ASSER PRESS

Information Technology and Law Series | IT&LAW 32

Regulating New Technologies in Uncertain Times

Leonie Reins *Editor*

Information Technology and Law Series

Volume 32

More information about this series at http://www.springer.com/series/8857

Leonie Reins
Editor

Regulating New Technologies in Uncertain Times

Editor
Leonie Reins
Tilburg Institute for Law, Technology,
and Society (TILT)
Tilburg University
Tilburg, The Netherlands

ISSN 1570-2782 ISSN 2215-1966 (electronic)
Information Technology and Law Series
ISBN 978-94-6265-278-1 ISBN 978-94-6265-279-8 (eBook)
https://doi.org/10.1007/978-94-6265-279-8

Library of Congress Control Number: 2018965892

Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

This T.M.C. ASSER PRESS imprint is published by the registered company Springer-Verlag GmbH, DE
part of Springer Nature
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Series Information

The *Information Technology & Law Series* was an initiative of IT*e*R, the national programme for Information Technology and Law, which was a research programme set up by the Dutch government and The Netherlands Organisation for Scientific Research (NWO) in The Hague. Since 1995 IT*e*R has published all of its research results in its own book series. In 2002 IT*e*R launched the present internationally orientated and English language *Information Technology & Law Series*. This well-established series deals with the implications of information technology for legal systems and institutions. Manuscripts and related correspondence can be sent to the Series' Editorial Office, which will also gladly provide more information concerning editorial standards and procedures.

Editorial Office

Contents

Part I Introduction

1 Regulating New Technologies in Times of Change 3
Ronald Leenes

2 Regulating New Technologies in Uncertain Times—Challenges and Opportunities 19
Leonie Reins

Part II New Technologies and Impacts on Democratic Governance

3 Between Freedom and Regulation: Investigating Community Standards for Enhancing Scientific Robustness of Citizen Science 31
Anna Berti Suman

4 Human Rights in the Smart City: Regulating Emerging Technologies in City Places 47
Tenille E. Brown

5 Automated Driving and the Future of Traffic Law 67
Nynke E. Vellinga

6 Coercive Neuroimaging Technologies in Criminal Law in Europe 83
Sjors L. T. J. Ligthart

Part III New Technologies and Market Regulation

7 Planting the Seeds of Market Power: Digital Agriculture, Farmers' Autonomy, and the Role of Competition Policy 105
Tom Verdonk

8 Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights" 133
Silvia Martinelli

9 Regulating Smart Distributed Generation Electricity Systems in the European Union 153
Theodoros G. Iliopoulos

Part IV The Data in New Technologies—The Utilization of Data and the Protection of Personal Data

10 A Public Database as a Way Towards More Effective Algorithm Regulation and Transparency? 175
Florian Wittner

11 Access to and Re-use of Government Data and the Use of Big Data in Healthcare 193
Miet Caes

12 The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI 225
Sascha van Schendel

13 Regulating Data Re-use for Research: The Challenges of Innovation and Incipient Social Norms 241
Hannah Smith

14 European Cloud Service Data Protection Certification 261
Ayşe Necibe Batman

15 Data Privacy Laws Response to Ransomware Attacks: A Multi-Jurisdictional Analysis 281
Magda Brewczyńska, Suzanne Dunn and Avihai Elijahu

Part V Conclusion

16 Concluding Observations: The Regulation of Technology—What Lies Ahead—And Where Do We Want to End Up? 309
Leonie Reins

Editor and Contributors

About the Editor

Leonie Reins is an Assistant Professor at the Tilburg Institute for Law, Technology, and Society ("TILT") at Tilburg University in the Netherlands. Previously, she was a Postdoctoral Researcher at KU Leuven, Belgium, where she also wrote her Ph.D. thesis on the coherent regulation of energy and the environment in the EU. Leonie completed an LL.M. in Energy and Environmental Law at KU Leuven, and subsequently worked for a Brussels-based environmental law consultancy, providing legal and policy services for primarily public sector clients. Leonie's research focuses on the intersections of international and European energy, climate and environmental law.

Contributors

Ayşe Necibe Batman Frankfurt am Main, Germany

Magda Brewczyńska Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

Tenille E. Brown Faculty of Law, University of Ottawa, Ottawa, Canada

Miet Caes Leuven Institute for Healthcare Policy, Leuven, Belgium

Suzanne Dunn Faculty of Law, University of Ottawa, Ottawa, Canada

Avihai Elijahu Faculty of Law, University of Haifa, Kiryat Shmona, Israel

Theodoros G. Iliopoulos Hasselt University, Hasselt, Belgium

Ronald Leenes Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

Sjors L. T. J. Ligthart Department of Criminal Law, Tilburg Law School, Tilburg University, Tilburg, The Netherlands

Silvia Martinelli University of Turin, Turin, Italy

Leonie Reins Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

Hannah Smith Centre for Health, Law, and Emerging Technologies, University of Oxford, Oxford, UK

Anna Berti Suman Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

Sascha van Schendel Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

Nynke E. Vellinga Faculty of Law, University of Groningen, Groningen, The Netherlands

Tom Verdonk Institute for Consumer, Competition & Market, University of Leuven (KU Leuven), Leuven, Belgium

Florian Wittner Department of Law, Hans-Bredow Institute for Media Research at the University of Hamburg, Hamburg, Germany

Chapter 8
Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"

Silvia Martinelli

Contents

8.1 Introduction to the "Platform Economy": Network Effects and Switching Cost 134
8.2 The Right to Data Portability as a Milestone for Competition Law, User's Protection and Privacy: An Introduction 137
8.3 The Right to Data Portability in the General Data Protection Regulation and in the Guidelines of the Article 29 Working Group: The Privacy Concern 140
8.4 Non-personal Data and Professional Users: The Proposals of the EU Commission 145
8.5 Provided, Observed and Inferred Data: Regulating New Technology in Uncertain Times 148
References 151

