CIPPM Centre for Intellectual Property Policy & Management

Jean Monnet
Centre of Excellence 2018-2021
for European Intellectual Property
and Information Rights

CIPPM / Jean Monnet Woking Papers

No. 02-2019

Data portability and regulation of digital markets

Maurizio Borghi

September 2019

Bournemouth University

Co-funded by the
Erasmus+ Programme
of the European Union

The Centre for Intellectual Property Policy and Management of Bournemouth University is a Jean Monnet Centre of Excellence for European Intellectual Property and Information Rights (2018-2021), co-funded by the Erasmus+ Programme of the European Union.

This Working Paper Series is peer reviewed by an Editorial Board led by prof. Ruth Towse and prof. Roger Brownsword.

Data portability and regulation of digital markets*

Maurizio Borghi

Abstract

The new General Data Protection Regulation introduced the "right to portability of personal data". Conceived to give effectiveness to individual interests, the regulation is at the same time a pro-competitive tool with important regulatory effects on digital markets. As a result of the extensive interpretation of "personal data" that has been consolidated in European law, the right to portability actually applies to a wide range of data, thereby overlapping and conflicting with a range of diverse interests. If the application of the right raises questions about the balancing of those interests, its effectiveness as a regulatory instrument depends strongly on the structure of the markets. The paper argues that the pro-competitive effect of portability is more pronounced in markets with common data processing systems, while it is more uncertain in the absence of shared interoperable standards.

Keywords: GDPR, data protection, interoperability, lock-in, barriers to entry, Digital Single Market

* An Italian version of this paper ("Portabilità dei dati e regolazione dei mercati digitali") has been published in *Mercato, Concorrenza, Regole*, Vol. 2, 2018, 219.

Table of contents

Introduction

The right to portability is one of the most significant innovations introduced by the General Data Protection Regulation (GDPR).[1] The basic idea is simple: to allow each user of online services to "bring" their data from one service to another, so that they can reuse them independently without losing the wealth of information previously created. The example which is commonly given concerns the use of online platforms such as social networks, which collect a large amount of personal data and information from their users, as well as material such as photos, text and videos. The new right to portability allows users to obtain a copy of their data and store it on their computer, or transmit it to another platform so that they can be reused and exploited there.

The rule introduced by the European legislator is broad and applies to all entities that process personal data electronically, regardless of the type of service offered and the size of the company: from large e-commerce platforms and cloud storage services down to small start-up companies that develop a smartphone application, all operators that process personal data must allow their users the portability of their data. The main *raison d'être* of the norm is the strengthening of individual rights in a digital environment increasingly focused on the commercial exploitation of personal data. In this sense, the norm reinforces the principle that data belong to the individual even when in the possession of others, and that the individual must be able to make independent and autonomous decisions on the use others make of her of his own data. But, as it is configured, the norm has a considerable impact on the relationship between individuals and businesses, and between businesses themselves, in the digital environment. Indeed, the right to portability introduces for the first time a mechanism regulating access to data and the way data are transmitted, which has a significant impact on the processing, exchange and re-use of data in digital markets. It is, in short, not only an individual right, but also a real instrument of market regulation that responds to precise objectives of competition policy.

This paper aims to examine the new right to data portability from the point of view of its regulatory effects, in order to identify its potential and limitations as a competitive tool. The paper is divided into four parts. The first part reconstructs the genesis of the right to portability as a rule protecting both individual and collective rights, its legal basis and related policy objectives, as well as its legislative history. The second part addresses the functioning of the right as such, its purpose of application and limitations. Part four discusses the complex balance with other conflicting rights, such as intellectual property rights, trade secrets and rights arising from contract. Finally, the fifth party critically questions the pro-

[1] Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 20.

competitive effects of portability and its future in the framework of the legislative interventions supporting the European digital single market.

1. Data portability in the digital markets

Data portability is a broad concept that applies in various contexts in the Single Market, and generally refers to the absence of technical and legal impediments to the use of one's own data through different tools, or in relation to different services, or in different countries of the Union[2]. In telecommunications, even before the advent of the digital economy, national legislation imposed *mobile data portability* (MDP), i.e. the transfer of mobile phone numbers from one operator to another, and these rules were then harmonised by the Universal Service Directive of 2002.[3] In the banking sector, the PSD2 Payment Services Directive provides for a form of portability of customer account data to a banking institution in favour of payment services[4]. In the area of public administration, certain rules contained in the Public Sector Information Directive (the so-called PSI2 Directive) require the adoption of standards to facilitate portability between information systems.[5]

Article 20 of GDPR introduces for the first time a "horizontal" provision in relation to the transfer of data. There are several market regulation profiles in this new norm. First, the norm requires data to be provided to the data subject "in a structured, commonly used and machine-readable format". This effectively requires the adoption of interoperable standards in data storage. The data subject then has the right to transmit the data received to another data controller "without hindrance" by the original data controller. This facilitates the circulation of data and their re-use. Furthermore, the request for portability must be fulfilled free of charge and expeditiously, which reduces switching costs and entry barriers. Finally, as already mentioned, the regime applies horizontally to all entities processing personal data, regardless of sector and size, and, perhaps even more importantly, regardless of the existence of a dominant positions. In this sense, the right to portability operates preventively as a pro-competitive rule to access and circulation of data.

---

[2] In the latter sense, see Regulation 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market.

[3] Directive 2002/22/EC of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (as amended by Directive 2009/136/EC).

[4] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, Articles 66 and 67.

[5] Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

1.1. The legal and policy basis

The elements just highlighted are implicit in the reasons that led to the adoption of this instrument in the GDPR. As mentioned above, the main objective of the new law is to strengthen control over one's own personal data when such data is held by others, based on the principle - widely accepted in European doctrine - that the protection of personal data serves interests that go beyond the protection of privacy and extend to "informational self-determination".[6] The principle is still enshrined in Article 8 of the EU Charter of Fundamental Rights, which explicitly mentions "the right of access to data collected concerning him/her", extending its scope. Indeed, by providing individuals with the legal means to transfer personal data at will, the GDPR consolidates the exercise of individual freedoms in the digital environment.[7]

But together with the strengthening of individual rights, portability also explicitly pursues competitive objectives. Indeed, the Strategy for the Digital Single Market in Europe states that "an obstacle to the flow of data across borders and the development of new services [...] is the lack of open and interoperable systems and services and the portability of data between services".[8] How, then, does portability of personal data help to remove this obstacle?

