimes, which result in some form of control over data (2). The third section briefly presents legal regimes aiming to enable third parties to get access to certain data (3). Deriving from this classification, the presentation brings general legal frameworks together with the railway sector-specific ones. This presentation does not aim to provide detailed and *a fortiori* exhaustive explanations of the legal regimes involved.[103] Emphasis is rather laid in the following question: how and how far is the current regulatory framework fit for the purpose of establishing a data marketplace? The last section will therefore wrap up more general conclusions as for how the legal framework is at odds with a data marketplace (4).

[103] For thorough outlines of the legal frameworks having an impact on the "ownership" of data, see (Duch-Brown, Martens, and Mueller-Langer 2017; Union 2016)

3.1. Intellectual property rights

3.1.1. Copyright

Legal basis	Subject-matter, requirements and applicability to the scenario	Right holder and right debtor(s)	Legal regime
InfoSoc Directive [104] – currently under revision[105] - as transposed into national law; further national law[106] **Database directive (Chapter II) as transposed into national law**	Protection of works, expressed in a form and vested with originality. Originality implies that the work expresses the author's own intellectual creation by making free choices[107].	The initial right holder is the author of the work. The right holder can oppose her rights against any infringing third party (*erga omnes* effect).	The author is granted: - Moral rights: [109] at least the rights of paternity and integrity. Some Member States grant further moral rights. - Economic rights (harmonized by the InfoSoc Directive): exclusive right of reproduction [110], exclusive right of communication to the public[111], and exclusive right of distribution[112]. Economic rights can be assigned to or transferred to third parties.

[104] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19, hereafter the InfoSoc Directive.
[105] Commission, 'Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market' COM(2016) 593 final.
[106] Beyond the transposition of the InfoSoc Directive, national law shall provide for moral rights to the authors, as stated by the Berne convention for the protection of literary and artistic works 1886/1971.
[107] Case C-5/08 Infopaq International A/S v Danske Dagblades Forening, 16 July 2009, ECLI:EU:C:2009:465, para 36-39; case C-145/10 Eva-Maria Painer v Standard VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, Spiegel-Verlag Rudolf Augstein GmbH & Co KG, Verlag M. DuMont Schauberg Expedition der Kölnischen Zeitung GmbH & Co KG, 1st December 2011, ECLI:EU:C:2011:798, para 88-93.
[109] Article 6 bis of the Berne convention.
[110] Article 2 (a) of the InfoSoc Directive.
[111] Article 3 (1) of the InfoSoc Directive.
[112] Article 4 (1) of the InfoSoc Directive.

	Copyright exists without any prior without registration requirements[108].		This protection is however limited by exceptions and limitations and in particular: - Time limitation – in principle lifetime of the author and 70 years. - Exhaustion of the exclusive right of distribution through the first sale[113] or equivalent transfer of ownership. - List of mandatory and optional substantial exceptions, as stated in the InfoSoc Directive[114] and pursuant to national transposition.
	Application to the scenario: raw data do not qualify as authorial work for lack of originality(Drexl 2017, 45). They could however be protected by copyright – *inter alia* and subject to legal assessment analysis *in concreto*: the structure of databases[115] although it does not extend to the contents,[116] computer programs, visualization webpages. The copyright protection however only extends to the embodiment of the work, and not merely to the abstract ideas.		

3.1.2. *Sui generis* legal protection of databases

Legal basis	Subject-matter, requirements and applicability to the scenario	Right holder and right debtor(s)	Legal regime

[108] Article 15 (1) of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979) - TRT/BERNE/00.
[113] Article 4 (2) of the InfoSoc Directive.
[114] Article 5 of the InfoSoc Directive.
[115] In accordance with the specific legal provisions of Chapter II of the Directive 96/9/EC (see reference in 117).
[116] Article 3 (2) of the Database Directive.

Database Directive[117] **– as transposed into national law.**	Specific protection of database, namely "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".[118] Requirements for protection: the maker shall demonstrate that there has been "qualitatively and/or quantitatively a substantial investment" in the database making, namely in obtaining, verifying, or presenting the contents […][119]. The investment shall concern the database itself and not the creation	The right holder is the "maker" of the database (natural or legal person according to national law)[121], namely to the "person who takes the initiative and the risk of investing".[122]	The right holder may prevent unauthorized extraction and/or reutilization of the whole or substantial parts of the data by third parties[123]. In other words, the *sui generis* protection covers the contents of the database. While unauthorized non-substantial extraction, reutilization of the data or mere consultation of a database would not constitute an infringement, a *constant availability* of data sources by means of a data marketplace could constitute substantial reutilization.[124] The protection shall last 15 years.[125] While this term may seem short, it runs as from the "date of completion of the making of the database". Databases are often ever-evolving and therefore never fully completed so that the protection

[117] Chapter III of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28, hereafter the Database Directive.
[118] Article 1 (2) of the Database Directive.
[119] Article 7 (1) of the Database Directive.
[121] Article 7 of the Database Directive.
[122] Recital 41 of the Database Directive.
[123] See article 7 of the Database directive.
[124] Case C-202/12, Innoweb v. Wegener ICT Media, 19 December 2013, ECLI:EU:C:2013:850, para 23-54.
[125] Article 10 of the Database Directive.

	of "independent materials [120] (e.g. data) although practically drawing the line may prove difficult.		may "last indefinitely" (Union 2016, 15), namely on the "substantial investment" made[126]. The Directive provides for optional exceptions that Member States may implement in their national law.[127]
	Application to the scenario: databases bringing together data captured in the course of the business may prove not to be covered by the *sui generis* protection, failing to prove *specific investment* in the making of the database itself. However, many databases used by the different actors involved are likely to be protected, subject to *in concreto* analysis. In particular, and subject to specific legal analysis, the blockchain ledger at stake might be protected by the *sui generis* protection. Determination as to who is the "maker" holding the legal protection is subject to controversy, especially with regard to public blockchains. In the case of a private blockchain and subject to the operational arrangement between the concerned actors, the maker could be the IT integrator providing and running the blockchain or the actors involved jointly.		

[120] Case C-46/02, Fixtures Marketing Ltd v Oy Veikkaus Ab, 9 November 2004, ECLI:EU:C:2004:694, para 30-40; case C-203/02, The British Horseracing Board Ltd and Others v William Hill Organization Ltd, 9 November 2004, ECLI:EU:C:2004:695, para 25-36.
[126] Article 10 (3) of the Database Directive.
[127] Article 9 of the Database Directive.

3.2. Other regulations related to the control of data

The following pieces of legislations are hereby brought together on the ground that they result in narrowing the scope of the data that can be brought to the data marketplace by providing for some form of control over data. However, they happen to differ on other aspects. Firstly, they differ with regard to which party is legally granted some control over the data, namely the data holder or some other party. Secondly, while some grant the right to control data or information, others (such as safety and (cyber-)security legal frameworks) make the control over data an obligation rather than a right. This great diversity is illustrated in the table by the different applicable legislations that somehow relate to confidentiality of data or information.

3.2.1. Trade secrets legal protection

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Trade Secret Directive[128] **as transposed into national law**	Protection of trade secrets[129] that: - is secret[130], - "has commercial value because it is secret" and - "Has been subject to reasonable measures to be kept secret". Industrial data could be subject to trade secret protection, subject to national law transposing the directive.(Surblyte 2016, 9) It would necessarily entail that "reasonable measures" have been taken to keep	The trade secret holder is the person "lawfully controlling the trade secret".[131] The trade secret legal protection can be held against "infringers".[132]	Acquiring, using or disclosing trade secrets may qualify as unlawful according to the circumstances and to the quality of the entity at stake.[133] Notably, the disclosure of trade secrets in breach of a confidentiality agreement can qualify as unlawful use or disclosure within the meaning of the directive. [134] Further, the directive prohibits commercial activities (such as production and placing on the market) of "infringing goods", namely goods "significantly benefit[ing]" from unlawful activity regarding trade secrets, when performed with knowledge of the unlawful activity.[135] The directive provides for extensive remedies that the trade

[128] 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, OJ L 157, 15.6.2016, p. 1–18.
[129] Article 2 (1) of the Trade Secrets Directive.
[130] "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", article 2 (1) (a) of the Trade Secrets Directive.
[131] Article 2 (2) of the Trade Secrets Directive.
[132] Article 2 (3) of the Trade Secrets Directive.
[133] Article 4 of the Trade Secrets Directive.
[134] Article 4 (3) (b) and (c) of the Trade Secrets Directive.
[135] Article 2 (4) and article 4 (5) of the Trade Secrets Directive.

	them secret. Trade secrets may be in electronic form or in other forms.		secret holder may exert against infringers, not only on the merits[136] – but also provisional measures.[137] The directive not only provides for exceptions[138] subject to balancing tests grounding in fundamental rights and freedoms – such as the freedom of expression. It also lays down the conditions under which use, disclosure and particularly acquisition of trade secrets shall be deemed lawful.[139]
	Application to the scenario: many data or information of different sorts directly or indirectly related to the trading within the context of the data marketplace could theoretically be protected by the legal protection of trade secrets, such as raw data but also algorithms and/or the data that they produce.[140] However, it remains to be seen how the Trade Secrets Directive applies to data produced by algorithmic applications and, more specifically, to the scope of protection. The datasets as a subject-matter would seem to better fit the definition of trade secret than single data, in particular with a view to the condition that secrecy grants commercial value. Indeed, "particular value may arise from correlations with other data" rather than from a single datum.[141] In the case of data analytics made on the data transactions within the context of the data marketplace, it still remains to be seen who the beneficiary(ies) of the legal protection would be, or in other words who the party lawfully controlling the information within the meaning of the Trade Secrets Directive would be. Such questions would require *in concreto* legal analysis.		

[136] Articles 12 to 14 of the Trade Secrets Directive.
[137] Article 10 of the Trade Secrets Directive.
[138] Article 5 of the Trade Secrets Directive.
[139] Article 3 of the Trade Secrets Directive.
[140] (Surblyte 2016, 9) In (Zech 2016, 465), the author suggests that raw data could be protected as trade secret, subject to specific legal analysis of the case.
[141] (Drexl 2017, 23) This submission is also made by the European Commission in the 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 {COM(2017) 9 final}, 20.

	Disclosure of data to some third parties does not, theoretically, absolutely preclude them from qualifying as "trade secret", provided they still remain "secret" and under the control of the right holder within the meaning of the directive. This remains however subject to judiciary application given the newness of the directive. In any case, 'trading' data on a data marketplace to various – anonymous or pseudonymous – business partners beyond the "need-to-know" basic principle of confidentiality seems at odds with the requirement to keep information secret. A specific legal analysis should, where appropriate, be conducted given the specificities of the case and notably on the quality of the actors involved in the data marketplace and the rationale for disclosure. Generally speaking, sharing data obviously tends to make it more difficult to protect secrecy and therefore to invoke the protection of trade secrets[142]. In turn, this may have a chilling effect on the willingness of actors to share 'their' data.[143]

[142] This finding is also underlined in the Commission Staff Working Document on the free flow of data and emerging issues in the European data economy, accompanying the document Communication Building a European Data Economy, {COM(2017) 9 final}, 20.

[143] As underlined in (Zech 2016, 466), legal protection of trade secrets "resembles the protection of possession". Loss of actual control of the information therefore logically implies a loss of legal protection.