Abstract This chapter analyses the right to data portability and its peculiarities in the platform economy, where this right is fundamental for competition law, users' protection and privacy, because of the presence of strong direct and indirect network effects and consequent high switching costs. In particular, it analyses the right to data portability as set out in the GDPR, together with the interpretation given by the Article 29 Working Group, and the other "porting rights" in the Digital Single Market strategy and in the European Commission Proposals "for a Regulation on a framework for the free flow of non-personal data in the European Union", "for a Regulation on promoting fairness and transparency for business users of online intermediation services" and in the proposed "Directive on certain aspects concerning contracts for the supply of digital content". It underlines six critical issues related to the right to data portability: (1) a privacy issue, due to the huge sharing of

S. Martinelli (✉)
University of Turin, Turin, Italy
e-mail: silviamartinelli89@gmail.com

L. Reins (ed.), *Regulating New Technologies in Uncertain Times*,
Information Technology and Law Series 32,
https://doi.org/10.1007/978-94-6265-279-8_8

data of other individuals; (2) the need to establish the portability of non-personal data; (3) the need to establish the portability for professional users that are not natural persons; (4) the need to protect the rights of the controller and his investment when data is not merely collected but also reworked; (5) the risk of decreased competition with a strong and non-scalable regulation; (6) the necessity to pay attention to the technical solutions available in order to assure practicable application methods, in particular considering the needs of smaller operators.

Keywords Data portability · Social network · Platform economy · Consumer · Competition · Privacy

8.1 Introduction to the "Platform Economy": Network Effects and Switching Cost

In the so-called "networked information economy",[1] where "data is at the centre of the future knowledge economy and society",[2] platform users continuously generate huge amounts of information and content, often without commercial goals. However, new business models are able to exploit the contents created or the analysis of the data generated for commercial purposes.

Social networks like Facebook enable new forms of communication and connection between users, who meet and communicate through the platform providing rich and detailed information about themselves. They can be defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and transfer their list of connections and those made by others within the system".[3]

The vast majority of social networking services are provided free of monetary charges; however, they can be monetised through other means, such as advertising or charges for premium services.[4] The companies foster the perception that the social media services are provided for free, but they have a precise business model based on the collection and analysis of data to offer targeted advertising services.

"Personal information operates as a currency"[5] and the value of the data is extracted in a four-step "personal data value chain" consisting of (1) collection and access, (2) storage and aggregation, (3) analysis and distribution and (4) usage of

[1] Benkler 2006.

[2] European Commission 2014a.

[3] Boyd and Ellison 2007.

[4] European Commission 2014b.

[5] European Commission 2015, Article 3.1; EDPS 2014, 2016a; Resta 2018; Colangelo and Maggiolino 2017.

personal datasets.[6] The results of the data analysis, crystallized in new data, are possible thanks to sophisticated algorithms that are able to provide different kinds of user-advertising services.

Platform as social networks can be also defined as "multi-sided platform". The platforms "serve distinct groups of customers who need each other in some way, and the core business of the two-sided platform is to provide a common (real or virtual) meeting place and to facilitate interactions between members of the two distinct customer groups".[7] There are two or more groups of users and the matching between all of them is made possible by the platform itself.

Social networks are a particular multi-sided platform where users usually provide data in order to receive the social network' services; the platform provides the service to the first group of users, analyses the data and process these data to offer advertising services to another group of users.[8]

It is possible to identify a second type of multi-sided platform which serves distinct groups of customers but uses a different business model, not based on advertisements. We can use the term "intermediary platform" (or "exchange platform") to define the multi-sided market platforms which enable the meeting between sellers and buyers of goods and services: for example Booking, Airbnb, BlaBlaCar, but also Amazon (when the company is not the seller directly).

In these cases the platform, through the use of data analysis and algorithms, makes the meeting between two or more groups of users possible while offering other facilities which allow for the reduction of transaction costs.[9] The fundamental role of these platforms is to "enable parties to realize gains from trade or other interactions by reducing the transactions costs of finding each other and interacting".[10] Different platforms engage in these activities to different degrees, with no profit or commercial purpose. It is also not uncommon that the platforms devise rules and regulations in order to reduce externalities and to increase the trust in the platform as a whole.

The two described types of platforms, "social network platform" and "intermediary platform",[11] are now spreading across the web and they are becoming the "new square" and the "new market" where people met and interact, because of the

[6] EDPS 2014; European Commission 2017a.

[7] Evans et al. 2011; Frank 2014.

[8] Stucker and Grunes 2016; Graef 2015; EDPS 2016a.

[9] It is estimated that around 60% of private consumption and 30% of public consumption of goods and services related to the total digital economy are transacted via online intermediaries. European Commission 2018a.

[10] Evans et al. 2011.

[11] The present analysis is limited to these two types of platforms here described and it not includes search engine, because in the opinion of the writer in the latter case there are substantial difference. In particular, the content listed by the search engine is not created on the "search engine platform" but it's only a second representation and organisation of a content published in another website. Furthermore, in the case of search engine the user's profile has a different and lower importance, based on the creation of the filter bubble rather than on the public representation of the user.

chance they offer to reach a selected audience. For example, Airbnb allows non-professional individuals to offer rooms or apartments and to find interested individuals. This became possible only thanks to the platform and because of the use of Big Data and algorithms and it is likely to increase in the upcoming years.

The major problem of these new "squares" and "markets" is the market dominance by a few actors versus a variety of suppliers and traders. The large size of a few platform widely used around the world is a concern, because they are private regulators of the community of users and they acquire more and more power.

A few platforms emerged due to network effects and switching costs, which reduce competition in the market. The effects are moreover amplified by network effects caused by the use of Big Data, which are fundamental for the success of this type of platform and as a result only a limited number of successful platforms assert itself in the global market.[12]

To better understand these effects, it is necessary to distinguish between "direct" and "indirect network effect": in the first case the value of joining the platform for the individual user increases with the number of users ("if all my friends are there, I want to be there"); in the second case, more users on one side of the platform attract more users on the other side of the platform ("if my consumer/target is there, I want to sell/promote my products there").