The first and most immediate consequence of portability is that it facilitates the transition from one service to another or "switching". The right strengthens the ability to choose between competing services. It reduces switching costs and facilitates multi-housing, i.e. the simultaneous use of services using the same data. For example, a Facebook user can transfer their content to another platform without having to "delete" their profile from Facebook. More than a right to switching, portability is in fact a right to replicate data on multiple services, which can reuse the same data in different ways. Thus, to give another example, the user of an application that calculates the calories and composition of food consumed during meals can "take" the data collected and feed into another application that calculates the calories consumed during sport, which can then provide additional information by combining the two sets of data. The right to portability thus enables the *re-use of* data and removes an obstacle to the development of new services and applications.

---

[6] For an analysis of the principles underlying data protection in Europe see O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford: Oxford University Press, 2015. In particular, on information self-determination see also F. Ferretti, "The foundations of EU data protection law", *European Data Protection Law Review* 2/16, (2016).

[7] We do not address here the question of whether portability implies the creation of a right of "ownership" over personal data. The point is discussed in I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *Tilburg Law School Legal Studies Research Paper Series*, no. 22/2017, pp. 6-7. It can be agreed with the authors that portability, even in combination with the right of cancellation (Art. 17 GDPR), does not create an *erga omnes* exclusion right comparable to intellectual property rights.

[8] Communication from the Commission, Strategy for Europe's Digital Single Market, COM(201), 0192 final, § 4.1.

The indirect consequence is to stimulate competition between services. By reducing switching costs, portability makes it more difficult for digital market players to "lock" users into their service. In this sense, Art. 20 is a competitive remedy: it prevents the emergence of lock-in situations due to unjustified switching costs imposed on customers, and this in turn reduces barriers to entry to other companies.

These two main effects form the backbone of Article 20, and partly explain its legislative history.

1.2. The legislative history of Article 20

In the Commission's intentions, the right to data portability meets the general objective of "building trust in online environments", in particular by providing users with tools to exercise effective control over personal data held by online service providers.[9] The right appeared for the first time in the proposed Regulation published in January 2012, in the section that included the rights of rectification and deletion.[10] In this first formulation, the right was divided into three distinct elements: (1) a right of the data subject to obtain from the data controller a copy of the personal data "where [...] they are processed by electronic means and in a structured and commonly used format", so that the data subject can make "further use of them"; (2) a right to transmit such data "to another system […] without hindrance by the controller" if the data have been provided for processing based on consent or a contract; and finally (3) the possibility for the Commission to specify the electronic format and technical modalities of transmission of personal data to give full effect to the right in its two components ("obtaining" and "transmission"). In subsequent revisions, the rule was initially merged with the right to access one's own data to form a "right of access and to obtain data",[11] before reappearing as an autonomous institution in the final version.[12]

During the negotiations, the introduction of a right to portability has been the subject of much criticism and reservations from Member States, particularly with regard to the possible conflict with the intellectual property rights and trade secrets of data controllers. Some countries challenged the inclusion of portability in the Regulation on the ground that the matter was more related to competition and consumer rights than to the protection of personal data. However, the introduction of the new law appeared to be consistent with the stated aims of the Regulation to strengthen data subjects' control over their data and

---

[9] Commission Staff Working Paper, Impact Assessment, SEC(2012) 72 final.

[10] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final, Article 18.

[11] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)), Amendment 113. The term "portability" was removed from the text of the Regulation and the related right became a subset of the "Right of access by the data subject" (Article 15).

[12] Art. 20 GDPR.

ensure their free movement within the Single Market. In order to temper the possible negative effects on the interests of third parties, the final version introduced the clause that the exercise of portability "shall not adversely affect the rights and freedoms of others".[13] Finally, the determination of the standards to be used for data transmission was left to market self-regulation, and no longer decided centrally by the Commission.[14]

In order to prepare data controllers for the application of the new right to portability, the Article 29 Working Party (WP29)[15] published in April 2017 guidelines on the application of Article 20 of the Regulation.[16] The right thus became effective with the entry into force of the GDPR on 25 May 2018.

So what is the scope of this new institute? And how does it have a regulatory effect on the markets?

2. The application of the right to data portability

The exercise of the right to data portability is defined by three related elements: firstly, the type of data on which it is exercised; secondly, the way in which its implementation is regulated; and finally, the limits imposed on its exercise.

2.1 What data is subject to portability?

The right to portability is exercised on "personal data which [...] concern" a data subject, and which have been "provided" by the data subject "to a data controller".[17] The first condition excludes data which do not relate to a natural person, such as those relating to a commercial activity, a company or an organisation. The second excludes data that do not concern the person requesting to exercise the right to portability. This includes not only data concerning other persons, but also data made completely anonymous, i.e. no longer capable of identifying a natural person.[18]

---

[13] Art. 20(4) GDPR.

[14] In the language of Recital 68, Article 20 is limited to "encourage[ing]" data controllers "to develop interoperable formats that enable data portability".

[15] The Article 29 Working Party is an advisory group established by Article 29 of Directive 95/46, composed of representatives of the data protection authorities of each Member State. With the entry into force of the GDPR on 25 May 2018 it was replaced by the European Data Protection Board.

[16] Article 29 Working Party, Guidelines on the right to 'data portability', adopted on 13 December 2016, as amended and adopted on 5 April 2017, 16/EN, WP 242 rev.01

[17] Art. 20(1) GDPR.

[18] Anonymous data are excluded from the application of the GDPR (as well as the previous Directive 95/46). The definition of "completely anonymous" data, i.e. unsuitable to identify a person, is extremely problematic especially in the big data environment (P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation", *UCLA Law Review,* 57 (2019)). See also Working Group Art.29, Opinion 05/2014 on anonymisation techniques, adopted on 10 April 2014.