3.2.2. Data protection and privacy

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Data protection and privacy – in particular GDPR[144] and national law	"Personal data" is defined broadly. Within the meaning of the GDPR, personal data refers to "any information relating to an identified or identifiable nature person (data subject". Identification can even be indirect, namely by means of reference to "an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic,	The right holder is the "data subject".[146] The right debtors are, primarily, the controller(s)[147] and secondarily, the processor(s).[148]	The data marketplace deals with industrial data related to the condition of railway infrastructure assets so that no personal data shall in principle be involved and no further discussion is provided here. However, given the broad definition of "personal data", *in concreto* legal compliance analysis would need to be conducted in the case where such a data marketplace would be deployed. Notably, the data analytics performed on the basis of the data marketplace could involve the processing of personal data (such as location and time of data transactions together with the IP addresses). Some data traded as part of

[144] 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), OJ L 119, 4.5.2016, p. 1–88.
[146] See in particular article 4 (1) and Chapter III of the GDPR.
[147] The controller is, according to article 4 (7) of the GDPR, "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".
[148] The processor is, according to article 4 (8) of the GDPR, " a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

	mental economic, cultural or social identity of that natural person".[145]		the data marketplace could also involve personal data, e.g. as part of the railway assets maintenance track record.

3.2.3. Confidentiality obligations: safety and (cyber) security regimes

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Protection of confidential information – safety and (cyber-)security **EU law and national law**	The NIS Directive [149] and the ECI directive[150] may apply to the railways subject to national transposition and designation. Besides, the Railway Safety Directive [151] applies to the railways.	Depends upon national legislation.	These directives do not regulate as such the confidentiality of safety or (cyber-)security sensitive information. They make it compulsory for Member States and, respectively, the railway operators (the IMs) to set up national regulatory frameworks protecting safety and security which would imply confidentiality of safety or security-sensitive information. The legal regime of confidential information based on safety and/or security therefore depends upon national law.

[145] Article 4 (1) of the GDPR.
[149] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.
[150] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)
OJ L 345, 23.12.2008, p. 75–82.
[151] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety (Text with EEA relevance), OJ L 138, 26.5.2016, p. 102–149.

			Confidentiality of safety or security-sensitive information would typically entail classification of information and criminal penalties in case of unauthorized access to or misuse of confidential information.
	Application to the scenario: these specific regulatory frameworks imply – especially for the IM – a duty to filter the information or data to be exchanged on the data marketplace. For instance, information relating to past safety or security incidents are very likely to be considered secret. This could also be the case of information on past failures of railway infrastructure assets, predictions of failures, and/or of instructions to maintain them, among others. Filtering would be all the more required from the IM if the data marketplace is comprised of many and pseudonymous actors. Indeed, and save the case of high-ranked classified information whose access may simply be prohibited, confidentiality would usually be grounded in the "need-to-know" principle. This principle would imply that a contracting company providing maintenance services may be granted access to some information that a third party would be denied access to. This would obviously have a chilling effect on the IM. The IM may (have to) go further by imposing confidentiality obligations on its suppliers with the information that they may derive from confidential information related to railways. For instance, it is likely that the national law or the IM would also impose confidentiality obligations on a supplier of data analytics based on railway infrastructure maintenance data. As a result, confidentiality obligations relating to safety and security would also have an impact on the data produced by third parties – and in particular contractors of the IM.		

3.2.4. Confidentiality obligations: public procurement

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Protection of confidential information – public procurement – Utilities Directive [152] **as transposed into national law**	As part of public procurement regulation, the Directive provides for confidentiality obligations falling on the "contracting entity" to the benefit of the "economic operators". Confidential information is "information forward[ed] by economic operators which they have designed as confidential, including but not limited to, technical or trade secrets and the confidential aspects of tenders".[153]	The contractors of the IM – IT service provider, maintenance providers, etc. – are the right holders *vis-à-vis* the IM as contracting entity.	The information identified by the economic operators as confidential, shall not be disclosed by the contracting entity (the IM). In that sense, public procurement rules provide for extensive protection of information disclosed by the economic operators to the contracting entity. These provisions are, however, without prejudice to national law (e.g. as part of right of access). National law could in particular further regulate contracts concluded on the basis of public tendering procedures.[154]
	Application to the scenario: the IM, as a contracting entity, may be subject to confidentiality obligations *vis-à-vis* some data or information provided (prior) economic operators and service providers, which would limit its ability to trade these data and information to that extent.		

[152] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance, OJ L 94, 28.3.2014, p. 243–374.
[153] Article 39 (1) of the Utilities Directive.
[154] For instance, Belgium regulates contractual relations between a contracting entity and an economic operator with the Royal Decree of 14th January 2013, 2013-01-14/09 (Arrêté Royal établissant les règles générales d'exécution des marchés publics or Koninklijk besluit tot bepaling van de algemene uitvoeringsregels van de overheidsopdrachten).

	More generally, the IM and respectively its service providers may be subject to further statutory regulation of contracts concluded on the basis of public tendering procedures, which may have an impact on their ability to trade data.

3.2.5. Confidentiality obligations: railway market regulation

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Protection of confidential information – railway market regulation – EU Directive [155] as transposed into national law	Protection of the commercial confidentiality of the information provided by or related to customers of the IM (RUs and applicants).[156]	The respective customers of the IM (RUs and applicants) are the beneficiaries of the legal protection that they can invoke against the IM.	The directive makes it compulsory for the IM to respect the "commercial confidentiality"[157] of the information provided to it by the applicants or customers within the context of capacity allocation. The directive does not provide for further explanation about what is to be considered as confidential. The directive does neither specify what legal regime the tag of "confidential information" entails, nor the sanctions incurred in case of violation of confidentiality. Therefore, it falls within the regulatory competence of the Member States.[158]

[155] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area Text with EEA relevance, OJ L 343, 14.12.2012, p. 32–77

[156] Within the meaning of Directive 2012/34/EU, an applicant is "a railway undertaking or an international grouping of railway undertakings or other persons or legal entities, susch as competent authorities under Regulation (EC) No 1370/2007 and shippers, freight forwarders and combined transport operators, with a public-service or commercial interest in procuring infrastructure capacity" (article 3 (19) of the Directive). In other words, an applicant is a functional notion referring to an entity that requests or is likely to request infrastructure capacity.

[157] See article 29 (4) and 39 (2) of the Directive 2012/34/EU.

[158] Whether the legal regime shall be aligned with this of the new Trade Secret Directive or not is for the time being an open question.

	Application to the scenario: the information to be considered confidential is, firstly, the information related to capacity allocation and charging that allow identification of a customer and of its business model. Infrastructure assets maintenance information, for instance, are less likely to include information that would be confidential in relation to the commercial interest of the RUs. However, information about the technicalities of the trains may in certain instances be considered confidential, subject to national law and to specific legal analysis of the case. Generally speaking, the legal duty to protect its customers' confidentiality is likely to have a chilling effect on the willingness of the IM to share data to third parties, other than on a "need-to-know" basis, although the confidentiality regime depends upon national transposition.

3.2.6. General contract law

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
General contract law [159] **– national law**	Save when prohibited by the law, parties to a contract may as a rule organize their respective rights and obligations one with another. The parties may in this way contractually design a legal regime for the information or data that they exchange or share.	The parties to a contract, one *vis-à-vis* the other(s).	The CJEU confirmed[160] that, contrary to databases protected by copyright or *sui generis* protection (see above), other databases are not subject to the protection granted by Article 15 of the Database Directive. The latter makes null and void any contractual clause which amounts in substance to overriding exceptions to the legal protections on databases to the benefit of lawful users. This judgement creates a paradox in that it allows makers of databases, which do not qualify for legal protection of databases, to impose on third parties, by

[159] For a general presentation of contract law, see Deliverable D4.1, section 4.
[160] Case C-30/14 Ryanair Ltd v PR Aviation BV ECLI:EU:C:2015:10 ('Ryanair'), 15th January 2015.

	The most commonly found is "non-disclosure agreement" by which the party(ies) exchange information but subject to confidentiality obligations or to otherwise contractual restrictions in the use that can be made of them.		way of a contract, limitations on the access and use of the contents of the database that makers of protected databases are denied (save if prohibited by national law). The sanctions in case of violation of contractual obligations would obviously depend upon the national legal order at stake. The most commonly found sanctions would be the termination of the contract and/or damages.
	Application to the scenario: every actor could be concerned by contractual arrangements priorly entered into with third parties which could limit their freedom to share or trade data. Similarly, the actors involved may want to subject the sharing of 'their' data in the data marketplace to different conditions or compensation. As already mentioned, the legal regime of the contents of the blockchain ledger on the one hand, and this of the data analytics produced on the basis of data transactions on the other hand, may be rather unclear and anyway subject to the analysis of the concrete arrangement entered into by the parties. Recourse to contractual arrangements would notably prove needed in the case where all the actors involved would be found jointly holders of rights.		

This brief presentation gives an illustration of the fact that a data marketplace sets in motion various legal regimes that interact in a complex way. This presentation in particular challenges the implicit premise, in the data marketplace scenario, that the data holder is the one to decide upon the data and to trade them. Indeed, some of the confidentiality regimes rather provide for confidentiality obligations falling onto the data holder to the benefit of other parties (e.g. in the case of the confidentiality obligations provided for in railway market regulation) or for the purpose of public order objectives (e.g. safety and (cyber-)security regimes).

3.3. Regulatory frameworks granting access to data

While the previous sections presented legal regimes aimed to enable or make it mandatory to control data, this section presents regulatory regimes aiming to enable or make it mandatory for a data holder to make data available for access and/or re-use.

3.3.1. Access and re-use of data held by public sector bodies

Legal basis	PSI Directive regime	Right holder and right debtor	Beyond the PSI regime in force
PSI Directive [161] as transposed into national law – the PSI Directive is under revision.	The PSI directive requires public sector bodies to make the information that they hold available for re-use by third parties for commercial and non-commercial purposes.[162] Conditions for re-use are regulated, such as the level of	Right debtors are "public sector bodies". [165] Right holders are any third parties in their quality as "applicant".[166]	Although the PSI Directive does not apply to public undertakings,[167] Member States remain free to extend the scope of their transposing legislation to such bodies, subject to conditions stated in their national law.[168]

[161] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, 1OJ L 345, 31.12.2003, p. 90–96.
[162] Article 3 (2) of the PSI Directive.
[165] Article 2 (1) of the PSI Directive.
[166] See in particular article 4 of the PSI Directive.
[167] Article 2 (2) (a) of the PSI Directive.
[168] This is notably the case of France with the Act n°2016-1321 (Loi pour une République numérique) and of Belgium with the Act 2016-05-04/17 of the 4th May 2016 (Wet inzake het hergebruik van overheidsinformatie or Loi relatif à la réutilisation des informations du secteur public), which regulates re-use of data held by federal public bodies.

	compensation that the public sector body may impose in exchange. The PSI directive applies to information subject to the right of access as part of national law, so that the scope of the directive depends on national law in this regard.[163] Further, numerous exceptions and limitations are provided, among others, in relation to the nature of the information, which notably excludes security-sensitive information, commercial confidential information or information protected by intellectual property rights of third parties. [164] Against this background,		Further, the PSI Directive is under a revision process. In its proposal of 25th April 2018,[169] the Commission in particular proposes to extend the scope to information produced by public undertakings active in the railway sector as part of the scope of their general interest activities. [170] The Commission contemplates a two-tier approach where public undertakings would be subject to softer regime than public sector bodies. With a view to respecting their economic activity, the Commission proposes that public undertakings would not be subject to an obligation to make the information they hold available for re-use;[171] but in case they would, they would be subject to harmonized conditions of re-use.[172] The process of the revision is on-going so that the regime proposed by the Commission may change in a stricter or lighter way over the course of the decision-making process.

