Intersection between the Right to Data Portability within the GDPR and the Sui Generis Database Right

Do the two rights interfere with the free flow of data generated from connected devices?

Jyoti Gogia

Master's Thesis in European and International Trade Law

HARN63

Spring 2021

LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Table of Contents

Abstract

The internet has brought about vast knowledge in the form of "data" to the 21st century. As a part of its digital single market strategy, the European commission has sought to develop a European data economy and consequently the regulation and allocation of data is becoming increasingly important. Both the General Data Protection Regulation ("GDPR") and the Database Directive 96/9 ("DbD") confer rights for certain people who have interest in relation to the data encoded in connected devices. In relation to the GDPR, the right is given to individuals whose personal data is processed and in regards to the DbD the right to exclude others from extracting part(s) of his or her investment made in his or her database. It has come to show that the two rights may not be adequate for the EU data driven economy. The reason for the foregoing is that the two rights overlap or intersect where one can be used to bar the other, which may result in a segmented "data" landscape for the purposes of data aggregation which is crucial for technological developments, artificial intelligence, machine learning and connected devices. The thesis focuses on describing, to what extent the intersection, if any, may lead to a segmented data driven economy and provides recommendations on possible amendments that can be made to mitigate the extent of "clash" of the two rights or alternatively the ways in which the intersection between the two rights may be legally bypassed.

Foreword

I would like to thank the Professors at Lund University for assisting and guiding me throughout the Master's program, "International and European Trade Law." Despite the year 2020/2021 being marked by a pandemic and hardships, the quality, dedication and efforts put into the teaching/curriculum by the faculty at Lund University is commendable! Also, being given the opportunity to act in the capacity of a student representative has made the academic year extra fruitful for me.

I would like to dedicate this thesis to my "Big, small" family of nine, (soon to be ten), namely Kailash Gogia, Kishan Chand Gogia, Yashoda Chhabra, Om Prakash Chhabra, Nirmal Gogia (Chhabra), Chander Gogia, Malin Gogia (Gulati), Tarun Gogia, Vandna Gogia and the little newcomer toddler arriving as a blessing in July/August 2021.

The year 2020/2021, marked by a pandemic and lockdowns (in some countries) has been extraordinary in many ways, for example, by putting to test one's own capabilities, immunity and in many ways ability to stay "rational." We have sat behind our PC's and laptops and figured out ways to go about as "normal," as possible thanks to digitization. Some businesses have thrived and been unaffected by the pandemic, "Zoom" being one of the examples. The foregoing, led me to want to unravel and investigate why this is the case and the answer that I found was, "data" i.e. bits and bytes, binary 0/1 systems etc. Data, an ever important contemporary phenomenon needs to be investigated and exposed, especially from a legal spectrum. This is exactly the reason why I decided to choose the topic or subject matter of my thesis. Happy Reading!

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interfaces
BGH	Bundesgerichtshof (German Federal Supreme Court)
CJEU	Court of Justice of the European Union
DbD	Database Directive
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Right
ISP	Internet Service Provider
ML	Machine Learning
OECD	Organisation for Economic Co-operation and Development
RDF	Raw Data Feed
RtDP	RtDP
SGDR	SGDR
SIS	Satellite Information Services Limited
TFEU	Treaty on the Functioning of the European Union
WP29	Article 29 Data Protection Working Party

1. Introduction

1.1 Background

The internet has brought about vast knowledge in the form of information or in other words, "data" to the 21st century.[1] As a part of its digital single market strategy, the European commission has become committed to developing a European data economy describing data as a "key" source of innovation and growth and therefore effective data regulating regimes should be a priority.[2]

The General Data Protection Regulation (hereafter "GDPR")[3] came into effect on the 25th May 2018 and forms a regulatory innovation within EU law and was enforced by the Commission in efforts to create security and confidence for individuals whose personal data is collected by businesses[4] within the EU digital single market. The right to data portability (hereafter "RtDP") introduced by article 20 of the GDPR is a novel right and allows for individuals to gain control of their personal data *and* enjoy increased choice of service providers by being able to transfer their personal data from one service provider to another without any *hindrance*. The scope of the GDPR is limited to the processing of personal data, hence "*only information relating to a natural person who is identified or identifiable can be subject to a data portability request. Truly anonymous data is excluded."*[5] RtDP facilitates control for the purposes of reuse and may be collected in connected devices for technological developments, as will be outlined in chapter two of this thesis.

[1] Ivan Stepanov 'Introducing a property right over data in the EU: the data producer's right – an evaluation' [2020] 34 IRL 1, Computers & Technology 65, 81.

[2] Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space" (2018) COM 232 final.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ 2 119/1 (General Data Protection Regulation – GDPR)

[4] Businesses are termed controllers in the GDPR.

[5] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1360.

Similarly, within EU law there exists a sui generis database right (hereafter "SGDR") in databases encapsulated within the database directive 96/9[6] (hereafter "DbD") which protects investment made into the creation of databases and is an Intellectual Property Right (hereafter "IPR"). The DbD provides for protection of databases which may contain personal data of these individuals. The DbD goes beyond the level of protection provided by international law with the objective of harmonising the protection of the investment made in databases in all EU member states.

The DbD does not have direct applicability yet it may have direct effect. On the other hand, the GDPR is a binding legislative act which must be applied in its entirety across the EU and has direct effect and is directly applicable in all EU member states. For the foregoing reasons, legislative judgements, decisions and the scope of interpretation remain somewhat disseminated in relation to the DbD among individual member states; however this is not the case in relation to the GDPR due to its legal instrumental capacity. What the two regimes regulate is "data", albeit of different capacities and forms. Data, coined the new prized economic assets of the 21st century,[7] is what new business models compete for in order to survive in the digital market. This is the reason why *de facto* dominant market players such as Google, Amazon and Facebook have been able to rise to such superiority by way of using their users or customers data with algorithms and deploying it to leverage their own market performance and outperform others.[8]

Connected devices including the Internet of Things (hereafter "IoT") generate big data and are profoundly data dependant. In fact, IoT thrive on access to big datasets as indispensable inputs for training algorithms for Machine Learning[9] (hereafter "ML.") The interaction between connected devices and intellectual

[6] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20 (Database Directive – DbD).

[7] Michael Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' [2017] 51 UC Davis Law Review, 65, 133.

[8] Mike Sands 'Customer Data Is the Secret to Silicon Valley's Success.'(2017) Forbes, Accessed April 22, 2021 >https://www.forbes.com/sites/mikesands1/2017/11/29/customerdata-is-the-secret-to-silicon-valleys-success/#135386886c3b>

[9] Bertin Martens,'The impact of data access regimes on artificial intelligence and machine learning' [2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

property plays a vital role as the latter affects the generation, analysis and use of data derived from connected devices.[10]

Without the ability to monetise revenue from the data there would be no incentive to collect them. Justifications for the wide sharing of data may diminish its economic value which is what the RtDP may bring about as controllers are obliged to transfer personal data to another service provider, leading to horizontal competition i.e. within the same industry. As with any IPR, when these are not protected then they can easily be copied by anyone, therefore they require protection and remuneration ought to be given for inventors of such efforts.[11]

1.2 Aim and research question

The purpose of this thesis is to describe and analyse the interfaces and supposed conflicting nature between the RtDP and the SGDR, using the example of data which is collected, generated and transferred by connected devices. Towards the end of the thesis, recommendations backed by scholarly opinions will be discussed and analysed in order to demonstrate how the hypothetical tensions, if any, between the two regimes may potentially be mitigated.

To fulfil the research purpose, the following questions will be answered:

1. Describe the extent to which the RtDP interacts with the SGDR of the database rights holder?
2. To what extent can one prescribe the relevant law to the case of connected devices in a big data setting?
3. Are there any justifications for the amendment to the RtDP or the SGDR in the absence of exclusive rights or do the two legal frameworks result in a segmented data landscape where data aggregation is hard to achieve for the proper functioning connected devices?

[10] Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' [2019] 10 JIPITEC 1, 1.
[11] Bertin Martens,'The impact of data access regimes on artificial intelligence and machine learning' [2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

1.3 Scope and constraints

Interplay within the two data access regimes exists which may either allow for access **to** personal data or it may limit it as a result of measures that give exclusive control to de facto data holders and by market forces that drive access, transfer, trade and pricing of data. Consequently, it is vital to define the legal effect of the data access regimes. Since the GDPR and the topic at hand is fairly novel, there is not a lot precedent that may be referred to which may pose to be a constraint in the analysis of topic of this thesis. Furthermore, there are only a few precedents/cases in relation to the DbD which are referred to within the thesis. The commission has recently announced their incentive to create a digital single market within the EU[12], which, when introduced may allow for further elucidation of the subject matter that is analysed and discussed in the thesis

1.4 Materials and method

To fulfil the purpose of this thesis and to answer the research questions, a legal scientific (dogmatic) method will be applied. Consequently, the methodology will be to (i) describe the concerned rights within the frameworks regulating the RtDP and SGDR, respectively (ii) prescribe how these rights interact with each other and (iii) justify why a supposed change is required so as to mitigate the tension between the two rights within the European data economy. As a part of deploying a legal scientific method, this thesis focuses on primary legislation such as the Treaty of the functioning of the European Union (hereafter "TFEU") secondary legislation (regulations, directives and decisions) derived from the principles and objectives set out in the treaties. EU based legislative actions, in the form of white papers and working party papers and legal literature in the form of journals are used to explain concepts within the regimes. In addition, supplementary sources such as empirical studies, impact assessments, and private initiatives along with public consultations by different private and public entities are referred to.

[12] Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European Data Economy' SWD(2017) 2 final, 47.

1.5 Structure

Chapter two introduces the importance of data in the new digital economy and fleshes out the economic incentives of data collection. Connected devices which generate big data are elucidated and concepts such as machine learning, artificial intelligence, the Internet of Things are explained and the role that data plays for their proper functioning. Economic concepts such as economies of scope and economies of scale are explained to demonstrate the effect that data has from a financial stance. Big market players collecting data leading to competition between these firms and other aspects are explained to set the scene for the legislation that revolves data and how it impacts the free flow of data.

Chapter three sheds light on the GDPR and the RtDP and the prerequisites for the right to be invoked. The constituents of the conditions for the right are thoroughly examined in light of connected devices. In the discussion part of the chapter, scholar's opinions are discussed as to the interpretation of the RtDP and if there are any exceptions to it.

Chapter four introduces the SGDR enshrined within the DbD and the prerequisites for the right to be invoked. The constituents of the conditions for the right are thoroughly examined in light of connected devices which generate big data. Case law and judgements are thoroughly examined and compared to establish the elements present which comprise of the right to exclude others from copying the database maker's database. In the discussion part of the essay scholars opinions are discussed as to the interpretation of the SGDR and if there are any exceptions to it.

