CMS Law.Tax

Data according to private law

2020

Data according to private law[1]

Although data represents the cornerstone of the new economy and possesses significant economic value as a crucial component of companies (together with human, material and financial resources), the study of data has yet to stretch beyond a certain type: personal data. However, data can actually be unwrapped to reveal further groups, including both protected and unprotected data. With that in mind, this article has sought to provide a legal definition of data in a bid to conclude that data is information represented symbolically in computable form. The piece analyses the physical aspect of data, its content, the questions regarding data as such and the relevance of the reality to which it refers, as well as taking a glance at the category of data on data. The relationship of this concept with existing legal categories has also been outlined, not to mention the ideas of a "thing" and a "legal asset", to determine that data itself is not a thing, rather by and large a legal asset subject to entitlement and protection, as well as other rights. Arguments as to whether data can be owned have been put forward in view of the different data categories, with a particular focus on unprotected data. A detailed examination has been included of the regulations applicable to unprotected data and its entitlement, possession or custody, free flow, transfer and other legal transactions, as well as succession by way of *mortis causa*. Lastly, given that data by its very nature exemplifies a shifting landscape, the conflict of rules which allow us to pinpoint the legislation applicable to data – whether personal or non-personal – under International Private Law have also been reviewed.

Javier Torre de Silva
Attorney for the Council of State (on professional leave of absence)
Partner, CMS Spain
T +34 91 451 9321
E javier.torredesilva@cms-asl.com

*A Spanish version of this paper could be found in Anuario de Derecho Civil, vol. 72 n. 3, 2019, pp. 825-877.

[1] Research backed by the *Cátedra Google sobre Privacidad, Sociedad e Innovación* [Google Professorship on Privacy, Society and Innovation]. Speaker at the "Don Federico de Castro" civil law seminar organised by the ICT division of the *Real Academia de Jurisprudencia y Legislación* [Royal Academy of Jurisprudence and Legislation] (May 2019).

Contents

Introduction

The historic digital revolution we are currently witnessing is founded upon a type of asset which did not even exist 80 years ago. That asset is data, understood as computable information. Given its lack of an evident physical location, data cannot be likened to a "thing" (it is found in many places such as the servers on which it is hosted, albeit its location is afforded minimal importance due to a susceptibility to change and the possibility that the subject may not even be aware of the data's whereabouts when "in the cloud"). The transitory nature of data is also key insofar as its propensity to change just like the ones and zeros which represent the information. Data is not akin to the contractual rights regulated by the principle of relativity of agreements. While always present on a device, data has an external dimension and is occasionally subject to being safeguarded from third parties (protection, claim, access) beyond the limits of liability for non-contractual damages.

Data represents a relatively new landscape yet to find its place among traditional civil law categories. Clearly, the 19th century Spanish Civil Code did not have data in mind at the time of its writing. Questions concerning the international private law rule which applies to data (*lex rei sitae*, contract laws or another applicable Law?), whether data can be subject to possession, ownership or a form of entitlement, who is entitled – as the case may be – to newly-generated data (do the rules of taking on ownership such as acquisitive prescription apply?), by what means can data be transferred (is the acquiring party afforded the protection offered by Article 464 of the Spanish Civil Code?) and which *mortis causa* transactions can be executed over data are just some of the themes yet to be fully addressed by law, especially when it comes to non-personal data.

Data represents a relatively new landscape yet to find its place among traditional civil law categories.

Economic significance of the subject

Telefónica Chairman José María Álvarez-Pallete recently said that "data is set to be the future's most valuable resource".[2] While companies used to represent a collective of human, material and financial resources, we must now add data (digital resources) to that list: they are now forces of human, digital, material and financial means.

As individuals and consumers, we are familiar with the importance and regulation of personal data. We have all seen business models centred on information about individuals, the creation of continually-updated profiles relating to such persons and personalised advertising based on those profiles. Google, Tencent and Facebook are just a few examples of such models.

However, the volume and economic significance of non-personal data are far greater than those of personal data. The digital revolution we are undergoing[3] uses non-personal data to increase efficiency at an exponential rate in a bid to reduce both CAPEX and OPEX. Examples of the former are well-known: companies offering retail distribution services with few or no commercial outlets (Amazon), hotel services without owning hotels (Airbnb), financial brokerage services without bank branches or having to commit their own resources (FinTechs and some banks), air travel reservations without having been granted airport slots (Amadeus) or air transportation without owning planes (many airlines) and urban transport services without owning any vehicles (Cabify, Uber and Moovit). The services that these companies offer to their clients are essentially information, representing colossal resources of non-personal data, not to mention the personal data provided upon acceptance of the service by natural person clients. An example of the latter

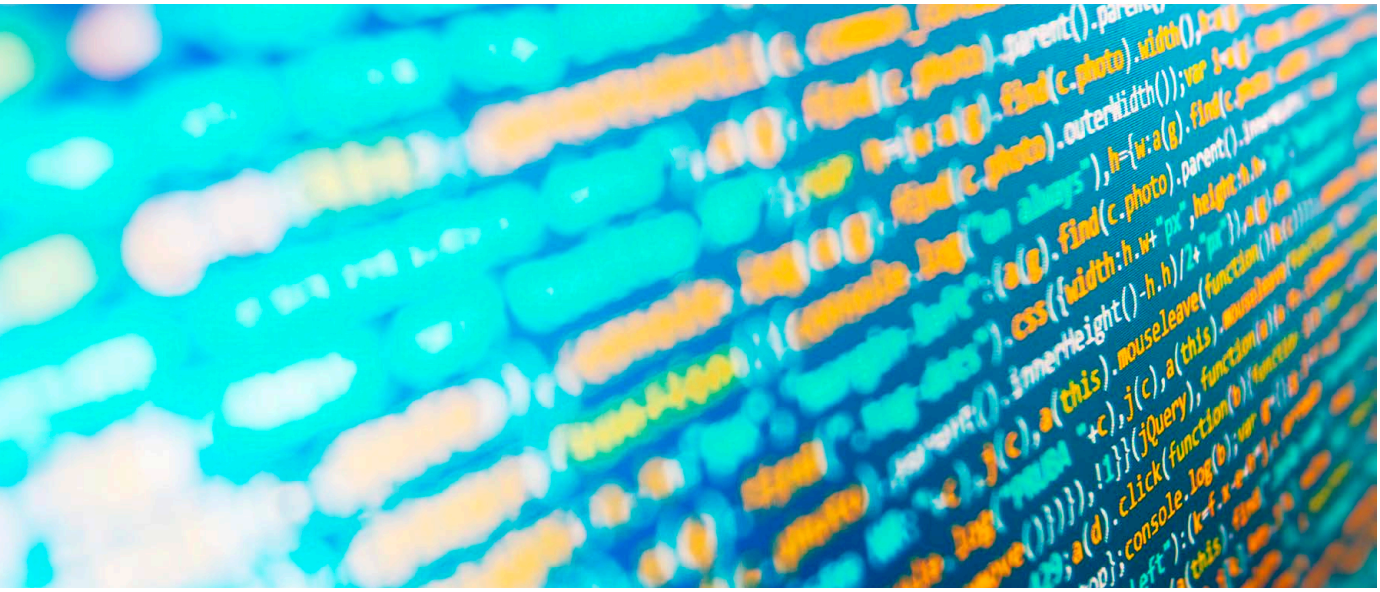
[2] https://cincodias.elpais.com/cincodias/2017/06/19/companias/1497861452_912952.html.

[3] As early announced by Katsh, E., Law in a Digital World, 1995, p. 241.

is industrial maintenance: General Electric's business model for the maintenance of aircraft engines is characterised by the installation of an increasing number of engine sensors which enable the mechanics to work more efficiently. As opposed to the entire maintenance team attending a job, only those who are required in each particular case are sent based on the information gathered from the sensors beforehand, allowing for more efficient working. Again, the most valuable resource in this instance is information. This phenomenon is applied through the so-called "Internet of Things", which enables certain objects – such as vehicles – to continuously "communicate" with their manufacturers and inform them of any incidents. While in some cases such issues can actually be resolved remotely and even before the user becomes aware of them, the objects are also able to "converse" with other elements to ensure coordination. Even if the objects are "unaware of" who owns them, in the not too distant future they are set to become permanent issuers of both personal and non-personal data.

Data is set to be the future's most valuable resource.

Telefónica Chairman, José María Álvarez-Pallete



The concept of "data"

The concept of "data" is ambiguous. Regulation (EU) 2016/679 of 27 April 2016 (the General Data Protection Regulation – GDPR) and the Spanish Constitutional Act on Data Protection and the Guarantee of Digital Rights (*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales*, or "LOPDG") equate the legal concept of "data" to "information". However, for the purpose of this article, "data" will be identified as "computable information". In other words, "information represented symbolically in a format which can be reduced to "ones" and "zeros" on a computer". This definition of "data" is more constrained (by excluding data not processed by automated means)[4] than the meaning given under data protection legislation.

A subgroup within "data" are the "digital contents", as defined in articles 2.1 and 3.1 of the Directive (EU) 2019/770, of the European Parliament and of the Council, on certain aspects concerning contracts for the supply of digital content and digital services, a concept also used in LOPDG. "Digital content" are "supplied" data (in the Directive, by a trader to a consumer; in LOPDG, by a consumer to a trader), a narrower category within the numerous data used by the companies (which include data observed, inferred or deduced by them, and their own data not supplied by them to third parties, nor by third parties to them). The paper below will refer to all "data", irrespective of whether they are labelled as "digital content" or not.

[4] Excluding non-computable data, which fits into the scope of application under the GDPR. The non-automated processing of information is subject to Article 2.1 (in relation to Articles 4.1 and 4.2) of the GDPR: this Regulation applies "*to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*". The GDPR identifies "data" as "*information*".

Symbolic representation

Information which is not represented symbolically is not data. A user's positive reaction to a photograph must be represented symbolically in order to be made known: for example, giving the thumbs up in real life. Only when such symbolic representation is also computable does information become data in a digital sense. The "emojis" or "likes" used on electronic devices are essentially binary combinations of "ones" and "zeros" on a computer rendering the information computable, which it would not otherwise be even if represented symbolically.

The physical aspect of data, its content and data itself

While data has a physical dimension due to its link to a storage medium, its content is intangible and open to unlimited duplication. This is essentially the heart and soul of data. However, data must not be labelled one or the other. It is the representation of the content using computable digits, with both heart and soul present.

From a physical perspective, data remains a certain combination of open or closed binary electronic circuits (symbolised by ones and zeros) on the microprocessors of electronic devices (for example, a server) located somewhere on the planet. This physical aspect is important as it determines data's connection – albeit casual and changeable – to a location. The location of data on a server can be used as a connecting factor to ascertain international jurisdiction (for example, where a judgment is to be enforced: Article 24.5 of Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) or, within certain limits, the procedural law relating to the enforcement of judgments (Article 45 of the same Regulation and, as far as protective measures are concerned, Article 40). The physical location of the server on which the data is hosted is also of great significance in the application of criminal laws and mandatory rules (servers hosting data concerning human trafficking or arms smuggling), even if the activity is carried out abroad. Nonetheless, such application represents an uphill task from a practical perspective.[5]

In contrast, the content (a concept not to be confused with the "digital content" referred to above) is the information represented within the data, which is not actually the data itself, although the data falls under the same regulation: information protected in the real world is also safeguarded when represented digitally as the protected interest is the same regardless of how the information is represented (trade secrets are protected irrespective of the format in which the information is presented – or represented – and the same occurs with the protection of personal data and intellectual property). Moreover, the punishment handed down to illegal content is reflected onto the data that represents it symbolically. The restrictions on the illegal transfer of content also extend to the data which represents such content and serves as a medium (illegal copies of audiovisual productions protected as intellectual property).

Having said that, data and content cannot be confused: the element subject to intellectual property embodied in data comprising content is not the data as such, rather the original creation contained in and represented by the data. An original creation can be found in multiple physical forms (a book, theatrical performance, musical production) and on digital storage media, and will always remain the same piece of work subject to ownership. The element subject to intellectual property is not usually[6] the storage medium, rather the original creation. In view of the above-mentioned exceptions, the right of exclusive appropriation granted by law refers to content and not to the data representing it.

Data itself, which is neither its storage medium (being able to spread beyond it) nor its content – despite relying on both –, has its own identity and distinguishing elements. It is the logical, computable representation of the content which can be copied identically onto another device.

---

[5] Often, data located in the "cloud" cannot be hosted on a single server, rather split virtually across a network of servers in different countries. Accessing just one of the servers might not grant access to the information sought. Against this backdrop, an authority's request to access the information held on a certain server may not be possible.

[6] While specific devices are protected under the Spanish Intellectual Property Act (*Ley de Propiedad Intelectual*), the general rule can be found in Article 10 of the Act's consolidated text: "*The subject matter of intellectual property shall comprise all original literary, artistic or scientific productions expressed in any mode or form, whether tangible or intangible, known at present or that may be invented in the future*". The minimal protection offered to certain media is found under Article 56 (owners of original works having the right to display the piece in public).

The reality to which data refers

While data comprises a reality to which the information refers, the regulation of such reality is not usually imposed on the data itself. A digital photograph of a work of art is not generally subject to cultural heritage legislation. A company may hold performance data on an aircraft engine or the occupancy of holiday apartments as a crucial part of its protected know-how without actually owning an aircraft engine or holiday apartment.

As an exception, a legal system may establish a relationship between the data and its reality. When the information represented in the data differs from its reality, the data controller is sometimes forced to fine tune it to the actual situation (quality or accuracy-related obligations[7] under personal data protection).

Data on data: derived data

In practice, data is usually generated on other data. So-called "big data" (new data obtained from other anonymised mass data sets, open to processing irrespective of the source and for varying purposes), metadata (data on data or which classifies data, deemed important because data requires context to be useful: time references, links to other data, inclusion under certain categories), new data generated by artificial intelligence algorithms or neural networks based on other data and combinations of all of the above are essentially data produced from other data. This creates problems with regard to entitlement and the rights held over derived data in a similar but not identical scenario to the issues faced by derivative works in matters of intellectual property.

While data comprises a reality to which the information refers, the regulation of such reality is not usually imposed on the data itself.

[7] Pursuant to Article 5.1.d) of the GDPR, data shall be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')*". For example, where a database previously showed a person as being bankrupt but said individual is now solvent, they are entitled to have their personal data updated to reflect the current situation.