[163] See article 1 (2) (c) and article 1 (3) of the PSI Directive.
[164] See article 1 (2) of the PSI Directive.
[169] Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (recast), {SWD(2018) 127 final} - {SWD(2018) 128 final} - {SWD(2018) 129 final} -{SWD(2018) 145 final}.
[170] See article 1 (1) (b) and article 1 (2) (b) of the Proposal.
[171] Recital (22) of the Proposal states that "the decision whether or not to authorize re-use should remain with the public undertaking concerned". If adopted as such, it is in this regard still unclear whether this would still allow Member States to impose on public undertakings to make their information available for re-use.
[172] See in particular recital (22). Fundamentally, the Commission proposes to apply an "original Directive 2003/98" regime, namely the regime in place before the revision brought by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013.

	the public sector body is in the position to balance the contradictory interests at stake in order to decide, subject to judicial supervision, whether information should be made available for re-use.		
	Application to the scenario: the scope of the PSI directive is limited *rationae personae* and **would in principle not apply to railway infrastructure managers** in their quality as public undertakings.[173] Depending upon national law and subject to the development of the PSI revision process, the IM may however be subject to PSI obligations. For the IM, making data that it holds available on the data marketplaces would then amount to making data available for re-use. In particular, the conditions in which the data are made available for re-use would then be regulated, such as the compensation imposed by the IM or other contractual conditions. In such case, such conditions shall be inserted into the parameters of the data marketplace. Just like for other legal regimes, the PSI regime depends to some - admittedly limited - extent upon the quality of the third party willing to re-use the information and the purpose for requesting re-use. In this regard, a situation where a public sector body would request data held by another public sector body to be made available "in pursuit of [its] public task" would not be considered as "re-use" within the meaning of the PSI Directive.[174] This would, for instance, prevent the IM – where subject to PSI obligations – to use the data marketplace as the *only* channel for making data available.		

[173] See article 2 (1) and (2) of the PSI directive. In particular, railway infrastructure mangers shall remain out of the scope on the basis of article 2 (2) (a) which excludes bodies "established for the specific purpose of meeting needs in the general interest [...] having an industrial or commercial character".
[174] Article 2 (4) of the PSI Directive.

3.3.2. Public access to environmental information

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Environmental information – Directive[175] as transposed in national law	The Environmental Information Directive provides for a harmonized right of access to environmental information held by public authorities.[176] Environmental Information is broadly defined and covers in particular, and with a view to the railway infrastructure management, "the state of the elements of the environment, such as […] soil, land […], factors, such as substances, […] waste, discharges […] affecting or likely to affect the elements of the environment.[177]	The obligations are imposed on "public authorities" which are broadly defined in the Directive.[180] A railway IM can qualify as a public authority as a "[…] legal person having public responsibilities or functions, or providing public services, relating to the environment under the control of a body or person falling within (a) or (b)".	The Directive provides for a harmonized regime of access to environmental information "held by or for" public authorities.[181] The directive provides for: • Access upon request on the one hand, • Active dissemination of some environmental information by public authorities to the public for some of the information.[182] With regard to "access upon request" obligations: in principle, the public authority shall make environmental information available in the format requested by the applicant, unless it can invoke legitimate grounds not to, as exhaustively listed in the directive.[183] Charging of the access to information is

[175] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, 1OJ L 41, 14.2.2003, p. 26–32.
[176] Article 1 of the Environmental Information Directive.
[177] Article 2 (1) (a) and (b) and recital (10) of the Environmental Information Directive.
[180] Article 2 (2) of the Environmental Information Directive.
[181] Article 3 (1) of the Environmental Information Directive.
[182] Article 7 of the Environmental Information Directive.
[183] Article 3 (4) of the Environmental Information Directive.

	Environment information may be in electronic form but also on other forms.[178] However, public authorities shall "make all reasonable efforts to *maintain* environmental information" in electronic form.[179]		regulated. In the case of online access to information, charges shall not "exceed a reasonable amount".[184] The public authority may (or has to) refuse access to some environmental information based on statutory exceptions provided for in the Directive and further transposed in national law.[185]
	Application to the scenario: some of the data held in particular by the IM may qualify as environmental information and are therefore subject to the Environmental Information Directive as transposed in national law. Unless stated in national law beyond the scope of the Directive, the information held by the IM would generally not qualify as information that should be actively disseminated – but only made available upon request by applicants. As a result, actively placing them on a data marketplace would go beyond the statutory obligations.		

[178] Article 2 (1) of the Environmental Information Directive.
[179] Article 3 (4) (b) of the Environmental Information Directive.
[184] Article 5 (2) of the Environmental Information Directive.
[185] Article 4 of the Environmental Information Directive.

3.3.3. Railway law: mandatory provision of information

Legal basis	Subject-matter and requirements	Right holder and right debtor	Legal regime
Railway market regulation – EU law as transposed into national law	As a monopolist provider of infrastructure capacity, the railway IM is subject to strict regulation. With specific regard to information relating to the condition of the infrastructure, railway law imposes: • The making publicly available of information as part of the "network statement" on the one hand and as part of the "register of infrastructure" on the other hand.	The market regulation obligations are incumbent on the IM to the benefit of its customers. However, the obligation to make information publicly available could be found to be invoked also by third parties.	Obligations to make information publicly available: as part of its "network statement", the IM shall publish information on "the nature of the infrastructure [186] which is available to [RUs]".[187] Such information shall be made public free of charge.[188] Further – and based on interoperability objectives – the Interoperability Directive[189] provides for the creation and publication of a "register of the infrastructure".[190] The register shall include updated "values of the network parameters […] as set out in the relevant TSI" [191] pursuant to the format and further rules adopted by the Commission.[192]

[186] A list of the railway infrastructure assets is provided for in Annex I of the Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area Text with EEA relevance, OJ L 343, 14.12.2012, p. 32–77.
[187] Annex IV (1) of the Directive 2012/34.
[188] Article 27 (1) of the Directive 2012/34.
[189] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (Text with EEA relevance), OJ L 138, 26.5.2016, p. 44–101.
[190] Article 49 of the Interoperability Directive and subject to further regulations adopted by the Commission on the basis of article 49 (5) of the Interoperability Directive.
[191] Article 49 (1) and (4) of the Interoperability Directive.
[192] Article 49 (5) of the Interoperability Directive.

	• Provision by the IM of information to its customers: railway market regulation further provides for an obligation falling on the IM to provide information to its customers, as part of the provision of the use of the infrastructure.		Provision by the IM of information to its customers: Directive 2012/34/EU provides for the obligation falling on the IM to provide its customers (RUs) with "all other information required to implement or operate the service for which capacity has been granted".[193] The compensation for providing such information is included in the strictly regulated track-access charges.[194] Further, "supplementary information"[195] that the IM may choose to supply to its customers is also subject to (lighter) regulation in the case where the IM is the only supplier of such information. In particular, Directive 2012/34/EU limits the compensation that the IM may claim as counterpart to "the cost of providing it, plus a reasonable profit".[196]
	Application to the scenario: the obligations to make some information publicly available do not legally prevent the IM from attempting to monetize this very same information, but obviously deprives it of economic value. Such regulation does not, however, prevent the IM from		

[193] Annex II (1) (f) and article 13 (1) of the Directive 2012/34/EU.
[194] Article 31 and 32 of the Directive 2012/34/EU and Commission Implementing Regulation (EU) 2015/909 of 12 June 2015 on the modalities for the calculation of the cost that is directly incurred as a result of operating the train service (Text with EEA relevance), C/2015/3766, OJ L 148, 13.6.2015, p. 17–22
[195] Annex II (4) (b) of the Directive 2012/34/EU
[196] Article 31 (7) of the Directive 2012/34/EU. The definition of "reasonable profit" is provided for in article 3 (17) of the same directive.

	monetizing other information related to its infrastructure, such as more detailed information on the condition of the infrastructure and/or data resulting from data analytics. The obligations for the IM to provide information to its customers does not prevent it from monetizing information on a data marketplace. However, this accommodation of a privileged regime for its customers, as opposed to other third parties, would make it difficult for the IM to use the data marketplace as its only means to supply data, given the anonymous or pseudonymous character of the data marketplace. The result is that the IM would have to make a commercial choice: either to provide information to its customers via other means (with privileged conditions), or to apply the privileged conditions to all potential data customers within the context of the data marketplace.

3.4. Data marketplace: difficult fit in the legal patchwork relating to data

The previous section briefly presented various legal regime that could have an impact on the sharing or trading of data in a data marketplace in order to provide regulatory guidelines. This section will now bring together this presentation in order to draw general findings as for the adequacy of the legal framework with the idea to create a data marketplace in the railways.

3.4.1. A patchwork of rights: data as indirect legal subject-matter

It appears, quite obviously, that data are impacted by very different legal regimes with regard to:

- Their *objective* concerning the data: following the classification adopted in the previous section, it appears that some legal regimes aim to enable or make it mandatory for the right-holder to exert control over data (e.g. protection of trade secrets, copyright, protection *sui generis* for databases). On the contrary, some others aim to enable access or use of data by third parties (e.g. PSI regime, publicity obligations in railway law).
- The *branch of law* at stake: legal regimes having an impact on a data marketplace can be found in intellectual property law which constitutes horizontal legislation but also in specific regulations, such as railway law, obviously with very various rationales.
- The determination of the *right holder(s) and of the right debtor(s)*: in particular, some legal regimes have *erga omnes* effect - such as IP rights (and the protection of trade secrets to some extent) -, while others can only be invoked against specific parties (rights *ad personam*). For instance, most of the railway law provisions can only be invoked by railway actors (namely the customers of the IM) *vis-à-vis* the IM.
- The *rights and obligations* themselves, the extent of the legal protection *rationae materiae* and of exceptions, the degree of details of the regulation.
- The *geographical scope and applicable law*: while the previous section presented EU harmonized legislation, most of the legal regimes at stake depend upon national law to some extent.

This results in a patchwork of rights, which sometimes conflict one against the other as one data (operation) may simultaneously be impacted by several legal regimes. For example, and from the perspective of the IM, the PSI regime can be found to be in conflict with security-related confidentiality obligations or with right to confidentiality of third parties (e.g., its customers, based on railway market regulation or its contractors on the basis of public procurement law). As observed by De Franceschi and Lehmann,(Franceschi and Lehmann, n.d., 53–54) data are rarely the direct subject-matter of legal protection but they can be indirectly protected by legal regimes aimed to protect “wider interests”, such as trade secrets, privacy, protection of intellectual property or also, in the present case, protection of the railway market structure. Put another way, the legal regimes do not tackle data as such but data *on the ground of some other feature*. Data may be protected because of the nature of the information that they

carry (e.g. protection of trade secrets on the "semantic" level[197]), or because of the source of data (e.g. *sui generis* protection of databases), etc. One datum is rarely - if ever – the subject-matter of the legal rights or obligations. Even in the case of the *sui generis* protection on databases which covers, to a certain extent, data, the legal question is not if *this* datum is covered by legal protection but rather whether the *operation* of extraction or respectively re-utilization of the database entails that a "substantial part" of the contents of the database is concerned, be it from a qualitative or quantitative perspective. Therefore, a single datum may be subject to legal protection in a case and not in the other, subject to the analysis of the operation in question.[198] This does not easily accomodate the willingness to trade data uniformly and on a massive scale.

