The Data Act: Implications for trade secrets and intellectual property

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data is analysed.

ÁNGEL GARCÍA VIDAL
Professor of Corporate & Commercial Law, University of Santiago de Compostela
Academic Counsel, Gómez-Acebo & Pombo

1. Data in the digital economy: protection from the free flow of data

1.1. The importance of data in today's economy is beyond doubt. One need only consider the rise of the big data phenomenon, which involves the accumulation of huge amounts of data and its subsequent management and analysis by algorithms to find therein repetitive patterns that can be used to make predictions of all kinds. Data collection for these purposes is not new. But the current capacity to generate and collect such data is. In fact, big data is often identified with the so-called "four Vs" - data that is characterised by its volume, its variety, the velocity at which it is generated, stored and analysed, and its veracity.

This exponential generation of information and data derives from different sources: Internet search engines, social networks, websites that use cookies, etc. But among these sources of data generation, the so-called internet of things, a set of goods or objects of everyday use that incorporate technology that allows them to collect data and communicate with other objects, stands out in particular. In

other words, if the traditional internet consists of millions of computers or servers connected to each other, it is now the case that the connection and communication does not take place between servers, but between any object (smartphones, watches, cars, glasses, fridges, toasters, etc.).

1.2. The economic importance of data (which have been described as the petroleum of the 21st century) explains the interest in their protection, which has given rise to two opposing currents. On the one hand, the possibility of legally controlling access thereto and use thereof (by means of trade secrecy, *sui generis* database law, unfair competition or contractual protection, sometimes even proposing the creation of a new exclusive right in big data) is advocated. On the other hand, and in contrast to the exclusive protection and control of data, emphasis has also been placed on the need to guarantee free flow as a way of promoting the so-called data economy.

1.3. The European Union has just adopted the so-called 'Data Act', a key piece of legislation for today's digital economy. This is Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data.

This new regulation is based on the premise that a certain person, referred to as the "data holder", has control over the data, acquired on a contractual basis. And, on that premise, the Data Act imposes on these data holders the obligation to allow access to the data to certain persons, mainly users of connected products and related services. More specifically, the Data Act regulates and facilitates the exchange of business-to-consumer (B2C) and business-to-business (B2B) data; lays down the obligation to make data available to public sector bodies, the Commission, the European Central Bank and EU bodies for special needs; regulates the switching between data processing services; and sets out the essential requirements for data interoperability and data exchange mechanisms and services.

In this way, the European Union highlights the free access to and flow of data and expressly abandons the possibility of creating an *ex novo* property right in big data (a possibility that was mentioned in the European Commission's own 2017 Communication "Building a European Data Economy"). This is highlighted in Recital 5 (according to which "this Regulation should not be interpreted as recognising or conferring any new right on data holders to use data generated by the use of a connected product or related service") or in Recital 25 (when it is stated that "this Regulation should not be understood to confer any new right on data holders to use product data or related service data" and it is stressed that the legal basis under which a data holder uses and controls the data is the contract it has entered into with the user of the products).

In facilitating the flow of data, the Data Act follows a course already initiated by the European Union in previous legislative texts, such as Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, Directive (EU) 2019/1024 on open data and the re-use of public

sector information, or other sectoral legislation requiring data holders to allow third parties to access their data, either free of charge or on fair, reasonable and non-discriminatory terms: e.g. smart transport (Directive 2010/40/EU); electricity grid [Regulation (EU) 2015/703 and Regulation (EU) 2017/1485]; payment services [Directive (EU) 2015/2366] or automobiles [Regulation (EC) No. 715/2007].

2. Access to data generated by connected products and related services

2.1. The new Regulation (EU) 2023/2854 addresses the data generated by connected products and related services, establishing as a basic principle that users of such products or services should be able to access the data generated by the use of such products or services and to use or share them with third parties of their choice.

In this regard, any type of data falls within the scope of the Data Act, meaning "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording", whether or not they are personal data, in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

In turn, a connected product is defined as "an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user". And a "related service" is defined as "a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product".