Contrast between personal and non-personal data

While this article delves into both personal and non-personal data, greater attention will be paid to the latter. In order for data to be considered personal, it must refer to an identified or identifiable natural person,[8] albeit with the caveat that data which has undergone "*pseudonymisation*", i.e. that which "*could be attributed to a natural person through the use of additional information*" is considered personal data.[9] By way of example, individuals' IP addresses are recognised as such because additional information can lead to the identification of a natural person. Data which has undergone pseudonymisation could have a substantial impact on the future "Internet of Things" (IoT) due to being data concerning things often used by natural persons. Data is considered personal when the use of additional information enables a natural person to be identified. A further example would be the data linked to the registration of a private vehicle owned by a natural person, which can be attributed to such person through additional information, even where the service provider does not know the person's name. All remaining data (i.e. that which cannot be attributed to a natural person even through the use of additional information) is considered non-personal. Such non-personal data includes truly anonymised data which cannot be linked to certain or determinable natural persons.

---

[8] Article 4.1 of the GDPR defines 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[9] As stated in Recital 26 of the GDPR: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

This category is examined in the Communication from the Commission to the European Parliament and the Council of 29 May 2019 COM (2019) 250 final, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*", pp. 5 to 8.

The largest part of data related to the internal operations of companies and the activities of delivering goods and providing services is not considered personal data. This includes data on the provision of goods and services, cost structures, internal management (financial, accounting, internal control, inventory and IT system data, etc.) and data pertaining to the sales of goods or services provided to other companies. At a bank, this would be almost the entirety of the information on corporate banking and M&A, as well as risk management models. For insurance companies, it would be the actuarial models underpinning their businesses and for vehicle manufacturers, production figures as well as machine (engines, etc.) and vehicle performance metrics. At a law firm, it would be the archives of records comprising the corporation's know-how, without which it would be unable to advise its clients. Statistics and public service management data (traffic, etc.), as well as environmental information and scientific research data (astronomic and satellite observations, anonymised pharmaceutical, medical or veterinary research, etc.), among others, are not considered personal data. The bulk of the information available on Wikipedia and similar websites is viewed as non-personal data. As mentioned above, derived data such as big data, some metadata and anonymised data generated through artificial intelligence do not fall into the personal data category. Data on the Internet of Things (where anonymised)[10] and cryptocurrencies (where it is not possible to identify a natural person account holder) do not constitute personal data.

The flow of non-personal data required for and produced by these processes is monumental, as is the storage volume of such data. According to Professor Gregory La Blanc of the University of Berkeley[11], the aircraft engines for internal US flights generate 2.5 billion terabytes of data per year[12] (2.5 zettabytes, given that 1 ZB = 1,000 EB = 1,000,000 PB = 1,000,000,000 TB), although fortunately not all of it is stored. To provide an idea of the sheer magnitude of those figures, in 2018 the total storage capacity of the servers belonging to Grupo Telefónica was 66,000 terabytes of data[13] (66 petabytes, given that 1 PB = 1,000 TB), some 37,000 times less. Publicly accessible, non-personal big data can easily be found on the Internet, such as the records – which do not include personal data – of all the trips made by taxis in New York[14]. The information available on computers throughout the entire world is measured in yottabytes (1 YB = 1,000 ZB) and continues to grow at a rate of knots. The Internet of Things is set to pave the way for vast volumes of non-personal data which until present would have been considered inconceivable. Rafts of data comprising both personal and non-personal data are known as "mixed data sets".[15] Said mixed data sets, where the personal and non-personal data elements are "inextricably linked", are governed in terms of their corresponding rights and duties under the most protective regulation, i.e. the laws on personal data.[16]

---

[10] As mentioned under Recital 9 of Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. This Regulation lists the Internet of Things among sources of non-personal data. However, this would have to be analysed on a case-by-case basis to find out whether the data can be linked to an identified or identifiable natural person.

[11] Conference held on 28 November 2018.

[12] According to Professor La Blanc's calculations, 20 TB per hour per engine, with 2 engines per plane and 28,537 daily flights across US airspace lasting 6 hours over a period of 365 days equals 2,499,841,200 TB.

[13] Speech given by the Chairman of Telefónica at the company's general shareholders' meeting on 8 June 2018.

[14] https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page

[15] Please see in the Communication from the Commission to the European Parliament and the Council of 29 May 2019, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*.

[16] Ibidem, p. 10.

The flow of non-personal data

2.5bn terabytes

The aircraft engines for internal US flights generate 2.5 billion terabytes of data per year.

(2.5 zettabytes, given that 1 ZB = 1,000 EB = 1,000,000 PB = 1,000,000,000 TB)

66,000 terabytes

The total storage capacity of the servers belonging to Grupo Telefónica was 66,000 terabytes of data.

(66 petabytes, given that 1 PB = 1,000 TB).

1 yottabyte (YB) = 1,000 zettabytes (ZB)

The information available on computers throughout the entire world is measured in yottabytes (1 YB = 1,000 ZB) and continues to grow at a rate of knots.

Legal landscape: assets and things

It is often said that data is the fuel driving the new economy. In fact, life would be a lot more straightforward for lawyers if data was fuel. Unfortunately, it is not. Data's place in the Spanish legal system requires us to explore different ideas.

Data and things

Data as such is not a thing, although its physical existence on electronic devices can be considered that way.

There is no legal definition of "*things*". While few conclusions can be drawn from Article 333 of the Spanish Civil Code,[17] codification offers no doctrinal assertions. Legal doctrine is also divided. Firstly, there are those who consider "*things*" as something with a material existence, regardless of whether they are subject to appropriation. Secondly, others prefer to broaden the idea of a "*thing*" to encompass any object which is not a person. As part of the first group, Díez-Picazo argues that "*things should be understood as anything in the outside world with a material existence*",[18]

It is often said that data is the fuel driving the new economy. In fact, life would be a lot more straightforward for lawyers if data was fuel. Unfortunately, it is not.

[17] *"All things which are or may be subject to appropriation are considered movable or immovable property"*

[18] DÍEZ-PICAZO Y PONCE DE LEÓN, L. *Fundamentos del Derecho Civil Patrimonial* [Foundations of Civil Patrimonial Law], IV, 2012, p. 37.

therefore contrasting with immaterial objects ("*elements which, where not embodied and essentially recognised as a creation by the human mind, are viewed by the legal system as open to subjective rights because they are given an economic value*"). The same criteria is used by Lacruz Berdejo and Delgado Echeverría[19] and Clavería Gonsalbez,[20] albeit with some minor tweaks. Among the second group[21] are Marín Castán and Albaladejo. Marín Castán believes a "*thing*" to be "*all imaginable realities other than people*",[22] whether appropriable or not, whereas Albaladejo views "*things*" as "*all impersonal material or non-material elements which are unique and, in their entirety, open to belonging under an independent right*",[23] including creations of the human mind, provided that they are subject to appropriation.

Given the need to apply an unambiguous notion which leaves no room for error, Professor Díez-Picazo's definition is the most appropriate.

From a non-legal perspective, data is information, and information is immaterial, widespread and changeable. As already stated, data does not occupy space, and although it is stored on electronic devices, it can be found on multiple media at any given time. Data has the gift of omnipresence which so many human beings long for in the fast-paced society we live in (as stated by Byung-Chul Han). In reality, with cloud technology (offered by AWS and other companies) the holders of data are often unaware of its location, which is of little legal significance (although not fully irrelevant, as we shall observe) and can change rapidly without warning.

Data is also somewhat time-bound, not only because it is always linked to a point in time (when produced by an IT system) and often represents a variable with an ever-changing value or which flows continuously or discontinuously, but also due to its propensity to become outdated. The commercial value and usefulness of static information can plunge quickly if not updated.

Even where data is hosted on multiple servers, it remains identical on all of them given its form as the symbolic and computable representation of information (a combination of ones and zeros). Thus, data is an immaterial "creation of the human mind". Although it can be brought to life (on electronic devices such as the servers on which it is hosted), it must not be confused with the things on which is stored. Data as such is not a thing, rather hosted on things through the use of computer applications. In this regard, it can be compared to intellectual property, which is also stored on media.

The extent to which data is integrated into the devices on which it is stored is somewhat less than the level of integration of contractual rights in securities, for example. As with securities, which allow for contractual rights to be attached to movable things, data is by its very nature hosted on things (servers), sometimes on many things simultaneously. These things belong – or may belong – to several people in accordance with the traditional rules of civil law. Nevertheless, this comparison is limited from a legal perspective given the contrast of the casual and changeable nature of the bond between data and server with that of the contractual right and security which represents it.

The faculties held – or not – over data by the owners of servers on which such data is hosted will be analysed later in this article. For all intents and purposes, the server or electronic device on which the data is hosted is a material thing (ownership, possession, etc.).

---

[19] LACRUZ BERDEJO, J.L. et al (rev. DELGADO ECHEVERRÍA, J.), *Elementos de Derecho Civil* [Elements of Civil Law], I-3, 2005, pp. 3 to 9.

[20] CLAVERÍA GONSALBEZ, L., *"Artículo 333", Comentario del Código Civil Comentario del Código Civil* ["Article 333", Commentary on the Spanish Civil Code], Ministerio de Justicia [Ministry of Justice], 1993, vol. 1, p. 922: it is highly questionable for attributes, ideas and creations to be things, therefore "*not all assets are things, since things are merely individual embodiments in two or three dimensions (land, cupboard), objects with an existence which can be verified by our senses or using instruments (vehicles, electricity) respectively*".

[21] As LACRUZ and DELGADO recall (p. 2), GAIUS distinguishes in his Institutes (2.13 and 2.14) between *res quae tangi possunt* and intangible things comprising *iura, "such as inheritance, usufruct and obligations"*. However, this assertion is merely instructive, and no conclusions can be gleaned from it.

[22] MARÍN CASTÁN, F., *Comentario del Código Civil* [Commentary on the Spanish Civil Code], Bosch, 2000, p. 7.

[23] ALBALADEJO, M., *Derecho Civil* I [Civil Law I], Ed. Edisofer, 2013, p. 355.

The content of data and data itself as legal assets

According to Ulpian, assets ("bona") are *ea "quod beant, id est, beatos faciunt"* (Digest 50.16.49). Clavería Gonsalbez summarises the issue as follows: "*Pursuant to prevailing case law, all things are assets, but some assets are not things (attributes, ideas and creations)*".[24] Lacruz Berdejo and Delgado Echeverría suggest a much wider concept of "*assets*" than the scope of "*things*" that encompasses energy (which is only partially regulated by the rules applying to things, given the inability to establish usufruct or gratuitous bailment) as well as ideas, creations[25] and personal attributes,[26] among other realities.[27] Díez-Picazo also distinguishes "immaterial assets" from "embodied things" as creations of the human mind with an economic value and comprising "*intellectual literary, artistic, scientific or industrial works*", as well as distinctive signs.[28]

Marín Castán perceives "*everything that merits legal protection*"[29] as an asset, including protected elements such as the environment.[30] In my opinion, a sound criterion to use in distinguishing between things and assets is: anything that may be subject to compensable damage through non-contractual liability is a legal asset, whether a thing or not and whether appropriable or not from a technical and legal perspective.

Naturally, differing opinions do exist. While Albaladejo defines "*assets*" as "*a synonym of things in a legal sense*",[31] the Spanish Civil Code – as Lacruz Berdejo recalls – often uses the words "*assets*" and "*things*" interchangeably (most notably those subject to appropriation). However, the Code is known for its shortcomings in matters of doctrine.[32]

There are other assets which, despite being open to entitlement and transfer, are not things, such as companies as a legal entity, or their solvency and reputation. Companies provide a sound example in my opinion, defined by Gondra in terms of the activity attributable to their owner, stretching beyond the patrimonial doctrine which pared them down to a *universitas* of things.[33] Companies have a dynamic existence subject to aquilian protection (*tutela aquiliana*) and legal transactions without needing to be a thing or a combination of things. Using companies as an example is no coincidence. Nowadays, data and companies go hand in hand as the former (the flow of which provides the best description of corporate activity) represents a crucial element of a company alongside human resources and solvency. Solvency and business reputation are not things, rather assets. Should they be damaged contrary to Law, they would in theory be subject to aquilian protection, but not action in rem. Although solvency and the good name of a company are legal assets which merit protection, they are not things and cannot be reclaimed.

As regards data, it must be distinguished from its content, but both are legal assets.

---

[24] CLAVERÍA GONSALBEZ, ibidem, p. 922.

[25] Described as "*literary or aesthetic creation revealed in written or plastic works*", as well as "*databases; inventive ideas; structured ideas; distinctive signs and the personal execution of self or others' creations". To clarify, "this is about immaterial assets, even where appearing in or on material things (books, CDs, devices, etc.), as the idea or model is independent of any tangible display. The immaterial archetype which our senses do not recognise as a physical entity, rather something understood using intellect, is what is subject to law in this case". Elementos de Derecho Civil* [Elements of Civil Law], I-3, pp. 6 and 7.

[26] LACRUZ BERDEJO, J.L. et al (rev. DELGADO ECHEVERRÍA), *Elementos de Derecho Civil* [Elements of Civil Law], I-3, pp. 5 to 7.

[27] LACRUZ BERDEJO, J.L. et al (rev. DELGADO ECHEVERRÍA), *Elementos de Derecho Civil* [Elements of Civil Law], I-3, p. 5. Lacruz and Delgado identify "assets" as "subject to law", and therefore include conduct and abstention, as well as involvement in associations and companies, under the definition of the word. CLAVERÍA GONSALBEZ refutes this notion (ibidem, p. 922) by stating that while conduct and abstention are subject to law, they are not assets. However, discussing these differences would take us off course from the purpose of this article.

[28] DÍEZ-PICAZO, L. *Fundamentos del Derecho Civil Patrimonial* [Foundations of Civil Patrimonial Law], IV, Civitas, Cizur Menor, 2012, p. 37.

[29] Ibidem, p. 7. MARÍN CASTÁN uses the term "*subject to an individual or collective right*" as an example of legal protection. However, such a generic expression could be open to including the right to compensation for damages to the asset in question under non-contractual liability.