Chapter five examines the possible intersections between the RtDP and SGDR and which steps lead to the unlawful extraction of the databases. The chapter also discusses the potential claims that each rights holder may present in a case of their rights being infringed up against or vis-a-vis each other as a result of the RtDP being invoked. The chapter provides recommendations on how the potential or supposed rights may be reconciled for the free flow of data and innovative strategies.

2. Data and connected devices

2.1 Introduction

Data which is the very groundwork of the modern digital economy has been termed as "*the new oil*" in financial jargon owing to its resource like properties.[13] Prior to digitization information in the form of data took many formats. *"Text and figures were written on paper, sound recorded on a magnetic tape, pictures on a silver-coated transparent plastic tape, etc."*[14] Then, it was costly to store, process or transfer data and defining data ownership rights had little to no meaning as accessing forms of personal and company data was very costly and difficult. The protection of these privacy rights did not come into much play either. Due to the advancements of digital technology, the value of data has come to be seen in a totally different light. Interoperability costs have reduced a lot as a result of the universal digital (binary 0/1) data format carried via electronic means. Data can now be captured, stored processed and transmitted at a very low cost which in turn has led to massive quantities of data termed "big data" being transferred to digital information environments.[15] Furthermore, governments within the EU are seeking to make their cities into "smart cities" which are a result of superfast telecoms networks, electrification, artificial intelligence, IoT and digital payments. The interconnecting key elements of smart cities are connected devices networks in the form of sensors attached to real world objects such as roads, cars, electricity meters, domestic appliances and human medical implants which connect these objects to digital networks i.e. the IoT, "ubiquitous computing."[16]

2.1.1 Types of data

Connected devices encompass smart devices which generate big data and transmit that data trough wireless or wired communication such as the everyday appliances

[13]Michael Haupt, 'Data is the New Oil' – A Ludacris Proposition." [2016] >https://medium.com/project-2030/data-is-the-new-oil-a-ludicrousproposition-1d91bba4f294> Blog. Accessed March 27, 2021.
[14] Martens Bertin,'The impact of data access regimes on artificial intelligence and machine learning'[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).
[15] Ibid.
[16] Charlotte A Tschider, 'Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age' [2018] 96 Denv L Rev 87.

that we use including 5G networks, computers, tablets and smartphones. The data which is generated, stored and communicated through the use of these devices to a very large extent is influenced by human behaviour patterns. The form in which the data is collected and generated through the use of these devices is in its absolute "raw" form. Thereafter it is analysed and may, but is not limited to taking the form of datasets in databases. These smart devices or smart appliances do not function autonomously; rather they rely on data which they receive through other connected devices through non-wired and wired methods. Hence, *"autonomous" or "smart devices will often make use of data analytics, machine-learning and artificial intelligence."*[17] Thus, these smart connected devices do not autonomously produce "raw data" about personal behaviour patterns of any said individual. Furthermore, connected devices are not limited to those that communicate autonomously through the Internet of Things.[18]

Devices used by humans for the purpose of communication, such as PCs, tablets and smartphones, are equally covered, because it is not relevant to which extent data is stored or processed by the device with or without being influenced by the decisions of a natural person. We established that "data" may take many forms and it is through analysing the data that we involve more persons to reap fruit from the legal rights, obligations that come with these "forms" of raw data, datasets which will likely be encoded in databases, software or other constituent components of the connected device.

On a sematic level the personal data that has been encoded in a database in its pure or in its raw form i.e. bits and bytes remains unaffected. The GDPR on the other hand sets obligations as to what can and cannot be done with this personal data. Josef Drexl, in his study unravels the rights related to data and discusses whether an "ownership-like" right in personam or rem can be transcribed to parties who may have interests in the data.

[17]Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[18] Sylvia Zhang, 'Who Owns the Data Generated by Your Smart Car'[2018]32HJL&Tech299.

It is acknowledged that the closest that regulatory law has come to data ownership[19] is the DbD which establishes exclusivity rights for "databases", albeit with some prerequisites and exceptions. With the advancements of ML and AI which crave enormous amounts of data another question which needs to be answered is whether the current data access regimes allow for the innovation in the AI- driven technological world.[20]

2.1.2 Data and the rights vested therein

Both the GDPR and the DbD regulate the flow of data and thereby confer rights and obligations for certain persons. Each legal right that these rights holders possess relate to a corresponding legal obligation imposed on others. The RtDP confers a right for an individual to switch between controllers i.e. service providers at the individual's request.

The SGDR confers the right upon the database holder who makes a substantial investment in *verifying, obtaining or presenting* the contents of the database to prevent others from extracting or reusing part(s) of their database. Therefore, one may deduce that RtDP is a positive right i.e. it allows for an individual or data subject to take a certain action whereas the SGDR allows the database holder to preclude or prevent others from taking an action i.e. extracting part(s) of their database. In the case of intellectual property an exclusive right is given to the creators or inventors their works. In the case of the GDPR this is a right given to individuals seeing that there was a pressing need to do so in the wake of big data generation by for example connect devices.

2.2 Competition law and economic justifications for data

2.2.1 Introduction

Other aspects of the law, besides GDPR and SGDR considerations which touch upon "data" is competition law related to anti-competitive behaviour by big data firms. Articles 101 and 102 of the Treaty of the Functioning of the European Union (hereafter "TFEU") regulate anti-competitive practices within the EU. In

[19] Martens Bertin,'The impact of data access regimes on artificial intelligence and machine learning'[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).
[20] Josef Drexl et al, 'Position Statement of the Max Planck Institute for Innovation on the European Commission's "Public Consultation on Building the European Data Economy"' [2017] Max Planck Institute for Innovation & Competition Research Paper No. 17-08.

order to minimise abuse of dominance which leads to anti-competitive behaviour the Court of Justice of the European Union (hereafter "CJEU") has ruled that data holders could be obliged to allow data access under the requirements set out by the law.[21]

Data or "information", allows users or consumers on the digital market to make informed choices or transactions, but *de facto* data does not have any value in itself. Digital data affects transaction patterns and thereby prompts shifts within the economic value chain. So for example, in relation to digital car data, aftersales of a car are always affected by receiving access to the car data itself. Hence, there is a vertical relationship between the upstream data markets and downstream markets for transactions in goods and services: changes in access and conditions in the upstream market will affect the downstream market.[22]

From a competition law or market perspective, for businesses operating online this has led to competitive strategies being put in place between sellers which in turn lowers prices of goods and services which triggers positive and negative effects throughout society.[23] Economies of scope within the digital market occurs where businesses provide free services in return for collecting consumer behaviour patterns online which can later be monetised by showing ads to users, for example. The economic incentive of doing so is that the market value of individual personal data is very low compared to the consumer surplus value of the free service they receive in return from the data aggregator also known as economics of scope, mentioned below. The marginal cost of additional use of the algorithms are lowered where movements are made into making the connected device function more efficiently leading to economies of scale in ML.[24]

2.2.2 Economies of scale

Artificial intelligence and Machine learning mechanisms thrive on access to (big) datasets as necessary inputs for training algorithms. ML has changed the

[21] Case T-17/21 Miquel y Costas & Miquel v EUIPO (Pure Hemp) *OJ C72, 1.3.2021.*

[22] Bertin Martens 'An economic policy perspective on online platforms' [2016] JRC Digital Economy working paper 2016-05.

[23] Bertin Martens, 'What does economic research tell us about cross-border e-commerce in the EU Digital Single Market?' [2013] No 2013-05, JRC Working Papers on Digital Economy, Joint Research Centre.

[24] Bertin Martens,'The impact of data access regimes on artificial intelligence and machine learning'[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

production process for innovative data driven ideas and therefore ensuring access, and transfer to (personal) data becomes an important issue for promoting innovation. ML is a statistical technique and their closest and best estimates are dependent on the large size of the datasets generated by connected devices. For example, in IoT and/or connected devices several variables may be present in the large datasets and therefore it is crucial that robust predictions are generated to diminish the existence of any errors. ML requires larger datasets than humans need in order to learn as it requires thousands or millions of observations to learn some basic responses in contrast to humans who may only need a few observations. For example, *"a self-driving car algorithm can handle most traffic situations after having learned to drive from millions of kilometres of data inputs; a human driver only needs a few thousand kilometres of experience to become a proficient driver."*[25] The algorithm is able to comprehend millions of kilometres of data input in a shorter timespan in comparison to a human driver who needs to learn only several kilometres to learn to drive. Likewise the algorithm can drive many cars at the same time; a human driver can only drive one car at a time. Hence, investing in high quality datasets transmitted by connected devices for the purposes of training ML algorithms is expensive yet once trained the marginal cost of additional use of the algorithms have shown to be low which leads to economies of scale in ML.[26]

2.2.3 Economies of scope

When merging two or more datasets economies of scope transpires where the benefits of using a combined dataset is higher than using each dataset separately.[27] These datasets need not be completely separable; instead they should complement each other. For instance, web surfing data may produce insights on consumer behaviour and therefore combining these with mobile phone data may produce more insights, compared to studying both datasets separately. Some business models of aggregators merge data from various sources into a single consistent dataset which may for example allow for targeted advertisement such as in the

[25] Bertin Martens,'The impact of data access regimes on artificial intelligence and machine learning'[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

[26] Bertin Martens,'The impact of data access regimes on artificial intelligence and machine learning'[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

[27] Bergemann et al, 'Markets for data' [2012] >https://economicdynamics.org/meetpapers/2012/paper_538.pdf> Accessed 12 April.

example of combining consumer behaviour data with the content they view online. For example, individual car data on driving performance is valuable alone for insurance and maintenance purposes and there is no need to aggregate that data with other cars data. On the other hand, car navigation data needs to be aggregated by a navigation service provider in order to identify traffic jams and send this information back to drivers. All the data produced in abundance here is thanks to connected devices. There are considerable economies of scope in the aggregation compared to the marginal value of each individual car navigation dataset.[28] It is the ML that aggregates such data through trained knowledge of algorithms. [29] A similar conclusion can be drawn in the case of connected devices where the connected devices producing large datasets make use of ML that aggregates such data to improve the accuracy of the connected devices functioning leading to the devices' optimal performance. There are considerable economies of scope in the aggregation compared to the marginal value of each individual dataset.[30] These datasets may be encoded within software(s) of a connected device which *may* be protected by the SGDR under the DbD.

The RtDP i.e. *"the ability to move, copy or transfer data*"[31] is one of the instruments dictating control over data by an individual. As mentioned above, data can be seen as the "*new money*" so therefore it is important to weigh in the benefits of regulatory intervention regimes and how this affects the sharing, transfer, and trading of data. Now that it is established that the abundance of data generation and collection is shaping the livelihoods of our present and future, it is crucial to understand the legal basis of access, storage and transmission to third parties.

[28] Bergemann et al, 'Markets for data' [2012] >https://economicdynamics.org/meetpapers/2012/paper_538.pdf> Accessed 15 April.

[29] Bertin Martens,"The impact of data access regimes on artificial intelligence and machine learning"[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).