In the case of a data marketplace and *a fortiori* if anonymous or pseudonymous, the data 'acquirer' is also confronted with an asymmetry of information regarding the legal regime applying to the data transaction. In the case of copyright and the *sui generis* protection on databases, for instance, legal uncertainty also derives from the absence of registration of the right – as opposed to other IP rights, such as trademarks and patents, which calls for an *in concreto* analysis. The data acquirer may not, however, be in a position to determine whether the database from which the data originate actually qualifies for *sui generis* protection. To conclude, the absence of a clear legal status of data leads to legal uncertainty and may eventually limit the willingness to share or exchange data as a commodity (chilling effect).

3.4.2. The legal qualification(s) of data exchange

Pursuant to the above, not all data exchanges are alike from a legal perspective. When covered by IP protection, such as the *sui generis* protection on databases, a data exchange would qualify as a license while the same data exchange may qualify as a service contract,[199] generally subject to a broad contractual freedom if, e.g., the database is not subject to the *sui generis* protection on databases. The *identification of a legal protection* – hereby IP legal protection – therefore plays an important role in the legal qualification of the data exchange. Besides, the *identification of the parties* at stake may also have an impact on the legal qualification of the data exchange: a provision of data from the IM to an RU may qualify as the execution of the contract of use of the railway infrastructure (see above) and thereby subject to the respective legal regime while the same provision of data from the IM to a third party may not. Similarly, the sharing of data by the IM with another public sector body for the purpose of a public task may qualify as a service contract while the same sharing of data to the benefit of private companies would qualify as "re-use" within the meaning of the PSI directive. Consequently, one often faces a situation where different legal regimes apply to the same transaction.

---

[197] (Drexl 2017, 26) The author refers therein to trade secret protection, but also to data protection. In the latter case however, data can be found to consist of "personal data" not only on the basis of the semantic information that they carry but also on the basis of other considerations, such as their sources or the environment in which they are used, so long as they enable to identify the person to which it refers.

[198] The Database Directive was precisely designed in order to prevent legal protection of the contents of databases as such, see in this regard (Drexl et al. 2016, 11).

[199] On the legal qualification of contracts having data transactions as subject-matter, see (Zech 2017).

Regarding the aim to build a data marketplace and to handle data as a commodity, two major issues need to be addressed. Firstly, this is the question of whether data can be subject to secondary market transactions. Indeed, in the case of a sale, the acquirer of the good positively acquires property rights, which enable him to resell the good. Although data are not protected by ownership rights, the same question can be asked *negatively*: does the initial 'trader' of data retains (other) rights in the data after the exchange? The answer obviously depends upon the legal regime at stake. As discussed in the previous section, the party sharing the data may reserve contractual rights. In the case of IP rights, the sharing party may concede a non-sub-licensable license, which would legally prevent secondary trading of data to the benefit of the licensee.[200] Secondly, data traded by the data holder as part of the data marketplace may legally be subject to other concurrent arrangements. In other words, and based on the ubiquitous character of data, data may not be subject to *exclusive* trading by the data holder.

Provided they comply with what we termed a "legal patchwork" of regulations applying to data, in particular in the case of cross-exchanges, data holders may arrange "property-like" provisions by means of contracts. Their legal effects are, however, limited in several respects due to the nature of contracts as already discussed.[201] Further, they have legally binding effect only upon the parties to the contract (*inter partes*) - as opposed to ownership rights which have effect also on third parties (*erga omnes*) – or, in other words, are limited in their scope *rationae personae.* Subject to diverging national legislations on procedural law, contract law enforcement is usually left to the contracting parties and the role of the judge is often limited. The sanctions that a party could require from an infringing counterparty are also limited, subject to divergences in national law. In any case and to compare, they would not allow for criminal sanctions, such as in the case of counterfeiting or theft. To sum up, a party sharing data (sources) subject to mere contractual conditions would inevitably take the risk of the data escaping his control. Contract law can handle data sharing only with difficulty, given the duplicable feature of data.

4. Smart property – leveraging the blockchain technology to trade data

4.1. Introduction

This deliverable presented the (absence of) legal status of data and in particular the – generally admitted – absence of ownership rights in (raw) data. It situated this legal issue in a broader context by summarizing the difficulty for property law to tackle digital goods. Although often not directly protected by property law, data are nonetheless covered by or subject to different legal regimes that were presented in the third

[200] On this matter, see section 3.1 above and (Zech 2017, 8).
[201] For a more extensive presentation of contracts, see Deliverable D4.1, section 4.

chapter with regard to the specific context of the railway sector. Data – or more accurately data holders - are subject to different rights and obligations which were found to greatly depend upon the context, particularly upon the nature of the data, the nature of the holders, the nature of the counterpart etc. This results in a patchwork of – sometimes contradictory – legal regimes which is likely to have a chilling effect on data transactions.

4.1.1. The data marketplace scenario: technical attempt to overcome the perceived lack of status and ownership over data

In that sense, the cross-scenario "data marketplace for monetization and servitization" based on a blockchain can be seen as an attempt to overcome the complexities of the legal framework on data or even to design a technical alternative to the (sometimes perceived as) lack of ownership rights on data. The expected aim of building a data marketplace on a blockchain is to enable actors involved to "manage and control their data without the need of intermediary third party or centralized repository". The blockchain – by means of the protocol on the software infrastructure layer and of the smart contracts on the application layer – would also make it possible to "automat[e] governance logics […]" and to "tackle the problem of managing the marketplace dynamically". With an "auditable and immutable [blockchain], "authenticity of historical data and their usage [can be] ensured" which would in particular make it possible to monetize the data transactions, based on "predefined characteristics" such as, precisely, "the usage" of the data.

Beyond the data marketplace scenario, claims have been made in the blockchain community and in scholarship that the blockchain technology could "help extend and enforce individual property rights in new domains, such as the ownership of private data".[202] Furthermore, it has been argued that it would enable "one internet user to transfer a unique piece of digital property to another internet user, such that the transfer is guarantee to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer".[203]

4.1.2. Blockchain and property law: a complicated relationship

Private law implications of the blockchain technology – with the notable exception of contract law – have been rather overlooked. This is especially so for property law. (Herian 2017) However, as a matter of fact, holders of cryptocurrencies consider the latter as their property, or, more generally, they consider that the cryptocurrencies belong to them. They indeed exchange crypto-tokens, which are actually *transferred* and

[202] Zyskind, Guy, Oz Nathan, and Alex Pentland. 2015. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In 2015 IEEE Security and Privacy Workshops (SPW), 180–84. doi: 10.1109/SPW.2015.27 as referred in (Ishmaev 2017).
[203] This claim was made by Andreessen, Why Bitcoin Matters, N.Y. Times, 14th January 2015, as quoted in (Fairfield 2014, 5).

not merely copied. ('Cryptocurrencies in the Common Law of Property by David Fox :: SSRN' n.d.) The legal characterization of cryptocurrencies in property law has been largely surpassed by legal discussions arising from their usage as 'money'.[204] Now that the blockchain has found multiple applications beyond the realms of money and cryptocurrencies,[205] further legal consideration of the role of blockchain in property law appears to be needed. The scenario at stake illustrates this need for legal answers on that point: much like cryptocurrencies holders, the participants in the data marketplace consider the data that they hold as "belonging" to them and entrust the blockchain to secure the trading of these assets. It has been held that the blockchain technology can create new types of property on data and digital assets, as well as social institutions to manage and even enforce property.[206] This scenario invites to further look into the ability of the blockchain to create and/or manage and/or enforce property and the legal challenges that it poses.

4.1.3. Presentation of the chapter

This chapter does obviously not have the ambition, nor the space to discuss the impact of the blockchain technology on property law exhaustively. This is even more so by virtue of the fact that such an analysis would invite a legal analysis of the national law of every EU Member State given the fragmentation of the regime on the property of digital assets. Rather, this chapter focusses on the analysis of the data marketplace scenario and looks into the legal consequences of leveraging the blockchain to exchange data as a commodity.

This chapter starts from the assumption of the use of a public blockchain, as opposed to private blockchains, the (distinction between) two terms being well defined in Deliverable D4.1. Besides, this study is based on the legal analysis of smart contracts with regard to contract law included in section 4 of Deliverable D4.1 and aims to further look into specific usage of blockchain-based smart contracts as enabler/ manager of property.

The first section will try to define the terms used with respect to the ambition to leverage the blockchain to create or manage property. Through the analysis of the vocabulary, the first section will present the general background of the blockchain capabilities with reference to property law, in order to identify the specific framework of the data marketplace scenario (2). Against this background, the second section identifies the data marketplace scenario as an illustration of 'tokenization' of existing assets by means of the blockchain and assesses to which extend this can raise legal issues (3). With a view to provide forward-looking legal perspective, the last section analyses the legal challenges that could arise from the use of the blockchain as an alternative property institution as this of the law (4). This last section is based on a situation

[204] (Low and Teo 2017). For a thorough analysis of the qualification of cryptocurrencies and crypto-tokens under financial law, see (VANDEZANDE, n.d.).
[205] In the parlance of Fairfield, "a distributed public ledger system confers not just the power to transfer dollars but the power to transfer anything", in (Fairfield 2014, 4)
[206] See in this regard the claim made in (Abramowicz 2015, 2–3): "Bitcoin can be seen not just as a currency , but more grandly as an institution that creates and enforces property rights".

– not specifically discussed in its technical presentation made in Deliverable D5.1 and D4.1 - where the data marketplace scenario would not only leverage the blockchain technology but also "DRM-like systems" to control property over the blockchain network, as further explained and discussed below.

4.2. Vocabulary in the blockchain environment: reflection of the property-related expectations in the blockchain technology

The blockchain technology is the subject of high expectations, among other things with regard to property law or property law-like capabilities. Given the newness of the blockchain technology and the fact that the legal scholarship is only beginning to analyze its impact on property law, this first section further looks into the blockchain vocabulary and, on that occasion, presents interface points between the blockchain technology and property law. The aim is, on the one hand, to better understand the general framework of the relations between the blockchain technology and property law in the digital environment, and, on the other hand, to practically bring order and rightly identify the specific framework in which the data marketplace scenario takes place.

4.2.1. Smart property, digital property, etc.: definitions

As part of the virtues allegedly brought by the blockchain, smart property refers to an ambitious one. Just like with smart contracts, there is no unanimous definition of smart property. Again, like with smart contracts, the concept of smart property is credited to have been coined by Nick Szabo in 1994, namely before the creation of the blockchain technology. He considered smart property to be created "by embedding smart contracts in physical objects":(Szabo n.d.) this definition tackles only physical objects – to the exclusion of digital assets – while the focus is rather placed on the means to enforce this 'property', namely by technological means and in a contractual way. The Ethereum white paper also refers to smart property, but rather as a given concept and with a focus on the tokens, namely the fact that tokens represent smart property.(Buterin n.d.) The Ethereum white paper refers to the definition provided on "bitcoin.it/wiki" according to which smart property "is property whose ownership is controlled via the bitcoin blockchain using contracts". Examples are then provided which include both physical property ("such as cars") and non-physical "property" ("like shares in a company or access rights to a remote computer"). The core criterion appears to lie in the blockchain operation to *manage* property: "making property smart allows it to be traded with radically less trust" and therein provides the example of a collateral.[207] The concept of smart property has then been broadly used in the blockchain community and amongst the scholarship(Wright and De Filippi 2015, 33–36; Herian 2017) with reference to the ability of blockchain networks based on smart contracts, to manage and/or enforce property of tangible and intangible assets without the need to rely on legal enforcement. Smart property is conceived of as one of the outcomes of smart contracts.