[30] Using as an example the judgment delivered by the European Court of Human Rights on 9 December 1994 (López Ostra vs. Spain), which found the Spanish State guilty of a violation of the right to a healthy environment for those living in the vicinity of a waste treatment plant. Among these assets, MARÍN CASTÁN includes the objectives of legislative policy such as the transparency of general contractual terms (ibidem), which perhaps represents a misjudgement of the words ("asset" under its civil meaning and "asset" as being subject to legislative policy) with no useful purpose.

[31] ALBALADEJO, ibidem, p. 357.

[32] Ibidem, vol. I, p. 2.

[33] Please see GONDRA, J.M., "*La estructura jurídica de la empresa (El fenómeno de la empresa desde la perspectiva de la teoría general del Derecho)*" [The legal structure of companies (enterprise phenomenon from a general theory of law perspective)], in *Revista de Derecho Mercantil* [Corporate Law Magazine], nº 228, 1998, pp. 493 et seq.

That data is not a thing does not mean that in general its content, i.e. the information it symbolically represents (for example, a digital photograph or written piece), is not a legal asset held by an individual and subject to numerous layers of protection and possible transactions.

In cases limited by a *numerus clausus* (as described below), the content of data may also be subject to fundamental rights (the protection of personal data) or form part of the scope of an actual ownership right, as is the case for trade secrets and intellectual property. However, in the latter example, the subject of the right of ownership is not the data but its content, as explained further down this article. In such cases, the fundamental or ownership right to which the content is subject will prevail over the status of legal asset, which such content will also hold.

In the remaining cases, i.e. where the content is not protected, it remains a legal asset. Where content is lost due to data corruption, for example during a cyberattack affecting the integrity of the information, a claim for compensation for the damages caused to the asset (the content of the data) may be filed, irrespective of whether the content is considered intellectual property or know-how, or is protected under any guise or not. As a legal asset, the unprotected content of the data will also be held by an entitled person (unless found within the area of intellectual property known as the "public domain", as prescribed under Article 41 of the consolidated text of the Spanish Intellectual Property Act,[34] the "TRLPI"). Where not considered personal data, such entitlement may be transferred.

Consequently, the content of the data, whether personal or not and protected by an intellectual property right, trade secret and other rights or not, is considered a legal asset. This conclusion is especially useful when it comes to mixed data sets, i.e. rafts of different types of data.

Data as such is usually a subsidiary legal asset or derived from the principal asset, which is as previously mentioned the content, i.e. the represented information. Data is not usually an autonomous legal asset separated from its content. The holder of the content (trade secret, personal information, original creation, etc.) is usually also the holder of the data which represents such content (electronic files containing the trade secret, personal data, original creation or other protectable right – please refer to Article 10 of the TRLPI regarding original creations "expressed in any mode or form").

Only on an exceptional basis will the digital expression of information hold its own value independent of the value of the content represented by such digital expression. Data as a separate and autonomous legal asset is recognised in at least two types of cases: (i) when the only digital version available of content stored in analogue format (for example, on paper) is lost, cannot be accessed or is damaged, where both versions are held by the same person: for instance, the single digital version of information comprising the trade secrets of a company, with said information – and therefore the content – kept on paper, or (ii) when the content belongs to what the TRLPI labels as the "public domain". The value lies within the effort made in digitising this content (to illustrate, the digitisation of an old library or the Factum Foundation project to scan documentation of cultural heritage[35]).[36] In these exceptional cases, data can also be a separate legal asset, as well as non-subsidiary or not derived from the principal as usually occurs when the content is protected. In such special cases, the value lies within the symbolic representation of the information rather than the information itself, and any damages will be compensated even if they do not entail the loss of the content of the data.

This conclusion can also be extended to all types of data. In essence, all data types constitute a legal asset regardless of whether they are protected by a fundamental, intellectual property or other right.

In layman's terms, references to data as a legal asset will actually be made to the content of the data and not the data itself.

---

[34] "*Works in the public domain may be used by any person provided that the authorship and integrity of the work are respected*", even though the disclosure of an unpublished piece found in the public domain leads to the consequences described under Article 129 of the TRLPI.

[35] Please see at https://elfuturoesapasionante.elpais.com/factum-foundation-escaner-salvar-obras-arte-milenarias/

[36] Article 128 of the TRLPI affords a 25-year intellectual property right to any person who "*takes a photograph or other reproduction produced by means of a process akin to photography*".

Is data – or its content – subject to appropriation? Ownership and entitlement

The first port of call is to address the issue of when the content of data is subject to appropriation. Only then will we move on to looking at the possibility of appropriating data itself (the symbolic representation of the information per se).

Debate in the US on the ownership of the content of data: an excursus

Foreign case law, particularly in the US, boasts two conflicting theories. Firstly, there are those which generally advocate a right of ownership over data (including personal data) or its content, based on the existence of an interest subject to transaction and protected by an *erga omnes* right over an object (for example, Schwartz[37]).[38] Secondly, there are those who distinguish between the right of ownership – where existing – over the content of data and the remaining cases in which neither the data nor its content are subject to ownership or exclusive protection, nor is the information to which the data refers, notwithstanding indirect protection in the event of unfair competition or other unlawful acts (for example, Determann[39]). The latter theory feeds the principle of unrestricted access to publicly available information on the Internet.

Strictly speaking, this debate differs from the one surrounding the possibility of freely using information published on the Internet for general knowledge and application. It may be that such information published for general knowledge and application (a photograph, Wikipedia page[40]) is protected – and continues to be protected following publication – by copyright (which, for example, prohibits plagiarism and requires the corresponding citation or certain conditions of use). Free software is another example. While the word "free" refers to an extensive public usage licence, it does not mean that the software was not someone's original creation, the moral right of which is inalienable.

It is also possible for information which in principle and by its very nature can be freely used without third-party protection (due to not being protected by a right of ownership or data protection right) not to be made public, to be kept confidential or access to it to be subject to an agreement (such as a licence or other agreement, for instance requiring user identification and the prior acceptance of contractual terms).

---

[37] SCHWARTZ, PAUL M., "Property, Privacy, and Personal Data", 117 *Harvard Law Review*, 2055 (2004). The author refers to personal data and defends its private ownership and potential to form part of a transaction, albeit limited in certain cases where market failures are identified. Please see other authors along the same lines in DETERMANN, LOTHAR, "No one owns data" (February 14, 2018). UC Hastings Research Paper No. 265, footnote 15.

[38] Naturally, the issue directly depends on the concept of ownership, which under common law is broader than in EU law. For example, SCHWARTZ (cit., p. 2058) defines it as "*any interest in an object, whether tangible or intangible, that is enforceable against the world*". CALABRESI and MELAMED defined the protection afforded by ownership as that which could/should be acquired in a voluntary transaction under which the value of the transfer is agreed between the purchaser and seller (please see CALABRESI, G. and MELAMED, A.D., Property Rules, Liability Rules and Inalienability: One View of the Cathedral, Harvard Law Review, Vol.85, p. 1089, April 1972), a much broader concept than the continental European idea.

[39] DETERMANN, LOTHAR, "No one owns data" (February 14, 2018). UC Hastings Research Paper No. 265.

[40] Although the information published on Wikipedia is accessible to the general public, this does not mean that some of it is not copyright protected. The owner of Wikipedia is the Wikimedia Foundation, a non-profit organisation headquartered in San Francisco, California. The website requires those who provide contributions to accept certain public usage conditions, although does not propose that they waive their moral (inalienable) rights or authorship of the content which in the case of original creations and protected photographs is subject to intellectual property. While this requirement will not always be met, the fact that the information is publicly accessible does not mean that the intellectual property over it is not maintained.

Nevertheless, the debate on the ownership of data is naturally underpinned by the power to exclude third parties (the possibility or not to freely use the information published on the Internet for general knowledge and application). If the owner of the content of data maintained ownership rights over such content following publication, as happens with intellectual property (especially regarding author's moral right), such person could exercise a right of pursuit (*reipersecutoriedad*) against any third party who has found the free information on the Internet and wishes to use it for their own means in violation of such rights. Where not holding such right of ownership with a right of pursuit, any powers to exclude third parties who have not accepted contractual restrictions concerning the subsequent use of the information are relinquished once it becomes public.

The question as to whether the content of the data is owned by the person who holds it is, for example, exposed in disputes stemming from companies which make information available to the general public (without the requirement to sign up to an account) or use social networks on which natural persons publish personal data for public knowledge without restriction, with the company subsequently intending to refuse access or use of the content by other enterprises which (directly or through automatic application, e.g. "bots") extract the public data without entering into an agreement to do so – "data scraping" –, as well as storing or using the data for their own means.

One such example would be HiQ versus LinkedIn. HiQ is a company which uses so-called "bots" (from "robots", i.e. automatic applications) to extract data on LinkedIn users which their subjects have wished to make public and which may be viewed without even having a LinkedIn account to offer analytical services to employers, including those looking to hire said users.

LinkedIn issued a cease and desist letter to HiQ and attempted to terminate the latter's ability to access the website. District Judge Edward M. Chen of California issued an order granting a motion for preliminary injunction[41] in which he considered HiQ's conduct as lawful, comparing it to an individual looking at a sign displayed in a storefront window publicly visible to all. The order addresses the idea that the content of this data, where made public by the user (therefore waiving their right to privacy granted under US law), is not owned by LinkedIn and the company therefore does not hold the authority to exclude third parties. The users' privacy was not considered decisive on the judge's understanding that if they had consented to the information being made public, their actual privacy interests were "*at best uncertain*", given they should have expected their profile to be subject to searches, date mining, aggregation and analysis. In fact, the judge believed that the free flow of information on the Internet was more deserving of protection, refuting the notion that LinkedIn – having made the information public – was entitled to deny third parties (using technology solutions) the subsequent use of such information. If the judge had believed that LinkedIn held a right of ownership over the data which had previously been made public, there is no doubt that he would have ruled the other way.

A very similar case was observed in Russia between VKontakte LLC and tech start-up LLC Double. LLC Double is a company which generates credit profiles of loan applicants based on the personal data published by VKontakte, Russia's Facebook equivalent. The case is awaiting resolution (the initial ruling went against LLC Double, albeit the judgment was thrown out on appeal, with the case referred back to the court of first instance, which is now tasked with delivering a new sentence).

[41] The order can be found at: https://assets.documentcloud.org/documents/3932131/2017-0814-Hiq-Order.pdf.

The issue in Europe: introduction

A similar dispute to the one raised by the HiQ vs. LinkedIn case would be out of the question in Europe given the protection afforded to personal data under the GDPR. The US approach to this issue tends to focus on safeguarding privacy as opposed to the right to personal data protection. The fact that the holders of the data consented to its publication on LinkedIn (therefore waiving their privacy) does not mean from a European personal data protection perspective that they also accepted its subsequent processing by HiQ. Such data processing by third parties without lawful grounds pursuant to Article 6 of the GDPR would violate the Regulation[42] regardless of the fact that the data subjects had made the information public and would require a subsequent notification to said subjects in accordance with Article 14.2.f) of the same legal text.

For this reason, in order to discover a comparable case in Europe we must look no further than the disputes surrounding non-personal data published on the Internet. Regarding non-personal data, the Court of Justice of the European Union and the Spanish Supreme Court have ruled that website owners do not hold a *sui generis* intellectual property right over databases. What's more, both courts have permitted data scraping, provided that there is no contractual relationship (which does not exist just by visiting a website without expressly accepting its general conditions) between the parties: *a sensu contrario*, the judgment delivered by the European Union Court of Justice on 15 January 2015 (Ryanair vs. PR Aviation)[43] and the judgment of the Civil Chamber of Spain's Supreme Court of 9 October 2012 (Ryanair vs. Atrápalo). Spain's Supreme Court believed that the existence of an agreement could not be recognised by simply using information from Ryanair's website, not to mention doing so in violation of the site's terms and conditions. With no agreement blocking it and no other regulations infringed (such as unfair competition), Atrápalo's conduct was lawful. Clearly, the outcome would have been different if an agreement was in place, albeit not by virtue of a non-existent right in rem of Ryanair (which is what matters now), rather based on the agreement itself.

---

[42] Without this outcome being undermined by Article 9.2.e) of the GDPR, which only removes the requirement for specific consent linked to the special protection afforded to health-related data, etc., but not general legal grounds. In this regard, please see MARTÍN, B. "*La publicidad del dato personal no otorga per se legitimidad para su tratamiento*" ["Personal data in the public domain does not automatically grant authorisation to process it"], available at https://cms.law/es/ESP/Publication/La-publicidad-del-dato-personal-no-otorga-per-se-legitimacion-para-su-tratamiento.

[43] Judgment of the Court of Justice of the European Union of 15 January 2015, case C-30/14, Ryanair Ltd. vs. PR Aviation BV. PR Aviation "operates a website on which consumers can search through the flight data of low-cost air companies, compare prices and, on payment of commission, book a flight. It obtains the necessary data to respond to an individual query by automated means, inter alia, from a data set linked to the Ryanair website also accessible to consumers. Access to that website presupposes that the visitor to the site accepts the application of Ryanair's general terms and conditions by ticking a box to that effect", which excluded the possibility of Ryanair tickets being sold by third parties or the data being extracted for marketing purposes. The Court understood that visitors to the website assumed the contractual obligation not to use the data for such purposes, which was lawful.

General principle: exceptional nature and numerus clausus of the right to appropriate information

Given that data is widespread in the information society, it is no wonder that the question as to whether the content of data is subject to appropriation cannot be whittled down to just a single response.