The second condition is more specific: it requires personal data to have been *provided* by the data subject, and is in turn subject to further qualification, including only those data provided by the data subject which are processed by automated means, *either* on the basis of the data subject's consent *or* in the performance of a contract signed by the data subject.[19]

The object of the right to portability is therefore defined by a series of cumulative conditions: first of all the *nature* of the data on which the right is exercised ("personal" and "concerning" the person exercising the right), together with its *origin* (it must be "provided by" that person); then the *legal basis of the* processing ("consent or contract") and finally the *way* the data is *processed* ("automated"). These conditions define the scope of the right to portability and must be examined in some detail here.[20]

a) Personal data provided by the data subject

The definition of personal data contained in the GDPR takes over that given in Directive 95/46 and includes any information relating to a natural person who is identified or identifiable, directly or indirectly, having regard to the means by which such identification can reasonably be achieved.[21] As mentioned, completely anonymous data are excluded from the application of the Regulation and therefore also from the purpose of the right to portability. But the growing availability of *data analytics* tools that allow the identification of individuals also from anonymous or non-personal[22] data has led to an increasingly expansive interpretation of the concept of "personal data", also supported by the case law of the European Court of Human Rights and the Court of Justice of the EU[23]. Biometric data, real estate values, dynamic IP addresses, meteorological information, vehicle speed, are just a few examples of data that may fall under the definition of "personal data". As stated by the Court of Justice in the *Nowak* case, the use of the expression "any information" in Art. 2(a) of the Data Protection Directive reflects the legislator's aim to give an extended meaning to the notion of personal data, such as to encompass potentially "all kinds of information […] provided that it 'relates' to the data subject".[24] In the case under consideration by the Court, the candidate for a professional examination sought access to the examiner's corrections and comments on his or her own work on the grounds that those corrections and comments

[19] Art. 20(1)(a) and 20(1)(b) GDPR.

[20] We omit the fourth condition (processing by automated means), which is met by definition in the digital markets covered by this article.

[21] Art. 2(a), Directive 95/46, and Art. 4(1) and Rec. 26, GDPR.

[22] P. Ohm, "Broken Promises," *cit.* , p. 170.

[23] For a thorough overview see Nadezhda Purtova "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, 10:1 (2018), 40-81.

[24] Case C-434/16, *Peter Nowak v. Data Protection Commissioner* (2017), § 34.

constitute "personal data" over which the applicant could exercise his or her right of access.[25] In upholding this interpretation, the Court affirmed the principle that information is to be regarded as personal data where it relates to a particular person "by reason of its content, purpose or effect".[26]

If, therefore, information can relate to a particular person even by virtue of its *effect* (i.e. regardless of its actual content), it is clear that a large part of the information generated by the use of online services and digital platforms falls within the scope application of the GDPR and, consequently, the right to portability. In particular, and by analogy with the *Nowak* case, the user of commercial intermediation platforms such as eBay or Airbnb can "bring" with him/her ratings, reviews and comments posted by other people. Scores awarded by other users and not made public by the platform may also be part of the portable personal data, insofar as they "affect" the person – for example, by determining their ranking in the relevant search results.

However, this broad interpretation is limited by the fact that the right is exercised only on the data that the data subject "provides" to the data controller. This is a specific condition of the right to portability, which is not reflected in other related institutions such as the rights of access, rectification and deletion.[27] According to the interpretation proposed in the WG29 guidelines, "data provided by" should be understood not only as data consciously and *actively* provided *by the data subject,* such as name, address and other personal details usually included in the sign-in form, but also, to a certain extent, data *passively provided,* i.e. data that the data controller "observes" *on* the data subject during the use of the service. This includes, for example, data transmitted by the smartphone, or by wearable technologies such as activity trackers or other "Internet of Things" devices, such as data on geo-location, heart rate, speed and combinations thereof. On the other hand, data that the data controller "drifts" or "inferred" by means of data analysis, such as user profiles, scores and forecasts about the user's behaviour, would be excluded. Such data would in fact be considered "created" by the data controller, and not "provided" by the data subject.

The distinction between data *observed on* the data subject and data *created by* the data controller is crucial to define the scope of the right to portability, but it is also one of the most difficult to make and requires case-by-case examination. The criterion proposed by the WG29 refers to a classification made by the OECD at the 2014 summit on privacy in the data-driven economy and then taken up by the World

---

[25] Article 12, Directive 95/46 (now Article 15, GDPR).

[26] Ibid., § 35. The three criteria follow the interpretation recommended by the Working Party Article 29, Opinion 4/2007 on the concept of personal data, 20 June 2007.

[27] For example, the right to deletion (or "right to be forgotten") applies to any data held by the data controller, regardless of their origin (Art. 17, GDPR). On the differences between these rights and their impact on the re-use of the data, please refer to B. Custers and H. Uršič, "Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection", *International Data Privacy Law*, 6(1) (2016), 4.

Economic Forum. In that context, a distinction was made between "derived" data, i.e. data created mechanically to identify patterns and taxonomies, and "inferred" data through probabilistic analytical processes. The data sets of those who operate on digital markets typically contain a wide typology of data that span between these two extremes: on the one hand, information knowingly provided by the interested party and, on the other, data created by the service provider through data analytics. Data towards the latter side of the spectrum would be excluded from portability. On them, the data subject may exercise a more limited right of information and opposition where such processing is for the purpose of automated decision-making processes concerning him/her, including profiling.[28] However, he would not have the right to obtain such data from the data controller.

b) Data processed on the basis of consent or contract

Secondly, the right to portability only applies to personal data processed on the basis of the consent of the data subject[29] or for the needs arising from the fulfilment of a contract[30]. Data processed on the basis of other legal grounds, in particular the legitimate interest of the data controller, are therefore excluded.[31] Article 20(3) then expressly excludes portability when the processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller".[32] The rationale for this exclusion is probably to prevent the use of the right to portability to obtain de facto indiscriminate access to public authority documents, which are, moreover, subject to specific obligations to make them available to the public under the aforementioned PSI2 Directive.[33]

More significant appears the exclusion of data processed without consent, but on the basis of the legitimate interest of the data controller. This legal basis is of primary importance in the big data environment, where it is impossible to obtain the data subject's consent for all forms of processing to which the data are subjected.[34] The scope of this principle is therefore fundamental to define the scope of the right to portability and its impact on digital markets. Some forms of processing that have been

---

[28] Art. 21 and 22 GDPR (right not to be profiled).