[30] Bergemann et al, 'Markets for data' [2012] >https://economicdynamics.org/meetpapers/2012/paper_538.pdf> Accessed 12 April.

[31] Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European Data Economy' SWD(2017) 2 final, 47.

2.3 Discussion and summary

The *sine qua non* of the EU Data Economy is determined to be "data" which constitutes the very foundation for overflow of information in the digital economy. The interaction between connected devices and intellectual property plays a vital role as the latter affects the generation, analysis and use of data derived from connected devices. Without the ability to monetise revenue from the data, there is no incentive to collect data. Justifications for the wide sharing of data may diminish its economic value from an IP perspective, yet it may allow for improvements of IoT devices or connected devices and for the furtherance or improvement of ML purposes. The conclusions that are drawn are that connected devices including the Internet of Things generate big data and are profoundly data dependant. Access to big datasets is an indispensable for the purposes of inputs for training algorithms for ML. Smart connected devices do not autonomously produce "*raw data*" about personal behaviour patterns of any said individual. These data are analysed by machines since ML and AI make use of statistical techniques and their closest and best estimates are dependent on the large size of the datasets generated by connected devices. In connected devices several variables may be present in the large datasets and therefore it is crucial that robust predictions are generated to diminish the existence of any errors. The larger the dataset the closer the prediction will be leading to better accuracy for user experiences and the functioning of devices.

Other aspects of the law, besides GDPR and SGDR considerations which touch upon "data" are competition law related to anti-competitive behaviour by big data firms. Articles 101 and 102 of the Treaty of the Functioning of the European Union regulate anti-competitive practices within the EU. In order to minimise abuse of dominance which leads to anti-competitive behaviour the Court of CJEU has ruled that data holders could be obliged to allow data access under the requirements set out by the law. The next chapter discusses the requirement of data processing by controllers under the GDPR and the RtDP.

3. The right to data portability within the GDPR

3.1 Introduction

The digital market has given rise to a new world of possibilities for data collection, processing, storage, sharing and analysis.[32] Legal uncertainty within the digital market most certainly leads to reduced competition along with customer security and privacy being exposed to potential breaches. As a result of individual privacy and security concerns, the GDPR was introduced as an attempt to restore individual confidence online.[33] The GDPR lays an obligation on data controllers to store personal data in a manner which does not go beyond necessity.[34] The rights of the data subject were developed with the right to erasure[35] and the RtDP.[36] These rights are not absolute rights, subject to third party interests.[37] The background and adoption of the GDPR was based on the individual's right from denying controllers the possibility to misuse or mismanage their personal data. The OECD Privacy Experts[38] are of the view that challenges to traditional personal privacy principles in the current data environment are ever more pertinent due to the introduction of connected devices and these complications are intensified which leads to the deterioration of individual security and privacy rights.

[32]Commission, 'Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data' (Commission Staff Working Paper) SEC(2012)72 final 7.

[33] Communication from the Commission to the European Parliament and the Council 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' {SWD(2020) 115 final}.

[34]GDPR article 5.

[35]GDPR article 17.

[36]GDPR article 20.

[37]GDPR article 20(4).

[38]Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking [2014], Available at >https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en> Accessed 24 May 2021.

The basis of the introduction of the GDPR lies in the EU Charter of Fundamental Rights [hereinafter the Charter] article 8(1) which expresses that *"everyone has the right to the protection of personal data."* The qualifying right mentions within article 8(2) that *"such data must be processed fairly for specified purposes.*"[39] Finally, article 8(3) states that *"compliance with these rules shall be subject to control by an independent authority."* Supervisory authority is mentioned in article 51 of the GDPR "*responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.*" The Working Party (WP29)[40] has published draft guidelines clarifying the conditions under which the RtDP is applicable.[41] The introduction of the RtDP came about so as to enable users to switch services provided by controllers easily, with the domino affect that this may generate competition between service providers.

3.2 Scope of the right to data portability and prerequisites therein

3.2.1 Introduction

Article 20 of the GDPR specifies: "*The data subject shall have the right 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"* In other words, the scope of the RtDP is two-folded: (i) a right to receive and transfer personal data[42] (indirect portability), and (ii) a right to have it transmitted directly from one controller to another[43] (direct portability), "*without hindrance.*"

Article 20(3) specifies that the RtDP is *"without prejudice to the right of erasure"* and thus the personal information about the data subject may remain with the original controller after the RtDP request is made. This is, however unlikely since the GDPR is founded on seven core principles of which one stipulates that the

[39] GDPR articles 5(1) (a), (b).
[40] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).
[41] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).
[42] GDPR article 20(1).
[43] GDPR article 20(2).

controller shall only keep the information about the data subject only if necessary as per the principle(s)[44] of data minimisation.[45] The requirement of the data being in a "*machine-readable*" format cannot be underestimated as the RtDP *"should not create an obligation for controllers to adopt or maintain processing systems which are technically compatible"* as per recital 68 of the GDPR. This may prompt the controller to anonymise the raw data which may limit the data subject's RtDP. Article 20(4) provides that the above rights are qualifying rights and these should not limit the "*interests of third parties.*" Furthermore, the RtDP as per the same provision only applies to data that is processed by *automated*[46] means and thus precludes data collected manually, including hand-written notes.

Before the RtDP can be exercised by the data subject the grounds for data processing must be satisfied pursuant to article 6 of the GDPR. Processing thus needs to be based on consent[47] or on a contract[48] or data processed on any other legal ground including legitimate interest under article 6(1)(f) of the GDPR. The exception here for the data processing is the other grounds than legitimate interest.[49] Then, are controllers able to prevent data subjects from relying on the RtDP by invoking a legitimate interest as a ground for processing personal data? Article 20(3) and even recital 68 of the GDPR respectively, exclude portability of data when 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 controller."*

3.2.2 The data has to be "personal data"

The RtDP consists of two main elements: Firstly, the right to obtain a copy of data, and secondly the right to transmit data to another controller provided that they do not limit the interests of third parties. The GDPR article 4(1) consists of broad list of factors specific to "*personal data*". Within the article "*personal data*" is defined as "*any information relating to an identified or identifiable natural person"* or the "*data subject"*. Any data which is anonymous may be rejected for

[44] GDPR article 5.

[45] GDPR article 5. (The other principles are (1) lawfulness, fairness and transparency (2) purpose limitation (3) accuracy (4) storage limitation (5) integrity and confidentiality).

[46]GDPR article 20(1)(b).

[47]GDPR article 6(1)(a).

[48]GDPR article 6(1)(b).

[49]GDPR article 6(1)(f).

a portability request; however this does not preclude pseudonymous data[50]. An "*identifiable natural person*" is a person who *"can be identified, directly or indirectly"*. Not only name and ID are characterised as "personal identifiers" but *"location data, an online identifier or (...) factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity"* are also classified as personal data. In addition articles 4(13)-(15) of the GDPR mentions genetic data; (ii) biometric data; and (iii) data concerning health are also included in the list of personal data. Since the foregoing list is somewhat exhaustive, recital 26 of the GDPR specifies that in determining whether data falls in the category of personal data a "*test of reasonable likelihood of identification"* ought to be applied.[51] The cost and the amount of time required for identification is a matter to be considered in determining whether a person is identifiable. [52] In a CJEU case, it has been established that an IP address can be classified as "personal data" from an Internet Service Provider's (hereafter "ISP")[53] for the purposes of the GDPR. Therefore, a data controller is obliged to port or provide the access to the "data" at the request if the data subject.

Lastly, as per the GDPR, only personal data, relating to a natural person who is identified or identifiable can be subject to a data portability request. Anonymous data is excluded. Pursuant to article 11(1) of the GDPR data controllers are not required to maintain data in an identifiable form for the purposes of meeting a portability requests. When read together, articles 20 and 11 GDPR may motivate controllers to opt for processing pseudonimysed datasets so as to avoid the obligations of data portability when they are unwilling to share for the purposes of sharing their datasets. As specified in article 11(2) GDPR, when data is pseudonymous, data controllers are not obliged to re-identify, *unless* the data subject *"provides additional information enabling his or her identification"* which is likely to be the case in a portability request.

[50]GDPR article 11(2).

[51]Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) LIT 40, 44.

[52] GDPR Recital 26.

[53] Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771 para 51.

3.2.3 The data has to be "provided to the controller"

Controllers may only port data that has been "*provided to the controller"* pursuant to article 20(1) of the GDPR. The GDPR does not provide an explanation as to the meaning of *"provided*" and thus, this provision is subject to interpretation. The interpretation includes all data processed by the controller on the grounds of contract or consent to which the data subject has agreed. According to the WP29, "*provided data*" is "*data actively and knowingly provided by the data subject*" and "*observed data provided by the data subject by virtue of the use of the service or the device*."[54] WP29 is of the view that "*provided*" data should be limited to certain constraints and that personal data should preclude personal data that has been "*inferred*" and "*derived".*[55] Health assessments and credit scores are "*created*" by the controller by for example an "*analysis*" of data and therefore the data subject has not themselves "*provided*" such data. In short, "*provided by*" should not include subsequent analysis of the first observance of data subject activity.

The OECD privacy experts[56] distinguished between data that is provided, observed, derived, and inferred. The difference between derived and inferred is that data is derived and created in a *"mechanical"* way *"to detect patterns . . . and create classifications*" in a manner "*not based on probabilistic reasoning*," while inferred data is "*product of probability-based analytic processes*." The distinction and fine line between the data that is inferred, derived and provided may make it difficult for data subjects to invoke their RtDP. The extent of controller involvement into the "alteration" of the raw personal data is unclear from what has been communicated by the OECD and WP29.

3.2.4 Processing by means of contract or consent

Article 20(1)(a) specifies the conditions under which information should be supplied to the data subject: [When] "*the processing is based on consent pursuant to point (a) of article 6(1) or point (a) of article 9(2) or on a contract pursuant to*

[54] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 10.

[55] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 10.

[56] Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking [2014], available at >https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en> Accessed 14 May 2021.

point (b) of article 6(1).” If the data has been shared under contract or consent of the data subject then it is covered by the data portability requirement. Article 4(11) of the GDPR defines consent as “*any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”* The previous definition and criteria of consent is also dependant on the lawful ground of processing as stated within article 6 of the GDPR. The WP29[57] stated that the data subject should be able to withdraw their consent as freely as they have provided it. Where data is collected by automated means or by sensors, issues related to processing grounds and consent are intensified.

3.2.5 Right to data portability and the rights and freedoms of others

The RtDP is subject to limitations in the interests of third parties as laid down in article 20(4) GDPR. These could be data protection rights of other platform users[58] but also IP rights, rights of others, and more. It can be deduced that the RtDP is closely linked to the right of access. A limitation to the right of access under article 15(4) of the GDPR is stated within recital 63 *“A data subject should have the right of access . . . and to exercise that right easily and at reasonable* intervals… *That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.”* The interplay between IP and the RtDP will be discussed further in chapter five of this thesis. The WP29 comments about the foregoing recital in a manner which is unclear as to the limits and scope of releasing information by data controller that may be protected by IP to the data subject. Thus, they merely state that data controllers may transfer the personal data “in a form” that does not infringe any IP right.[59]

[57] WP29 Data Protection Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017.