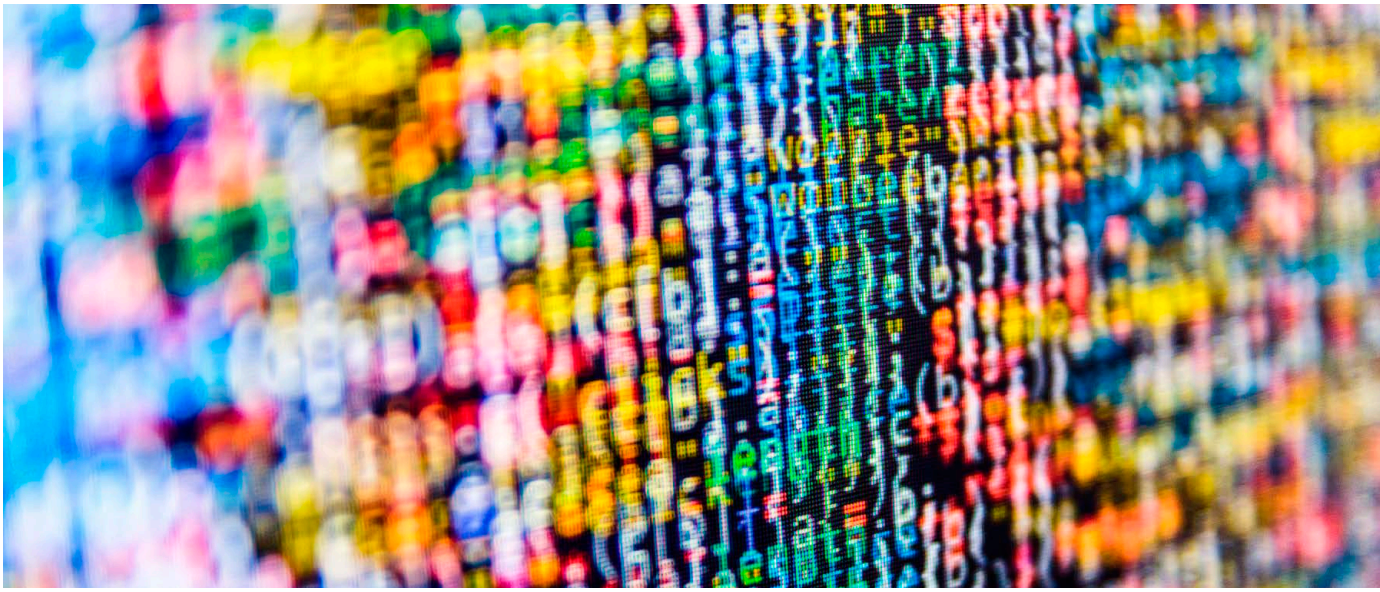
In my opinion, information (the content of data) – which is not a thing – is not subject to ownership except in cases where prescribed by a legal system on an exceptional basis: basically, by establishing intellectual or industrial property or trade secrets, i.e. *numerus clausus* cases with legal reservations. The relationship of personal data with its holder is not one of ownership, nor is the relationship between such data and those who hold contractual rights to use it (data controllers and processors). In all other cases, information is not owned, nor is there a right to exclude third parties based on an actual legal relationship, although: (i) there may be (if duly concluded) a valid contractual agreement between the parties, the fulfilment of which limits access to the information or its use; and (ii) there also may be an *ex lege* obligation to refrain from using the information for purposes of unfair competition or others prohibited by law, which would represent an alternative legal framework (not ownership) and refers to using the data as opposed to the data itself.

From a legislative policy perspective, the information society requires certain freedom in the flow of the content of unprotected data (that which is not personal and is not subject to special rights of ownership such as trade secrets and intellectual property). A system based on the general principle of the appropriation of information would turn the Internet into a maze of closed smallholdings. Naturally, ring-fenced areas should exist, such as intellectual property rights which reward the work that goes into original creation, as well as protected trade secrets. However, beyond these cases the principle of online freedom must prevail.[44]

From an alternative legislative policy point of view, competition is only excluded through exclusive rights recognised by the State in the wake of significant public interest which justifies the granting of monopolistic faculties (as in the case of industrial and intellectual property or trade secrets, which reward creative or corporate efforts). Only by way of exception should a right be granted to exclude others from the lawful obtaining and use of data needed for corporate activity. Continuing along the same lines, economic activity should be performed in an open environment. While some sections may be closed off, an excess of smallholdings and ring-fenced areas would be unwelcome. What's more, a shortage of common ground would render competition impossible. No obstacle would be more daunting for free competition than generic ownership of any type of data handled by a company, including publicly accessible and known data.

The relationship of personal data with its holder is not one of ownership, nor is the relationship between such data and those who hold contractual rights to use it (data controllers and processors).

[44] As stated by DETERMANN (cit., p. 43), *"new property rights in data are not suited to promote better privacy or more innovation or technological advances, but would more likely suffocate free speech, information freedom, science, and technological progress. The rationales for propertizing data are not compelling and are outweighted by rationales for keeping the data "open". No new property rights need to be created for data".*



In other words, when a legal system does not recognise a right of ownership over the content of data (the information represented within it), the process of digitising does not represent a change of tack, i.e. what is not owned in the real world is not subject to ownership in the digital sphere. In fact, that would occur in the case of content which does not meet the requirements to be considered an original creation or subject to intellectual property (*sui generis* right to databases, photographs), trade secrets or any other form of protected information.

One of the defining features of ownership is the faculty to exclude third parties, not by virtue of accepting an agreement (terms and conditions of a website), rather as a mere consequence of an actual in rem right. Díez-Picazo and Gullón[45] break it down into two: its preventative aspect, as in the faculty to avert the potential interference or disturbance of third parties, and its repressive aspect, namely the power to take action against third parties to put a stop to a disturbance or damages caused. These faculties would be combined with the right of pursuit, or the "*legally protected faculty to pursue or seek out the thing wherever it may be found and whoever may be in possession of it*".[46]

Aside from the cases in which a special right of ownership is held over non-personal data (such as intellectual property or a trade secret), unprotected data can be legitimately found in the hands of many people at the same time, all of whom could in theory make a claim to acquire it and none of whom would hold a right to exclude the others.

[45] DÍEZ-PICAZO, L. and GULLÓN, A., Sistema de Derecho Civil [The Civil Law System], vol. III, 9th Ed., Madrid 2016, pp. 44 and 45. In the same vein, Montes Penades, V., Artículo 348, Comentario del Código Civil [Article 348, Commentary on the Spanish Civil Code], *Ministerio de Justicia* [Ministry of Justice], 1993, vol. 1, p. 952, highlights that this faculty also exists under other rights. LACRUZ BERDEJO and DELGADO ECHEVERRÍA take it a step further by referring to "*exclusivity or absoluteness*" based on which "the holder of the right in rem can block others from having any influence on the thing to the detriment of such right", a faculty that "*follows the thing wherever it goes and whoever holds it in their possession*".

[46] DÍEZ-PICAZO, L. and GULLÓN, A., ibidem, p. 51.

In my opinion, unprotected information which is kept confidential only on a de facto basis (where it is not disclosed to third parties) or by way of an agreement (under confidentiality obligations or a website's terms and conditions) cannot be owned. In the case of unprotected information kept confidential under the terms of an agreement, while the protection measures can be invoked when a party breaches the confidentiality obligation by accessing certain information, this does not mean that the information can be reclaimed by its alleged owner. A determining factor is if the person who accesses a website's information is in possession of such information in breach of the agreed terms and conditions of the site, publishes it or transfers it to a third party with whom the website has not entered into any form of agreement, the original website owner is unable to bring action against the third party for merely being in possession of the information in question.[47] There is no right of pursuit or enforceable right against said third party. As I understand, such information (content) comprising non-personal data and not protected under special ownership is therefore not subject to appropriation.[48]

This does not mean that data with unprotected content (non-personal and not subject to ownership), which as we have seen represents a legal asset, cannot be kept confidential, nor that its holder cannot request the conclusion of an agreement to allow access to such data. A failure to meet the requirements for works of human ingenuity to be recognised as an original creation or trade secret does not mean that anyone is entitled to access or use it if it has not been published by the data holder.

---

[47] Concurring with the text of the new Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. Under the Directive, consumers are permitted to designate a third party to receive the content, who in turn will allow the consumer to access such content through a physical or virtual facility, which does not entail an exception to the foregoing (in this instance, the third party is operating in the consumer's interest). Further references to third parties also fall in line with these ideas. Article 8 stipulates that content must be free of intellectual property rights, and Recital 37 finally salvages the situation where there are no further obligations once the agreement has been terminated if the consumer has lawfully provided the content to third parties in accordance with the agreement.

[48] Contra, OSBORNE CLARKE LLP, Legal study on Ownership and Access to Data, report for the European Commission, 2016, which states that in accordance with "*the language used in both the EU Data Protection Directive and in the glossary of terms of the Spanish Data Protection Act, the data subject is defined as "the natural person to whom the data undergoing processing pertain". It is our understanding that this definition would be also translatable to those scenarios in which the data does not pertain to a natural person or which does not qualify as personal data. In such case, the data would be the property of the entity or individual that directly or indirectly generates/produces such data" (p. 75). "In the absence of specific provisions, I consider that Article 348 of the Civil Code protects each company to "enjoy and dispose" of the data collected, provided you do so in a way that does not violate the Law*" (ibidem, p. 76). In contrast, coinciding with the criteria of the text, albeit without referring specifically to Spanish law (rather to other European systems in general), VAN ASBROECK, B., DEBUSSCHE, J. and CÉSAR, J. (Bird Bird), Building the European Data Economy – Data Ownership White Paper, 1 January 2017, p. 120: "*the current legal framework relating to data ownership is not satisfactory. No specific ownership right subsists in data and the existing data-related rights do not respond sufficiently or adequately to the needs of the actors in the data value cycle. Up until today, the only imaginable solution is capturing the possible relationships between the various actors in contractual arrangements*".

A person who as a result of their efforts has created or catalogued information not considered an original creation or trade secret is not duty bound to share it with everyone. As a declaration of their personal freedom, such person could decide to keep the information for themselves or simply hand it over to those who enter into an agreement with them (setting forth a faculty of exclusion or usage restriction). However, this person cannot consider themselves as the owner of the information and, where making it public, would not be able to pursue those who use it without entering into a pertinent agreement.

The power to exclude third parties borne out of an agreement (between the host company and holder of the data as a legal asset, or between the holder and a client) – a faculty usually applying on the Internet in relation to content which has not been legally protected – is not enforceable against third parties, rather existing and expiring under the scope of the agreement (Article 1257 of the Spanish Civil Code). This is different to protected personal data or intellectual property, for example, which can be enforced against anyone in unlawful use of the protected content, even if there is no contractual relationship with its true holder.

Other legal assets such as news reporting or financial information, a company's credit rating, business opportunities or reputation cannot be owned. While compensation can be claimed if they are damaged in violation of the law and, as legal assets they can be considered held, they cannot be reclaimed when lost and are not subject to actual in rem rights.

The fundamental right to the protection of personal data is not ownership

In my opinion, it is clear that the fundamental right to the protection of personal data is not a right of ownership, nor could it ever be. It does not require the civil principle of ownership to justify protection and the action afforded to the holder and other affected parties.

Fundamental rights are a legal concept with their own defining features and do not need to rely on other principles such as ownership to demonstrate their substance. It is neither pertinent nor necessary to apply the civil principle of ownership to account for the faculties arising from a fundamental right such as personal data protection. Nobody owns themselves or their personal attributes, with the opposite entailing the undue patrimonial appropriation of non-patrimonial assets (referred to by De Castro as "*bienes de la personalidad*"[49]).

This fundamental right is enforceable on an *erga omnes* basis, i.e. generating a positive duty to protect which is imposed on other individuals and stretches far beyond the general responsibility of *neminem laedere*.

The right of the data controller, defined under Article 4.7 of the GDPR as "*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*", does not represent a right of ownership. As the name suggests, the position of controller is someone who is responsible for a set of obligations in addition to holding rights. Their obligations are executed in the interest of a third party, namely the holder of a fundamental right (the "*data subject*"), or for the protection of a public interest protected by law which the data controller cannot decline. Under the latter exception, the data subject holds the right to demand that the data be erased (the "*right to be forgotten*"), the right to restriction of processing (Article 18 of the GDPR) and the right to data portability (Article 20 of the GDPR), all of which are inalienable and extra commercium. In my opinion, the imposition of a penalty or charge against the exercise of these rights cannot be sustained (as opposed to the scenario set out in Article 2.3 of Spanish Constitutional Act 1/1982 of 5 May with regard to image rights). The data controller acts within the scope of a mandatory and inalienable fundamental right of others which the controller will never hold. The controller's right, surrendered upon erasure of the data by the data subject, is not and could never be a right in rem.

---

[49] Please see in DE CASTRO, F., *Estudios jurídicos del Profesor Federico de Castro* [Legal Studies of Professor Federico de Castro], vol. II, 1997, pp. 873 et seq. An alternative version can be found in De Castro, F., *Temas de Derecho Civil* [Matters of Civil Law], Madrid, 1976, pp. 7 et seq.

A further issue is that of the algorithms and new data created based on personal data. Using personal data, controllers can generate or refine algorithms and even feed artificial intelligence programmes. When referring to an identified or identifiable individual, said algorithms or new data would fall under the scope of the fundamental right to personal data protection and therefore must be erased if the holder legitimately exercises their right to be forgotten. Conversely, when the algorithms or new data refer to the general public (even if they have been created and enriched with individual experiences) or generically-identified persons who meet a certain profile which cannot be linked to specific individuals, they are not recognised as personal data and should not be erased. When an artificial intelligence programme has learned the behaviour of users of a platform in order to interact with them, even where said users de-register from the platform and exercise their right to be forgotten, there is no obligation for the programme to "unlearn" what it has acquired in relation to human nature or the behaviour of the platform users, who in this instance take on the consideration as generic and unidentifiable. This data would be non-personal and usually unprotected (please see below).

Since the data controller's duties are performed in the interest of a third party (the data subject holding the fundamental right), the faculties of the controller are restricted in relation to matters of dignity. The data subject must provide consent within such limits and cannot lawfully consent to the abusive deployment of the restrictions to the detriment of their own dignity.[50]

Focus on intellectual property law

Data may contain original literary, artistic or scientific creations[51], photographs protected by intellectual property[52] or databases which, while not original creations, merit sui generis protection on the back of representing a "substantial investment" made by their owner "to obtain, verify or present their content".[53]

As a true right of ownership, it enjoys a right of pursuit and is enforceable against third parties. There is no requirement for a contractual relationship to exist between those who use intellectual property without a licence and the corresponding owner of the work in order for the latter to be protected by the courts.

---

[50] As stated by SANDEL: "*some of the good things of life are corrupted or degraded if turned into commodities*" (SANDEL, M., What money can't buy, Penguin, 2012, p. 10). The public order-based restriction relating to the constitutional principle of dignity will always be present in legal transactions involving personal data. Along the same lines, albeit more broadly speaking, RADIN, M.J., *"Prorietá e ciberspazio", Rivista critica del diritto privato* ["Ownership and cyberspace", A critical review of private law], XV-1 (1997), p. 90, criticising the "commercialisation" of the Internet.