[29] Art. 6(1)(a) and, for certain categories of data, Art. 9(2) GDPR.

[30] Art. 6(1)(b) GDPR.

[31] Art. 6(1)(f) GDPR

[32] GDPR, Art. 20(3) and Rec. 68.

[33] Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. The Directive requires public sector bodies to make their documents available "where possible and appropriate, in open machine-readable formats together with their metadata". (Article 5), but excluding "documents access to which is excluded or restricted [...] on the grounds of protection of personal data" (Article 1(1)(cc)).

[34] For a critical examination see F. Ferretti, "Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?", *Common Market Law Review*, 51 (3) (2014), 843.

considered lawful on this basis include the processing of data to protect your website from cyber attacks,[35] or the processing of personal data made available on the internet to make information accessible to other users via search engines – without prejudice to the data subject's right to have the data removed from search results.[36] The legitimate interest does not apply only to publicly accessible personal data, even if the fact that data processed without consent is contained in public sources is relevant to the balance of rights required by Art. 6(1)(f) GDPR and its equivalent in the previous legislation.[37]

The exclusion of data processed on legal bases other than consent and contract places a further, important, restriction with regard to "observed" data, since a significant portion of them is processed without the consent of the data subject. For example, data that a search engine or platform has on the number and origin of searches made on the data subject, or access to his profile, and so on, are likely to be excluded from portability.

2.2 How is portability exercised?

Article 20 imposes specific conditions as to how the data subject must receive the data from the data controller. These conditions represent the most peculiar aspect of the right to portability and define its content, also with respect to the related institutions mentioned above. There are three components to be considered: first, the data subject has the right to receive the data in an interoperable format, i.e. allowing their re-use in other systems; then he or she has the right to transmit them to another data controller "without hindrance"; and finally he/she has the right to obtain direct transmission from one data controller to another "if technically feasible". Taken together, these three requirements create a de facto obligation for the data controller to use formats that allow the re-use of personal data by other operators.

The data controller must provide the data subject with a copy of the data "in a structured, commonly used and machine-readable format". Recital 68 takes over the text of the Article and clarifies that this format must be "interoperable". The concept of data portability is balanced here with the concept of *interoperability*, i.e. the possibility to transfer data and information in general from one system, application or device to another and to use them on each of them.[38] Although the concept is not new in the European agenda on the regulation of digital markets, an obligation to adopt interoperable formats in data

[35] Case C-582/14, *Breyer v Germany*.

[36] Case C- 131/12, *Google Spain v Costeja*.

[37] Case C-468/10, *ASNEF v Aministracion del Estado*.

[38] See J. Palfrey and U. Gasser *Interop. The Promise and Perils of Highly Interconnected Systems*, New York: Basic Books, 2012, p. 5. At European level, the term is defined in Decision 922/2009/EC as follows (Art. 2(1)): "The ability of diverse and diverse organisations to interact towards mutually beneficial and agreed common goals by means of the sharing of knowledge and information between organisations, through the business processes they support, through the exchange of data between their respective ICT systems".

management is here introduced for the first time. The above-mentioned PSI2 Directive requires public sector bodies to make their documents available "in open and machine-readable formats", but only "where possible and appropriate" and "in so far as possible" (Art. 5(1)). The requirement under the GDPR is much stricter, however, and leaves no discretion to data controllers.

As has been pointed out, the previous text of the proposal for a Regulation gave the Commission the task of specifying the electronic format in which data should be transferred from one system to another.[39] In its final wording, however, the legislator left this task to self-regulation, including in Recital 68 a generic reference to "encourage data controllers to develop interoperable formats that allow data portability".[40] This reference is then tempered by the same Recital, which further clarifies that the data subject's right to receive and transmit his data "should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".[41] This means that portability should not affect the processing system, but only the way the data are transferred. In other words, portability requires data to be *transferable* in an interoperable format, not to be *processed* with compatible systems.

The second condition imposed by art. 20 is that the data subject must be able to exercise the right to transfer his/her data to another data controller "without hindrance" by the initial data controller. The obligation to use interoperable formats is functional to the transfer to other subjects, but the right to portability also requires that any other impediment to such transfer is removed. In particular, there must be no financial (such as payment of a price) or legal impediments. This last point is of great importance, as it implies the nullity of contracts limiting portability, both directly and indirectly. For example, cloud computing services may impose contractual clauses that limit the freedom to bring their content to another operator (so-called "data hostage" contracts)[42]. Such clauses are to be considered null and void after the entry into force of the GDPR.

Although portability is a right exercisable only by the person concerned, i.e. by a natural person, *direct* transfer to another holder "if technically feasible" falls within the exercise of this right.[43] This imposes a limit on the exercise of the right in the sense that the controller may reject a request for direct transfer where the necessary technical conditions are not met.[44]

---

[39] Proposal, Art. 18.

[40] Rec. 68.

[41] Ibid. As the WG29 stresses "portability aims at producing interoperable systems, not compatible systems" (p. 19).

[42] R.H. Carpenter, "Walking from Cloud to Cloud: The Portability Issue in Cloud Computing", *Washington Journal of Law, Technology & Arts*, 6 (2010), 1.

[43] Art. 20(2) GDPR.