[58] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 12.

[59] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).

3.3 The "provided to the controller" criteria in connected devices

3.3.1 Introduction

Likewise, data comprising of "*personal data"* under the GDPR is comprehensive. Within connected devices, any personal data may be a part of collection of independent materials since data may be useful for the attainment of the database separately[60] and also in the combination of datasets.[61] Therefore, the dataset independently and combined or both can contain personal and non-personal data.

One needs to assess that "*personal data provided by the data subject"* as a condition of the RtDP under the GDPR is satisfied. The gap appears within this part of the analysis in that the connected device "*observes"* the data and thus the data is not "provided" by the data subjects. Drexl[62] argues that *"observed"* data that is collected from the user of a connected device should be covered as data "*provided by the data subjec*t" and thus this requirement within the GDPR should be interpreted broadly.[63] "*One may argue that limiting the RtDP to "provided data," as opposed to data that is "derived" or "inferred", is a result of regulatory balancing of a data protection right and the IP rights conducted by the legislator."*[64]

The scope of the RtDP is limited since it has been established that still, the RtDP provision does not apply to "*inferred"* or *"derived"* data which is generated through additional steps of data analyses for example for ML purposes.[65]

---

[60]Herbert Zech, 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 (6) JIPLP 460, 467.

[61]Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[62] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[63] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[64] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1374

[65] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016). At 12.

3.4 Discussion and summary

The RtDP allows for innovation through its free flow of data as switching between service providers. The scope of the RtDP is two-folded: (i) a right to receive and transfer personal data[66] (indirect portability), and (ii) a right to have it transmitted directly from one controller to another[67] (direct portability). The data subject is allowed port the data to another controller in a *"structured, commonly used and machine-readable"* format.[68] The WP29 has in their executive summary stated that the RtDP is closely related to the right to *access* under article 15 of the GDPR where the former may only be invoked by the data subject in limited circumstances.[69] Drexl agrees to the pervious account of the close proximity of the data access right (article 15) and the RtDP (article 20).[70] Article 20 can be invoked only in relation to the data being *"provided"* by the data subject to the controller, and only when processing is *automated*[71] and based on *consent*[72] or on a *contrac*t.[73] Hence, data control, sharing and reuse describe RtDP in the best possible manner and enables free flow of data among controllers. RtDP should be considered as a tool of access which allows individuals to switch when access to data is crucial for competition.[74] The RtDP aspect of granting "control" over data has been under scrutiny by scholars since the inception of the GDPR. [75]

Further, recital 68 of the GDPR, states that the right should *"further strengthen [data subjects] control*" over their personal data. Inge Graef et al concur that the RtDP may not belong within the scope of the fundamental right to data protection and ought to be perceived as a tool to stimulate competition and innovation.[76]

---

[66] GDPR article 20(1).

[67] GDPR article 20(2).

[68] GDPR article 20.

[69] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016). At 10

[70] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[71] GDPR article 20(1)(b).

[72] GDPR article 6(1)(a), 9(2)(a).

[73] GDPR article 6(1)(b).

[74] Josef Drexl, 'Designing Competitive Markets for Industrial Data — Between Propertisation and Access,' [2017] 8 JIPITEC 257, 286, para. 155.

[75] Lucio Scudiero, 'Bringing Your Data Everywhere: A Legal Reading Of the Right To Portability' [2017]3 EDPLR, 127.

[76] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1357.

WP29 notes that *"[t]he primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem.*"[77] As per WP29 and other than preventing service lock-ins, the RtDP *"[i]n essence . . . is expected to foster opportunities for innovation and sharing of personal data between data controller . . . under the data subject's control."*[78] The emphasis on data sharing and reuse is reinforced by the requirement for the format of transmitted data and in accordance with article 20(1) GDPR, it has to be *"structured, commonly used and machine-readable,"* aiming to produce interoperable systems.[79]

WP29 suggests the use of Application Programming Interfaces ("APIs") would enable automated data portability[80] and allow businesses in assisting individuals with their data management. It would also capitalise on reuse of personal data collected by others as the use of APIs "*would enable individuals to make requests for their personal data via their own or third-party software or grant permission for others to so do on their behalf (including another data controller.)"*[81] This would then have the effect of preventing lock-ins and promoting innovation by reuse.

Article 20(4) of the GDPR specifies that the RtDP "*hall not affect the rights and freedoms of others*," which paves the way for uncertainty as to the breach of the RtDP. In the data controllers defence, they could argue that the refusal of switching to another data controller "*affects the rights and freedoms of others*". Who these "other" people consist of is undefined, yet recital 63 provides that this may include IP rights holders, which will be further elucidated in below.

The RtDP does not only act as a compliance instrument but also incentivises firms to set up a business strategy which allows for data creation and reuse. Albeit, the RtDP's introduction lies in *"improving access to privately held personal data,*

[77]WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 4.
[78] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 5.
[79] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 5.
[80]WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 5.
[81]WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 5.

access to data through portability has a flip side for the addressees—the private parties collecting, analysing, and trading in the data."[82]

[82]Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1375

4. The sui generis database right

4.1 Introduction

The Database Directive 96/9 introduced a database-specific SGDR deriving from the Scandinavian *catalogue* protection rights.[83] Within the DbD two provisions; a copyright[84] (individual data protection) and a SGDR[85] which protects the structure and the investment made in the databases creation. As opposed to the Copyright protection, the SDGR does not require any intellectual creativity in the making of the database by the rights holder. Instead the investment in the making of the database is protected within the SGDR. Both the copyright and the SGDR work in conjunction with each other and preclude free-riding on someone else's investment of the creation of a database. The SGDR came about as a result of the need to incentivize the production of databases[86] besides the harmonization of national laws on the copyright protection of original databases.[87] The SGDR also provides an additional layer of protection to the producers of the database.[88]

The SDGR derives from the common law doctrine of sweat of the brow[89]which stipulates that a creator of a work may reap the benefits of one's own work without any requirement of creativity. It is contentious whether mechanical and automated creations which are generated by ML would reap the fruit of the investments made into the creation of databases. The "sui generis right" which is latin for "*one of its kind or unique"* prevents the unauthorised substantial use of database contents so long as the producers have made a "s*ubstantial investment in obtaining, verifying or presenting the contents of the database."*

[83]Case C-203/02 *British Horseracing Board Ltd and others v William Hill Organization Ltd* [2004] ECLI:EU:C:2004:695, para 36.

[84] DbD article 3.

[85] DbD article 7.

[86] DbD recital 12.

[87] DbD recital 2.

[88] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report).

[89]Mark Schneider, 'The European Union Database Directive.' [1998]13 *Berkeley Technology Law Journal 1*, 551–564.

The Dbd was enacted as an attempt to promote the creation of databases within the European Union. For the purposes of minimising disparities between member states of the European Union, the law was enacted to harmonise the protection of databases. However, important to note is that as a result of the legal capacity of the directive Member State's courts decisions are not harmonised and therefore the judgements within this chapter of the thesis will include decisions of EU member state courts along with preliminary rulings from the CJEU under 267 of TFEU. In one seminal case revolving the database right it was stated that "*the Directive should serve as a yardstick for the interpretation of national law, even in those Member States which had similar provisions before the Directive was adopted".* [90]

4.2 Scope of the sui generis database right and the prerequisites therein

4.2.1 Introduction

The SGDR is an automatic right which subsists once the database exists in a recorded form. The right lasts for 15 years from the end of the year in which the making of the database was completed and can be renewed once every 15 years so long as a new considerable investment is made in the database. Protection commences 15 years from the end of the year in which the database was first made available to the public.[91] The right does not require any intellectual creation or originality. It does however grant one of the strongest forms of protection given to an IP creation.[92] Scholars argue that it may be "*one of the least deserving subject matters*"[93] which is protected as an IP right. A database right protects the collection of data, not its constituent elements which may or may not be protected in their own right independently from any protection afforded to the database as a whole. Any software which is used in the making or setup of a database is explicitly excluded from protection as a database, being protected by copyright as a literary work. Still, as software is frequently developed in modular form, it is

[90]Case C-203/02 *British Horseracing Board Ltd and others v William Hill Organization Ltd* [2004] ECLI:EU:C:2004:695, para 36

[91] DbD article 10(1).

[92]AKC Koo, "Database Right Decoded" [2009] EIPR, Vol. 7, pp. 313-319, 2010 , Available at SSRN: https://ssrn.com/abstract=1470676

[93]AKC Koo, "Database Right Decoded" [2009] EIPR, Vol. 7, pp. 313-319, 2010 , Available at SSRN: https://ssrn.com/abstract=1470676

still possible that in some rare cases a collection of software modules may be protected as a database. Also, some elements of a computer program (for example, on screen look up tables which users may search in order to find information) may constitute a database.[94] SGDR protects databases which are a result of substantial investment in the collection, verification, or presentation of its data.[95] These include datasets which are collected or cleaned, such as collections of user reviews and preferences. The investment amount varies within the EU member states. Investments amounting to 4,000 EUR have sufficed in some countries.[96] The right may be overridden where the use of the part(s) of the database is "*grounds of private use, non-commercial teaching and research, public security, and administrative or judicial procedure*."[97]

4.2.2 Defining the database

The SGDR is envisaged in article 1(2) of the DbD which defines a database as "*a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means."*[98] The definition lays more emphasis on the function rather than the form of the database by allowing for its subsequent search and retrieval. In order for the databases retrieval to occur the contents needs to be structured in a methodological way and comprise of constituent elements which are independent of each other. They should be retrievable without losing their intrinsic and autonomous value upon retrieval. In the CJEU case of Fixtures Marketing Ltd v Organismos Prognostikon Agonon Podosfairou AE (OPAP)[99] it was held that a football fixture list amounted to a database as the constituent data had individual inherent value as they could be separated based on dates, title, team members to interested parties. AG Stix-Hackl has indicated that a search engines that sorts and

[94]Terry Sanks, 'Database Protection: National and International Attempts to Provide Legal Protection for Databases,' [1998] 25FSULR4, 1003.
[95] DbD article 7.
[96] Martin Husovec,'The End of (Meta) Search Engines in Europe?' [2014]14Chicago-Kent JIP1, 145-172.
[97] DbD article 9.
[98]DbD article 1(2).
[99] Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou [2004] ECLI:EU:C:2004:697(OPAP).

indexes data will suffice the systematic or methodical requirement.[100] Simple structures like XML or PDF are categorized as a database in the case law.[101]

4.2.3 Investment made in "obtaining, verifying and presenting"

Pursuant to article 7(1) DbD, the SGDR is vested in the database maker, i.e. "*the person who takes the initiative and the risk of investing"* (excluding subcontractors).[102] Protection is afforded in the database whose database maker is able to prove that that there has been "*qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.*"[103] In a seminal case i.e. British Horseracing Board v William Hill,[104] the CJEU clarified the scope of the *"investment made in the verification, obtainment and presentation of a part(s) of database"* criteria under the directive. The case concerned a horseracing database which was maintained by the British Horseracing Board (BHB) comprising of information in relation to owners, trainers, jockeys, horses and records of the performances in each race. Thus, the database contained essential information for the purposes of those who were involved in the horseracing and also radio and telephone broadcasters. The investment made in maintaining the database amounted to about £4 million per annum. Racing pages authorise the Satellite Information Services Limited ("SIS") to transmit data to its own subscribers in the form of a "raw data feed" ("RDF"). The RDF includes a large amount of information, including the names of the horses, names of jockeys, the saddle cloth numbers and the weight for each horse. William Hill who was a subscriber to the SIS displayed a small, specific amount of information from BHB's database on its website. BHB brought an action, alleging that William Hill's use of the information infringed BHB's database right.