The existence of strong direct and indirect network effects in the platform economy[13] creates and increases the current dominant positions and in both cases the large use of Big Data[14] profiling is a factor which multiplies these effects: "volume and quality of data are positively correlated with the variety and quality of the offered products and services, since companies can offer better products by analysing 'more' consumer behaviour".[15] Traditional network effects, as evidenced by social networks like Facebook, are now multiplied by network effects involving the scale of data, network effects involving the scope of data, and network effects where the scale and scope of data on one side of the market affect the other side of

[12] European Commission 2018a.

[13] The term "platform economy" is here used to refers to social media platform and exchange platforms, as mentioned and described above.

[14] "Big Data" are commonly defined by the use of the three "V" (or sometimes four or five): volume, variety (which refers to mostly unstructured data sets from sources as diverse as web logs, social media, mobile communications, sensors and financial transactions) and velocity (or the speed at which data is generated, accessed, processed and analysed). The definition is still vague and "the problem still with the 3Vs and similar definitions is that they are in continuous flux, as they describe technical properties which depend on the evolving state of the art in data storage and processing". See also OECD 2014. More simply, in the words of Viktor Mayer-Schönberger and Kenneth Cukier, "big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more". See also Mayer-Schönberger and Cukier 2013.

[15] Engels 2016.

the market (i.e. as advertising).[16] In fact, there is a strong tendency of market concentration in the data industry: "simply put, the more data is fed into the analysis, the better and more efficient the service becomes".[17] This is also called "big data advantage".[18]

"Switching costs" are the barrier costs that users may face when trying to switch to another platform. They can increase due to network effects. When the costs are getting higher, it becomes more difficult for the users to move to a different platform. In fact, we are witnessing consolidation of platform lock-ins, due to not only strong network effects and consequent high switching costs ("I don't want to change the platform because my friends/consumers/sellers are there" and "If I decide to change platform I will lose all my friends/customers/connections"), but also due to the difficulty of transferring reputation and relevant data: a user planning to move to a different platform will lose his "history", meaning the interactions and reputation built day by day on the platform.

Because of the joint presence of the effects described it is particularly difficult for the user to move to a new platform and, as a consequence, it is difficult for a new platform to be competitive with the major platforms operators. Furthermore, a limited number of platforms can manage all the data and relationships between the users.

In the light of the above considerations, it is fundamental to increase the competition in the "platform market" and this could be done through the widespread use of "the right to data portability" and "portability rights", with meaning the rights which can favour the sharing and transfer of the data between the platforms. In the multi-side market platforms, more than in different areas, competition, and hence portability, becomes an imperative. However, at the same time, it is fundamental to analyse and understand the problems associated with the right to data portability, in order to identify legal and technical solutions to mitigate the negative effects of this right and to make sure that the implementation effectively increases competition, not limits it.

8.2 The Right to Data Portability as a Milestone for Competition Law, User's Protection and Privacy: An Introduction

"Data portability" means the ability to move data between applications or platforms and may be a milestone for boosting competition in the data economy and, in particular, in the platform economy, because of the strong network effects described.

At present, the right to data portability is set out in the new Regulation 679/2016 of the European Parliament and of the Council of 27 April 2016 "on the protection

[16] Stucker and Grunes 2016.

[17] European Commission 2017a.

[18] Stucker and Grunes 2016.

of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (General Data Protection Regulation), as a right of the data subject. The right, provided by Article 20 of the GDPR, is the right of the data subject to "receive the personal data concerning him or her" and it is set out in the GDPR with regard to "personal data" of a "natural person".

If strictly interpreted, the right to data portability, as affirmed in Article 20, does not extend to "non-personal data" and to the data referred to a "professional user". Nevertheless, the European Union argued in favor of general portability or transferability of raw personal and non-personal data[19] and the European Commission has already put forward some proposals to extend such form of portability also to "non-personal data" and professional users.

Data portability is fundamental not only for privacy, but also for the growth of the Digital Single Market and it involves competition law, user protection[20] and privacy as a fundamental personal right. The European Data Protection Supervisor underlines these connections in the "Preliminary Opinion" on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", where it is affirmed that implementing the right to data portability, as set out in the GDPR for the protection of personal data, by giving the user options to withdraw their personal information and to port it to another service provider "would potentially empower individuals while also promoting competitive market structures". In particular, the right to data portability goes further than the principle of transparency, which means the right of the data subject to know everything about the data process and the possibility to exercise "data access" to know exactly what data were processed. Data portability is the right to download data in a "structured, commonly used and machine-readable format" and transmit these data to a different data controller. It would allow users to transfer data between online services and to give them to third parties.

Concerning competition law in the platform economy, the advantages are manyfold:[21] in a market characterized by dominant positions and strong network effects, where the use of data emphasizes more traditional network effects, emphasized by the network effects caused also by the use of large amounts of data, data portability and the sharing of these data are essential. Only with plain data portability new platforms and business models can some form of competition emerge. Users regain the power to switch to another platform without losing the time invested in the previous one. If the user can take a copy of his data from a

[19] European Commission 2016.

[20] The term "user protection" is used instead of "consumer protection" because in the case of the users of these platforms there is a lack of negotiating power not only for the contract between consumers and the platform, but also for contracts between the platform and professional users.

[21] Vanberg et al. 2017; Graef et al. 2014; Engels 2016; Graef 2015; Lynskey 2017; Graef 2016; Colangelo and Maggiolino 2017.

platform and transfer all the data to a new one, this will also reduce the network effects directly linked to data access.[22] For example, the dealer of hats who uses the platform Amazon to sell his products can decide to leave for the new platform "BuyBuyBuy" without losing the description of the products created on the first platform and maybe, if the current obstacle to a plain right to data portability were to be removed, the comments of the buyers in the reputational feedback system could be ported too.