[44] The European Telecommunications Networks Operators' Association (ETNO) has argued that, in the absence of shared interoperable formats in the industry, the direct transfer obligation should be considered inapplicable (ETNO Data Portability

2.3 Conflict with the rights of others

The right of data portability can be exercised regardless of the purpose for which transfer of data is requested. However, it is subject to the condition that it "shall not adversely affect the rights and freedoms of others".[45] As clarified in Recital 68, the limitation primarily concerns other individuals whose data may be shared with the person exercising the right to portability, either because the same data concern more than one person, or because data of more than one person are present in the data set of the data controller[46]. In this case, the re-use is subject to the limitations deriving from the general rules on the lawfulness of the processing; in particular, the processing of the data by the subsequent data controller (i.e. the controller to whom data has been transferred) may not have a different purpose from that for which the other person had given initial consent to the previous data controller (unless, of course, a new consent is requested, or a different legal basis for the processing is found).[47] Moreover, the transfer of data must not affect other rights provided for in the GDPR, such as the right of access, rectification and deletion. In this sense, the data controller may object to a request for direct transfer to another data controller not only when it is "technically impracticable", but also when such a transfer could compromise the rights and freedoms of other data subjects. Indeed, it can be said that, in this case, the data controller has a specific duty to oppose the transfer.

The "rights and freedoms of others" consist primarily of the rights of other persons to the personal data that are subject to portability. However, as pointed out by the WG29, the limitation is also applicable to any intellectual property rights, whether held by other persons or by the data controller itself.[48] Although such rights are not directly relevant to portability, and for this reason they are not mentioned in Recital 68 concerning Article 20, they must nevertheless be understood as included in the definition of "rights and freedoms of others". Indeed, Article 15 on the right of access contains a provision identical to Article 20(4), namely that "the right [...] shall not adversely affect the rights and freedoms of others".[49] And the relevant Recital 63 clarifies that these rights include "industrial and business secrecy and intellectual property, in particular copyright protecting software" – specifying, however, that "such considerations

Memo, available at https://etno.eu/home/positions-papers/2017/367). For a discussion on this point please refer to Graef, Husovec and Purtova, "Data Portability and Data Control", *cit.*, p. 19-20.

[45] Art. 20(4) GDPR.

[46] "Where, in a certain set of personal data, more than one data subject is concerned, the right to receive personal data should be without prejudice to the rights and freedoms of the other data subjects" Rec. 68 GDPR.

[47] The most common legal basis for processing without consent is the legitimate interest of the data controller (Art. 6(1)(f)) GDPR.

[48] "Although not directly related to portability, this can be considered to include "*industrial and business secrecy and intellectual property, in particular copyright protecting software*" (Guidelines on the right to "data portability", *cit.* , p. 13).

[49] GDPR, Art. 15(4).

should not lead to a refusal to provide the data subject with all information". It is therefore on the basis of the analogy with the right of access that the WG29 includes intellectual property among the rights that must not be affected by portability, and again on the basis of this analogy it concludes that the existence of such rights on the part of the owner must not constitute an obstacle to portability. On this basis, the WG29 identifies a single situation where the right to portability may be limited by the existence of intellectual property rights, namely when the person concerned *abuses* the information obtained in order to infringe an intellectual property right or commit unfair commercial practices. For example, a user may exercise decompilation or reverse engineering on the data obtained under Art. 20 in order to access the underlying trade secrets in data management. In this case, and only in this or similar cases, the exercise of portability would adversely affect legitimate rights of the data controller.

It should be noted, however, the WP29 argument has some flaws. While the analogy with the right of access is certainly justified in more than one respect, the conclusion regarding the balance between the rights in question does not seem to the work in the same way for "access" and "portability". In the case of the right of access, the data subject has the right to *obtain* a copy of his data and a set of information concerning the processing of his data. Obtaining the data is per se a private use, which is generally exempt from liability under intellectual property regimes.[50] With the right of portability, however, the data subject also has the right to *transmit* this copy of the data to other data controllers. This has very different consequences for any intellectual property rights that may exist in or around the data in question. If the balance of rights in favour of the data subject appears justified in the case of the right of access, the same cannot be concluded in the case of the right of portability, which can have a considerable impact on the intellectual property rights of the data subject[51]. It therefore does not seem correct to assume that, *as a general rule*, the existence of intellectual property rights or trade secrets cannot constitute an obstacle to portability.[52] In particular, such an impediment could be invoked even in the absence of abusive behaviour on the part of the person concerned.

---

[50] See e.g. Directive 2001/29 on copyright in the information society, Article 5(2)(b) (reproductions for private use), Directive 96/9 on databases, Article 9 (extraction from non-electronic databases for private use), Directive 2009/24 on the protection of computer programs, Article 5(2) (backup copy of software). See in general S. Karapapa *Private copying*, London, Routledge 2011. In the case of trade secrets, on the other hand, the "acquisition", even in a personal capacity, is sufficient to constitute an infringement, but on condition that it is the effect of "unlawful conduct" (whereas acquisition in good faith is not punishable): see Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Art. 4(2).

[51] It is perhaps no coincidence that the legislator has avoided such a balance, remaining silent in the second case.

[52] See, in the same vein, Graef, Husovec e Purtova: "we contend that WP29 underestimates the extent of potential conflict between the [right of data portability] and the IP rights" ("Data Portability and Data Control", *cit*., p. 11).

3. Balancing of rights and the functioning of data markets

The balance between the right to portability and intellectual property rights requires some further consideration, not least because both derive from fundamental rights of equal rank recognised by the EU Charter of Fundamental Rights[53]. In this connection, the issue is relevant to the extent that it underlies a possible conflict between two regulatory objectives for the functioning of the European digital market: on the one hand, the incentive for creation of digital content and innovation in new technologies and, on the other, the stimulation of competition between services. Intellectual property rights are typically characterised as *incentives* for creation and innovation, while portability, as has been seen, at least indirectly pursues the objective of greater competitive openness of markets. The conflict between these two objectives may undermine the regulatory effect of portability. Let us examine here three scenarios in which such conflict can materialise.

3.1. Conflict with rights held by the data controller on databases

Raw data as such are not in themselves protectable by intellectual property rights. However, their systematic and methodical collection in a "database" may be subject to copyright or sui generis database right[54]. The latter arises automatically when the maker of a database has made a "significant investment" in obtaining, verifying and/or presenting the contents of that database.[55] In principle, any operator in the digital marketplace who has invested non-trivial resources in the collection and processing of personal data can claim an exclusive right to the resulting database. To what extent can this right prevent data portability? The sui generis right gives the right "to prevent extraction and/or re-utilisation of the whole or a substantial part" of the database's contents, or of "non-substantial' parts if they are extracted and/or re-utilised in a "repeated and systematic" manner which prejudices the legitimate interests of the maker.[56] The transfer of personal data "provided by" by an individual may not in itself constitute an extraction of a "substantial part" of the database, or a repeated and systematic extraction that cause prejudice to the maker's economic interests.[57] However, an operator receiving repeated transfers of data from different

---

[53] Art. 8 ("Protection of personal data") and Art. 17(2) ("Intellectual property is protected").