Based on these definitions, the Data Act starts from the premise that the generation of data is the result of the interaction of at least two parties: the designer or manufacturer of the connected product, which in many cases is also the provider of related services, and the user of the product or service (whether this user is a natural or legal person, including the general government). Against this background, the Data Act requires connected products to be designed and manufactured, and related services to be designed and provided, in such a way that the data they generate (including the relevant metadata necessary to interpret and use such data) are, by default, easily and securely accessible to a user, free of charge, in a comprehensive, structured, commonly used and machine-readable format. In addition, where technically feasible, such data should be directly accessible to the user.

Data holders are also obliged to facilitate access to the data by users or third parties to whom the user has requested a data

holder to provide access to the data. Both in the case where access is provided to the user and in the case where it is provided to a third party, the data holder shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

In any case, the persons to whom the data are communicated, whether users or third parties, shall not use them to develop a connected product that competes with the connected product from which the data originate, nor share the data with a third party with that intent. Nor may they use the data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable, the data holder.

2.2. Furthermore, although the obligation to share data is imposed, the Data Act is based on the principle of contractual freedom and therefore recognises that the parties are free to negotiate the precise conditions under which data are communicated. However, it does list (see Article 13) a number of contractual terms unilaterally imposed by one enterprise on another that are considered to be unfair and others that are presumed to be unfair.

2.3. The obligation for data holders to make data available to users or third parties may in certain circumstances conflict with European Union regulation of other matters. This will be the case when the data are of a personal nature, are protected by trade secrets or by intellectual property rights. This explains why the Data Act pays attention to these possible collisions.

3. Third-party access to and availability of personal data

As regards personal data, the Data Act expressly recognises [Art. 5(1)] the primacy of the previous General Data Protection Regulation [Regulation (EU) 2016/679].

This being the case, where the user of connected products or related services also has the status of data subject under Regulation 2016/679, there is no conflict between the two regulations. Indeed, in these cases the right of access to data and the right to demand that it be made available to third parties complements the data subjects' right of access to their personal data and the rights to data portability under Articles 15 and 20 of Regulation (EU) 2016/679.

However, problems may arise when the user is not the data subject whose personal data are requested. In such a case, the Data Act expressly provides [Arts. 4(12) and 5(7)] that the data holder shall make personal data generated by the use of a connected product or related service available to the user or to a third party indicated by the user only where there is a valid legal basis for processing under Article 6 of Regulation (EU) 2016/67. Therefore, where "the user is not the data subject, this Regulation does not create a legal basis for providing access to personal data or for making personal data available to a third party and should not be understood as conferring any new right

on the data holder to use personal data generated by the use of a connected product or related service" (Recital 7 of the Data Act).

4. Data and trade secrets

Although the Data Act is, as mentioned above, part of the trend in favour of the flow of data, as a driver of the digital economy, and although it expressly states that it does not create a new exclusive right in data, this does not mean that the Data Act excludes data protection. The fact is that, even in such hypotheses, the Data Act imposes an obligation to provide access to data.

The Data Act imposes an obligation to provide access to data even if they are protected as business secrets

In this regard, one of the channels of data protection may be trade secrets, regulated in Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (and in the Business Secrets Act 1/2019 of 20 February).

As is well known, according to the aforementioned piece of legislation, information is protected as a trade secret if: *a*) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; *b*) it has commercial value because it is secret; and *c*) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. And all these requirements can be met by big data, as the best scholarly writings have demonstrated [See, for example, Gómez Segade, "La protección de los macrodatos (big data) mediante las normas sobre secretos empresariales", in García Vidal (Dir.), *Big data e internet de las cosas: nuevos retos para el derecho de la competencia y de los bienes inmateriales,* Valencia, 2020, p. 115 ff)].

Indeed, data can be kept secret, if reasonable measures are taken to do so. Certainly, it is possible that some of the numerous data generated by connected products or related services may be public or accessible by third parties, but secrecy is not to be predicated on specific data, but on the body thereof, as established in the act and directive on business/trade secrets, which refer to the secrecy of information "as a body or in the precise configuration and assembly of its components". And as regards the value of the data, although trivial information is not protectable as a trade secret, and although much of the data generated by connected products or related services is, what is no longer trivial and may have commercial value is the data as a body, even if in isolation it is trivial.