[51] Article 10 of the consolidated text of the Spanish Intellectual Property Act enacted by Royal Legislative Decree 1/1996 of 12 April.

[52] Article 129 of the TRLPI.

[53] Articles 133 et seq in relation to Article 34 of the TRLPI.

Publishing the content of the data (for example, an original creation) on a publicly accessible website does not mean that its possible protection under intellectual property is lost. In fact, the possibility remains to pursue those who download the work without authorisation and subsequently publish it in paper format or on their own website (usage in violation of Article 17 of the TRLPI). As previously mentioned, moral rights and usage restrictions may exist over freely available software or the content at our fingertips on Creative Commons or Wikipedia Commons published on the Internet and accessible for all. The same is true for a photograph, which holds a right afforded under Article 129 of the TRLPI, or databases, which may enjoy a *sui generis* right under Articles 133 et seq (in relation to Article 34) of the same legal text.[54]

Many debates have been had as to whether content (represented by data) produced by artificial intelligence machines can be considered the intellectual property of those who have prepared and used such apparatus. Bercovitz[55] casts doubt over whether it can be recognised as an "*original creation*", although does not rule out the possibility altogether. It is becoming increasingly difficult to tell original creations born directly out of human intelligence apart from original creations produced by human intelligence with the help of artificial intelligence.

Based on pre-existing intellectual property, it is possible to create derived data,[56] leading to the need to distinguish between simple reproduction, transformation (derived creation) and independent works (which do not require the consent of the holder of the original work).

Focus on industrial property (trademarks)

As potentially protected content of certain data, trademarks are also subject to ownership, in this case as industrial property. Unlawful conduct in this instance is linked to the illegal use of the data as a distinctive sign.

In contrast, patents are not protected content given that their publication represents the assumption they are protected.

Right of ownership over trade secrets

The Spanish Trade Secrets Act 1/2019 of 20 February (*Ley 1/2019, de 20 de febrero, de Secretos Empresariales*) transposing Directive (EU) 2016/943 of 8 June 2016 was published recently.

Said Act has devised a new, special right of ownership over "*any information or knowledge, be it technological, scientific, industrial, commercial, organisational or financial, which meets the following conditions:*

1. *it is a secret, meaning that in its entirety or the exact arrangement and form of its components is not generally known by persons operating in the areas where such information or knowledge is normally used, nor do they have straightforward access to it;*
2. *it has actual or potential business value due to being a secret, and*
3. *those in possession of it have implemented reasonable measures to ensure it remains a secret".*

---

[54] Please see the judgment delivered by the Court of Justice of the European Union (Fourth Chamber) on 5 March 2009 (reference for a preliminary ruling: Sofiyski gradski sad - Bulgaria) - Apis-Hristovich EOOD / Lakorda AD (Case C-545/07), which stated that "*the fact that part of the materials contained in a database are official and accessible to the public does not relieve the national court of an obligation, in assessing whether there has been extraction and/or re-utilisation of a substantial part of the contents of that database, to verify whether the materials allegedly extracted and/or re-utilised from that database constitute a substantial part, evaluated quantitatively, of its contents or, as the case may be, whether they constitute a substantial part, evaluated qualitatively, of the database inasmuch as they represent, in terms of the obtaining, verification and presentation thereof, a substantial human, technical or financial investment*".

[55] BERCOVITZ RODRÍGUEZ-CANO, R., Comentarios a la Ley de Propiedad Intelectual [Commentary on the Spanish Intellectual Property Act], 4th Ed., Madrid, 2017, p. 111: "*it would be absurd to even consider the possibility that the author of a work of ingenuity could not be a human"; "we therefore refute the notion that those holding copyright over the program could reclaim the status of author over the opus stemming from the application*". In addition, BERCOVITZ refutes the general existence of originality (which would have to be analysed under the spotlight of Article 10 of the Spanish Intellectual Property Act.

[56] Please see the judgment delivered by the Provincial Court of Tenerife on 15 June 2001: "*The appellee refers to the criteria used by certain courts (...) by highlighting that (i) the mere existence of elements of a piece of work in another does not entail the existence of plagiarism or transformation per se; (ii) both the identical and differing elements must be assessed, categorising them as essential or accessory; (iii) based on this, we must establish (i') whether the additions or contributions are insignificant and lack creative value, giving rise to simple reproduction under Article 18 of the Intellectual Property Act; (ii') whether such contributions are deemed original creations in secondary or accessory elements but retain a substantial part of the previous piece, suggesting the transformation mentioned in Article 21 of the same legal text, or (iii') whether the additions are so significant and specialised that they generate an original piece of work which differs from the previous one*".

Not all data contains trade secrets and not all trade secrets are the content of data. Trade secrets are different from the data within which they may be expressed, and in fact do not necessarily have to be represented symbolically through data. In any event, the protected element is not the data, unless safeguarded indirectly.

The vague nature of the definition given to the subject of special ownership is somewhat concerning. In other words, the terms "*generally known*" by persons "*operating in the areas where such information or knowledge is normally used*" are too generic and unclear as legal concepts. However, there is little room for manoeuvre given that it is a transposition of an EU Directive.

This right enjoys a right of pursuit and is enforceable against third parties insofar as the interpretation of Article 7 of Act 1/2019 reveals that the *non domino* acquisition of a trade secret is not upheld, providing the reason why the transferring party – in exchange for consideration – lacking entitlement to the data is forced to compensate the acquiring party.

Those who infringe this right are protected through injunctions, even where a contractual relationship between the parties does not exist, thus reinforcing the right of pursuit and enforceability against third parties but failing to build a decisive argument (certain injunctions used to defend legal interests do not necessarily represent rights of ownership, such as the one described under Article 32 of the Spanish Competition Act – *Ley 3/1991, de 10 de enero, de competencia desleal*).

The content of unprotected data as a legal asset

Beyond the above-mentioned cases, and as already stated, certain information at a person's disposal could be considered a legal asset, the confidentiality of which may be protected on a de facto or contractual basis. While there is no obligation to publish this information, it is not subject to ownership.[57] Such information could become highly valuable to its holder if resulting from individual work or a significant investment of time or money, without representing an original creation or protected trade secret. For example, where the holder makes the information public on their website, such as financial or scientific data records which do not comprise a database afforded *sui generis* protection, or corporate know-how disclosed by the company to persons who have not signed a non-disclosure agreement.

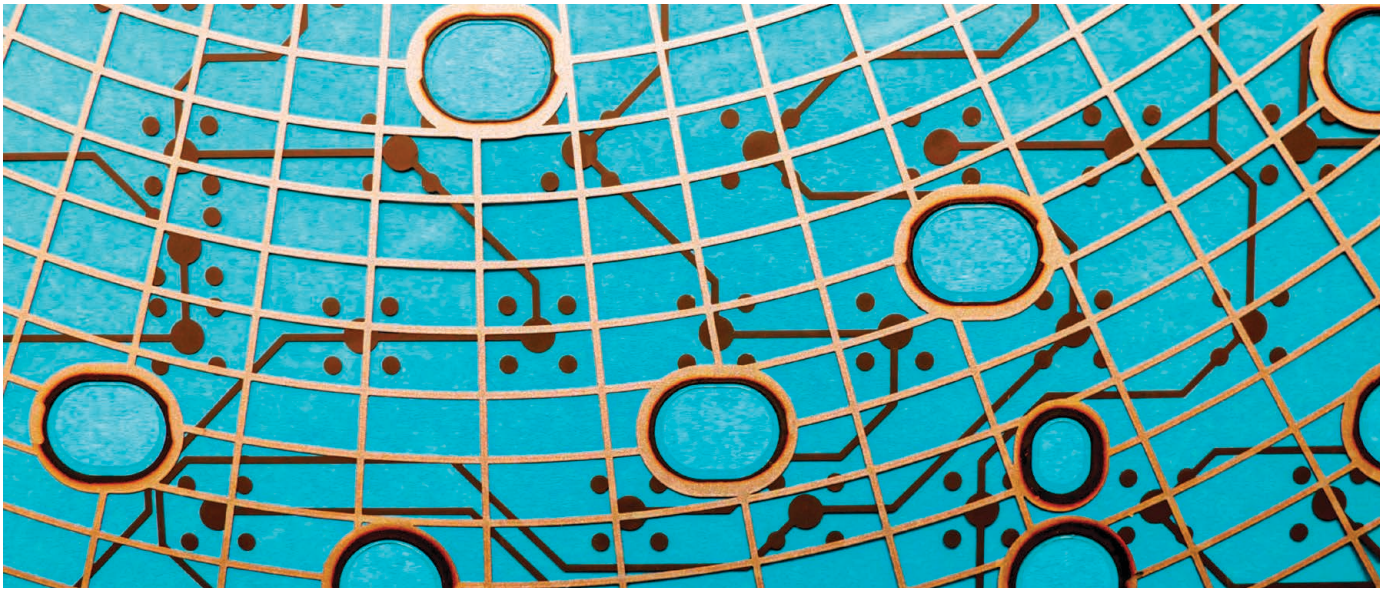
Where information not protected for the purposes described above (data protection, intellectual property, etc.) has economic value[58] but is lost due to the actions of a third party, the holder of such information would be able to file for non-contractual liability under Article 1902 of the Spanish Civil Code or unfair competition in order to claim the corresponding compensation for damages, but not action to recover the damages.

The legal treatment of this unprotected data will be looked at in more depth later in this article.

---

[57] RADIN, M.J., "*Prorietá e ciberspazio", Rivista critica del diritto privato* ["Ownership and cyberspace", A critical review of private law], XV-1 (1997), sets out three criteria de lege ferenda advisable for the recognition of a right of ownership: scarcity, system costs and market failures. Unprotected data may (or may not) be scarce, depending on its content, and the costs of a system which grants ownership rights over such data would be exorbitant (where original creation is not required, many parties could allege entitlement to the data and its variants), not to mention the fact that the market failures would be enormous (by paralysing the use of the information and hindering open interaction on the Internet).

[58] This would not be the case, for example, with public information which is freely accessible under the Spanish Transparency Act (*Ley de Transparencia*). Conversely, for the purposes of intellectual property, being in the public domain does not mean that the information cannot hold certain economic value. For instance, where an individual finds and digitises a new Sophocles tragedy unknown by the public. If damages are caused, they will be deemed subject to compensation.



Distinction between protecting the content of data and the legal restrictions on its use

Unfair competition law, in particular Act 3/1991 of 10 January, does not directly afford any form of protection to the data or content of the data of a company. The protected element is not the content of the data itself, rather the competitive activity which could be damaged through the exploitation of work done by others.

The Spanish Supreme Court has traditionally been reluctant to uphold lawsuits based on unfair competition, especially those relating to the exploitation of work done by others (please see Supreme Court judgment 572/2012 of 9 October, Ref 2012/11059).

Regarding patent law, a legal restriction is imposed on using the content of certain data, although never on the disclosure of the data itself (the protection afforded by the patent is based precisely on its publication), as previously mentioned.

Is data itself, as opposed to its content, subject to ownership?

In cases whereby the content of the data is protected, such safeguarding extends to its symbolic representation, i.e. the data, which bears the fruit of identical protection.

In all remaining cases, the legal asset (that which pertains to the holder's interest) will usually be the information comprising the unprotected content of the data (non-personal and not representing intellectual or industrial property, nor a trade secret). Data will normally be a legal asset because of the information it contains.

As mentioned, on an exceptional basis the data itself could constitute a legal asset as the computable, symbolic representation of information that would otherwise appear in non-digital format or could not be found in another format.

In theory, such entitlement over unprotected data as a legal asset does not afford a protectable right of ownership[59] or right of pursuit, and does not permit action against a third party using the digitised, unprotected information, even if the claimant is the one who carried out said digitisation. Digitising information is not usually considered an original creation, often rather a mechanical process. This is notwithstanding potentially unfair competition for the exploitation of the work of others, although as we have observed, this is not actually a case of protecting the data or its content, rather the unlawful nature of certain uses of the data.

[59] Please be aware that in the case of digital photographs protected under Article 129 of the TRLPI, among others, the data (digital expression of an image) is protected. However, such protection is by way of intellectual property.

Ownership of storage media

All data, including that hosted in the "cloud" (the name often given to AWS' or other hosting service providers' servers), is held on one or more electronic devices. The storage medium, electronic device or hard disk on which the data is found (traditionally a server although sometimes in more inconspicuous locations) is clearly subject to ownership given its physical existence. Such ownership grants certain legal faculties relating to the availability of the thing, including – in principle, and unless prohibited or restricted by law or by virtue of an agreement – the hosting of data, access to the data, its processing, use, amendment and updating, erasure and the faculty to exclude third-party access (directly or remotely) to the physical device. The exercise of these faculties can be limited by legal and contractual obligations. For example, such legal obligations regarding personal data are construed as the requirement for lawful grounds as set out under Article 6 of the GDPR or to adopt security measures to protect personal data, not to mention those outlined in intellectual property and trade secret legislation. The contractual obligations assumed with the data holders could consist in obligations to maintain server availability, access guarantee, preserve the data, adopt cyber security measures, etc. (these obligations invoke contractual liability towards the obligee).

Where meeting certain requirements, operators of certain electronic devices on which storage services are provided (known as hosting, which comprises "*storage of information provided by the recipient of the service*") are also exempt from liability under Article 16 of the Spanish Information Society Services Act (*Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información*, the "LSSI"),[60] which does not apply to the provider of the stored information, representing a further reason not to confuse the first with the second.

The physical devices on which data is hosted can also be subject to possession, as well as benefit from what was formerly known as interdictum (the protection afforded under the current Article 250 of the Spanish Civil Procedure Act – *Ley de Enjuiciamiento Civil*), as well as everything linked to ownership.

[60] Article 16 of the LSSI: "Liability of data hosting or storage service providers. 1. Providers of brokerage services consisting of hosting data provided by the recipient of the service will not be held liable for the information stored at the recipient's request, provided that: a) they are not actually aware that the activity or stored information is unlawful or damages third-party assets or rights subject to compensation, or b) If they are aware, they make their best efforts to remove the data or block access to it. The effective awareness of the service provider referred to under section a) shall be understood as when a relevant body has declared the unlawfulness of the data, ordering its removal or blocking access to it, or where the existence of damages has been declared, and the provider was aware of the corresponding resolution, irrespective of the detection methods and withdrawal of content the provider applies under voluntary agreements and other means of effective awareness that may be established. 2. The exemption from liability prescribed under section 1 shall not apply in the event that the recipient of the service is acting under the direction, authority or control of the provider".