[100]Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou [2004] ECLI:EU:C:2004:697), (OPAP) Opinion of AG Stix-Hackl, para 40.

[101]Technomed Ltd. v. Bluecrest Health Screening Ltd. [2017] EWHC (Ch) 2142 [75]

[102] DbD recital 41.

[103] DbD article 7(1),

[104] Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd [2004] ECLI:EU:C:2004:695.

Firstly, in adjudicating the case, the CJEU had to consider whether a there had been *"substantial investment"* made by BHB in "*obtaining, verifying or presenting the contents of the database*." The CJEU decided that the expression "*investment*" refers to the resources used to seek out existing independent materials and collect them together to construct a database. The protection did not cover the investment involved in *de facto creating the data* which made up the contents of the database. Thus, the investment should "*refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database."*[105] Moreover, "*insubstantial*" part must be interpreted as meaning "*a part which does not reach the threshold for a substantial part in terms of quality or quantity. That threshold forms the upper limit […] the sui generis right does not cover individual data.*"[106] On the facts, the Court found that BHB had made substantial investment in the *creation* of the data *itself* but not in *obtaining, verifying or presenting* t*he contents of the database.* There was therefore, no *substantial investment* that qualified for database right.

4.2.4 Substantiality and the act of "extraction and re-utilisation"

A person infringes an *"investment made"* in a right holders database right if they extract or re-utilise[107] all or a substantial part of the contents of a protected database without the consent of the database owner. Legal definitions of the terms of extraction and re-utilisation are provided within article 7(2) of the DbD.

"Extraction" is defined as the permanent or temporary transfer of the contents to another medium by any means or form. An example of this is for example, copying some or all of the contents of one database into another database. *"Re-utilisation"* means making the contents of a database available to the public by any means. Extracting or re-utilising a substantial part of the contents can result from the repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of a database. SGDR protects against extraction and reutilisation

[105] Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd [2004] ECLI:EU:C:2004:695, para 84, para 94,

[106] Case C-203/02 *British Horseracing Board Ltd and others v William Hill Organization Ltd* [2004] ECLI:EU:C:2004:695, para 84, para 94.

[107] DbD article 7(1).

of substantial part of the database, or also of its insubstantial part if made systematically.[108]

In a number of cases,[109] the CJEU has drawn a distinction between the acts of extraction and re-utilisation and mere consultation of a database. It is clear that where the creator of a database makes the contents of the database accessible to the public, the consultation of that database does not, by itself, constitute an infringement of database right. In the seminal case of BHB v William Hill[110] mentioned above[111] the CJEU considered the issue of *an extraction or re-utilisation of a substantial part of the contents of a database* affirming that the question should be addressed both *quantitatively and qualitatively*. In order to ascertain whether the data amounted to a *substantial part in the quantitative sense*, the data *extracted or re-utilised* must be assessed in relation to the *total volume* of the content of the database. The use by William Hill of the data from the database represented a very small part of BHB's whole database. Further, any unauthorised act of appropriation and distribution to the public of the whole or a part of the contents of a database would amount extraction or re-utilisation, however in the present case the contents of a database were made accessible to the public by its maker or with his consent and "*did not affect the right of the maker to prevent acts of extraction and/or re-utilisation of the whole or a substantial part of the contents of a database."* There was therefore no extraction or re-utilisation of a substantial part in the *quantitative sense*. In addition, when determining whether the data constituted a *substantial part* in the *qualitative sense*, the CJEU referred to the *scale of investment* in the obtaining, verification or presentation of the contents of the database that are extracted and/or re-utilised (and not the value of the contents extracted). Since no separate effort had been employed to obtain, verify or present the particular part of the database used by William Hill, such part could not be substantial in the qualitative sense.

---

[108] DbD article 7(1).

[109] Case C-46/02 Fixtures Marketing Ltd v. Oy Veikkaus AB [2004] ECLI:EU:C:2004:694; Case C-338/02 Fixtures Marketing Ltd v. Svenska Spel AB [2004] ECLI:EU:C:2004:696; Case C-444/02 Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou [2004] ECLI:EU:C:2004:697; Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd [2004].

[110] Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd [2004] ECLI:EU:C:2004:695, para 84, para 94.

[111] The facts of the case are stated within 4.2.1 of the thesis.

In the same light, in *Fixtures Marketing v Oy Veikkaus, Fixtures Marketing v OPAP and Fixtures Marketing v Svenska,*[112] the CJEU gave its judgment along with its judgment in *BHB v William Hill.* Fixtures Marketing had brought actions against three defendant organisations contending that they had extracted and re-utilised data from football fixture lists for the English Premier League, which Fixtures Marketing develops and managed at a cost of over £11.5 million a year. Here, the CJEU held that *only investment to pursue existing materials* and collect them into a database will give rise to a database right. Therefore, drawing up a fixture list for the purpose of organising football league fixtures and using resources to establish the dates, times and the team pairings for the various matches in the league does not provide protection. Hence, resources utilized for the *creation of materials* that make up the database does not lead to protection as was the case in *BHB v William Hill*.

There is a correlation between the substantial investment and the infringement of as evidenced by economy justification for the SGDR by allowing the database maker to recover costs that they have made in creating the database as per recital 48 of the DbD. Recital 48 further mentions that provisions of the DbD are without prejudice to data protection legislation recognised in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. As the DbD came into force before the introduction of the GDPR, it is uncertain whether the same can be extended in relation to the GDPR whose crux lies in the realms of right to privacy.

[112] Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou (OPAP) [2004] ECLI:EU:C:2004:697.

4.3 The "obtaining, verifying, presenting" criteria in connected devices

4.3.1 Introduction

Several devices that we use daily may all at once be connected to the internet. So for example, smart cities thrive on the use of connected devices and the IoT.[113]

Firstly, one needs to define the database as per the article 1(2) of the DbD which states that "*materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means"*[114]. Secondly, when it is established that data fits the definition of a database, a second criteria would be that a 's*ubstantial investment be made in obtaining, verifying and presenting its contents*" pursuant to the SGDR.

In the *Autobahnmaut*[115] decision it was held by the Bundesgerichtshof (German Federal Supreme Court) that a highway company could claim a sui generis right in a database of machine-generated data about motorway use or toll data. The highway company had made a substantial investment in the *"obtaining"* of pre-existing data on cars on the motorway and in the *processing of such data* through software "*verifying*" and "*presenting*". Provided that the same line of reasoning is extended to data that is generated via the use of sensors and connected devices, then the database owner would have a right to exclude *others* from extracting or re-utilising the data held within the database. The investment in creating the raw material may oftentimes exceed the investment made in segmenting and aligning that pre-existing raw material. In such a case, it might be inadvertently difficult to rely on the SDGR protection. Moreover, the criterion of *"verification"* of the database contents may become ever more pertinent, especially in a big data context which allows analytics of unstructured data generated from connected devices.

[113] Sylvia Zhang, 'Who Owns the Data Generated by Your Smart Car'[2018]32HJL&Tech299.
[114] DbD article 1(2).
[115] BGH, 25 March 2010, I ZR 47/08.

4.4 Discussion and summary

The DbD refers to the database maker's investment in *"obtaining, verifying and presenting of the contents"* and provides a right *"to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."* The directive also mentions in its recitals that a database includes *"collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed."* These prerequisites, according to Bernt Hugenholtz, *"squarely rules out protection – whether by copyright or by the sui generis right – of (collections of) raw machine-generated data*."[116] The use of noSQL technologies may imply that big data are not protected by the SDGR. Likewise, machine produced outputs (such as new data corpora) based on analyses of big data resulting from connected devices are neither "*obtained"* nor "*collected"*; they are generated by the machine. This would seem to leave them unprotected by the SGDR.[117] Several CJEU judgements have explained that an investment in the *creation* of the data does not render database protection.[118] A conclusion from this can be drawn that, in connected devices the data is "*created*" instead of it being "*obtained*," the latter being a condition for protection. It is known that the differentiation of data that is "*obtained*" and "*created*" in machine generated circumstances is problematic.

It will be increasingly difficult to satisfy the SGDR protection requirements in a data economy context, given that the processes of obtaining, verifying and/or presenting the data will happen more and more automatically, using algorithms.[119]Also, the criterion of "*verification*" may become less and less

[116] P. Bernt Hugenholtz, 'Data Property: Unwelcome Guest in the House of IP', Available at >https://www.ivir.nl/publicaties/download/Data_property_Muenster.pdf>Accessed 25 April 2021.

[117] Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' [2019] 10 JIPITEC 1.

[118] Case C-46/02 Fixtures Marketing Ltd v. Oy Veikkaus AB *[*2004] ECLI:EU:C:2004:694; Case C-338/02 Fixtures Marketing *Ltd v. Svenska Spel AB* [2004] ECLI:EU:C:2004:696; Case C-444/*02* Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou [2004] ECLI:EU:C:2004:697; Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd *[2004]* ECLI:EU:C:2004:695, para 42

[119] Case C-203/02 Horseracing Board Ltd and others v William Hill Organization Ltd *[2004]* ECLI:EU:C:2004:695, para 35.

pertinent, particularly in an environment which allows for analytics of unstructured data.

5. Intersection between the sui generis database right and the right to data portability

5.1 Introduction

To what extent does the SGDR limit the RtDP and do these rights intersect or clash? Scholars contend that the WP29 underestimates the conflict of SGDR and RtDP.[120]

The SGDR lend exclusivity to their beneficiaries and defines acts which third parties cannot undertake without the permission of beneficiaries. On the other hand, RtDP assures the data subject's right to their own information and for it to be transferred to a third party at their request. The right also sets the duties of the data subject vis-à-vis the controller and vice versa. The RtDP prompts the disclosure and use by the data subject; and use by the subsequent new data controller. The WP29's stance on the application of recital 63 to article 20 of the GDPR, read together is that there is a conflict between the two rights which is certainly a higher threshold than a mere "*interference*."[121]

It is within a semantic or pragmatic scope that the individual has a RtDP[122]. A semantic scope encompasses information or knowledge that can be deduced from the data. It is logical that the RtDP is a right on a semantic level and that no "*ownership like*" right is given to the data subject, similar to an IP right, since this would prove to be dangerous for the purposes of innovation.[123] The types of data

[120] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1375.