Regarding users' protection (both consumer or professional), the right to data portability can improve the power of the data subject on his data, in particular if the right will be used in connection to the right to erase. If a user can take a copy of the data, ask and obtain the deletion of all his data on the platform, he has more contractual power in the platform relationship. In the previous example, the dealer can decide to move to a new platform also because of unsatisfactory contractual conditions and delete all his information from the previous one. If a lot of users will act in the same way, the platform may decide to amend some clauses. As a second example, on a social media platform such as Facebook, if a user loses his trust in the transparency of the platform, he can take the copy of his data, history and relationship, move to a new one and delete all the information he uploaded on Facebook.

It is not as easy as it sounds because of the network effects described: the user will only move to a new platform where he can find his buyers or his friends. However, with the possibility to exercise a full right to data portability he will not lose his "history" and the time spent to upload all the information on the platform. Furthermore, the transfer of the data will reduce the additional network effect caused by data: the new competitor platform will easily receive large amounts of data, which will enable the platform to improve the offered services.

As a consequence, if the variety of the platform offer is wider and the cost of the transition is not excessive, users would have more contractual power and the risk of abuse of dominance would be avoided.

The possibility for the user to port, share and also delete data is therefore a milestone for the digital economy and EU Digital Single Market. "Building a European data economy"[23] is part of the European Union "Digital Single Market strategy". It aims at "enabling the best possible use of the potential of digital data" and "unlock the re-use potential of different types of data and its free flow across border".[24]

---

[22] Also the OECD underlined that "The monetary, economic and social value of personal data is likely to be governed by non-linear, increasing returns to scale. The value of an individual record, alone, may be very low but the value and usability of the record increases as the number of records to compare it with increases. These network effects have implications for policy because the value of the same record in a large database could be much more efficiently leveraged than the same record in a much smaller data set. This could have implications for competition and for other key policy items such as the portability of data". See OECD 2013.

[23] European Commission 2018b.

[24] Ibid. Data sharing and re-use can be generally understood as making data available to or accessing data from other companies for business purposes; European Commission 2018c.

This contribution will first analyse the right to data portability as set out in the GDPR and in the interpretation given by the Article 29 Working Party.[25] Therefore, it will analyse the other "porting rights" in the Digital Single Market strategy and in the European Commission Proposals "for a Regulation on a framework for the free flow of non-personal data in the European Union", "for a Regulation on promoting fairness and transparency for business users of online intermediation services" and in the proposed "Directive on certain aspects concerning contracts for the supply of digital content".

A broad interpretation and application of the right to data portability raises important concerns about privacy and data protection. Data portability increases personal data circulation, but it constitutes the best way to diminish or slow down the concentration of power and monopolisation. In a context where "platformisation of our economy and, more generally, our society"[26] is actually becoming true, it is important to improve competition and enable new platforms to compete. In addition, it constitutes a good reference to underline some further problems concerning data protection law and its problems in relation with other European legislation and proposals.

8.3 The Right to Data Portability in the General Data Protection Regulation and in the Guidelines of the Article 29 Working Group: The Privacy Concern

The General Data Protection Regulation aims to protect natural persons in relation to the processing of personal data, as a fundamental right set out in Article 8 of the Charter of Fundamental Rights of the European Union, an "integral part of human dignity, and a prerequisite for many other social goods such as free expression and innovation".[27] The Regulation shall apply when there is a processing of "personal data", that is any information relating to an identified or identifiable natural person, which is called "data subject".[28]

[25] Article 29 Working Party 2017.

[26] Belli and Zingales 2017.

[27] Buttarelli 2017. See also Floridi 2016; Lynskey 2015; UNESCO 2016.

[28] As established in Article 4 of the GDPR, "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The right of data portability is set out in Article 20 of the Regulation as the right of the data subject to "receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided". The data subject could also ask for the direct transmission from one controller to another, where technically feasible (Article 20.2).

Within the scope of the previous Directive 95/46/EC the data subject could exercise a right of access to know all the data related to him, but he was constrained by the format chosen by the data controller to provide the requested information; on the contrary "the new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another".[29]

The right to data portability means only a right to move, copy or transmit the data. The exercise of the right of portability and the right to be forgotten (Article 17) are independent: data portability "does not automatically trigger the erasure of the data from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted".[30]

The Article 29 Working Party released the "Guidelines on the right to data portability"[31] providing guidance on the way to interpret and implement the right. The most important part of this document concerns the conditions under which this new right applies.

The right to data portability as regulated by Article 20 of the GDPR applies where the processing is based on consent[32] or on a contract ("where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract").[33]

The Article 29 Working Group specifies that the right to data portability regards not only data provided knowingly and actively by the data subject but also the personal data generated by his or her activity. In particular, it includes: (a) personal data concerning the data subject; (b) the data which the data subject has provided to a data controller. With regard to letter (a), it is necessary to specify that the Article 29 Working Group includes "pseudonymous data that can be clearly linked to a data subject", but not anonymous data. With regard to letter (b) the Group distinguishes three categories of data: (1) data actively and knowingly provided by the data subject, (2) observed data and provided data, (3) inferred data and provided data. In the platform economy, the first category includes all the data uploaded to the platform by the data subject, for example the information on the profile, photos, description of the products, etc. In the second category, there are the data generated

[29] Article 29 Working Party 2017.

[30] Ibid.

[31] Ibid.

[32] Article 6.1, letter a or Article 9.2, letter a of the GDPR.

[33] Article 6.1, letter b of the GDPR.

on the platform by the user's activities, for example traffic data and search history. In the latter group, there are the data created by the data controller analyzing the first two categories. For the Article 29 Working Group the right to data portability must be interpreted broadly: the first two categories of data fall into the scope of data portability and only the latter must be excluded.