[207] https://en.bitcoin.it/wiki/Smart_Property, last visited 17th October 2018.

Other concepts used in the blockchain community or in scholarship appear to concurrently attempt to report the same or similar abilities, such as the new concepts of "crypto-property" referred to as the "value [which] is transferred" on the blockchain by means of smart contracts,(Jaccard 2018, 3; Finck 2018, 672–73) "Blockchain Crypto Property",[208] or "cryptographic ownership" referring to the ability for a blockchain user to manage his "property", such as cryptocurrencies or "ownership of private data".(Ishmaev 2017) General terms are also being used – namely, non-blockchain-specific terms – such as "digital property" or "virtual property" with reference to the alleged ability of blockchain to create property.(Fairfield 2014; Ishmaev 2017)

Generally speaking, "smart property" appears to stem from the technical community and to focus on the *property management* capabilities of the blockchain while digital property (or "virtual property") is mostly used by lawyers as referring to the alleged ability of blockchain to *create* property in the legal sense. In relation to property law, mainly two claims therefore appear to be made *vis-à-vis* the ability of the blockchain technology: the blockchain technology would make it possible to create digital property on the one hand. On the other hand, the blockchain technology would make it possible for blockchain users to manage and enforce their property by means other than legal and deemed more efficient.

4.2.2. Blockchain-enabled property?

Setting aside financial law considerations, the ability of the blockchain to *create* digital property has been mainly discussed from the perspective of the legal status of cryptocurrencies in private law as presented in the first chapter of this deliverable. Legal scholars have attempted to determine whether a chosen national legislation allows for bitcoins and other cryptocurrencies to qualify as property.(Abramowicz 2015; Jaccard 2018) Eventually, some regulators have also clarified their position, such as the US Internal Revenue Service, which concluded that, for taxation purposes according to US federal law, "virtual currency is treated as property".[209]

The US scholar Fairfield(Fairfield 2014) conceptualized the paradigm shift that blockchain technology represents for property law, what he named "Bitproperty". As discussed in Chapter 1, property law has struggled to adapt to digitization. There is hardly any digital equivalence to ownership regimes in physical things. As a result, users of digital products such as "e-books, MP3s, software, or downloaded movies"(Fairfield 2014, 8) are usually deprived of ownership that they would enjoy for the same products

[208] The term was coined by the Swiss law firm MME, as referred to in (Jaccard 2018) Blockchain Crypto Property (or BCP) is defined as «(1) Digital information containing all elements of a property right, (2) that is registered on a Blockchain or in an alternative distributed ledger, (3) which can be transferred via a protocol, (4) and that may (or may not) carry out additional functions governed by an SCS, following coded and/or manual input».

[209] IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply, IRS 2014-21 and IRS 2014-36, 2014, https://www.irs.gov/newsroom/irs-virtual-currency-guidance, last visited 17th October 2018.

in the "analog environment". According to Fairfield, Blockchains would enable "peer-to-peer property transactions, with no […] trusted intermediaries" needed to intervene in determining "who owns what", such intermediaries forming a large array of entities: for instance centralized banks (with reference to exchange of fiat money) or platforms such as Facebook that users need to trust to keep their Facebook account running. Fairfield underlines the core disruption brought by the blockchain technology to property law, namely its ability to avoid double spending: by enabling scarcity – or uniqueness - of crypto-tokens, the blockchain solves the long-lasting issue of duplication of data, without having to resort to a trusted third party. By "making digital assets rival", Fairfield therein argues that the blockchain technology invites to re-think conceptual ground for digital property and in particular the legal characterization of a "thing" within the meaning of property law. Beyond merely attempting to determine criteria for a principle of equivalence between physical and digital assets, he argues that "tangibility has long stood as a bad proxy for rivalrousness", as opposed to intangibility standing for non-rivalry and therefore calls for revisiting the legal criteria triggering "thing-ness", or more generally of what is subject-matter of ownership.

4.2.3. From virtual property to blockchain property

Against this background, the blockchain would represent a second step in the history of the emergence of digital property, while virtual property (see chapter 1) would constitute the first one.[210] With virtual property, the delineation and artificial creation of scarce digital assets have been made possible, however only to the cost of centralization of "ledgers representing digital rights" and therefore heavy reliance upon the intermediary. Virtual property in virtual online games worlds, for instance, entirely depends upon the code developed and maintained by the game publisher, to such an extent that scholars have argued about the legal consequences that recognition of property in virtual property of players may have on the game publisher. Shall the game publisher bear a subsequent obligation to positively maintain the property? (Lehdonvirta and Virtanen 2010, 14–17) Would the game publisher be bound by an obligation of persistency of the virtual environment of the virtual property or - conversely - would this question only illustrate the lack of sufficient persistency of the digital asset for it to qualify as property? On a larger scale and by way of example, the same can be said of ICANN managing domain names: only by delegating the task of maintaining and enforcing a repository of domain names has it been made possible to allow for uniqueness and scarcity of domain names. In all these cases, the action of an intermediary is a *sine qua non* condition for a digital asset to possess the features needed to be vested with property rights, namely rivalry and persistency. The blockchain technology would take digital property a step further. Not only would it enable rivalry and persistency of digital assets, but also it does so without reliance upon trusted intermediaries. Some authors additionally consider that dispensing with trusted intermediaries would make crypto-tokens more persistent (Szilagyi 2018, 2–4) in that a public blockchain is said to be immutable and to not be controlled (McGrath 2016) by an intermediary likely to shut it down. Against this background, the

[210] See therein the development of the US IRS in handling digital property, from virtual currencies and virtual assets in virtual environments to crypto-currencies, (Fairfield 2014, 43–46).

blockchain technology undeniably questions property law and invites lawyers to re-think property law in respect of digital assets.[211]

4.2.4. Crypto-tokens

Concretely, "the block chain constitutes a complete transaction history of all transfers of the asset, going back to the creation of the asset"(Fairfield 2014, 18), based on the consideration that "whoever controls the [colored] coin controls the commodity". The transfer technically consists of the "conveyance of the ledger entry" or, in other words, of the cryptographic keys.(Fairfield 2014, 30) The subject-matter of the exchange on the blockchain is a (crypto-)token whose transactions can be traced on the blockchain. A token can generally be defined as "a thing serving as a visible or tangible representation of a fact, quality, feeling, etc." while secondary definitions would also focus on *what* is represented and on the *legal value* of the token – e.g. in the case where tokens serve as evidence.[212] There is neither a commonly agreed definition of tokens in the blockchain environment nor even a consensus on their name. They are mostly referred to as 'tokens', 'crypto(-)tokens', blockchain-tokens or 'coins'. (Savelyev n.d.) According to the legal definition provided by Savelyev, a crypto-token[213] is "a kind of a digital asset, which exists in the blockchain ecosystem, and is bundled with the right to use it". (Savelyev n.d.) Functionally, a crypto-token may represent "any digital assets, financial instruments or real-world assets"[214] so that the token serves as an "alter-ego" on the blockchain, something referred to as "tokenization".(Savelyev n.d.) The tokens in a blockchain are unique: they are "the vehicle through which blockchain technology re-introduces scarcity into the digital domain".(Bodó, Gervais, and Quintais n.d.) It is based on this ability to introduce scarcity in digital assets that the blockchain has sometimes been considered as the second peer-to-peer revolution after the creation of the Internet. B. Barraud argues that the internet allowed sharing of 'things' while the blockchain now allows for their *transfer*,[215] thereby implying that the initial thing would not simply be copied but that the control would genuinely be passed on from a party to the other. Without the blockchain, transfer of data is made possible only by resorting to trusted intermediaries.

4.2.5. Classifications of crypto-tokens

Existence of property rights in cryptocurrencies is being discussed in legal scholarship. However, it remains to be seen, beyond this discussion, how to handle other crypto-tokens. To push the logic to the end, assuming that property rights would be recognized on cryptocurrencies, would that automatically entail that property rights could be recognized on all crypto-tokens? In the data marketplace scenario, tokens

[211] The inappropriateness of property law with reference to digital assets is also underlined in (van Erp 2017, 7).
[212] https://en.oxforddictionaries.com/definition/token, last visited 18th October 2018.
[213] Cryptotoken or crypto-token are being used in the blockchain community and in the scholarship as referring to the same thing, see for instance (Wright and De Filippi 2015, 26).
[214] William Mougayar. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, 2016. P. 90, as quoted in (Savelyev n.d.).
[215] (Barraud 2018, 5).

exchanged on the basis of the blockchain represent raw data (data sources). Does exchanging these raw data on the basis of a blockchain token automatically attract property rights in the raw data or, alternatively, in the tokens representing them in the blockchain? While crypto-tokens may represent anything, there is an obvious need for classification through the lens of property law.

Several classifications of crypto-tokens have been endeavored in the blockchain community in both legal and technical scholarship, but also by the regulators themselves. Many of the existing legal classifications regard the qualification of ICOs ("Initial Coin Offerings") in financial laws, such as the recent classification issued by the Swiss Financial Market Supervisory Authority FINMA in February 2018.[216] While recognizing the absence of general classification of ICOs and tokens, FINMA distinguishes mainly three types of tokens, classified, for the purpose of Swiss financial market law, according to their "underlying economic function" while highlighting that the economic functions may overlap in one single token:

- "Payment tokens" or cryptocurrencies are "intended to be used […] as a means of payment […] or as a means of money or value transfer. [They] give rise to no claims on their issuer".
- "utility tokens" are "intended to provide access digitally to an application or service by means of a blockchain-based infrastructure".
- "asset tokens represent assets such as a debt or equity claim on the issuer". The FINMA therein gives the examples of "a share in a future company earning", therein qualifying as "equities, bonds or derivatives". Tokens representing "physical assets to be traded on the blockchain" also make part of this category. Generally, qualification as asset token implies qualification as security within the meaning of financial market regulation.[217]

Although this classification may prove helpful for the purpose of the application of financial market regulation to the blockchain environment, it is not entirely fit for the purpose of the application of property law to tokens. As underlined by Savelyev, it mostly demonstrates the fact that tokens may potentially represent anything. (Savelyev n.d.) Classification exercises are all the more difficult that the blockchain technology keeps developing so that new (kind of) tokens are created. A complete classification of crypto-tokens within the meaning of property law is obviously beyond the ambit of this paper, but some guidance needs to be laid down, which will be conducted in the following section.

[216] FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), Published 16 February 2018, accessible on https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/, last visited 18th October 2018.
[217] Point 3.2.3 "asset tokens" of the Guidelines.