[121] Martin Husovec, 'Trademark Use Doctrine in the European Union and Japan,'[2017] 21 MIPR 1.

[122] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[123] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-

that are dealt with within the GDPR are also raw data. Similarly, Drexl[124] submits that the data controller is not under obligation to provide personal information or data from his database when the RtDP by the data subject is invoked.[125] Primarily, this is due to the fact that the raw data encoded into the connected device is unlikely to be in a "s*tructured, machine readable format*" which is one of the requirements under RtDP and therefore "*the specific interest protected by the GDPR only relates to the semantic level of the machine-generated data*."[126] The right holder of the database is obliged to provide the personal information which is in the form of raw data within the database. We can take the example of software within the connected device which *observes* the personal information and analyses it. Data in its most natural state which has not been analysed can be provided.[127] Therefore, it has been recommended that controllers should also make use of API's which allows for data to be in their most interoperable formats for the purposes of compliance with the GDPR or else the data subject will not be able to claim access to the data and neither is the data controller under any obligation to transfer it to another service provider. The processing of the data has to be based on consent or contract.[128]

121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[124] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[125] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[126] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[127] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016). At10.

[128] GDPR article 6.

5.2 The right to data portability leading to the "extraction and re-utilisation" of the database

5.2.1 Introduction

Can the RtDP affect the database maker's SGDR? In other words, is there a right for the individual to port his or her own personal data from a database maker's database given that they have a right to do so under the GDPR? If so, is the database maker allowed to raise his own defence and prevent such extraction and re-utilisation of parts of the database? The SGDR protection *"prohibits extraction of all or a substantial part"* of the database contents to another medium. Pursuant to recital 45 of the DbD "*the existence of a right to prevent the unauthorized extraction and/or re-utilisation of the whole or a substantial part of works, data or materials from a database should not give rise to the creation of a new right in the works, data or materials themselves*." This includes the copying of the individual data collected in a database. However, once the database contents are made public then the database maker cannot prevent third parties from using it.

A RtDP request under the GDPR may be interpreted as unlawful extraction. The receiving controller, through the use of database portability, may make the contents available to the public and thus be infringing the database maker's right to prevent re-utilisation. However, important to note here is that when the data subject requests for their personal information to be transferred to another controller due to the requests excessive and repetitive character, then the controller may either as per 12 (5)(a-b) of the GDPR:

"1. Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or 2.refuse to act on the request."

Indeed, therefore there is a possible clash between the RtDP and the SGDR, where the latter can be invoked to bar the former in both regimes[129]

The RtDP is subject to limitations in the interests of third parties as laid down in article 20(4) of the GDPR. These could be data protection rights of other platform

[129] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

users[130] but also IP rights such as the SGDR. The extent of the conflict of these interests in not known by the CJEU.

The commission has expressed that *"there is also no explicit right for the individual to extract his/her own personal data (…) from an application or service.*"[131] Direct and indirect portability may amount to permanent transfer of the personal data to another medium which would impede the investments made in databases.

5.2.2 Basis for the database maker to prevent the portability request

Where a data subject invokes their right under article 20 of the GDPR, in his or her defence the database right holder may claim that their right to not disclose any information is already given to them under article 20(4) of the GDPR. The SGDR may provide an additional layer of protection where the database maker can claim protection under both the provisions of GDPR article 20(4) and the SGDR which would protect their investment made in the database.

A limitation to the right of access under article 15(4) of the GDPR is stated within recital 63 *"A data subject should have the right of access…That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject."* This suggests that the SGDR may not be infringed where a data subject seeks to exercise their RtDP, yet also states that IP considerations should not result in the refusal to provide all information to the data subject. The WP29 has suggested that a middle ground to this would be that data controllers *"transmit the personal data . . . in a form that does not release information covered by trade secrets or IP rights."*[132]

[130] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016). At 12.

[131] Commission, 'Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data' (Commission Staff Working Paper) SEC(2012)72 final 7.

[132] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016). At 70.

Data portability tools needs to be taken account of when assessing if legitimate interest under article 6(1)(f) of the GDPR is a suitable processing ground when balancing interests of the controller vis-à-vis the data subject.[133] The controller needs to justify processing on another ground under article 6 of the GDPR i.e. contract or legitimate interest of the controller and thereby does not need to comply with the RtDP at the request of the data subject. Defining the "*database"* is essential in determining whether the "*extraction"* amounts to "*substantial"* or "*insubstantial"* part of the database. Here, the database maker can influence the *"substantial"* or *"insubstantial"* part of the database by limiting the personal data requested for portability. In essence, they could only define the dataset to include a smaller part of the database and this could bar the RtDP.

It has been argued that the where an individual invokes their RtDP and seeks access to the database then is could be denied, according to Drexl,[134] as the database maker has financial incentives involved within the database's right. Drexl expresses that right of access, which is closely linked to the RtDP should *"be vested in the persons who have a legitimate interest in getting access to the data generated by connected devices."*[135] The determining factor to the legitimate interest criteria would then be the individual who is dependent on the right. Therefore, it can be inferred that for the proper functioning of the connected device, the rights holder should be the database maker who has made a substantial investment into *"obtaining, verifying and presenting"* part(s) of the database contents. Evidently, several parties, such as the processor, service providers, manufacturers; are present in the creation of the software, hardware and other components of the connected device, but for the purposes of this thesis they will not be scrutinised further.

[133] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 8.

[134] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[135] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

WP29 maintains that *"[t]he RtDP is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights*."[136]

5.2.3 Basis for the right of the individual to invoke their right to data portability leading to the extraction or reutilisation of the database

If the conditions for processing of personal data by the database maker are not fulfilled they may not collect these data. The basis of processing is consent, contract or another legitimate ground as laid down by law.[137] The individual whose personal data has been collected may just as well use one of the exceptions under the DbD to extract data from the database. They may for example extract *"insubstantial parts"* or for "*grounds of private use, non-commercial teaching and research, public security, and administrative or judicial procedure"*[138]

Furthermore, if an individual is able to prove that one of the six principles[139] for lawful processing within the GDPR have not been applied in the processing then these could justify extraction by the individual.[140] However, it is clear that when the RtDP is set against the SGDR, the database right holder has a stronger incentive to protect their database as they have a legitimate interest to do so, considering that they have made a substantial investment in the database.

5.3 Discussion and summary

Intellectual property rights create incentives which can encourage further production or commercialization for the entire class of innovation. Therefore, IP rights contain an exclusivity prerogative which allow for uses of a protected investment allowed only with the consent of right holders. It is common that then the right holders commercialize their IP to exclude others from holding

[136] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 12.

[137] GDPR article 6, article 9.

[138] DbD article 10(1).

[139] GDPR article 5.

[140] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

commercial rights in their IP or alternatively they may also commercialize them through markets, either on their own or through licensing.[141]

The way in which data portability policies may encumber IP rights holders investments and cause friction between the two are; firstly, the mandatory portability can force disclosure of valuable data which would otherwise not have been disclosed to competitors. Secondly, it may also prompt data sharing where exclusivity was previously assured as a reward. Thirdly, it can encumber revenue that the potential beneficiary anticipated from their licensing activity and consequently broadly innovation incentives.[142]

An extensive analysis of the RtDP will obscure its interface with IP law.

Similarly, there are many open complications in relation to the extent to which businesses will be able to invoke their IP rights on datasets to prohibit data subjects from moving their personal data to another service provider or controller.

The extent of control the RtDP will carry is contingent on how its balancing with IP law is led in practice. While the GDPR is intended as a general-purpose control mechanism that applies irrespective of the type of reuse of data, the compromise of the GDPR with IP rights might again limit the follow-on use of ported data by purpose-specific considerations. It is evident that the one of the two rights must be compromised if a data subject were to invoke their RtDP right.

Gervais argues that big data are unlikely be protected by the SGDR in databases due to the nature of "*non-relational databases or no SQL*"[143] which are common a characteristics of big data.[144] The Commission is of the view that exchange and access of data between market players is "essential" in order for the EU financial market to reach its full potential.[145]

---

[141] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1375.

[142] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 1375.

[143] Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' [2019] 10 JIPITEC 1, 1.

[144]Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' [2019] 10 JIPITEC 1, 1.

[145] Commission, "FinTech Action plan: For a more competitive and innovative European financial sector Brussels," 8.3.2018 COM(2018) 109 final, at 5.

In order to do so open standards, interoperability and a simplification of data access regimes must be developed so as to increase competition and innovation.[146] One may be able to deduce the importance of interoperability of data held within a database to be exchanged and made use of for the advancement of the European digital market. It has been argued that data from connected devices is unlikely to be protected by the SGDR, it is yet to be seen which rights are vested in data deriving from connected devices and better yet how IP can adapt or become more malleable for the purposes of generating, processing and making use of data generated from connected devices.

5.4 Recommendations

5.4.1 Introduction

The WP29's stance on the application of recital 63 to article 20 of the GDPR, read together is that there is a conflict between the two rights which is certainly a higher threshold than a mere "*interference*."[147] Therefore, below I discuss possible options that may mitigate the potential "interference" of the RtDP and SGDR.

Repealing the DbD so that it is fit for the purpose of not barring the RtDP is inconsistent for resolving of safeguarding portability of personal data and does not account for other potential problems and consequences. A solution to the problem of the SGDR barring the RtDP renders the following realistic possibilities.

So as to limit the clash of the SGDR vis-à-vis the RtDP, one recommendation would be that the SGDR is made into a registrable IPR as it would be necessary for the database holder to actively seek registration and only where there is an incentive to do so.[148] A registrable SGDR might lead to a growth in planned registration.[149] Registrable protection could prevent the sharing of users personal data with third parties, upholding the data subject's right to privacy.

[146] Commission, "FinTech Action plan: For a more competitive and innovative European financial sector Brussels," 8.3.2018 COM(2018) 109 final, at 7.
[147] Martin Husovec,'The End of (Meta) Search Engines in Europe?' [2014]14Chicago-Kent JIP1, 145-172.
[148] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report).
[149] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report).

The enactment of a compulsory licensing system could prevent the SGDR from barring the RtDP, as the database maker would be obliged to allow a license upon the data subject's and/or the new controller's request, whereby the parties would have to settle upon a remuneration.[150]

Case-law interpretation as a candidate would entail that when a potential dispute is sent to the CJEU in the capacity of a preliminary ruling under TFEU 267 then they could rule that article 20(4) GDPR prevails and confer full dominance of the SGDR over the RtDP. Such a ruling is unlikely and has not been given. Yet this would not only hamper individuals from accessing their personal data, but also have a domino effect in reducing competition between service providers and in turn limit the right of the individual to possess control over their data creating a lock-in effect.[151] Thus, case law interpretation would represent a negative precedent for other cases of legitimate interest in accessing data.