The distinction in three categories stems from the need to solve two of the main problems related to data portability: a privacy issue, due to the huge sharing of data of other individuals, and the need to protect the rights of the controller and his investment when the data are not merely collected but also reworked. In this contribution the first one will be analysed.

In a traditional process of data, the data controller collects and analyses data provided by the data subject and sometimes he extracts new data from provided data. In the platform economy the set-up is more complex because the data subjects can interact with each other and generate new data using the platform. For example, in a social network it is possible to publish a picture of a group of friends and "tag" all of them or publish a post about a friend in a group. In the exchange platforms, the connections between seller and buyer always concerns both parties, because the data with regard to the exchange contains personal data of both subjects. In addition, sometimes it is possible to inquire about a seller or a product through a previous buyer. The data will also involve personal information about other users. All these data, generated in the platform by the user's activity, regard more than one data subject and it becomes a limit to the right to data portability because it would require the permission of all the data subjects involved.

A broad interpretation of the right of data portability could easily lead to a wide sharing of data, which relates also to other data subjects. Considering the working of social network and intermediary platform, in the data "connected to a data subject" there is a lot of information which relates to all his contacts. The exercise of the data portability of one data subject could have implications, "privacy invasions", for a lot of different individuals.

How is it possible to balance the right to "share data" with the right to privacy of other individuals? What is the right balance between privacy and concurrence/consumer protection?

The GDPR does not solve the question but it underlines that the right to data portability "shall not adversely affect the rights and freedoms of others".[34] The Article 29 Working Group tries to extend the application of the right to data portability also to the data which involve more than one data subject. In particular, it said that when a data controller processes "information that contains the personal data of several data subjects", he "should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". The example the Working Group gives is the case of a telephone with numbers and messages from other individuals and personal data of multiple people; in this case the data controller should response to the data portability request because the data also concerns

[34] Article 20.4 of the GDPR.

the data subject, but if such data are then transmitted to a new data controller, the new data controller "should not process them for any purpose which would adversely affect the rights and freedom of the third-parties".

In the opinion of the writer it is clear that this could be a first compromise but not a solution, because it seems to enable the portability of data without the knowledge of all the data subjects involved. However, properly, it shifts responsibility for the protection of the first data subject to the new one (the next platform or the data subject itself if he processes the data not only for purely personal or household needs), making it easier for the first data controller to answer to the data portability request without much concern. It would be a problem for the next data controller, who should find another ground for the lawfulness of processing and also for third parties data involved.[35]

The Article 29 Working Party suggests that where personal data of third parties are included in the data set, another ground for the lawfulness of processing must be identified.

Because of the difficulty of distinguishing between the different scopes and grounds for lawfulness in the Big Data age, where data is collected without knowing its future utilisation and without distinguishing between different categories of data and processing, it could be reasonable to raise doubts that such distinctions and controls could ever be implemented.

Obviously, the implementation of consent mechanisms for other data subjects involved could be an easy solution to respect the third parties involved. For example, when a data subject decides to exercise his right to data portability, the platform can send a request to all the other data subjects involved for the consent to the transmission of the data referred to them. Through this mechanism the third data subjects could know about the portability request and consent or object. Although, a system based on the consent of all the data subjects involved requires the implementation of system to enable the exclusion of data in the case of objection.

Furthermore, the implementation of tools to "enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data"[36] might help.

These aspects have a direct bearing on practical and technical application of the right: the "structured, commonly used and machine-readable format" which support

[35] As an example, "when a data subject exercises his or her right to data portability on his or her bank account, since it can contain personal data relating to the purchases and transactions of the account holder but also information relating to transactions, which have been "provided by" other individuals who have transferred money to the account holder. In this context, the rights and freedoms of the third parties are unlikely to be adversely affected in the webmail transmission or the bank account history transmission, if their data are used for the same purpose in each processing, i.e. as a contact address only used by the data subject, or as a history of one of the data subject's bank account. Conversely, their rights and freedoms will not be respected if the new data controller uses the contact directory for marketing purposes".

[36] Article 29 Working Party 2017. The new version is lighter for data controllers: "Additionally, the data controllers should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. if they also want to move their data to some other data controller. Such a situation might arise, for example, with social networks, but it is up to data controllers to decide on the leading practice to follow".

re-use must also take account of this problem. In addition, it should be an opportunity to consider implementing new ways and tools to provide further utility for the end-user.[37]

There has never been a moment in history with so many reports of personal data exposure as the one experienced lately.[38] It seems that the right to data portability may have potential adverse effects on privacy[39] and could lead to a huge and uncontrollable use of data, as an open door for companies.[40] Although the right to data portability is crucial not only for competition among platforms, but also for data protection. In fact, the right to data portability was included in the General Data Protection Regulation as a right of the data subject, in order to enable him to control his data.

The Article 29 Working Party said that it "represents an opportunity to "re-balance" the relationship between data subjects and data controllers"[41] and there are those who believe that the right to data portability "is a stimulus for the IT design community to reflect on how to do […] privacy in a different way" and it "offers an opportunity to make the case for new privacy preserving business models".[42]

With regard to this, it is first important to underline that the exercise of data portability together with the "right to erase"[43] enables users to port data in a new platform and delete the data in the previous one. It reduces consumers' switching costs, improves their data control, can increase the data agents' demand and also helps individuals appreciate the value of personal data. If consumers are free to change between the platforms and they understand the value of the data, they can demand more from the collectors.[44] It is "about empowering users to exercise control and choice over how their data is handled" in order to obtain utility from accessing their data, "disrupt the established business models of platforms locking users in and importantly, to prompt creation of alternative commercial approaches to personal data in the market".[45]

The implementation and the use of "personal information management systems" (PIMS) could be a solution. PIMS are systems that allow individuals to manage their personal data in secure, local or online storage systems; users can permit certain service providers to either access their data from or analyse data in their PIMS. It therefore can be used as a clear point of control over access to the

[37] Urquhart et al. 2018.
[38] ENISA 2018.
[39] Van der Auwermeulen 2017.
[40] Ibid.
[41] Article 29 Working Party 2017.
[42] Urquhart et al. 2018.
[43] Article 17 of the GDPR. Allow me to refer to Martinelli 2017.
[44] Stucker and Grunes 2016, p. 322.
[45] Urquhart et al. 2018.

data.[46] These systems are at an early stage of development and the way they are designed and the underlying business models differ widely, but the objective is to put users in control of their personal information and to serve as an effective and user-friendly mechanism to provide or withdraw consent.[47] In addition, PIMS might be an instrument to facilitate the exercise of the users' right of access, rectification, erasure and right to data portability.