4.3. 'Tokenization' of existing assets: risk of regulatory misalignment

4.3.1. Tokenization of off-chain assets vs. pure on-chain assets

In the data marketplace scenario, a token represents raw data (or raw data sources) considered as an asset: *the token is not the raw data* but represents its "blockchain twin". This situation is in this regard similar to this of a token representing a piece of land or a car, both illustrating "asset tokens" within the meaning of the FINMA classification. A distinction between them can obviously be made, based on the nature of the represented asset: while a piece of land or a car are tangible and physical assets, raw data is an intangible 'asset' (without prejudice to its legal qualification or absence thereof). Other intangibles have been subject to blockchain "tokenization", such as company shares, carbon credits, etc.,(Reed et al. 2017) but more generally "anything" including non-"things" in the property law meaning such as contractual debts. Tokenization results in two different assets: the original one (raw data, car or piece of land) and its blockchain alter-ego in the blockchain, namely the token. A car or a piece of land, although represented by a token *in a specific blockchain network*, have an autonomous existence and were created outside the blockchain network. To sum up, two steps shall therefore be distinguished: firstly, the creation of the asset and, secondly the transactions about that asset. Raw data "tokenized" in the data marketplace scenario are firstly created by sensors placed on railway infrastructure assets. Only in a second time are they tokenized in a blockchain for the purpose of exchanging them. Reed et al. refer to "off-chain assets" as opposed to "on-chain" ones,(Reed et al. 2017) such as cryptocurrencies.

Cryptocurrencies are demonstrably different from tokens representing off-chain assets. They originate from a blockchain network and they do not exist without the blockchain network: their whole existence relies on that blockchain network. For instance, a Bitcoin would vanish as early as the bitcoin blockchain would vanish. Secondly, although closely related to the first, "the blockchain is the sole source of rights over the asset, i.e. the Bitcoin". As eloquently put by C. Reed et al., they are a "pure artefact of the ledger technology".(Reed et al. 2017) Other features of cryptocurrencies have been put forward, such as the fact that the token "itself has no intrinsic value. The source of its value is extrinsic to itself, imposed by the collective belief of the people who use it".('Cryptocurrencies in the Common Law of Property by David Fox :: SSRN' n.d., 5) Similarly, the way cryptocurrencies are created may be found specific: in the Bitcoin as well as in the consecutive blockchain networks, cryptocurrencies are being created as part of the operation of the respective network. Creation and allocation of cryptocurrencies remunerate the work of the active nodes – such as miners –, which has sometimes been justified by the effort and power that they spend to validate transactions.[218] The latter features however seem to be closely related to the purpose of such tokens, namely to serve as money. The developments of the blockchain technology beyond the realms of

[218] (Ishmaev 2017).

the financial sector however may lead to the creation of other kinds of "pure on-chain assets" [219] which may not fit the specific money-related features of cryptocurrencies.

4.3.2. Misalignment: off-chain asset vs. token respective regulations

In order to identify the specific legal challenges created by the tokenization of existing off-chain assets – as opposed to pure on-chain ones, we will now quickly turn to the work of Savelyev on the recently adopted blockchain-specific regulation in Belarus.[220] The law allocates property rights to blockchain-tokens, which, as analyzed by Savelyev, entails the risk to jeopardize the legal regime of respective assets subject to tokenization. To give an example, where a token representing IP rights[221] is itself legally considered as property, what is the legal regime of the whole transaction? The issue fundamentally arises from the misalignment between the regulation of the off-chain asset and this of its by-product, namely the token.

With specific regard to property law, the law distinguishes the "initial allocation of rights"(Arruñada 2017, 87) from the "recurrent allocation of rights".(Arruñada 2017, 87) The former refers to the determination of what can legally be subject-matter of property ("thing-ness") and the means to acquire original property. The latter refers to the regulation of property rights, namely how they can be transferred, leased, seized by public authorities, etc. The example of the Belarus legislation of blockchain-tokens has the merit of illustrating the specificities of tokenization of existing off-chain assets. In such a case, the legal question is not whether the tokens would or should attract property rights in their capacity to create scarcity – which is nonetheless a valid question with reference to pure on-chain tokens. Indeed, and as a matter of fact, the property of the token is not the ultimate expected outcome of the tokenization which is rather a means to "securely exchange" off-chain assets. The token is in this case a by-product of the off-chain asset. Therefore, and independently from the specific legal regulation of blockchain tokens in Belarus, the legal question is whether the blockchain may jeopardize the legal regime of off-chain assets by tokenizing them to exchange and trade them.

This challenge has been raised in the legal scholarship based on the statement that "code is law" (or can be made so) in the blockchain environment. With a reference to "Digital Rights Management", De Filippi and Wright consider the risk arising from the creation of "property rights management" (PRM) systems of physical assets being tokenized. "Just like DRM embeds the provisions of a copyright license into code, connected devices can incorporate specific contractual provisions related to the use of a physical asset. Code can stipulate a set of rules to manage devices precisely defining use criteria or restrictions". ('Blockchain and the Law — Primavera De Filippi, Aaron Wright | Harvard University Press' n.d., Blockchain

[219] See a discussion within the blockchain community on the situation of "cryptokitties", https://medium.com/@gmcmullen/do-you-really-own-your-cryptokitties-d2731d3491a9, last visited 6th November 2018.
[220] (Savelyev n.d.) The explanation of the Belarus Decree is based on this paper.
[221] Example given in (Savelyev n.d., section 3).

of things) By leveraging the power of the blockchain, the "technological owner" (as opposed to the legal owner) could enjoy "absolute sovereignty" over the asset, beyond legal property rights, always limited in scope and subject to exceptions. For example, the technological owner could prevent seizure of the asset "unless specifically provided for by the underlying code".(Wright and De Filippi 2015, 35) More generally, tokenization would enable blockchain users to turn anything into tokens and thereby exert absolute control on them. Is that or can it be the case of a data marketplace placed on a blockchain? In order to answer this question, a more thorough look into the premises of this statement need to be undertaken.

4.3.3. Off-chain assets: beyond the reach of the blockchain

This statement shall be qualified in that the reach of the blockchain does not extend technically to the off-chain asset but only to the tokens. What legal consequences does it trigger?

Blockchain as a supporting tool for contractually making data available **-** The blockchain is a network-centric technology, which requires intermediaries to interface off-chain assets – be they physical or digital - with their related token. The blockchain is indeed able to capture and monitor data from outside the blockchain ledger only by requiring "other agents, such as 'oracles' [in order to] trigger contractual execution" while "it is undeniable that [they] add some degree of centralization".[222] In the data marketplace scenario, it practically means that the blockchain is able to prevent double spending of a *token representing raw data* as from the moment of its creation as blockchain artefact, but not of raw data (as off-chain asset). As a result, the blockchain technology *per se* is able to control neither the creation of the raw data, nor their copying or otherwise processing outside the blockchain network, nor even the processing of the data once exchanged on the basis of the blockchain. Data exchange performed based on a blockchain would not technically prevent the initial data holder from exchanging the same data (a copy thereof) by other means, or in other words, the data exchange performed on the blockchain would not be *exclusive*: against this background, data is shared but not transferred. Similarly, the fact that the receiver of the data can technically copy the data received illustrates the fact that the data are not scarce. This entails that the promotion of the blockchain *as such* as a tool enabling users to control the data that they "tokenize" overestimates the capabilities of the blockchain technology.

From a legal perspective, the use of the blockchain as a supporting tool to exchange data does not affect the conclusion drawn in Chapter 2 that data as such are, as a matter of fact, a weak candidate for ownership, based on their features as volatile, non-excludable and non-rival. Such a situation should be legally analyzed as different forms of contractual making available of data, where the blockchain and smart contracts would be leveraged as tools to automate part of the contractual arrangement.[223] While this could give rise to legal

[222] (Arruñada 2017) The author goes on by predicting the "proliferation of a myriad of new specialists to provide effective contractual completion as well as interfaces between the virtual and real worlds to most end users and for most assets".
[223] On the automation of phases of contracts by means of smart contracts, see section 4 in Deliverable D4.1.

issues, this situation would not impact property law but should instead be analyzed within the regulatory framework of contract law, as discussed in section 4 of Deliverable D4.1, and with a view to the legal framework surrounding data exposed in chapter 3.

Combination of the blockchain technology with "DRM-like technologies" - It would take additional technical features ("DRM-like technologies") - thereby relying on intermediaries - to technically attempt to make raw data somehow scarce which is currently under research.[224] Such "DRM-like systems", when combined with the blockchain technology, may raise legal challenges which are further discussed in the following section. However, by delineating the contours of the blockchain and of its reach, this finding importantly curtails the risk – sometimes conversely presented as a capacity – that the management of property by means of the blockchain technology would be entirely beyond the reach of the law. In other words, tackling DRM-like systems should prove less challenging than tackling the blockchain itself, as they would not be vested with the blockchain characteristics of "tamper-resistance" which make a public blockchain a difficult regulatory target.

An opening **-** This more broadly invites to pay attention to the contours of the reach of the blockchain and of its consequential virtues. For illustration, a blockchain-specific law was passed in the US State of Arizona with the aim to enhance the use of the blockchain technology and of smart contracts. Among other provisions, the law defines the blockchain technology from which it derives that "the data on the ledger […] provides an uncensored truth".[225] These statutory provisions, however, serve as a proof of the misunderstanding regarding the operation of the blockchain. As summarized by A. Walch, "if a false piece of data is put on a blockchain ledger, it remains false, regardless of the fact that it appears on the ledger (the garbage in / garbage out idea)".[226] The limit to the reach of the blockchain – namely to the token itself and not to the underlying off-chain asset directly - was also illustrated by the many attempts to use the blockchain technology to handle property titles over the course of the transactions of intellectual property rights and immovable things, or in other words blockchain-based registries of ownership. The rationale for moving ownership registries to a blockchain would lie in the willingness to have a *publicly available* as well as *immutable* - and therefore allegedly *reliable* - record of ownership.(Bodó, Gervais, and Quintais n.d.; Clark and Burstall 2018; GRAGLIA and MELLON, n.d.) Setting aside the legal issues arising from the *operation* of the blockchain – particularly in the case of a public blockchain – which will be further analyzed in the following section, it was also found that the blockchain is not *per se* able to "check the validity of the information when it is first put into the system",(Bodó, Gervais, and Quintais n.d.) e.g., checking that the token holder is legally entitled to enter into the transaction. This is another way of saying the same thing, namely that the reach of the blockchain is limited and that intervention of intermediaries is needed with regard to, generally, "off-chain" assets.

---

[224] For instance, see (Bertram and Georg 2018).
[225] Act of Sept. 21, 2006, ch. 26, ARIZ. REV. STAT. ANN. § 44-7003 (2006) (amended by 2017 Ariz. Sess. Laws 2417), https://legiscan.com/AZ/text/HB2417/id/1528949, as referred to in (Walch 2017, 1)
[226] (Walch 2017).

The following section will now analyze the legal consequences attached to the situation where such "DRM-like systems" would be used in combination with the blockchain in order for blockchain users to manage their property, namely "their data" in the data marketplace scenario.