Where the data controller has real incentives to not disclose any personal information when the data subject invokes their RtDP, the data controller may even provide some form of remuneration to the data subject.[152] This possibility is likely the most highly unrealistic.

It is an imperative to take the big picture of the data economy into consideration. Rather than focusing exclusively on the RtDP or the SGDR, the superior solution would consist in the inclusion of a broader non-waivable exception in the DbD, whereby regimes on data access rights prevail over the SGDR.[153] The Max Planck Institute for Innovation and Competition has suggested for a non-waivable exception for those with a legitimate interest in a non-waivable data access right

[150] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report)

[151] Josef Drexl, '*Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC'* (2018) BEUC >https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdfaccessed 9 June 2019> accessed 20 April 2021.

[152] Inge Graef et al, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' [2018] 19 GLJ 0, 17.

[153] Josef Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' [2018] BEUC accessed 9 April 2021 'BEUC Study' 83, 161. <https://www.be uc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf>

(not restricted to personal data), such a right, under which the RtDP can be regarded as a special classification.[154]

The Second Evaluation Report considered a non-waivable exception and determined that it could be protected under an amended version of DbD,[155] which is comprehensible with the recognized necessity to assure greater access to data.

Although providing for an exception within the DbD would resolve the clash of the RtDP with the SGDR, it would not suffice in a wider framework, as it could be by-passed. To be effective, the access right needs to take account of other laws (such as privacy, trade secrets, contract law) to provide for a reliable and methodical regime.[156] In the long run and so as to achieve the best outcome, this would require analysis of empirical studies in diverse legal divisions to recognise where precisely alterations are essential, which also speaks against a case-law option, which cannot deliver for such a far-reaching and synchronized option.

As well as covering the RtDP, the general access right exception has some clear advantages. Firstly, it could include likely upcoming forms of data portability, as well as other general access regimes developed based on the needs of new data business models. This broader provision would render it more time resilient. Second, database makers "law shopping" could be at least reduced, as it avoids circumventing one access provision within legislation by choosing to invoke another right.[157]

The intersection between data protection and IPRs might not be very innate in a first moment; however such encounters are inclined to increase significantly within the data-driven economy. EU data economy's development could be disadvantaged by disregarding the potential harmful effects that non-regulation of

[154] Josef Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' [2018] BEUC accessed 9 April 2021 'BEUC Study' 83, 161. https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_c onnected_devices.pdf

[155] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report) 4.

[156] DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report) 4.

[157] Josef Drexl, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC' [2018] BEUC accessed 9 April 2021 'BEUC Study' 83, 161. <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf>

data regimes may cause. The Commission has determined not to carry out a legislative interference with the DbD for now.[158]

5.4.2 An ownership right in data

No single regime deal with per se "*ownership of data"* generated by connected devices which is a topic that has been under scrutiny with calls for regimen that regulate data as seen by some scholars as a move forward for the digital single market.[159] So as to limit clashes between the RtDP and the SGDR, scholars are of the opinion that data portability should be linked to a property-rights approach to data protection or data ownership.[160] In Rubinstein's opinion this is called "*property-related actions like trading, exchanging, or selling data*"[161] instead of the central element of property rights i.e. the right to exclusion. Hence, scholars urge that *"The global community urgently needs precise, clear rules that define ownership of data and express the attendant rights to license, transfer, use, modify, and destroy digital information assets."* [162] Adding further that, *"industries have called for data ownership principles to be developed, above and beyond current privacy and data protection laws."*[163]

The justifications for the existence of an "ownership" type right in data are manifold as data can be traded and therefore its economic reality *"cannot be denied."*[164] Albeit, on a constitutional level, information in the form of data should be freely accessible and thus no one should have a priori right over them.[165]

The Staff document has noted that *"[T]he Database Directive did not intend to create a new right in the data. The CJEU thus held that neither the copyright protection provided for by the Directive nor the sui generis right aim at protecting*

[158]Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space" (2018) COM 232 final.

[159]Jeffrey Ritter & Anna Mayer, 'Regulating Data as Property: A New Construct for Moving Forward,'[2018] 16 *Duke Law & Technology Review* 220-277.

[160]Peter Swire et al, 'Why the RtDP Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,' [2013] 72 MD. L. REV. 335, 373.

[161]Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?'[2013] 3 IDPL, 74–87,84.

[162]Jeffrey Ritteret al, 'Regulating Data as Property: A New Construct for Moving Forward,' [2018] 16Duke *L*aw *&* *T*echnology *R*eview 220-277.

[163]Jeffrey Ritteret al, 'Regulating Data as Property: A New Construct for Moving Forward,' [2018] 16 Duke *L*aw *&* *T*echnology *R*eview 220-277.

[164]Andreas Boerding et al. 'Data Ownership - A Property Rights Approach from a European Perspective' (2018) 11 J Civ L Stud 323.

[165]Art 11(1) of the EU Charter of Fundamental Rights.

the content of databases. Furthermore, the ECJ has specified that the investment in the creation of data should not be taken into account when deciding whether a database can receive protection under the sui generis right."[166] Scholars argue that *"if ownership itself is not recognized and enforceable under the rule of law, then the vitality, integrity, and potential of the data-driven economy is at risk."*[167] Nevertheless, an indication of creating a new exclusive right in data was not mentioned in the April 2018 document on the creation of a "*European data space.*"[168]

[166]Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European Data Economy' SWD(2017) 2 final, 47.

[167]Jeffrey Ritter, 'Regulating Data as Property: A New Construct for Moving Forward,' [2018] 16 Duke Law & Technology Review 220-277.

[168]Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space" (2018) COM 232 final.

6. Summary and conclusions

To answer the research question at hand, this thesis applies a legal scientific (dogmatic) method. Consequently, an attempt is made to describe the concerned rights within the frameworks regulating the RtDP and SGDR, prescribe how these rights interact with each other and finally justify why a supposed change is or is not required so as to mitigate the tension between the two rights within the European data economy. To do so in the following questions are sought to have been answered. (i)The extent to which the RtDP interacts with the SGDR of the database rights holder. (ii) The extent to which one can prescribe the relevant law to the case of connected devices in a big data setting. (iii) Justifications for the amendment to the RtDP or the SGDR in the absence of exclusive rights and whether the two legal frameworks result in a segmented data landscape where data aggregation is hard to achieve.

In chapter two, the *sine qua non* of the EU Data Economy is determined to be "data" which constitutes the very foundation for overflow of information in the digital economy. The interaction between connected devices and intellectual property plays a vital role as the latter affects the generation, analysis and use of data derived from connected devices. Without the ability to monetise revenue from the data there is no incentive to collect them. Justifications for the wide sharing of data may diminish its economic value. The conclusions that are drawn are that connected devices including the Internet of Things generate big data and are profoundly data dependant. Access to big datasets is indispensable for the purposes of inputs for training algorithms for ML. Smart connected devices do not autonomously produce "*raw data*" about personal behaviour patterns of any said individual. These data are analysed by machines since ML and AI make use of statistical techniques and their closest and best estimates are dependent on the large size of the datasets generated by connected devices. In connected devices several variables may be present in the large datasets and therefore it is crucial that robust predictions are generated to diminish the existence of any errors. The

larger the dataset the closer the prediction will be leading to better accuracy for user experiences and the functioning of devices.

Other aspects of the law, besides GDPR and SGDR considerations which touch upon "data" is competition law related to anti-competitive behaviour by big data firms. Articles 101 and 102 of the TFEU regulate anti-competitive practices within the EU. In order to minimise abuse of dominance which leads to anti-competitive behaviour, the CJEU has ruled that data holders could be obliged to allow data access under the requirements set out by the law. The example of car navigation systems is given in chapter two stating that car navigation data needs to be aggregated by a navigation service provider (controller) in order to identify traffic jams and send this information back to drivers. There are considerable economies of scope in the aggregation compared to the marginal value of each individual car navigation dataset since benefits of using a combined dataset is higher than using each dataset separately. These datasets need not be completely separable; instead they should complement each other. Similarly, economies of scale prompt investments made in high quality datasets transmitted by connected devices for the purposes of training ML algorithms. This is expensive to achieve yet once trained the marginal cost of additional use of the algorithms have shown to be low. The justification for using these financial analytical techniques was to demonstrate the monetary value. A well-known fact is that smart cities, connected devices, AI and the digital economy as a whole thrive on data and the access to it. Limiting the free-flow of data may lead to a downward spiral for the purposes of the advancements in technology underpinned by the aforementioned techniques. With the advancements of ML and AI which crave enormous amounts of data, the question posed at the end of chapter two was whether the current data access regimes allow for the innovation in the AI- driven technological world.

The RtDP stipulates that data must be provided in *"structured, commonly used and machine-readable format"* which allows for scalability. Secondly, data subjects have a right to *"transmit those data to another controller without hindrance*" which allows for aggregation and reuse. The data controller is obliged to provide the personal data for no monetary remuneration which lowers the barriers to entry and mandates a low threshold for access to the data. Hence, in the

next chapter the foregoing economic justifications are linked to the requirement in the chapter three which discusses the requirements for the RtDP under the GDPR.

In chapter three it is established the RtDP exists to *"further strengthen data subjects control*" (recital 68) over their personal data in an attempt to uphold the individual right to privacy EU Charter of Fundamental Rights as per article 8(1). The RtDP was introduced and the conditions for individuals to have their data ported between service providers. The scope of the RtDP i.e: (i) a right to receive and transfer personal data (indirect portability), and (ii) a right to have it transmitted directly from one controller to another (direct portability), "*without hindrance*" is a qualified right contingent upon certain conditions for protection. Firstly, in order for a RtDP request to be successful the lawful processing ground must be fulfilled. Five main processing grounds exists which are (i) the data collected must be personal data (ii) the processing must be based on contract or consent (iii) the request may not affect the rights and freedoms of others (iv) the data has to be provided to the controller (v) data processed on any other legal ground including legitimate interest.

In an environment of connected device, personal data is said to be *"observed"* and not "*provided by"* the data subject. Hence, the RtDP may not be invoked by the data subject up against a database right holder in a "big data" scenario which is created with and by the use of connected devices. Furthermore, The RtDP is subject to limitations in the interests of third parties as laid down in article 20(4) of the GDPR. These could be data protection rights of other platform users[169] but also IP rights, rights of others etc. It can is deduced that the RtDP is closely linked to the right of access. A limitation to the right of access under article 15(4) of the GDPR is stated within recital 63 *"right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property."*

In chapter four, the conditions and scope for the protection under the SGDR right are discussed and the fact that the novel was introduced as a result of the need to incentivize the production of databases. Thus, investment in the creation of the database is protected. The conditions leading up to the protection are analysed.

[169] WP29 Art. 29 Data Protection Working Party, Guidelines on the RtDP, 16/EN WP 242 (Dec. 13, 2016).At 12.