However currently there are many obstacles to overcome: the highly technical nature of the subject and solutions involved, the need to demonstrate the value of use of such technologies to ensure user participation, the lack of consistency used in data formats, the presence of different policies between the platforms involved, the relational nature of the data and the management of the personal data of third-party, the capability of data to be copied, reused and propagated endlessly.[48]

8.4 Non-personal Data and Professional Users: The Proposals of the EU Commission

This section analyses the need to establish the portability of non-personal data and to also grant data portability to professional users that are not natural persons. These problems derive from the definition of personal data and the scope of the GDPR and they also give rise to some thoughts on the relationship between the General Data Protection Regulation and other European legislation and proposals.

The distinction between personal and non-personal data is crucial. If the data are non-personal the problems related to a large share of them through some portability right are significantly different from a huge sharing of personal data. In fact, if data is not personal, there are fewer privacy issues. There is always some concern regarding "group privacy",[49] but it probably needs a different solution beyond the traditional data protection. Despite this, if the data are non-personal it is doubtful whether the GDPR applies, and therefore also the right to data portability as set out in Article 20.

The Article 29 Working Party, in its Guidelines, establishes that the right to data portability applies not only to the data "actively and knowingly provided" by the data subject, but also to the "observed data" provided by the data subject by virtue of the use of the service or device. Anyway, it seems that only personal data belonging to these two categories can be the object of the right of data portability as set out in the GDPR. This is probably one of the reasons for the new proposals by the European Commission, in particular the Regulation on the free flow of data which enables the right to data portability of non-personal data.

---

[46] Ibid.

[47] EDPS 2016b.

[48] Urquhart et al. 2018.

[49] Taylor et al. 2017; Mantelero 2016.

The need of a "free flow of data" is clearly outlined in the European Commission "Proposal for a Regulation on a framework for the free flow of non-personal data",[50] with the objective of unlocking the potential of the data economy. The proposal applies to "non-personal data" and it aims to address three fundamental issues: "1) Improving the mobility of non-personal data across borders in the single market, which is limited today in many Member States by localisation restrictions or legal uncertainty in the market; 2) Ensuring that the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, remain unaffected; and 3) Making it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market".

The third point aims to provide consent to switch service providers and to port data when the user is a professional and data are "electronic data other than personal data". Hence it does not affect the Union data protection legal framework, and in particular the GDPR, but it integrates it. Nevertheless, some concerns have been expressed about the possibility of effectively implementing such a distinction and consequently on the opportunity of introducing new rules on the circulation of data outside the GDPR.[51]

Article 6 of the Proposal, "Porting Data", invites the European Commission to "encourage and facilitate the development of self-regulatory codes of conduct at Union level, in order to define guidelines on best practices in facilitating the switching of providers" and to ensure sufficiently detailed, clear and transparent information before a contract for data storage is entered into. In particular it establishes that the professional users have a right to port the data provided under the contract and that the technical implementation of this right, which must ensure a structured, commonly used and machine-readable format and allow sufficient time for the users to switch or port the data, should be "defined by market players through self-regulation, encouraged and facilitated by the Commission, in the form of Union codes of conduct which may entail model contract terms".[52]

The aim of the Proposal is both to protect professional operators in the use of providers, platforms and cloud services, to avoid the abovementioned lock-in and to enable the "free flow of data"; nevertheless the application is limited to "non-personal data" and the instrument chosen is the code of conduct, encouraged by the European Commission.

A similar aim inspired the new "Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services".[53] This Regulation would apply to "online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website

[50] European Commission 2017b.

[51] EDPS 2018.

[52] Recital 22 of the Proposal for a Regulation.

[53] European Commission 2018a.

users, respectively, that have their place of establishment or residence in the Union and that, through online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services". The aim is to protect business users from providers:

"The growing intermediation of transactions through online intermediation services, fuelled by strong data-driven indirect network effects, lead to an increased dependence of such business users, including micro, small and medium-sized enterprises, on those services in order for them to reach consumers. Given that increasing dependence, the providers of those services often have superior bargaining power, which enables them to effectively behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union".[54]

The core of the proposals is the introduction of a notice period for the modification of terms and conditions, a statement of reason based on objective grounds for suspension and termination, transparency for ranking and differentiated treatment, access to data and internal complaint-handling systems.

In particular, according to the proposed Article 6, regarding "Access to data", providers of online intermediation services "shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services". The description should include scope, nature and conditions of the access and "might refer to general access conditions, rather than an exhaustive identification of actual data, or categories of data, in order to enable business users to understand whether they can use the data to enhance value creation, including by possibly retaining third-party data services".[55] The aim is both to promote transparency and fairness in the use of data and to enable business users to obtain or bargain about the use of data.

Here again, new rules concerning data and professional users would be outside the GDPR, but in this case it is more about transparency and access than about data circulation. It is not yet a data portability right but only a right to know exactly the type of data and process, with a description in the contractual terms. In the opinion of the author, it is relevant for data portability because it is a prerequisite for enabling professional users to negotiate their rights on the data.

Furthermore, also the proposed "Directive on certain aspects concerning contracts for the supply of digital content",[56] even if it does not use the term "data portability", establishes that in case of termination of the contract, concluded

[54] Recital 2 of the proposed Regulation.

[55] Recital 20 of the proposed Regulation.