4.4. Technological ownership by means of leveraging the blockchain technology

The remainder of this chapter is based on the assumption that the data marketplace scenario implies the successful use of "DRM-like" techniques combined with the use of a blockchain *strico sensu,* as described above. The statement that the blockchain could result in "technological ownership" may seem surprising at first glance. The data exchanges supported by the blockchain technology are based on the transfer of value and asset as well as granular limitations in the ability to use it thanks to the smart contracts, which allow automation of contractual arrangements, which seem to mimic legal contracts rather than legal property law. De Filippi and Wright indeed consider that, based on the blockchain and on smart contracts, "property ownership could vanish, replaced by a web of temporary leasehold interests governed by contracts".[227]

4.4.1. Blockchain as a property institution

Property institution: answering the "who owns what" question - Looking at the statement that the blockchain could provide technical ownership as an alternative to legal ownership implies that not only the individual exchanges between parties on the blockchain should be considered but also the blockchain environment as a whole. Ishmaev argues that the blockchain technology would be an "institution of property" operating as a "parallel normative structure" to this of the law.(Ishmaev 2017) Based on its protocol, a public blockchain sets the framework to decide upon 'who can perform what activity on which asset', or, in short - and without giving it a legal meaning - "who owns what". For example, the Bitcoin blockchain (then followed by the other public blockchains) regulates the initial allocation of ownership of newly created Bitcoins – which 'belong to' the miners. It equates possession of the token with ownership or, in non-legal terms, it is structured such that whoever controls the token can dispose of its use – and this of the related off-chain asset where appropriate. Notably, the token controller can prevent third parties from using it or can have third parties using it as he so wishes, based on the conditions of the smart contract. In the data-marketplace scenario for illustration, the initial data holder would be able to exchange data (sources) based on the blockchain and to have them used by third parties *without subsequently losing control over the data once shared*. He would retain some form of remote control, based on the conditions included in - and on the operation of - the smart contracts.

[227] (Wright and De Filippi 2015).

Although every blockchain network has its own specific rules enshrined in the protocol, they all share similarities. Instead of relying upon trusted intermediaries, the blockchain is based on peer-to-peer consensus and validation of transactions. However, nodes' validation of transactions is not based on the same rules as the "validation" of the transaction by a trusted intermediary in a sale according to the law: in the latter case, the notary or the bank are vested with responsibility to ensure that the sale is consistent with legal substantive regulation in force. In the former case however, the nodes do not check compliance with legal substantive regulation: quite on the contrary, they have no say on the content of the transaction. As highlighted by Arruñada (Arruñada 2017, 85), the validation of transactions on blockchains is only based on the prevention of double-spending of the token within the said blockchain environment. It only aims to allow actual transfer of the tokens rather than their mere copy. The validating nodes do not validate the merits or legality of the transaction itself.[228] As summarized by Ishmaev, "Bitcoin [*nota bene:* the same could be said of other public blockchains] replaces third-party authority with the distributed ledger built on the blockchain". (Ishmaev 2017)

Blockchain as an alternative property institution **-** In that sense, the blockchain as a means to exchange value and as an institution of property is demonstrably based on possession or rather, in the digital environment, control of the token. Whoever controls the token is considered the "owner" *within the blockchain network*. Concretely, it means that the controller of the token may exert any transaction on the token within the blockchain network. (Arruñada 2017, 82–85) Possession of the thing plays a role in all property law regimes, subject to national differences as well as differences according to the nature of the thing (and in particular immovable vs. movables). However, possession is legally never equated with ownership: on the contrary, property regimes as a means to deal with scarcity precisely and fundamentally rely on separation between possession and ownership. (Arruñada 2017, 84–85) Against this background, the blockchain as a property institution is misaligned with the legal institutions.

As underlined by Arrunada, the blockchain protocol does not "merely represent a change in ownership of the car: it additionally *transfers* actual physical control or possession of the car".(Arruñada 2017, 85) This note illustrates the regulatory nature of the blockchain technology. Saying that the blockchain would and/or can constitute an alternative regulatory framework to this of the law and of legal institutions is illustrated by the statement that "code is law". This goes further than only observing that the blockchain environment is based on alternative *substantive* rules as these of the law, among others the observation that blockchain networks are based, as property institutions, exclusively on the control of tokens for determining ownership, in contradiction to the provisions of the law. Possession being equated to ownership in the blockchain environment should not be understood as a *provision* in the legal sense. The blockchain regulation – *lex cryptographia* in the parlance of De Filippi and Wright (Wright and De Filippi 2015) – mainly

[228] Abramowicz therein explains the following: "Bitcoin can be seen not just as a currency, but more grandly as an institution that creates and enforces property rights. It is an institution, however, that can resolve only one type of decision: whether purported transfers of Bitcoins will be validated and added to a list of approved transfers, known as the block chain", in (Abramowicz 2015, 2–3)

departs from the law with regard to *how it is enforced*. Legal obligations to transfer ownership from A to B – be it contractual arrangements[229] or statutory provisions – would be firstly laid down and then complied with or, failing that, enforced by judiciary or otherwise public authority. As opposed to that, the blockchain creates the technical conditions for the transfer to happen. As a form of technological normativity, the blockchain "*embodies* [norms]".[230] To be clear, stating that a blockchain would consider possession as the *criterion* for *deciding* on ownership would be wrong. Rather, the blockchains' protocols make tokens' holder able to handle tokens – or even the related off-chain assets - as their property: they enable tokens' holders to control (rather than merely 'deicide') how their 'property' can be used and by whom, their property being anything that they possess. Blockchain users could thereby create and enforce their own law by simply exchanging assets on a blockchain based on a token. As a result, the blockchain would constitute an alternative (among others, property) institution, deemed stronger than this of the law, otherwise described as a specific form of private ordering(Bodó, Gervais, and Quintais n.d.) allowing for "absolute ownership".

Intermediary conclusion **-** Tokens representing off-chain assets shall be differentiated from "pure on-chain assets" in that the latter exist only in relation to the blockchain network and do not represent off-chain assets. In the case of off-chain assets, the action of the blockchain extends to the management of the assets (transactions of the assets) based on "tokenization", but not to their *creation* - outside the blockchain network. The reach of the blockchain is, however, technically limited to the token, while additional technical mechanisms are required so that the blockchain is connected to and has influence over off-chain assets. Assuming that this is the case, legal challenges arise from the fact that controllers of tokens can circumvent the (property) law regimes on the assets, by managing their asset (the term asset being used here in the broadest sense) by means of its blockchain token. The risk would be even more significant such that the technical features of the blockchain technology would make it difficult to control, thereby allowing token holders to exert "absolute ownership" on their assets.

Everything can be tokenized and managed on a blockchain, but the legal consequences depend upon the nature of the "thing" which entails specific legal regimes. The next section will then analyze the specific case of data (sources) as subject-matter of tokenization.

4.4.2. Data (sources) as property within a blockchain

The statement made by De Filippi and Wright on the risk that blockchain could constitute a "Property Rights Management" system similar to "Digital Rights Management" is described as applying to physical things with a view to applications in the field of the "Internet of Things".[231] Others have discussed the use of the blockchain technology and of smart contracts to support licensing of copyrighted works.(Bodó, Gervais, and

[229] On this matter, see Deliverable D4.1, section 4.
[230] (Durante 2013), referring to M. Hildebrandt.
[231] (Wright and De Filippi 2015) The discussion on "smart property" is further extended in ('Blockchain and the Law — Primavera De Filippi, Aaron Wright | Harvard University Press' n.d., 156–69).

Quintais n.d.) While the blockchain and smart contracts could theoretically be used by the token holders to exert "absolute ownership" over whatever related off-chain asset, what concrete legal consequences would the case of data (sources) entail?

To compare: tokenization of "things" within the meaning of property law - Physical devices and copyrighted works have one thing in common: broadly speaking, both are subject-matter of (intellectual) property rights by the virtue of which *erga omnes* rights to exclude their use by third parties are attached to them. Although they are very different, (intellectual) property rights are always instrumental – in the sense that they serve a legal purpose: they never grant absolute sovereignty to the right holder. As discussed in Chapter 2, the legal protection granted by ownership rights is always qualified by various sorts of limitations and exceptions to the benefit of third parties and/or of public authorities. For example, the exclusive right of reproduction of the copyrighted work may be subject to exceptions or limitations for private use.[232] The use of the blockchain and smart contracts to execute or "enforce" lease or licensing contracts could therefore result in circumventing the conditions or limitations of (intellectual) property law[233]. De Filippi and Wright ('Blockchain and the Law — Primavera De Filippi, Aaron Wright | Harvard University Press' n.d., 156–69) contemplate the situation where a connected device manufacturer could use the blockchain to "create personal property servitudes" instead of respecting the law which would imply a sale of the device to customers – or in other words a transfer of ownership rights. The right holder of a copyrighted work could violate private use exceptions of a licensee, such as DRMs are blamed for doing, but deemed to be more efficient based on the blockchain virtues of immutability and tamper-resistance.

To summarize, the use of blockchain and smart contracts to handle one's property on physical goods or IP-protected works could result in a misalignment between the law and the conditions enforced in the blockchain, legally resulting in a violation of (intellectual) property law. Can the same be said in the case of data and/or data sources as subject-matter of tokenization?

Data (sources) as subject-matter of blockchain tokenization: conclusion - This question refers to chapters 1 to 3 outlining the absence of an overarching legal status of data and the legal patchwork surrounding data and information. Against this background, data (sources) can be divided into two categories: on the one hand, (operations on) data and information which are subject to legal provisions and, on the other hand, (operations on) data and information which are not subject to any legal provisions. Chapter 3 therein

[232] Article 5 (2) (b) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167 , 22/06/2001 P. 0010 – 0019 ("InfoSoc Directive")

[233] In this regard, it is worth noting that Sony filed an application for a patent for a "blockchain-based digital rights management system" which would take into account limitations to the exclusive rights of the right holder, see United States Patent Application 20180115416, available here: http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=20180115416.PGNR.&OS=dn/20180115416&RS=DN/20180115416 (last visited 22nd November 2018).

described the need as well as the difficulty to assess *in concreto* whether (an operation on) data (sources) is subject to legal provisions. As a result, categorization of data is highly circumstantial and cannot be equated with a legal "status" of data as such. In the case where (operations on) data are subject to legal provisions, handling them based on tokens and smart contracts could in some circumstances constitute a misalignment or even an infringement to the respective bodies of law. For instance, where the IM would be subject to the PSI regime *mutatis mutandis* according to the applicable national law, they would not be allowed to use the blockchain and smart contracts to prevent re-use of data once shared with a third party or to impose a compensation beyond the PSI regulated price for making data available for re-use.[234]

In the opposite situation where (operations on) data are *not* subject to legal provisions, one could leverage the blockchain to create "technological ownership" on the data (see above). While the law would obviously not protect or enforce this "technological ownership", would the law altogether prohibit this technological appropriation of data? The "technological ownership" over data by means of the blockchain technology appears to illustrate a form of "*de facto* ownership", broadly exposed in the Communication of the Commission "Building a European Data Economy".[235] The Commission is indeed concerned that some parties along the value chain of data – among others, manufacturers or service providers of machines generating data - would end up becoming "*de facto* owners of the data" by means of contractual but also technological restrictions to the use of the data. In this regard, a blockchain-based technological ownership would appear to be a serious form of appropriation, in that it would enable the "technological owner" to retain control over the data while trading them.

As *avant-garde* as it seems, this description in turn ties back to the legal uncertainty surrounding the legal status of data highlighted in Chapter 2. In other words - and save for the cases of *specific* regulatory regimes applying to (operations on) data - what is or should be the legal status of data *by default*? Where data would be found to be *by default* vested with "common good" legal status prohibiting appropriation (see Chapter 2 section 2.3), "technological ownership" would be found to be illegitimate. On the contrary, where data would be found not to have a status by default, technological appropriation would be a possible means to circumvent the absence of ownership rights on data or other goods. This finding meets the call of Van Erp for property law to "be revisited and reevaluated for digital assets. Otherwise, we are creating a lawless virtual reality where the rule of technology governs instead of the rule of law". (van Erp 2017, 241) While the question of the *by default* legal status of data may have been mostly theoretical until now, the emergence of the blockchain technology (among others) as a means to design "technological property" makes it a practically relevant and timely problem.