Special considerations regarding the civil law treatment of unprotected data

This section aims to delve further into the civil-related aspects of an existence which has not be adequately addressed by civil case law: the data we label "unprotected" due to being non-personal and which is not subject to rights of ownership as already mentioned.

Entitlement

As legal assets, both unprotected data and its content can have a holder. The holder of a legal asset is who would be compensated if such asset is damaged.

Such entitlement of unprotected data and its content – as a legal asset subject to exploitation (non-exclusive) or damage – stems from its mere availability. The person to which such data are lawfully available is a holder of such data, whether having generated the data themselves or having received it from a third party.

Generating unprotected data for the benefit of its holder can be done in many ways: through the individual creation of new digital content (where not representing an original creation, it would be recognised as intellectual property), via a user interface known as the "data producer" (where others input information), through the digitisation of analogue data, by anonymising personal data (which ceases being personal and is passed to a new holder) or through artificial intelligence processes applied to big data – so-called "data mining".

Possession?

The possession of unprotected data represents a challenging conundrum. Clearly, the answer to the problem depends on how loosely or strictly we interpret the concept of possession as a legal concept. In my opinion, although notwithstanding the possession of rights,[61] possession cannot be held over something which is not subject to appropriation, as stated in Article 437 of the CC: "*only things and rights which are capable of appropriation may be subject to possession*".

[61] Certain doctrine limits the rights subject to possession. For example, GOMÁ SALCEDO limits possession to rights in rem or contractual rights "which give rise to de facto relationships with the thing" (*Instituciones de Derecho Común Civil y Foral* [Civil Common and Regional Law Institutes], vol I, p. 804). DÍEZ-PICAZO and GULLÓN narrow it down to rights in rem (*Sistema de Derecho Civil* [The Civil Law System], III, p. 99), as well as the former believing that "the same core of possessory phenomenon is found in the special legal protection we call interdictum" (*Fundamentos del Derecho Civil Patrimonial* [Foundations of Civil Patrimonial Law], III, 5th Ed., 2012, p. 624). Please see *Fundamentos del Derecho Civil Patrimonial* [Foundations of Civil Patrimonial Law] III, cit., pp. 679 and 680, providing commentary on the judgment delivered by the Provincial Court of Madrid on 12 November 1974 which discussed the environment as a legal asset subject to possession, stating that such notion stirs up "*certain difficulty*".

We have already seen that, as with its content, unprotected data is not subject to appropriation. In my opinion, the logical consequence is that while data cannot be possessed,[62] it is open to being held de facto.

While certain doctrinal opinion on the possession of intangible assets does exist, it essentially refers to intellectual or industrial property rights (which some believe to be open to possession under such rights[63], whereas others are of the opposite persuasion[64] – the latter backed by an enduring judgment delivered by the Spanish Supreme Court on 16 April 1941[65]).

However, that is not the purpose of this article, which seeks to address unprotected data. By default, such data is not subject to intellectual property – given the lack of an original creation –, industrial property or trade secret. Specific doctrinal analysis on the possession of unprotected data is in short supply, although general opinion refuting the possession of intangible assets can be applied in this instance (notwithstanding the possession of the objects which bring them to life), such as those expressed with subtle differences by Coca Payeras[66] and Bustos Gómez Rico[67] suggest. Possession implies the exclusion of third parties which does not align to the situation of merely de facto holding unprotected information (or its digital representation), which may be simultaneous and compatible for many people at the same time.

Unprotected data and its content do not fit into the category of "rights", which are subject to possession. Contractual rights over data (for example, a contractual right against the digital service provider hosting the data), which in my opinion can be possessed, are not to be confused with the data to which such rights refer (nor with the content of such data).

That unprotected data cannot be possessed does not mean that it is not possible in certain scenarios, to make use of the oral trials established under Article 250 of the Spanish Civil Procedure Act (the former interdictum). For example, Article 250.4 of said Act affords action to those "seeking summary protection to hold or possess an asset or right by those who have been stripped of them or whose enjoyment of them has been disturbed". As J.M. Miquel recalls, this protection formerly known as interdictum is not only afforded to the possessor, stemming from the wording of the precept, which speaks of de facto "holding" as the grounds for action, as opposed to "possession". The simple de facto holding of unprotected data therefore exists.

The non-possession of unprotected data in a legal sense (coupled with a lack of ownership, as we have seen) raises numerous consequences. One example concerns the idea of a pledge, which is not possible when it comes to unprotected data (Article 1864 of the Spanish Civil Code: "All movable things which are subject to trade may be pledged, provided that they are capable of possession").[68]

Moreover, the true possession of the things on which the data is hosted – servers, USB drives, etc. – is also possible, as previously mentioned.

---

[62] Contra, ENCARNACIÓN ROCA, verbally-expressed opinion at the *Real Academia de Jurisprudencia y Legislación* [Royal Academy of Jurisprudence and Legislation].

[63] COCA PAYERAS, M., *Artículo 437, Comentario del Código Civil* [Article 437, Commentary on the Spanish Civil Code], *Ministerio de Justicia* [Ministry of Justice], vol. 1, p. 1180. COCA PAYERAS defends the possession of intellectual property as the possession of rights, as opposed to the possession of assets.

[64] FUCHS MATEO, L., *La propiedad intelectual como propiedad especial a lo largo de la Historia, tesis doctoral* [Intellectual property under special ownership throughout history, doctoral thesis], Universidad Complutense de Madrid, 2017, p. 3.

[65] "*Industrial property forms one of the categories of intellectual products protected and regulated as an independent class under modern law, thus granting the inventor exclusive enjoyment of the fruits of their mind – their idea – and therefore a right which, as opposed to the so-called rights in rem over specific material things, is considered intangible and not subject to possession, with possession understood in the sense of a current and exclusive possibility of exercising power over the same thing*".

[66] In essence, the author affirms the possession of intellectual property over intangible assets understood as the possession of rights. Where there is no intellectual property to possess – rendering the possession of rights unfeasible – the supported conclusion, *a sensu contrario*, appears to point towards possession being impossible, even if such outcome is formally established. Please see COCA PAYERAS, M., ibidem, 1993, vol. 1, p. 1180.

[67] DE BUSTOS GÓMEZ RICO, M., "*Artículo 437", Comentario del Código Civil* ["Article 437", Commentary on the Spanish Civil Code], Bosch, 2000, p. 395.

[68] This should not be confused with transferring as collateral any contractual rights against digital service providers allowing access to unprotected data, or indeed other contractual rights relating to such type of data.

Flow

Given its widespread and multi-location existence, data is especially inclined to move around and change its whereabouts. The free flow of non-personal data in the European Union is considered so important in upholding community principles and free competition within the single market that a block-wide regulation has been passed (Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union), backed by a Communication from the Commission.[69] Numerous authority regulations forced economic operators to host data on servers located within their respective domestic territories. According to Article 4 of the Regulation, "*data localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality*". This is more a public than private law norm, although does highlight that data is made to be circulated and that the flow of data is crucial for the development of the information society.

Portability

Data portability is different from the free flow of data and refers to the right which on occasions is attributed by the legal system to the person who pretends to request and obtain a copy of such data from digital service providers in a structured and machine-readable format for common use, whether to be sent directly to said person or to be directly transferred from controller to controller, where technically feasible. Such right encourages free competition by paving the way for a change in service provider.

The right to portability for personal data (bound to an inherent fundamental right) is not recognised under the same terms as for non-personal data. Regarding personal data, the right to portability is afforded under Article 20 of the GDPR, whereas for non-personal data Article 6 of Regulation (EU) 2018/1807 only obliges the European Commission to encourage and facilitate the development of self-regulatory codes of conduct to enable such right.

The reason behind this difference in treatment can be sought in doctrinal debates on the drawbacks of recognising the right to portability,[70] which in the case of personal data are eclipsed by the fundamental right that does not exist over non-personal data.

Nevertheless, in a small number of instances the right to portability may be recognised over non-personal data, although broadly speaking this is rare.[71]

---

[69] Communication from the Commission to the European Parliament and the Council of 29 May 2019, "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*".

[70] Essentially three-fold: (i) its high economic burden on SMEs (writing in EIM code entails further costs), (ii) the possible harming of intellectual or industrial property rights or trade secrets (note that the non-personal data which may be subject to portability is data which has been provided and observed, as opposed to inferred or deduced data, or indeed data generated by artificial intelligence devices based on provided and observed data), and (iii) the security risks (which are greater where portability exists). In addition, Articles 102 of the Treaty on the Functioning of the European Union and 2 of the Spanish Competition Act protect against service providers which abuse their dominant position, representing an alternative solution to portability. Against this backdrop, several authors have called the general recognition of the right to portability into question: DIKER VANBERG, A. and ÜNVER, M.B., "*The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*", European Journal of Law and Technology, vol, 8, No. 1, 2017, highlight the three reasons listed above; SWIRE, P. and LAGOS, Y., "*Why the right to data portability likely reduces consumer welfare: Antitrust and Privacy Critique*", 72 Maryland Law Review, 335 (2013) claim that competition law uses a "*rule of reason*" instead of a "*per se approach*"; portability "*fails to weigh pro-competitive efficiencies against anti-competitive harms*"; and lastly ENGELS, B., "*Data portability among online platforms*", Internet Policy Review, Vol. 2 Issue 2 (2016), defends portability for search engines but not always for marketplaces or social networks.

[71] For example, Article 16.4 of Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services affords a right to portability of digital content (which may include non-personal data) to consumers upon termination of the content or digital service agreement. In turn, Article 95 of the Spanish Constitutional Act on Data Protection and the Guarantee of Digital Rights stipulates that "*users of social network and equivalent information society services shall be entitled to receive and transfer the content provided to those rendering such services, as well as for the service providers to directly transfer the content to other providers designated by the user, where technically feasible*". The precept only applies to users of social network and equivalent services. Lastly, Article 96 of the same Constitutional Act sets out the regulations applicable to content handled by service providers when it comes to information on the deceased, which on occasions could lead to the portability of non-personal data. However, in the three instances mentioned and as far as non-personal data is concerned, these are isolated cases and do not reflect a general principle, which only exists in relation to personal data.

Inter vivos transfer

In the case of entitlement to a legal asset, said asset may be transferred unless prohibited by legislation (such as Article 525 of the Spanish Civil Code regarding rights of use and habitation). To draw an analogy, it is worth mentioning at this stage Article 1112 of the Civil Code relating to the transfer of credits.

Transfers through the sale and purchase of unprotected data and its content do not require the data to be subject to appropriation. Articles 1526 et seq of the Civil Code prescribe the sale and purchase of "*credits and other intangible rights*", including contractual rights, litigious rights or sets of "*rights, income or products*". There is also "*emptio spei*", the sale and purchase of business opportunities, the sale and purchase of exclusive or non-exclusive information, the sale and purchase of companies (which strictly speaking are not things, as mentioned earlier), etc. Therefore, there would be no barrier to the sale and purchase of unprotected data or its content with an economic value.

Other legal transactions

All types of legal transactions involving unprotected data are possible under the notion of autonomous free will. The item does not have to be an appropriable thing subject to a right of ownership for the transaction to be considered lawful.

Such legal operations, the greatest part of which are atypical, are similar to those executed with other intangible assets such as intellectual property. Against this backdrop, legal transactions relating to the following can be executed: access to data (exclusive or non-exclusive licences, usually bound to a specific period of time and geographic scope), the possible downloading of the data, its processing or transformation to create derived data (for the personal aims of the party acquiring the right), advertising sponsorship, economic use (including the trading of access rights in exchange for users' personal data), maintenance and protection against IT risks and data hosting.

In fact, the new Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services is being published at the time of writing. Said Directive sets out a legal transaction which enables consumers (or a third party chosen thereby) to access or download digital content offered by a company and regulates matters such as the conformity of the digital content under contract, the correct integration of the content by the supplier, liability for infringement, contract termination and the amount of compensation owed for damages, as well as the possibility for the supplier to modify (where required) or update the content during the contract term.

Succession

In the wake of a recent legal ruling and the passing in Spain of the Constitutional Act on Personal Data Protection and the Guarantee of Digital Rights, doctrine has begun to take notice of personal and non-personal data succession. A leader in this field is Sergio Cámara.[72]

The subject stretches far beyond the scope of this article. The majority of reviewed judicial rulings and enacted laws (for example, Articles 3 and 96.2 of the LOPDG) essentially refer to the personal data of the deceased, although occasionally delve into non-personal digital content (in particular, Article 96 of the LOPDG).

Furthermore, as previously said, data is a broader concept than digital content managed by information society services providers (those to which Article 96 LOPDG refers). Succession should be referred to all data lawfully hold by the deceased person.

In my opinion, Sergio Cámara is right to distinguish between that which does not form part of inheritance (the post mortem protection of the personal or moral aspects of personality) and that which, pursuant to Article 659 and 661 of the Spanish Civil Code, forms part of the estate as assets and rights which do not extinguish upon the death of the deceased. Digital content, which might not be personal data, would fall among the latter category, along with other non-personal data.

At this stage, it is pertinent to touch on the fact that in addition to digital content and other non-personal data, the inherited estate may include rights acquired contractually towards digital service providers (to be used through credentials, as Cámara mentions) if they do not extinguish upon the death of the creditor.

Naturally, the devices on which the data is hosted are things subject to ownership and therefore included in the inheritance (with the proprietary faculty to use the things to access their content, unless prohibited by law – although this is rare in the case of non-personal data given the scope of Article 96.1 of the LOPDG – or where the deceased had declared their wish for this not to occur, as also permitted under the aforementioned Article 96.1).