[54] Directive 96/9/EC on the legal protection of databases.

[55] Art. 7(1). The *rationale* of the *sui generis* right is precisely the protection of the "investment" made. As expressed in Recital 12: "such investment in modern information storage and management systems will not be made within the Community unless stable and uniform legal protection is introduced to protect database makers". On the merits of this *rationale,* which has no analogy in other intellectual property rights, see P. Hugenholtz, *Something Completely Different: Europe's Sui Generis Database Right,* in S. Frankel & D. Gervais (ed.), *The Internet and the Emerging Importance of New Forms of Intellectual Property,* Amsterdam, Kluwer Law International, 2016, p. 205.

[56] Art. 7(1) and 7(5).

[57] *The* European Court has ruled on the definition of "substantial part" in Case C-203/02 *The British Horseracing Board Ltd v. William Hill Organization Ltd*, § 73.

users could certainly cause harm, in particular if it actively and systematically induced users to exercise their right to data portability. For example, a new entrant in the market for hotel booking applications may systematically reuse data brought by users from another application, including hotel reviews and prices, in order to develop a competing service. While this is precisely the kind of effect expected from portability, it also opens up a potential conflict with the sui generis right that subsists in the initial database and the legitimate interests that its maker can assert. Given the automatic nature of the sui generis right and the breadth of its scope, it is easy to envisage a wide variety of situations in which this right may constitute an obstacle to data portability.

3.2. Portability and disclosure of trade secrets

The data forming the subject of the right to portability may contain information protected as confidential know-how or trade secrets, in particular if it is data "observed" on the data subject by means of specific data analytics tools or systems. Think, for example, of the loyalty programs of large commercial distributors: the data observed on users who are members of the program contain commercially valuable information on the habits and behavioural patterns of consumers, which are then processed by algorithms to determine offers, individualized prices and behavioural advertising. The functioning of these algorithms is often a secret know-how on which the distributor can enforce certain rights, now also recognized at European level[58]. In particular, the Trade Secrets Directive prohibits the "*unlawful* acquisition, use and disclosure" of secret information,[59] defined as such if it is not "generally known or easily accessible to persons normally dealing with the type of information in question".[60] Among other things, acquisitions of trade secrets by independent discovery or "observation" of an object lawfully in the possession of the person acquiring the information are not considered unlawful.[61]

The right to portability has a non-negligible indirect effect on the protection of trade secrets, and this in two respects: on the one hand, by obliging the data controller to disclose data at the request of the data subject, it extends the scope of information that is "easily accessible" and therefore no longer protectable as confidential information under the Trade Secrets Directive; on the other hand, for the same reason, it reduces the scope of the rights in such information, since it multiplies the possibilities of lawful acquisition through independent observation of the data.

---

[58] Directive 2016/943 on the protection of confidential *know-how* and confidential business information.

[59] Art. 1(1).

[60] Art. 2(1)(a).

[61] Art. 3(1)(a) and (b).

3.3. Rights licensed to the data controller

Finally, the data controller may be the licensee of rights in the data that are subject to portability, in particular when the data includes material protected by copyright, such as reviews, photos or other creative content provided by the user. It is beyond dispute that such content may be simultaneously subject to data protection and copyright laws, in particular if the content is an "original" work which at the same time "concerns" the natural person who provided it to the platform, i.e. to the data controller.[62] If, on the one hand, the data controller cannot claim an exclusive right to the personal data processed on the basis of consent, it may nevertheless request an exclusive licence to use the material of which the user is the author. Unlike the right on personal data, copyright is a real property right that can be negotiated according to all the lawful forms of contract law; therefore, any operator in the digital market can legitimately request, as a condition of use of the service, an exclusive license on the use of the works created by the user while using of the service. Where such a licence exists, a conflict arises with the right to portability, since the subsequent data controller cannot legitimately reuse the data in question without the licensee's permission.

In practice, the effect of copyright on portability is limited by the fact that user generated content platforms tend not to require exclusive content licenses from their users. The reason is that such platforms benefit from the "safe harbour" provided by the E-Commerce Directive, which exempts them from liability on information uploaded by their users to the extent that they act as neutral "hosting" services[63]. The acquisition of exclusive rights on third parties' content may cause the service to lose the immunity granted by the Directive, and for this reason online platforms tend to favour non-exclusive licensing on content uploaded by users[64]. However, as repeatedly mentioned, the portability of personal data applies horizontally to all data controllers, and not only to the so-called social media platforms. Therefore, there are many cases in which the data controller holds exclusive rights on the content "provided by" the data subject, and these rights would inevitably be affected by the request to exercise

[62] While copyright concerns the form of expression of the work and not its content, data protection law considers the work from the point of view of the *information* it conveys. The mere fact that a work bears the attribution to an author (i.e.: that the author's name or a reference to her/his identity appears on it) is already sufficient to consider it as "personal data". But the work can also constitute personal data by virtue of its expressive content, for example because it expresses a political opinion or a trait of its author's personality.

[63] Directive 2000/31 on electronic commerce, Article 14 ('hosting').

[64] An empirical study conducted a few years ago showed that the "*worldwide nonexclusive license*" formula was by far the most widely used by online services that allow the *upload of* content. However, there was a significant minority of services (around 14% of the sample) that required an exclusive licence for content, particularly in the music distribution sector. See M. Borghi, M. Maggiolino, M.L. Montagnani & M. Nuccio, "'Determinants in the online distribution of digital content: an exploratory analysis", *European Journal for Law and Technology,* Vol. 3, No. 2, (2012), 1, p. 23.

portability. Unless the component on which exclusive rights subsist can be separated from the rest of the data provided by the data subject, portability encounters here a potentially insurmountable obstacle.[65]

4. The effects of portability on the market

The right to portability imposes specific obligations on digital market players. As such, its scope extends beyond individual rights. It is a right that affects the structure of the market and arguably shapes its competitive dynamics. In particular, there are two desirable interrelated effects that must be considered from a regulatory point of view: on the one hand, from the consumer's point of view, the reduction of switching costs; on the other, from the company's point of view, the reduction of barriers to entry.