[234] Within the meaning of articles 2 (4), 3 (1) and 8 of the PSI Directive.
[235] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy" {SWD(2017) 2 final}, 10-11.

Bibliography

Abramowicz, Michael. 2015. 'Cryptocurrency-Based Law'. SSRN Scholarly Paper ID 2573788. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2573788.

Arruñada, Benito. 2017. 'Blockchain's Struggle to Deliver Impersonal Exchange'.

Barraud, Boris. 2018. 'Les Blockchains et Le Droit'. *Revue Lamy Droit de l'immatériel*, no. 147: 48–62.

Bartolini, Cesare, Cristiana Santos, and Carsten Ullrich. 2017. 'Property and the Cloud'. *Computer Law & Security Review*, December. https://doi.org/10.1016/j.clsr.2017.10.005.

Berger, Tristan. 2015. 'Qualifier Le Téléchargement Illégal de Données : Soustraire Ou Extraire, Telle Est La Question'. *Revue Lamy Droit de l'immatériel*, no. 117 (July). https://hal.archives-ouvertes.fr/hal-01206951.

Bertram, Sabine, and Co-Pierre Georg. 2018. 'A Privacy-Preserving System for Data Ownership Using Blockchain and Distributed Databases'. *ArXiv:1810.11655 [Cs]*, October. http://arxiv.org/abs/1810.11655.

'Blockchain and the Law — Primavera De Filippi, Aaron Wright | Harvard University Press'. n.d. Accessed 31 August 2018. http://www.hup.harvard.edu/catalog.php?isbn=9780674976429.

Bodó, Balázs, Daniel Gervais, and João Pedro Quintais. n.d. 'Blockchain and Smart Contracts: The Missing Link in Copyright Licensing?' *International Journal of Law and Information Technology*. Accessed 2 October 2018. https://doi.org/10.1093/ijlit/eay014.

Buterin, Vitalik. n.d. 'Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform'. Bitcoin Magazine. Accessed 3 September 2018. https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/.

Clark, Birgit, and Ruth Burstall. 2018. 'Blockchain, IP and the Pharma Industry—How Distributed Ledger Technologies Can Help Secure the Pharma Supply Chain'. *Journal of Intellectual Property Law & Practice* 13 (7): 531–33. https://doi.org/10.1093/jiplp/jpy069.

Conway, Heather, and Robin Hickey. 2017. *Modern Studies in Property Law*. Bloomsbury Publishing.

'Cryptocurrencies in the Common Law of Property by David Fox :: SSRN'. n.d. Accessed 12 September 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232501.

Determann, Lothar. 2018. 'No One Owns Data'. SSRN Scholarly Paper ID 3123957. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3123957.

Drexl, Josef. 2017. 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access'. *JIPITEC* 8 (4). http://www.jipitec.eu/issues/jipitec-8-4-2017/4636.

Drexl, Josef, Reto Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter, Gintare Surblyte, and Klaus Wiedemann. 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'. SSRN Scholarly Paper ID 2833165. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2833165.

Duch-Brown, Nestor, Bertin Martens, and Frank Mueller-Langer. 2017. 'The Economics of Ownership, Access and Trade in Digital Data'.

Durante, Massimo. 2013. 'Law, Normativity, and the Writing. <Emphasis Type="Italic">Oracle Night</Emphasis> and Human Indeterminacy'. In *Human Law and Computer Law: Comparative Perspectives*, 159–79. Ius Gentium: Comparative Perspectives on Law and Justice. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-6314-2_8.

Erlank, Wian. 2015. 'Introduction to Virtual Property: Lex Virtualis IPSA Loquitur'. SSRN Scholarly Paper ID 2753716. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2753716.

Erp, Sjef van. 2017. 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects'. SSRN Scholarly Paper ID 3046402. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3046402.

Fairfield, Joshua. 2005. 'Virtual Property'. *Boston University Law Review*, October. https://scholarlycommons.law.wlu.edu/wlufac/452.

———. 2014. 'BitProperty'. SSRN Scholarly Paper ID 2504710. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2504710.

Finck, Michèle. 2018. 'Blockchains: Regulating the Unknown' 19 (04): 28.

Franceschi, Alberto De, and Michael Lehmann. n.d. 'Data as Tradeable Commodity and New Measures for Their Protection' 01 (01): 22.

Geiregat, Simon. 2017. 'Digital Exhaustion of Copyright after CJEU Judgment in Ranks and Vasiļevičs'. *Computer Law & Security Review* 33 (4): 521–40. https://doi.org/10.1016/j.clsr.2017.03.005.

GIDROL-MISTRAL, Gaële. 2016. 'LES BIENS IMMATÉRIELS EN QUÊTE D'IDENTITÉ.' *Revue de Droit: Université de Sherbrooke* 46 (1).

Graf von Westphalen, Friedrich, and Friedrich Graf von Westphalen. 2017. 'Contracts with Big Data: The End of the Traditional Contract Concept?' In *Trading Data in the Digital Economy: Legal Concepts and Tools*, 245–70. Nomos Verlagsgesellschaft mbH & Co. KG.

GRAGLIA, J MICHAEL, and CHRISTOPHER MELLON. n.d. 'BLOCKCHAIN AND PROPERTY IN 2018' 12 (1): 27.

Grimmelmann, James. 2010. 'The Internet Is a Semicommons'. SSRN Scholarly Paper ID 1618905. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1618905.

Gutwirth, Serge, and Gloria Gonzalez Fuster. n.d. '(3) L' Éternel Retour de La Propriété Des Données : De l'insistance d'un Mot d'ordre | Request PDF'. ResearchGate. Accessed 12 September 2018. https://www.researchgate.net/publication/323639027_L'_eternel_retour_de_la_propriete_des_donnees_de_l'insistance_d'un_mot_d'ordre.

Herian, Robert. 2017. 'Blockchain and the (Re)Imagining of Trusts Jurisprudence'. *Strategic Change* 26 (5): 453–60. https://doi.org/10.1002/jsc.2145.

Hilty, Reto. 2015. '"Exhaustion" in the Digital Age'. SSRN Scholarly Paper ID 2689518. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2689518.

Hojnik, Janja. 2017. 'Technology Neutral EU Law: Digital Goods within the Traditional Goods/Services Distinction'. *International Journal of Law and Information Technology* 25 (1): 63–84. https://doi.org/10.1093/ijlit/eaw009.

Ishmaev, G. 2017. 'Blockchain Technology as an Institution of Property'. *Metaphilosophy* 48 (5): 666–86. https://doi.org/10.1111/meta.12277.

Jaccard, Gabriel. 2018. 'Smart Contracts and the Role of Law'. SSRN Scholarly Paper ID 3099885. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3099885.

Lehdonvirta, Vili, and Perttu Virtanen. 2010. 'A New Frontier in Digital Content Policy: Case Studies in the Regulation of Virtual Goods and Artificial Scarcity'. *Policy & Internet* 2 (3): 7–29. https://doi.org/10.2202/1944-2866.1070.

Low, Kelvin FK, and Ernie GS Teo. 2017. 'Bitcoins and Other Cryptocurrencies as Property?' *Law, Innovation and Technology* 9 (2): 235–68. https://doi.org/10.1080/17579961.2017.1377915.

Maeschaelck, Bram. 2018. 'Digital Inheritance in Belgium'. *Journal of European Consumer and Market Law* 7 (1): 37–41.

McGrath, Noel. 2016. 'Transacting in a Vacuum of Property Law'. SSRN Scholarly Paper ID 2786206. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2786206.

Mezei, Péter. 2015. 'Digital First Sale Doctrine Ante Portas – Exhaustion in the Online Environment'. *JIPITEC* 6 (1). http://www.jipitec.eu/issues/jipitec-6-1-2015/4173.

Pearce, Henry. n.d. '(3) Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law | Request PDF'. ResearchGate. Accessed 12 September 2018. https://www.researchgate.net/publication/325796681_Personality_property_and_other_provocations_exploring_the_conceptual_muddle_of_data_protection_rights_under_EU_law.

Reed, Chris, Umamahesh Sathyanarayan, Shuhui Ruan, and Justine Collins. 2017. 'Beyond Bitcoin – Legal Impurities and Off-Chain Assets'. SSRN Scholarly Paper ID 3058945. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3058945.

Savelyev, Alexander. n.d. 'Some Risks of Tokenization and Blockchainizaition of Private Law'. *Computer Law & Security Review*. Accessed 2 June 2018. https://doi.org/10.1016/j.clsr.2018.05.010.

Sein, Karin. 2017. 'What Rules Should Apply to Smart Consumer Goods? Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and "Normal" Contract Law'. *JIPITEC* 8 (2). http://www.jipitec.eu/issues/jipitec-8-2-2017/4559.

Storr, Christine, and Pam Storr. 2017. 'Internet of Things: Right to Data from a European Perspective'. In *New Technology, Big Data and the Law*, 65–96. Perspectives in Law, Business and Innovation. Springer, Singapore. https://doi.org/10.1007/978-981-10-5038-1_4.

Stănescu, Cătălin Gabriel. 2015. 'Self-Help and Contract Law'. In *Self-Help, Private Debt Collection and the Concomitant Risks*, 51–97. Springer, Cham. https://doi.org/10.1007/978-3-319-21503-7_3.

Surblyte, Gintare. 2016. 'Data as a Digital Resource'. SSRN Scholarly Paper ID 2849303. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2849303.

Szabo, Nick. n.d. 'Smart Contracts'. Accessed 17 October 2018. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Szilagyi, Katie. 2018. 'A Bundle of Blockchains? Digitally Disrupting Property Law'. SSRN Scholarly Paper ID 3161151. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3161151.

Tosza, Stanislaw. 2013. 'AIDP Global Report'. *Revue Internationale de Droit Pénal* 84 (1): 115–39. https://doi.org/10.3917/ridp.841.0115.

Union, Publications Office of the European. 2016. 'Legal Study on Ownership and Access to Data : Final Report.' Website. 28 November 2016. https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1/language-en.

VANDEZANDE, Niels. n.d. 'REGULATING VIRTUAL CURRENCIES':, 510.

Walch, Angela. 2017. 'Blockchain's Treacherous Vocabulary: One More Challenge for Regulators'. SSRN Scholarly Paper ID 3019328. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3019328.

'What Virtual Worlds Can Do for Property Law by Juliet M. Moringiello :: SSRN'. n.d. Accessed 1 October 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1366450&download=yes.

Wiebe, Andreas. 2017. 'Protection of Industrial Data – a New Property Right for the Digital Economy?' *Journal of Intellectual Property Law & Practice* 12 (1): 62–71. https://doi.org/10.1093/jiplp/jpw175.

Wright, Aaron, and Primavera De Filippi. 2015. 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia'. SSRN Scholarly Paper ID 2580664. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2580664.

Yu, Peter K. 2018. 'Data Producer's Right and the Protection of Machine-Generated Data'. SSRN Scholarly Paper ID 3271189. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3271189.

Zech, Herbert. 2016. 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data'. *Journal of Intellectual Property Law & Practice* 11 (6): 460–70. https://doi.org/10.1093/jiplp/jpw049.

———. 2017. 'Data as a Tradeable Commodity – Implications for Contract Law'. SSRN Scholarly Paper ID 3063153. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3063153.