Having determined the object of succession, under which the majority of unprotected data will be found, Article 96.1 of the LOPDG affords additional rights of access to digital content to persons other than the heirs. In principle, if the data subject provides their consent, a plethora of immediate family and relatives could be granted such rights ("persons linked to the deceased as family or on a de facto basis, as well as their heirs", the "executor, individual or organisation to whom the deceased had allocated the rights" and others in the case of minors or "persons with a disability" – civil disqualification does not appear to be required). Such legal provision is somewhat reprehensible and most certainly contrary to the deceased's wishes, especially when it comes to personal data (which is now irrelevant) and non-personal data as well. It beggars belief that a person would wish for their digital identity to be exposed to persons with family or *de facto* ties to them following their death. Article 96.1 of the LOPDG (which also applies in relation to Article 96.2 on personal social network profiles) provides a clear example of the shortcomings of legislative practice: it fails to correctly identify the persons it refers to (given there is no clear mention of the exact type of relationship, what degree of kinship affords access? Can closer relatives exclude more distant family members, or are all of them included? Who are the persons "*linked on a de facto basis*" to the deceased?) and to establish the prevalence among them (it appears that all parties are able to share the content unless the deceased states otherwise), as well as failing to provide answers to the issues which may be raised by the opposing wishes of those involved (which could easily be solved by choosing a specific category of persons, e.g. the heirs).

---

[72] CÁMARA LAPUENTE, S., *"La sucesión "mortis causa" en el patrimonio digital: una aproximación"* [An approach to "mortis causa" succession in digital heritage], in *El Notario del Siglo XXI* [21st Century Notaries], nº 84, March-April 2019. This paper contains a summary of the lecture given by him on this subject, masterfully and intelligently, before the Notary Association of Madrid on 24 January 2019.

In my opinion, if detaching the access to and protection of personal data from an inheritance can be justified, what cannot be vindicated is allowing persons other than the heirs to access the deceased's non-personal digital content after their passing. At this stage, it is important to point out that there is only one inheritance, as opposed to one for physical assets and another for digital content and contractual rights, hence the notice to heirs should follow the same path.

Article 96.1 of the LOPDG represents a form of *ex lege* notice to heirs parallel to the notice to heirs regulated under the Civil Code, restricted to the terms of access to digital content. Said parallel notice is found completely wanting given that non-personal data, as with the remaining assets and rights of the deceased which do not expire upon their death, forms part of the inheritance and must therefore correspond to the heirs or person designated by the deceased. Regarding the notice content, besides the terms set out for personal data under Article 3.2 of the LOPDG, the faculties comprising access to non-personal data (for instance, copying, updating, modifying and erasing) are unknown. Given the erroneous make up of this precept, I believe it should be interpreted in the strictest sense and the content stripped down to the terms prescribed by law, i.e. mere access. All other faculties would correspond to the heirs, in the absence of the person designated by the data subject for such purpose.

As is widely known, Catalan Act 10/2017 of 27 June on digital testament (*Llei de Catalunya 10/2017, del 27 de juny, de les voluntats digitals*) was declared partially unconstitutional by Constitutional Court judgment 7/2019.

Aquilian protection

In my opinion, the aquilian protection of data is evident, akin to that of any other legal asset which can be damaged. Protecting data by way of non-contractual civil liability is perfectly aligned to the wording and purpose of Article 1902 of the Spanish Civil Code.

Applicable international private law

As explained above, the location of data is usually irrelevant in economic terms and can be changed easily and at the drop of a hat. Data can be in several locations at once (on different servers across multiple continents), occasionally scattered in a virtual "cloud" which uses a group of servers found in numerous territories (which cannot be accessed separately). Therefore, the first question requiring an answer is which law would apply in determining the legal regulation of data?

The primary step would be to determine the applicable conflict of laws rule, which according to Article 12 of the Civil Code "*shall always be made in accordance with Spanish law*". Pursuant to Spanish law, the content of data (which brings with it the regulation of data itself) could be a fundamental right, asset subject to intellectual or industrial property, a right of ownership or none of the above.

The complexity of the task in finding a connecting factor for data – whether personal or non-personal – is demonstrated in the following text by Carrascosa:[73] "*if personal data gathered on the Internet in relation to a Belgian national residing in Spain is processed and hosted in France by a subsidiary of a US company established in Germany, we must determine*" the law applicable to each aspect of that situation.

Standard international private law does not provide a suitable solution to the specific issues surrounding data as regards that which lacks a correctly identified connecting factor. For that reason, new conflict rules have been created, especially for the subject of personal data.

Criminal and administrative laws (excluding the GDPR)

Article 8.1 under the Preliminary Title of the Spanish Civil Code states that "*criminal, police and public security statutes shall be binding on all persons within Spanish territory*". This precept has been subject to corrective interpretation by case law[74] in terms of the mandatory regulations applying to actions carried out in Spain, irrespective of whether the perpetrators are found in the country or not.

Regarding data, there are two cases in which Spanish criminal, police and public safety laws may apply: (i) data hosted on servers located in Spain, and (ii) activity performed in Spain.

---

[73] CARRASCOSA, J., in Calvo/Carrascosa, "*Obligaciones extracontractuales*" [Non-contractual obligations], in *Derecho internacional privado* [International private law], volume II, 2018, 18th ed., Granada, pp. 1250-1255.

[74] CALVO CARAVACA, A. and CARRASCOSA, J., *Derecho Internacional Privado* [International private law], vol. II, p. 358.

In terms of the former, an exception must be added to the corrective interpretation of Article 8 of the Spanish Civil Code usually accepted under case law: data found on servers located in Spain (and the activity of third parties relating to them, such as cyberattacks) will be subject to Spanish criminal, police and public safety laws even where the activity in question is performed elsewhere and the service provider is also located outside of Spain. Neither IT servers nor the data hosted on them are protected by extraterritoriality. Article 11.2 of the LSSI[75] affords the possibility to block access in Spain to certain data located abroad through collaboration with Internet service providers. *A fortiori*, domestic law would apply to data that is not only accessible from Spain, but is even located in the country. When it comes to content which violates public order, such as child pornography or illegal arms smuggling, we have to be able to block the data hosted on Spanish servers through the application of Spanish law, regardless of where the service provider or data recipient is located. Note that on occasions the data will be hosted in a virtual "cloud" across servers in numerous countries, which could make it difficult or even impossible to file action against the Spain-based server if unable to access the others. However, this would represent a technical challenge as opposed to a legal hurdle.

The above is without prejudice to the fact that the liability exemptions established for intermediary service providers – network operators, access suppliers and service providers which make temporary copies of the data, data hosting or storage providers and service providers which give out links to content or search engines (Articles 14 et seq of the LSSI) – under Spanish law will often apply in this regard. In these cases, Spanish law will apply, even if said law - following in the footsteps of an EU Directive – exempts from liability those who host or handle the data from Spain, as long as certain requirements are met (where not met, the opposite will occur).

From an alternative angle, data hosted on Spanish servers could gain relevance under Article 8.1 of the Civil Code due to being open to damage from malware or physical destruction.

Regarding the second issue (defining when the activity is deemed to have been executed in Spain), Article 8 of the Civil Code must be interpreted hand in hand with the LSSI. Data-related activity can often be difficult to pin down, whether in Spain or any other country. The wording of the LSSI affirms its applicability (unconditionally in conjunction with criminal and mandatory laws) to information society service providers incorporated in Spain or operating out of a permanent establishment in the country (Article 2), as well as in certain matters (although not all)[76] to information society service providers incorporated in other EU Member States when the recipient of the service is located in Spain (Article 3). As for such EU-based providers, the LSSI also applies in all cases when the services are specifically targeted to Spanish territory (Article 4.1), in which case the language used and location of the services provided in the real world, etc. must be taken into account.[77]

Note that on the subject of Article 3 of the LSSI, which represents an international private law rule, Spanish law would apply when the provider was incorporated in another EU or EEA Member State. It is striking that there is no similar regulation for cases of service providers established in countries outside of the EU and EEA. While the EU Directive does not cover this instance, perhaps Spanish law should.

---

[75] Act 34/2002 of 11 July on Information Society Services.

[76] a) Industrial and intellectual property rights. b) Advertising by collective investment undertakings. c) Direct insurance activity performed under a right of establishment or the freedom to provide services. d) Obligations assumed under contracts entered into by natural persons recognised as consumers. e) The contracting parties' choice of the jurisdiction applicable to the agreement. f) The lawfulness of unsolicited marketing communications via email or other means of electronic communication.

[77] By way of example, please see in this regard a similar case under Recital 23 of the GDPR: "In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union".

In addition to the foregoing, the scope of application of Article 8.1 of the Spanish Civil Code is broader than that of the LSSI. In fact, Article 1.2 of the latter outlines its subsidiary standing in relation to the regulations in force on certain matters:

"The provisions contained in this Act shall be understood without prejudice to the terms of other State or regional regulations external to the coordinated regulatory field or which aim to protect public health and safety, including the safeguarding of national defence, consumer interests, the taxation scheme applicable to information society services, personal data protection and unfair competition".

The purpose of the LSSI – which transposes an EU Directive into Spanish law – is to promote the freedom to provide services within the single market. Its precepts mainly reflect economic administrative law, in particular the requirement or not for qualification to perform activity and the general conditions for such activity within the coordinated regulatory field. From there, the LSSI takes a back seat in matters outside of said scope.

It is possible that in certain cases the Spanish LSSI was not applicable, but the country's criminal and mandatory laws should apply based on their connecting factor to Article 8.1 of the Civil Code, for example when other protected legal assets located in Spain (including damage to the victim's estate in scams such as the "Nigerian letter fraud") are harmed as a result of a crime or administrative infringement committed via information society services by a non-EU resident not specifically targeting Spain.

Focus on personal data protection legislation

With regard to personal data, the generally applicable regulation is the law of the State in which the data controller or processor is established,[78] unless such State does not belong to the European Union.

The above owes to the fact that in administrative matters, the applicable material law and international administrative competency go hand in hand, and that the GDPR (Article 56) allocates competency to the supervisory authority of the main establishment or of the single establishment of the controller or processor. This regulation topples the former case law of the Court of Justice of the European Union.[79]

Moreover, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State (Article 56.2 of the GDPR).

Note that other exceptions are provided under the GDPR, such as data processed by the courts or public authorities.

The key issue lies within cases whereby the data controller or data processor is not an EU incorporated enterprise. In theory, the GDPR is also applied extraterritorially – as stated in Article 3.2 – to processing by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;[80] or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[81]

---

[78] ALFONSO LUIS CALVO CARAVACA and JAVIER CARRASCOSA GONZÁLEZ, *Conflictos de leyes y conflictos de jurisdicción en Internet* [Conflict of laws rules and jurisdiction on the Internet], Editorial Colex, Madrid, 2001.

[79] Judgment of the Court of Justice of the European Union (Third Chamber) of 1 October 2015, case C-230/14 ("Weltimmo s.r.o."), request for a preliminary ruling under Article 267 TFEU from the Kúria (Hungary), made by decision of 22 April 2014, received at the Court on 12 May 2014.

[80] With regard to this matter, please see Court of Justice of the European Union (Grand Chamber) judgment of 7 December 2010, joined cases C-585/08 and C-144/09, "Pammer". Please also see Recital 23 of the GDPR, copied above.

[81] Please see Recital 24 of the GDPR: "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

In such cases, if any of these circumstances are observed in Spain, Spanish law will apply on the understanding that the data-related activity was performed in the country.

In practice, such extraterritorial application appears complicated due to a lack of international coordination and may lead to the simultaneous application of laws from several different States.

Other difficult problems arise when there are data co-controllers, or when the main establishment of the data controller is located in a different State than the main establishment of the data processor. In all those cases, the Law in which each undertaking (either data controller or processor) has its main establishment should be applied to the activity of such undertaking.

Despite being a fundamental right, it does not seem reasonable to apply the personal jurisdiction of Article 9.1; being mandatory territorial administrative regulations, Article 8 of the Spanish Civil Code should apply. Activity performed outside of Spain and not reflecting the case described under Article 3.2 of the GDPR is not subject to Spanish law.

There is usually no issue regarding the applicable Law to the civil liability associated to administrative infringements as the regulation is the same across the board in Europe (Article 82 of the GDPR).

Private law applicable to industrial and intellectual property

Data comprising content recognised as industrial or intellectual property has its own connecting factor leading to the country for which protection is claimed (Article 8 of the Rome II Regulation,[82] hereinafter "Rome II", and Article 10.4 of the Spanish Civil Code).

[82] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).

Private law applicable to trade secrets and unprotected data

Determining the rule of international private law applicable to non-personal data represents a greater challenge.

Data which qualify as trade secrets in accordance with the Spanish Trade Secrets Act[83] will be considered subject to ownership. Nevertheless, *lex rei sitae* (Article 10.1 of the Spanish Civil Code) will not apply, as in my view it cannot be invoked in relation to incorporeal assets linked to activities as opposed to things. As already affirmed, personal and non-personal data are not things. Their location is casual, unknown to their holder (when found in the cloud), changeable and widespread (with the ability to be simultaneously hosted on several servers). *Lex rei sitae*, which will often lead to the California legal system (data hosted in the cloud on a server located in that State), is therefore not fit for purpose in this regard. We believe that it would be more pertinent to apply the conflict of laws rule for unprotected data to trade secrets.

In turn, it is also difficult to determine the conflict of laws rule applicable to unprotected data. Clearly, when contractual or pre-contractual relationships are concerned (for instance, contractual credit rights held over a digital service provider), the corresponding conflict of laws rules (Regulation 593/2008 – Rome I – and Article 12 of Rome II) will have to be applied. The law applicable to contractual obligations will be the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence, such party being the digital service provider, even when the services are exchanged for the user's personal data. However, where consumers are involved, the specific regulation on the subject must be applied (laws of the consumer or user's habitual residence), prompted by Rome I (Article 6, with certain restrictions) and the LSSI (Articles 3.1.d) and 29).

Rome II will apply when unprotected data infringements give rise to unfair competition or morph into claims for non-contractual damages. Such a case would require an examination of the circumstances at play, although often enough the connecting factor for unfair competition could be applied, which (with certain exceptions) refer to the laws "*of the country where competitive relations or the collective interests of consumers are, or are likely to be, affected*" (Article 6 of Rome II). Where unfair competition is not recognised, the law applicable to damages invoking non-contractual liability would be the law of the country in which the damage occurs (Article 4.1 of Rome II), except for cases of a closer connection with another legal system (Article 4.3 of Rome II).