[56] European Commission 2015. The Directive shall apply "to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data".

between supplier and consumer, "the supplier shall take all measures which could be expected in order to refrain from the use of the counter-performance other than money which the consumer has provided in exchange for the digital content and any other data collected by the supplier in relation to the supply of the digital content including any content provided by the consumer with the exception of the content which has been generated jointly by the consumer and others who continue to make use of the content" (Article 13.2, letter b). Article 16.4, letter b. ("Right to terminate long term contracts") specifies also that "the consumer shall be entitled to retrieve the content without significant inconvenience, in a reasonable time and in a commonly used data format".[57]

If this proposal would be approved the right to data portability will know a new expansion and it would be easier to access, share and re-use data. Nonetheless, the question remains whether the collocation of the new rules outside the GDPR is the best solution. It is obvious that there are fundamental differences between personal and non-personal data and between data referring to a natural person or referring to a professional user who is not also a natural person. When the data are not "anonymous data" and when it is possible to link the data to an identified or identifiable natural person, the level of protection required by the law is higher. However, as described in the previous section, the privacy problem cannot be simply related to the rights of the person who uploads the data on the platform. The dataset charged in the platform by a user, professional or unprofessional, often contains personal data of a third party, to which the GDPR applies.

It is true that the GDPR seems to impact and include more and more areas of law and knowledge, but it is also true that it is the place in which the whole process of data is regulated and subjected to accountability. It would probably be better to integrate it in the GDPR, in order to better coordinate it with the existing rules and avoid the risk of a difficult interpretation and application which can lead to legal uncertainty.

8.5 Provided, Observed and Inferred Data: Regulating New Technology in Uncertain Times

With regard to the scope of the right to data portability, and in particular to the need to protect the rights of the controller, the distinction made by the Article 29 Working Party between provided, observed and inferred data becomes relevant. Provided data are the data "actively and knowingly provided by the data subject".

[57] Article 16.4, letter b, "Right to terminate long term contracts": "the supplier shall provide the consumer with technical means to retrieve all any content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent this data has been retained by the supplier. The consumer shall be entitled to retrieve the content without significant inconvenience, in reasonable time and in a commonly used data format". See also European Parliamentary Research Service 2016.

Observed data are "provided" by the data subject by virtue of the use of the service or the device. Inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". The first category does not present peculiar difficulties, which however can be found in the second and third categories.

The Working Group specifies that "the term 'provided by the data subject' should be interpreted broadly, and only to exclude 'inferred data' and 'derived data', which include personal data that are created by a service provider (for example, algorithmic results)". Thus, the term shall include "personal data that relate to the data subject activity or result from the observation of an individual's behaviour but does not include data resulting from subsequent analysis of that behaviour". All the data "created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability" shall be excluded. It is the writer's opinion that this category shall include also systems of reputation and feedback scores, because "the information referring to a person's reputation or feedback score is related to the data subject, even though this data was not given by the individual, and should therefore fall under the scope of data portability as personal data".[58]

In other words, nearly all data obtained (provided or produced) from data subjects will be "observed" data, while inferred or predicted personal data are "produced" by companies (e.g., through data mining).[59]

The issues that arise with regard to the distinction of these data from the "inferred data" and which data must remain in the sole availability of the data controller in order to safeguard his intellectual property, "particularly avoiding that the intellectual work of a digital service provider (data inferred about consumers, using complex algorithms) could be lawfully disclosed to competitive businesses for free".[60]

It is a limitation to the right to data portability aimed at protecting intellectual property rights which seems not only difficult to apply, but also inadequate for the protection of the interests and needs to which it intends to respond. The "inferred data" are in fact data generated by the data controller on the basis of data already in its possession, but these data can also be personal data. Take, for example, the case of inferred data generated by the algorithmic analysis of data about DNA, which can describe the probability of incurring a disease. It seems that the data subject has the right to access concerning these inferred data but not the right to data portability. Probably this would slow down the migration of data to another data controller, but it would not solve the problem of the protection of the invention behind this inferred data.

[58] Van der Auwermeulen 2017.

[59] De Hert et al. 2018.

[60] Ibid.

The solution, however, can only be found in the new system for the protection of intellectual property concerning algorithms and Big Data, still in the process of early theorising, which should allow a wide circulation of data without compromising the investments, the work and the genius of those who worked there.

Finally, in conclusion, in a changing world, where data portability rights will be essential, it seems necessary to underline three elements which should be always taken into account when developing new rules in the field of data portability.

First, too much regulation might reinforce and confirm existing dominant positions. Therefore, it is essential to module the obligations and the diligence required in relation to the dimensions and concrete technical possibilities of the platform/data controller. Within the scope of the GDPR this might be possible through a flexible interpretation of the "appropriate measures in terms of available technology and costs of implementation". It will be fundamental to take this problem into account when devising new rules.

Second, privacy, competition and contract/consumer law are strictly linked and their analysis, as well as any normative instrument, can only be joint and well correlated. In particular, the right of data portability can be a milestone for competition in order to avoid the risk of a market of platforms dominated by a few actors, which can control both the meeting and the relationship between users and the data and algorithm that govern them. Even if the data portability and a wide interpretation of this right can lead to a huge sharing of data, the effects of the absence of such right could be even worse.

However, it is necessary to find new solutions, such as a new consent-mechanism for an involved third party, in order to apply this new right without totally compromising privacy. Furthermore, the user' possibility to take all the data out from a platform and give it to another one, joined with the right to erase, could represent a new power of the user. If this mechanism of way-out would be effective, it would be possible that users and individuals discover the importance of the data for the platform and maybe they will try to obtain better gains and performances.

Third, the technology evolves fast. This means inevitably that legislators must always keep in mind the need for flexibility in order to allow the legislation to be applied even in a new technological context, but also that the technology itself could be helpful in order to achieve their goals. The implementation of the right to data portability in order to empower data subjects, users and consumers will largely rest in the hands of technicians. Some of these problems require new technical solutions, as new consent mechanism and PIMS, and all the data process and data security shall be reinforced by technical controlled measures which allow user's trust and controls on the procedures of right of data sharing.