Where data are protected as trade secrets, the Data Act, while still requiring data holders to disclose them to users or third parties chosen by the user, allows data holders to require the user or third parties to preserve the confidentiality of data considered as trade secrets (see Arts. 4 and 5). In this regard, it provides that the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the user or third party proportionate technical and organisational measures necessary to preserve the confidentiality

of the shared data, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct. The measures necessary to preserve confidentiality that have been agreed with the third party must also be respected by subsequent third parties to whom the third party provides the data [Art. 6(2)(c)].

Where there is no agreement on the necessary measures or where a user, or third parties of the user's choice, fail to implement agreed measures or undermine the confidentiality of the trade secrets, the data holder should be able to withhold or suspend the sharing of data identified as trade secrets. In such cases, the data holder should provide the decision in writing to the user or to the third party without undue delay and notify the competent authority of the Member State in which the data holder is established that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined.

Furthermore, it is provided that the data holder may refuse to share the data on the basis that it is considered to be a trade secret if it is able to demonstrate to the user or to the third party that, despite the technical and organisational measures taken by the user or by the third party, serious economic damage is highly likely to result from the disclosure of that trade secret. According to the Data Act, that "demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority" in charge of ensuring compliance with the Data Act [Arts. 4(8) and 5(11)].

In order to ensure the protection of trade secret data made available to users of connected products or third parties, the Data Act allows (Art. 11) a data holder to apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to the data, including metadata. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder. However, such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties.

5. Data and intellectual property

The Data Act also has implications from the point of view of intellectual property.

5.1. The Data Act is based on the principle that it does not affect the regulation of intellectual property rights, as expressly stated in Recital 13. On this basis, other recitals make it clear that the Data Act does not apply to certain elements that may be protected by intellectual property rights. Thus, "data that such sensor-equipped connected products generate when the user records, transmits, displays or plays content, as well as the content itself, which is often covered by intellectual property rights, inter alia for use by an online service, should not be covered by this Regulation" (Recital 16).

Similarly, the Data Act does not affect algorithms used for the analysis of data and their interrelationships, algorithms embedded in software that may be protected by intellectual property. And information inferred or derived from data after analysis by algorithms does not fall within the scope of the Data Act either (Recital 15), so that the data holder is not obliged under the Data Act to disclose it to users or third parties.

5.2. On the other hand, and from the intellectual property point of view, the Data Act introduces an important provision concerning the protection conferred by the *sui generis* right in databases, a *sui generis* right by virtue of which databases are protected which, without being considered as a work protectable by intellectual property, have entailed a substantial investment, evaluated qualitatively or quantitatively, in terms of financial means, time, effort, energy or others of a similar nature for the acquisition, verification or presentation of their content (Arts. 7 of Directive 96/9/EC on the legal protection of databases and 133(1) of the Copyright Act).

In order to understand the scope of the new rules of the Data Act, it should be recalled that the Court of Justice has understood the concept of investment for the purpose of obtaining the contents of a database to mean resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent materials. Because the "purpose of the protection by the *sui generis* right provided for by the directive is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database" (Case C-444/02 *Fixtures Marketing*, judgment of 9 November 2004, paragraph 40). This is what is known as the doctrine of exclusion of spin-off or by-product databases.

On that basis, doubts had arisen about the protection under sui generis law of data collected from sensors and connected devices - as is especially the case with the internet of things - as it was disputed whether the investment made to place and operate them is an investment for the creation of the data or for its collection.

Now such a debate has been settled in the Data Act, with Article 43 stating that the "sui generis right provided for in Article 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by a connected product or related service falling within the scope of this Regulation". Such a provision is made on the understanding that it is not an exception to the regulation of the Database Directive, but a simple clarification. This is indicated in Recital 112 of the Data Act, where it is stated that "it should be clarified that the sui generis right does not apply to such databases".

Disclaimer: This paper is provided for general information purposes only and nothing expressed herein should be construed as legal advice or recommendation.