Regarding unprotected data or know-how whose location is considered irrelevant or complicated, it would not be unusual for such closer connection not to exist in the place where the data is hosted. Given that data is widespread, in reality its location for this purpose should be insignificant. In the case of unprotected data or know-how, perhaps it is common for the State with which the circumstance has closer connection to be the one where the information society services provider in question is established, whereas for consumers it is their habitual residence. In my opinion, this connecting factor would be more arguable.

The Court of Justice of the European Union declared in its judgment delivered on 25 October 2011 (eDate case)[84] that Directive 2000/31/EU on certain legal aspects of information society services (from which the LSSI is transposed) does not contain a specific conflict of laws rule. Nevertheless, in relation to the coordinated field (basically, rules affecting the provision of information society services), it does require the conflict of laws rule of Member States – including civil law regulations – not to impose stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established. This criterion would not force an amendment to the foregoing conclusion unless Spanish law applies and is more restrictive towards the information society services provider than the laws of the State in which the provider is established.

---

[83] a) it is a secret, meaning that in its entirety or the exact arrangement and form of its components is not generally known by persons operating in the areas where such information or knowledge is normally used, nor do they have straightforward access to it; b) it has actual or potential business value due to being a secret, and c) those in possession of it have implemented reasonable measures to ensure it remains a secret.

[84] Judgment of the Court of Justice (Grand Chamber) of 25 October 2011, Joined Cases C-509/09 and C-161/1, *eDate Advertising GmbH vs. X and Olivier Martinez, Robert Martinez and MGN Limited, Reports of cases*, 2011, p. I-10269. [ECLI:EU:C:2011:685]

Brief mention of the competent courts

In matters of international legal competency, the provisions of Regulation (EU) 1215/2012 of 12 December 2012 would have to be applied, with minor tweaks under Article 79.2 and Recital 147 of the GDPR as far as personal data protection is concerned.

The general provisions of Regulation (EU) 1215/2012 applicable to non-personal data could raise particular issues in relation to certain connecting factors:

— "*In the courts for the place of performance of the obligation in question*" (contractual, Article 7.1.a)). The general provisions on the location of services rendered in electronic format must be taken into account for electronic-based services.

— The place "*where the harmful event occurred or may occur*" (delict or quasi-delict, Article 7.2). If ex delicto damage or non-contractual liability occurs in Spain, the Spanish courts would have jurisdiction and the applicable law would be that of the aforementioned country. As stated by Calvo Caravaca and Carrascosa, this connecting factor could lead to farcical scenarios in which a large number of jurisdictions are all recognised as competent at the same time.[85] Regarding data, the location of which is casual and irrelevant, the place where the damage occurs may not be so obvious. Although the applicable regulation is different for timing reasons, it is pertinent in this case to use the criteria set out in the Court of Justice of the European Union judgment of 25 October 2011 (the aforementioned eDate case), which believes that the place where the harmful event occurred could cover both the place where the damage occurred (where the alleged victim has their centre of interests) and the place of the event giving rise to it (the place in which the information society service provider causing the damage is established).

Under Article 79.2 of the GDPR, applicable to personal data, action may be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers, in which case action would have to be brought before the courts of that Member State.

In both cases, enforcement shall occur pursuant to the laws of the executing State (Articles 60, 61 and 66 of the GDPR and Article 24.5 of Regulation (EU) 1215/2012).

[85] ALFONSO LUIS CALVO CARAVACA and JAVIER CARRASCOSA GONZÁLEZ, *Conflictos de leyes y conflictos de jurisdicción en Internet* [Conflict of laws rules and jurisdiction on the Internet], Editorial Colex, Madrid, 2001.

Conclusions

The data constituting the cornerstone of the digital economy is information represented symbolically in computable form. This concept is somewhat stricter than the one assigned to data protection (which includes information not processed digitally).

We must not confuse the information represented in data, the data medium, the data itself and the reality to which the data refers. Each of these elements could reflect different legal landscapes and levels of protection which on occasions are imposed on the others or at least interact with them. Where existing, protection of the content of data usually affects and extends to the data itself. However, data as such is also subject to its own protection different to that of its content.

Given its intangible nature, omnipresence and the irrelevance of its location, data is not considered a thing in a legal sense, nor is it subject to the regulations applied to things (*lex rei sitae*). Nevertheless, the devices on which data is stored (servers) are considered as things.

Both the content of data (the information represented within it) and the data itself constitute legal assets subject to protection (including aquilian protection), and could also be subject to fundamental rights, intellectual or industrial property rights or trade secrets open to ownership.

Personal data is not subject to a right of ownership held by the data subject in possession of a fundamental right or the data controller. The concept of ownership is not necessary or appropriate for the protection of data. The data controller's legal position includes faculties and also duties to carry out certain actions and may only be understood in light of the external fundamental right to which it refers.

Neither non-personal and unprotected data (i.e. not protected by intellectual or industrial property, or trade secret) nor its content (the information represented within it) are subject to ownership, although as legal assets they are open to entitlement and protection. Moreover, they do not enjoy a right of pursuit. However, the devices on which the data is found are subject to ownership, affording their owner certain faculties imposed on the data in the absence of other applicable protection-based regulations.

Unprotected data is a legal asset subject to entitlement, although strictly speaking cannot be possessed (although can be simply de facto held). This type of data is able to flow freely in the European Union, may or may not be subject to a right to portability and can be transferred by way of inter vivos or other legal transactions, as well as through succession, under the described terms.

Existing international private law provisions are suitable for personal data but are found wanting when it comes to non-personal data. Thus, the connecting factors of non-contractual liability, unfair competition or the closest links to a legal system (which usually relate to where the information society services provider is established or where the consumer holding the non-personal data has her habitual residence) should be applied on a case-by-case basis. The location in which the data is found is usually unknown and irrelevant for the purposes of international private law, except in the use of criminal and mandatory laws or the enforcement of judicial and administrative resolutions in the place housing the device (server or other equipment).

The regulations on international legal competency for data-related matters are relatively well versed in terms of personal data, although are severely lacking in the field of non-personal data, which requires resolution through EU case law.

Bibliography

ALBALADEJO, M., *Derecho Civil I* [Civil Law I], Ed. Edisofer, 2013, pp. 355 and 357.

VAN ASBROECK, B., DEBUSSCHE, J. and CÉSAR, J. (Bird Bird), Building the European Data Economy – Data Ownership White Paper, 1 January 2017.

BERCOVITZ RODRÍGUEZ-CANO, R., *Comentarios a la Ley de Propiedad Intelectual* [Commentary on the Spanish Intellectual Property Act], 4th Ed., Madrid, 2017, pp. 111 et seq.

BOTTA, M. and WIEDEMANN, K., EU Competition Law Enforcement vis-à-vis Exploitative Conducts in the Data Economy – Exploring the Terra Incognita, Max Planck Institute for Innovation and Competition Research Paper, nº 18-08.

CALABRESI, G. and MELAMED, A.D., "Property Rules, Liability Rules and Inalienability: One View of the Cathedral", Harvard Law Review, Vol.85, p. 1089, April 1972 , también en Yale Law School Faculty Scholarship Series. 1983. https://digitalcommons.law.yale.edu/fss_papers/1983.

CALVO CARAVACA, A. and CARRASCOSA, J., *Derecho Internacional Privado* [International private law], vol. II, 2018, 18th Ed., Granada, pp. 358 and 1250-1255.

CALVO CARAVACA, A. and CARRASCOSA GONZÁLEZ, J., *Conflictos de leyes y conflictos de jurisdicción en Internet* [Conflict of laws rules and jurisdiction on the Internet], Editorial Colex, Madrid, 2001.

CÁMARA LAPUENTE, S., "*La sucesión "mortis causa" en el patrimonio digital: una aproximación*" [An approach to "mortis causa" succession in digital heritage], in El Notario del Siglo XXI [21st Century Notaries], nº 84, March-April 2019.

CLAVERÍA GONSALBEZ, L., "*Artículo 333", Comentario del Código Civil Comentario del Código Civil ["Article 333*", Commentary on the Spanish Civil Code], Ministerio de Justicia [Ministry of Justice], 1993, vol. 1, p. 922.

COCA PAYERAS, M., "*Artículo 437", Comentario del Código Civil* ["Article 437", Commentary on the Spanish Civil Code], *Ministerio de Justicia* [Ministry of Justice], 1993, vol. 1, p. 1180.

Communication from the Commission to the European Parliament and the Council of 29 May 2019, "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union".

DE BUSTOS GÓMEZ RICO, M., *Comentario del Código Civil* [Commentary on the Spanish Civil Code], Bosch, 2000, art. 437, p. 395.

DE CASTRO, F., *Bienes de la personalidad* [Individual assets], in *Estudios jurídicos del Profesor Federico de Castro* [Legal Studies of Professor Federico de Castro], vol. II, *Colegio de Registradores de la Propiedad y Mercantiles de España* [Spanish Association of Property and Companies Registrars], 1997, pp. 873 et seq.

DE CASTRO, F., *Bienes de la personalidad* [Individual assets], *Temas de Derecho Civil* [Matters of Civil Law], Madrid, 1976, pp. 7 et seq.

DETERMANN, LOTHAR, "No one owns data" (February 14, 2018). UC Hastings Research Paper No. 265.

DÍEZ-PICAZO, L., *Fundamentos del Derecho Civil Patrimonial* [Foundations of Civil Patrimonial Law], III and IV, Ed. Aranzadi, Cizur Menor, 2012.

DÍEZ-PICAZO, L. and GULLÓN, A., *Sistema de Derecho Civil* [The Civil Law System], vol. III-I, 9th Ed., Madrid 2016.

DIKER VANBERG, A. y ÚNVER, MB, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology*, vol, 8, No. 1, 2017.

ENGELS, B., "Data portability among online platforms", *Internet Policy Review*, Vol. 2 Issue 2 (2016).

FUCHS MATEO, L., *La propiedad intelectual como propiedad especial a lo largo de la Historia, tesis doctoral* [Intellectual property under special ownership throughout history, doctoral thesis], Universidad Complutense de Madrid, 2017.

GOMÁ SALCEDO, *Instituciones de Derecho Común Civil y Foral* [Civil Common and Regional Law Institutes], vol I, p. 804.

GONDRA, J.M., "*La estructura jurídica de la empresa (El fenómeno de la empresa desde la perspectiva de la teoría general del Derecho)*" [The legal structure of companies (enterprise phenomenon from a general theory of law perspective)], in *Revista de Derecho Mercantil* [Corporate Law Magazine], nº 228, 1998, pp. 493 et seq.

LACRUZ BERDEJO, J.L. et al (rev. DELGADO ECHEVERRÍA), *Elementos de Derecho Civil* [Elements of Civil Law], I-3, 2005, pp. 5 to 7 and 13 to 17.

MARÍN CASTÁN, F., *Comentario del Código Civil* [Commentary on the Spanish Civil Code], Bosch, 2000, p. 7.

MARTÍN, B. "*La publicidad del dato personal no otorga per se legitimidad para su tratamiento*" ["Personal data in the public domain does not automatically grant authorisation to process it"], available at https://cms.law/es/ESP/Publication/La-publicidad-del-dato-personal-no-otorga-per-se-legitimacion-para-su-tratamiento.

MONTES PENADES, V., *Artículo 348, Comentario del Código Civil* [Article 348, Commentary on the Spanish Civil Code], *Ministerio de Justicia* [Ministry of Justice], 1993, vol. 1, p. 952

OSBORNE CLARKE LLP, Legal study on Ownership and Access to Data, report for the European Commission, 2016.

PIÑAR MAÑAS, JOSÉ LUIS (Director), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* [General Data Protection Regulation. Towards a new European Privacy Model]. Reus, Madrid, 2016.

PIÑAR MAÑAS and RECIO GAYO, *La protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea* [Data protection under Court of Justice of the European Union case law], La Ley Walters Kluwer, Madrid, 2018.

RADIN, M.J., "*Prorietá e ciberspazio*", *Rivista critica del diritto privato* ["Ownership and cyberspace", A critical review of private law], XV-1 (1997).

SANDEL, M., *What money can't buy*, Penguin, 2012.

SCHWARTZ, PAUL M., "Property, Privacy, and Personal Data", 117 Harvard Law Review, 2055 (2004).

SWIRE, P. and LAGOS, Y., "Why the right to data portability likely reduces consumer welfare: Antitrust and Privacy Critique", *72 Maryland Law Review*, 335 (2013).

About CMS

Technology, Media and Communications expertise at CMS

CMS 'market-leading Technology, Media and Communications (TMC) group is made up of over 300 sector specialist lawyers in over 40 countries.

The rapid evolution of new technologies has opened up a wealth of opportunities for companies resulting in the need to adapt, diversify into new business lines, and often to grow, while all the time complying with new regulatory requirements. CMS helps clients tackle these challenges head on and navigate, what can be, complex regulatory regimes, particularly around data.

With our long-standing focus on TMC, we have been exposed to virtually every risk and challenge technology players, and its end users, face and are best placed to deliver solutions through our award winning disputes, corporate, IP, commercial, data privacy and security, employment and tax practices.

TMT Legal Adviser of the Year
TMT Finance M&A Awards 2019

Southeast Asia TMT Law Firm of the Year
Asia Legal Business 2018

Middle East TMT Firm of the Year
Asian-MENA Counsel Awards 2018

Deal of the Year
The Deal, 2019 for advice to Comcast on its bid for Sky plc

The Americas

Bogotá
Lima
Mexico City
Rio de Janeiro
Santiago de Chile

Europe

Aberdeen
Amsterdam
Antwerp
Barcelona
Belgrade
Berlin
Bratislava
Bristol
Brussels
Bucharest
Budapest
Cologne
Duesseldorf
Edinburgh
Frankfurt
Funchal
Geneva
Glasgow
Hamburg
Istanbul
Kyiv
Leipzig
Lisbon
Ljubljana
London
Luxembourg
Lyon
Madrid
Manchester
Milan
Monaco
Moscow
Munich
Paris
Podgorica
Poznan
Prague
Reading
Rome
Sarajevo
Seville
Sheffield
Skopje
Sofia
Strasbourg
Stuttgart
Tirana
Utrecht
Vienna
Warsaw
Zagreb
Zurich

Algiers
Casablanca
Johannesburg
Luanda
Mombasa
Nairobi

Africa

Dubai
Muscat
Riyadh

Middle East

Beijing
Hong Kong
Shanghai
Singapore

Asia-Pacific