References

Article 29 Working Party (2017) Guidelines on the right to data portability. Retrieved from http://www.ec.europa.eu/newsroom/document.cfm?doc_id=44099

Belli L, Zingales N (2017) Platform regulations. How Platforms are Regulated and How They Regulate Us. Off Outcome UN IGF Dyn Coalit Platf Responsib (United Nations Internet Gov Forum). Retrieved from http://bibliotecadigital.fgv.br/dspace/handle/10438/19402

Benkler Y (2006) The Wealth of Networks. How Social Production Transforms Markets and Freedom. Yale University Press, New Haven/London

Boyd DM, Ellison NB (2007) Social network sites: Definition, history, and scholarship. J Comput Commun 13:210–230

Buttarelli G (2017) Privacy matters: updating human rights for the digital society. Priv Secur Med Inf

Colangelo G, Maggiolino M (2017) Big Data, Data Protection and Antitrust in the Wake of the Bunderskartellamt Case Against Facebook. New Front Innov Compet Big Data Case Law 1:104–112

De Hert P, Papakonstantinou V, Malgieri G, et al. (2018) The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Comput Law Secur Rev 34:193–203

EDPS (2014) Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. Preliminary Opinion of the European Data Protection Supervisor. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en

EDPS (2016a) The coherent enforcement of fundamental rights in the age of big data. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/opinions/big-data_en

EDPS (2016b) Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data. Opinion 9/2016. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en

EDPS (2018) Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-framework-free-flow-non-personal-data_en

Engels B (2016) Data portability among online platforms. Internet Policy Rev J internet Regul 5:1–17

ENISA (2018) How Data is Under Siege like Never Before. Retrieved from https://www.enisa.europa.eu/publications/info-notes/how-data-is-under-siege-like-never-before

European Commission (2014a) Towards a thriving data-driven economy. COM(422/2014)

European Commission (2014b) Case M.7217 – Facebook/WhatsApp Commission decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004

European Commission (2015) Proposal for a Directive on certain aspects concerning contracts for the supply of digital goods

European Commission (2016) Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe - COM(2016) 288

European Commission (2017a) Enter the Data Economy. EPSC Strateg Notes 1–16

European Commission (2017b) Proposal for a Regulation on a framework for the free flow of data in the European Union

European Commission (2018a) Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online. COM(2018) 238

European Commission (2018b) Building a European data economy

European Commission (2018c) Study on data sharing between companies in Europe

European Parliamentary Research Service (2016) Contracts for supply of digital content. A legal analysis of the Commission's proposal for a new directive. Retrieved from http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2016)582048
Evans DS, Schmalensee R, Noel MD, et al. (2011) Platform economics: Essays on multi-sided businesses. Compet Policy Int 459
Floridi L (2016) On Human Dignity as a Foundation for the Right to Privacy. Philos Technol 29:307–312
Frank JS (2014) Competition Concerns in Multi-Sided Markets in Mobilr Communication in Drexi J et al. Competition on the Internet 2014
Graef I (2015) Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. Telecomm Policy 39:502–514
Graef I (2016) Blurring boundaries of consumer welfare How to create synergies between competition, consumer and data protection law. In: Personal Data in Competition, Consumer Protection and IP Law: Towards a Holistic Approach? Retrieved from https://ssrn.com/abstract=2881969
Graef I, Verschakelen J, Valcke P (2014) Putting the right to data portability into a competition law perspective. Retrieved from https://ssrn.com/abstract=2416537
Lynskey O (2015) The Foundations of EU Data Protection Law, Oxford University Press
Lynskey O (2017) Aligning data protection rights with competition law remedies? The GDPR right to data portability. Eur Law Rev 42:793–814
Mantelero A (2016) Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Comput Law Secur Rev 32:238–255
Martinelli S (2017) Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale. Giuffrè
Mayer-Schönberger V, Cukier K (2013) Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt
OECD (2013) Exploring the economics of personal data: A survey of methodologies for measuring monetary value. OECD Digit Econ Pap 40
OECD (2014) Data-driven Innovation for Growth and Well-being: Interim Synthesis Report, 86
Resta G (2018) Digital platforms and the law: contested issues. Medialaws 231–248. Retrieved from www.medialaws.eu/wp-content/uploads/2018/02/Resta.pdf
Stucker ME, Grunes AP (2016) Big Data and Competition Policy. Oxford University Press
Taylor L, Floridi L, Sloot B van der (2017) Group Privacy. New Challenges of Data Technologies. Springer
UNESCO (2016) Privacy, free expression and transparency. Redefining their new boundaries in the digital age. Retrieved from www.unesdoc.unesco.org/images/0024/002466/246610e.pdf
Urquhart L, Sailaja N, McAuley D (2018) Realising the right to data portability for the domestic Internet of things. Pers Ubiquitous Comput 22:317–332
Van der Auwermeulen B (2017) How to attribute the right to data portability in Europe: A comparative analysis of legislations. Comput Law Secur Rev 33:57–72
Vanberg AD, Ünver MB (2017) The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? Eur J Law Technol 8:1

Silvia Martinelli graduated in Law at the University of Milan, is a lawyer and a member of the Milan Bar Association and a Ph.D. Candidate from the University of Turin. She is the author of scientific articles and of a book on the right to be forgotten: "Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale", Giuffrè, 2017. She is also Affiliate Scholar at the Information Society Law Center of the University of Milan, a Teaching Assistant ("Cultore della materia") in both Private Law and Legal Informatics, a Member of the Editorial Committee of the Law Reviews "Ciberspazio e Diritto" and "Diritto, Mercato e Tecnologia", a Fellow of the European Law Institute and of the Italian Academy of Internet Code, and a Member of the European Law & Tech Network.