4.1 Portability and reduction of switching costs

Switching costs, i.e. the obstacles that consumers face when switching from one service provider to another, are a decisive factor for the functioning of a competitive market. When switching costs exceed the benefits that consumers can derive from switching to another provider, consumers are de facto "locked" in a service even when the market presents profitable alternatives. The higher the switching costs, the more consumers are locked-in, and the more difficult it is for an operator of a competing service to enter the market.[66] As already mentioned, the right to portability has, among other things, the stated objective of reducing switching costs and combating lock-in phenomena in the digital market.

An important feature of switching costs in digital markets is that these costs tend to increase with network effects: the more users make use of the service, the more difficult it becomes for one of them to switch to an alternative service. For example, a Facebook user who wants to leave the platform and "migrate" to another service would have to bear the costs of rebuilding their accumulated "friends" assets, unless they decide to migrate to the new platform as well. The right to portability does not directly affect this important element of switching costs, but can prevent anti-competitive behaviour based on network effects. In fact, a company can take actions that prevent its users from re-creating their network outside the service, or that make such re-creation excessively expensive. One way is to limit portability, for example, through the use of non-interoperable formats in data management.

---

[65] Distinguishing, within a given set, the component that can be protected by intellectual property rights is not always possible in practice. See N. Duch-Brown, B. Martens, F. Mueller-Langer, The Economics of Ownership, Access and Trade in Digital Data, Digital Economy Working Paper, 2016-10, JRC Technical Reports.

[66] For an analysis with reference to portability and big data, see G. Colangelo, "Big data, digital platforms and antitrust", *Mercato Concorrenza Regole* 3 (2016), 425, p. 455-6.

This issue has received examination from a competition law perspective in the case of the merger between Facebook and the WhatsApp instant messaging service. In this case, the Commission concluded that there was no evidence that the lack of data portability (contacts and messages) could constitute a significant impediment for consumers to switch to another messaging service, and this for three reasons: first, communication via app tends to consist of short conversations that have only limited-term value; second, in any case, the backup messages remain accessible to the user even when the user switches to another service; finally, the contact list can in fact be "ported" to another service, as it is stored on the user's smartphone and can easily be made accessible to another operator.

This last point is particularly important because it concerns another typical feature of switching costs in digital markets, namely the relevance of the data set controlled by the service provider. The more information the user accumulates in the provider's database, and the greater its value to the user, the higher the cost of switching to another service. A user who has "uploaded" a large amount of content to his or her Facebook page will have more difficulty switching to another platform than someone who has used the service only sporadically. The right to portability affects this element of switching costs in two ways: on the one hand, it requires the adoption of interoperable formats that allow the reuse of data accumulated in a given dataset; on the other, it establishes the principle that such data belong to the data subject and can therefore be transferred at any time without losing the benefits of using the service. Just as the contact list on my smartphone is "mine", so is the data accumulated on an online service – be it a platform, an app, or a cloud storage service.

With respect to this data, portability reduces the contractual autonomy of the data controller, for example by making data-hostage clauses null and void. Arguably, the right to portability reduces significantly the "legal" element of switching costs, i.e. costs due to contractual conditions imposed by the data controller.[67]

The overall effect of portability on reducing switching costs is difficult to assess and will require case-by-case examination. It is barely worth remembering that portability is only one of the elements affecting these costs, and that other factors require attention. In particular, it has been observed that in some "mature" digital markets, such as search engine markets, users tend to perceive switching costs as higher than they actually are[68]. Where this phenomenon occurs, the right to portability can have a very limited effect in the short time. However, in the long run, it may affect consumer habits and contribute to

[67] This is, of course, limited to the data covered by the law and taking into account the limitations discussed above. These include, as we have seen, the limitations due to the existence of intellectual property rights.

[68] M. Stucke & A. Grunes, *Big data and competition policy*, Oxford, Oxford University Press 2016, p. 183-5.

changing such perception, to the extent that it reinforces the sense of autonomy in the management of one's own data.

4.2 Interoperability and entry barriers

The reduction of switching costs should have an effect on a key element of the competitive market, namely entry barriers. By reducing switching costs and preventing lock-in situations, portability makes it less difficult for new entrants to attract users and achieve the scale necessary to sustain competition with other operators. In addition, subject to the limitations discussed above, it makes it possible to access the accumulated data assets of other operators that have been on the market for longer. As has been seen, portability materialises, from the perspective of data controllers, by imposing interoperable standards in the transfer of data. As with any other requirement introduced by the GDPR, the right to portability imposes higher costs on companies that process personal data. This means that new entrants have to bear additional costs to ensure that their procedures are compatible with the GDPR in general, and with Article 20 in particular.[69] They must, as seen above, adopt interoperability by design.

The net effect of these two opposing factors – easier access to data *vs.* higher compliance costs – depends on the structure of the market in question and is difficult to estimate in advance. In principle, a "positive" effect can be expected in markets where the adoption of interoperable standards is less costly, either because it is technically simpler or because, for structural reasons, it is already a shared standard. Conversely, in markets where such standards are not commonly adopted, or even not available, the net effect could be "negative", namely the cost of adopting interoperable systems could outweigh the benefit of easier access to data.[70]

Furthermore, the benefit of easier access to data accumulated by other operators depends in particular on the relative value of the data concerned, and how commercially relevant their re-use is. As seen, in the *Facebook/WhatsApp* case, one of the factors that led to the conclusion that the lack of portability was not a barrier to entry was precisely the low long-term value of the data in question, namely the "chats" history.[71] The portability of low-value data does not affect the reduction of entry barriers, unless the new entrant discovers an innovative way to extract value from those same data. In this sense, the value of the

[69] T. Körber, "Is Knowledge (Market) Power? On the Relationship between Data Protection, 'Data Power' and Competition Law', (2018) 23, p. 18.