The conditioned for protection are; (i) the definition of ”database” must be satisfied (ii) substantial investment in (iii) either the obtaining verification or presentation of the contents (iv)to prevent extraction and/or re-utilisation (v)of the whole or substantial part (v) evaluated qualitatively and/or quantitatively. The conditions are explained primarily with the opinion and judgment of one seminal case British Horseracing Board v William Hill. One major takeaway from the case is that the substantial investment should not be made in the resources used for the creation of materials which make up the contents of a database, but rather refer to the resources used to seek out existing independent materials. Further, extracting or re-utilising a substantial part of the contents can result from the repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of a database. SGDR protects against extraction and reutilisation of substantial part of the database, or also of its insubstantial part if made systematically.

When applying the above criteria to the case of data generated by connected devices, in the *Autobahnmaut* decision it was held that a highway company could claim a SGDR in a database of machine-generated data about motorway use. If the same line of reasoning may be applied by the CJEU provided a preliminary ruling is requested then big data would be covered, most likely.

In chapter five, the intersections between the RtDP and SGDR is discussed which occurs when the RtDP and the conditions therein are fulfilled which may lead to unlawful extraction of the database makers SGDR allowing him or her to prevent the extraction and re-utilisation of their database. It is not exclusively clear if the individual invoking their RtDP amount to the conditions of its “*extraction or re-utilisation.*”

It is determined that *“smart devices will often make use of data analytics, machine-learning and artificial intelligence.”* Thus, these smart connected devices do not autonomously produce “raw data” about personal behaviour patterns of any said individual. Furthermore, connected devices are not limited to those that communicate autonomously through the Internet of Things.

The right holder of the database is obliged to provide the personal information which is in the form of raw data within the database. We can take the example of software within the connected device which *observes* the personal information

and analyses it. Data in its most natural state which has not been analysed can be provided. Therefore, it has been recommended that controllers should also make use of API's which allows for data to be in their most interoperable formats for the purposes of compliance with the GDPR or else the data subject will not be able to claim access to the data and neither is the data controller under any obligation to transfer it to another service provider. The processing of the data has to be based on consent or contract.

The SGDR may indeed limit the free flow of data and creates a lock-in effect where the individual may be barred from exercising their right of control over their personal data. Conversely, upholding the rights of the database maker leads to innovation and provides incentives for the creation of databases.

It is discussed whether the SGDR even applies to data collected by connected devices, as it could be argued that the data included in such databases are "*created"* instead of *"obtained"*. In relation to the RtDP it is unlikely that the personal data that is "*observed*" by the connected or IoT device has been *"provided"* by the data subject. It is concluded that, it may become increasingly difficult to satisfy the SGDR requirements in a big data economy context, given that the processes of obtaining, verifying and/or presenting the data will happen more and more automatically, as they will be normally conducted using algorithms and analysis of raw data by ML and AI.

The extent of control the RtDP will carry is contingent on how its balancing with IP law is led in practice. While the GDPR is intended as a general-purpose control mechanism that applies irrespective of the type of reuse of data, the compromise of the GDPR with IP rights might again limit the follow-on use of ported data by purpose-specific considerations. It is evident that the one of the two rights must be compromised if a data subject were to invoke their RtDP right.

For the recommendations given of how to mitigate the interference of the two rights within chapter five it is deliberated whether granting the repeal of the DbD as a whole or only the SGDR would solve the clash with the RtDP. Yet, these drastic options are not proportionate for the explicit aim of ensuring the RtDP. Leaving the issue for courts that may not be familiar with a wide-ranging picture of the data economy can yield unwanted consequences, foreclosing data-driven

markets. Additionally, the likelihood of database makers evading a decision favouring the RtDP over the SGDR cannot be overlooked. A solution here could be to introduce an exception in the DbD authorising data access rights regimes to override the SGDR. This gives the institution the mandatory plasticity to stand the test of time, as well as the likelihood for the EU to ponder a comprehensive action though the acknowledgement of a non-waivable data access right for those with a legitimate interest in such access. Although providing for an exception within the DbD would resolve the clash of the RtDP with the SGDR, it would not suffice in a wider framework, as it could be by-passed. If a new regime were to be implemented, then, to be effective, the access right needs to take account of other laws (such as privacy, trade secrets, contract law) to provide for a reliable and methodical regime. In the long run and so as to achieve the best outcome, this would require analysis of empirical studies recognise where precisely alterations are essential, which also speaks against a case-law option, which cannot deliver for such a far-reaching and synchronized option.

It is mentioned in chapter five that not having defined data access rights may have a broader effect on the data economy, which relies on digitisation processes such as connected devices, the Internet of Things, artificial intelligence; as it becomes increasingly difficult to distinguish between the generation/creation and the obtainment of data in the context of such processes. The current legal regimes may not reconcile the developments in technologies and connected devices that generate big data or processes that perform data analytics. In relation to the RtDP, it becomes ever more difficult for an individual to exercise their RtDP where raw datasets containing personal information cannot be extracted due to the data being protected under the SGDR. Incentives to innovate should not be hampered by the RtDP nor should the SGDR, and their mutual interplay ought to be an incentive to recommend a change in the area.

In conclusion, this thesis has attempted to elucidate the interfaces between the RtDP and the SGDR and give a reference of their conflicting nature. The intersection known between the two rights is not as mute as put forward previously and leaves open unattended gaps, which can destabilise the RtDP's effectiveness.

Reference list / Bibliography

Official Publications

International Publications

- Summary of the OECD Privacy Expert Roundtable on Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking [2014], available at >https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en>

European Union Publications

- Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European Data Economy' SWD(2017) 2 final, 47.
- Commission, 'FinTech Action plan: For a more competitive and innovative European financial sector Brussels," 8.3.2018 COM(2018) 109 final, at 5.
- Commission, 'Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of such Data' (Commission Staff Working Paper) SEC(2012)72 final 7.
- Communication from the Commission to the European Parliament and the Council 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' {SWD(2020) 115 final}.
- Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the

Committee of the Regions, “Towards a common European data space” (2018) COM 232 final.

- The Execution of Criminal Penalties, and the Free Movement of such Data’ (Commission Staff Working Paper) SEC(2012)72 final 7.
- Working Party article 29 Data Protection Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017.
- Working Party article 29 Data Protection Working Party, Guidelines on the right to data portability, 16/EN WP 242 (Dec. 13, 2016).

Other Publications

- DG CONNECT, ‘Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report’ (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report).

Literature

- AKC Koo, “Database Right Decoded” [2009] EIPR, Vol. 7, pp. 313-319, 2010 , Available at SSRN: https://ssrn.com/abstract=1470676
- Andreas Boerding et al. 'Data Ownership - A Property Rights Approach from a European Perspective' (2018) 11 J Civ L Stud 323.
- Bertin Martens, ”The impact of data access regimes on artificial intelligence and machine learning“[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).
- Charlotte A Tschider, 'Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age' [2018] 96 Denv L Rev 87.
- Daniel Gervais, ‘Exploring the Interfaces Between Big Data and Intellectual Property Law’ [2019] 10 JIPITEC 1.
- Herbert Zech, ‘A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data’ (2016) 11 (6) JIPLP 460, 467.
- Inge Graef et al, ’Data Portability and Data Control: Lessons for an Emerging Concept in EU Law’ [2018] 19 GLJ 0, 1360.
- Ira Rubinstein, ‘Big Data: The End of Privacy or a New Beginning?’[2013] 3 IDPL, 74–87,84.

- Ivan Stepanov ‘Introducing a property right over data in the EU: the data producer’s right – an evaluation’ [2020] 34 IRL 1, Computers & Technology 65.
- Jeffrey Ritter & Anna Mayer, ‘Regulating Data as Property: A New Construct for Moving Forward,’[2018] 16 Duke Law & Technology Review 220-277.
- Jeffrey Ritteret al, ‘Regulating Data as Property: A New Construct for Moving Forward,’ [2018] 16 Duke Law & Technology Review 220-277.
- Josef Drexl et al, ‘Position Statement of the Max Planck Institute for Innovation on the European Commission’s “Public Consultation on Building the European Data Economy”’ [2017] Max Planck Institute for Innovation & Competition Research Paper No. 17-08.
- Josef Drexl, ‘Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organization BEUC’ [2018]
- Mark Schneider, ‘The European Union Database Directive.’ [1998]13 Berkeley Technology Law Journal 1, 551–564.
- Martens Bertin,’The impact of data access regimes on artificial intelligence and machine learning’[2018] JRC Digital Economy Working Paper, European Commission, Joint Research Centre (JRC).
- Martin Husovec, ‘Trademark Use Doctrine in the European Union and Japan,’[2017] 21 MIPR 1.
- Michael Burri, ‘The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation’ [2017] 51 UC Davis Law Review, 65, 133.
- Nadezhda Purtova, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10 (1) LIT 40.
- Peter Swire et al, ‘Why the RtDP Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,’ [2013] 72 MD. L. REV. 335, 373.
- Sylvia Zhang, 'Who Owns the Data Generated by Your Smart Car'[2018]32HJL&Tech299.
- Terry Sanks, ‘Database Protection: National and International Attempts to Provide Legal Protection for Databases,’ [1998] 25FSULR4, 1003.

Online sources

- Bergemann et al, ‘Markets for data’ [2012] >https://economicdynamics.org/meetpapers/2012/paper_538.pdf>
- Michael Haupt, ‘Data is the New Oil’ – A Ludacris Proposition.” [2016] >https://medium.com/project-2030/data-is-the-new-oil-aludicrousproposition-1d91bba4f294>
- Mike Sands ‘Customer Data Is the Secret to Silicon Valley’s Success.’(2017) Forbes. >https://www.forbes.com/sites/mikesands1/2017/11/29/customerdata-is-thesecret-to-silicon-valleys-success/#135386886c3b>
- P. Bernt Hugenholtz, ‘Data Property: Unwelcome Guest in the House of IP’, Available at >https://www.ivir.nl/publicaties/download/Data_property_Muenster.pdf

Cases

European Union

Court of Justice of the European Union

- Case C-203/02 British Horseracing Board Ltd and others v William Hill Organization Ltd [2004] ECLI:EU:C:2004:695.
- Case C-338/02 Fixtures Marketing Ltd v. Svenska Spel AB [2004] ECLI:EU:C:2004:696.
- Case C-444/02 Fixtures Marketing Ltd v. Organismos Prognostikon Agonon Podosfairou [2004] ECLI:EU:C:2004:697.
- Case C-46/02 Fixtures Marketing Ltd v. Oy Veikkaus AB [2004] ECLI:EU:C:2004:694.
- Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771.
- Case T-17/21 Miquel y Costas & Miquel v EUIPO (Pure Hemp) OJ C72, 1.3.2021
- Case Technomed Ltd. v. Bluecrest Health Screening Ltd. [2017] EWHC (Ch) 2142 [75].

List of German Case Law

- BGH, 25 March 2010, I ZR 47/08.