[70] It has been pointed out, for example, that in the telecommunications sector there are no interoperable formats for data transmission (ETNO Data Portability Memo, *cit.*). On the difficulty and risks of adopting interoperable practices see in general Palfrey and Gasser *Interop*, *cit.*

[71] § 113. However, it can be argued that the *long-term value* for consumers is not the same as for a data company, which can extract information and commercial value from the processing of large amounts of data.

data depends on one hand on its quality (accuracy, timeliness, etc.), but on the other hand, perhaps even more importantly, on the "business idea and technology used" to extract value from it.[72]

In principle it can be said that portability can reduce barriers to entry into markets where data retain value after use by the first comer and where low-cost interoperable standards are available. In other situations, the pro-competitive effect is more uncertain or even possibly negative.

4.3 A competition rule "per se"? Portability as an objective of the digital internal market

The right to data portability introduced by the GDPR is, albeit indirectly, an a priori competitive rule that applies indiscriminately to all those who process personal data, regardless of the existence of anti-competitive exclusionary practices such as refusal to provide essential facilities, denial of access or tying. For this reason, the rule introduced by the European legislator has attracted some criticism, especially from the US antitrust scholars, generally sceptic about the adoption of so-called "*per se* rules".[73] The objection against the "portability obligation" is similar to the one that is usually raised against rules that impose interoperability or other forms of "openness", namely that they reduce the incentives for innovation.[74] What is contested are not the benefits of interoperability, but the advantages of standards that make interoperability *mandatory*. Companies in digital markets often need to exercise exclusive control over the data provided by their consumers in order to develop innovative services. Moreover, many services require a certain scale, which can only be achieved and maintained by "keeping" their users within their own service. For example, traffic navigation apps operate on the basis of data provided in real time by a large number of users, as well as on previous data accumulated in their database. Many innovative services like these, based on crowd-collected data, may not see the light of day without the incentive provided by exclusive control over data. In such cases, a certain level of switching costs may encourage investment in new technologies, and the consumer would not be harmed, but rather would benefit from lock-in, if it was the necessary price to pay to have access to a highly innovative service.[75]

---

[72] G. Colangelo, "Big data, digital platforms and antitrust", *cit.* , p. 430.

[73] See in particular P. Swire and Y. Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique", *Maryland Law Review*, 72(2) (2013). Swire and Lagos' analysis is based on the text of the proposed Regulation. On the limits of the rules "per se" in digital markets see also A. Fatur, *EU Competition Law and the Information and Communication Technology Network Industries: Economic versus Legal Concepts in Pursuit of (Consumer) Welfare*; Oxford, Hart Publishing 2012.

[74] For a critical discussion see Stucke & Grunes, Big *data and competition policy,* cit. , p. 332.

[75] Swire & Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare" p. 340. Let's leave aside other less convincing criticisms made by Swire and Lagos, such as the one that portability increases *compliance* costs for new entrants (but the same can be said of all the rules introduced by the GDPR) and increases data security risks (but, as shown by the recent Facebook and Cambridge Analytica scandal, personal data are not necessarily "safer" if they remain in the hands of a single tech company).

The argument deserves consideration, not least because, as we have seen, the pro-competitive effects of the right to portability depend on multiple factors and are by no means unambiguous. However, it should be borne in mind that the same objections to portability can be raised, *mutatis mutandis*, against proprietary rights over data. The assertion that greater power of control over data stimulates innovation is just as (if not more) problematic than an unconditional trust in the pro-competitive effects of data portability and interoperability.[76] Ultimately, the issue is mainly about the *quality* of the innovation that the regulator intends to promote. In this sense, while portability and the related interoperability obligation may act as a disincentive to invest in proprietary innovation, it may nevertheless steer markets towards "open" innovation.

The extent to which this can happen depends to a large extent on how the right to portability is integrated with other rules governing digital markets. Indeed, the portability of personal data is the first piece of an evolving regulatory framework. The Proposal for a Directive on digital content, currently under consideration by the European Parliament, introduces the obligation for "suppliers of digital content" to provide the consumer who withdraws from the contract with "the technical means to retrieve all content provided by the consumer and any other data produced or generated as a result of the use of digital content by the consumer, to the extent that the data has been retained by the supplier". The rule also specifies that "the consumer has the right to retrieve the content free of charge and without particular inconvenience, within a reasonable time and in a commonly used format".[77] The provision differs from Art. 20 of the GDPR in that it enters into force only when the contract is terminated, but significantly extends its scope in that it applies to *all content* provided by the consumer (and not only to personal data), as well as to data *produced or generated by the supplier* around the use of digital content by the consumer, to the extent that they are retained by the supplier. The latter category of data may certainly include a portion of those "derived or inferred" data which, as seen above, are excluded from the scope of Article 20 of the GPSD.[78]

---

[76] For a general overview see J. Drexl, "Designing competitive markets for industrial data – between propertisation and access", *Max Planck Institute for Innovation and Competition Research Paper* No. 16-13 (2013).

[77] Proposal for a Directive on certain aspects of contracts for the supply of digital content. Brussels, 9.12.2015 COM(2015) 634 final, Article 13(2)(c). For a discussion of this rule see Graef, Husovec and Purtova, Data Portability and Data Control, *cited above,* p. 22-24.

[78] However, the first reading of the EU Council seems to have limited the scope of data covered by Article 13(2)(c). The wording proposed by the Council is: "the supplier shall make available to the consumer any digital content (...) to the extent that it does not constitute personal data, which was uploaded or created by the consumer when using the digital content or digital service supplied by the supplier". (EU Council, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (First reading) – General approach 9901/17 of 1 June 2017, p. 32). See Graef, Husovec and Purtova, "Data Portability and Data Control", *cit*., p. 23.

As an emerging concept of European law, data portability is becoming one of the pillars of the European digital single market. The task of regulators will be to ensure that the resulting portability and interoperability regime is not an end in itself, but a coherent tool at the service of open innovation.