HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

LAW SCHOOL

POSTGRADUATE PROGRAM..: LL.M. in International and European Legal Studies
SPECIALIZATION: Private Law and Business Transactions
ACADEMIC YEAR: 2021-2022

POSTGRADUATE THESIS

of Panagiotis Markos Kontizas

R.N.: 7340022101010

Personal data as the currency of the digital age having as an example art. 3 par. 1 (and Preamble No. 24) of Directive 2019/770

Thesis Committee:

a) Georgios Yannopoulos (Supervisor)

b) Antonios Karampatzos

c) Paraskevi Paparseniou

Athens, 31/10/2022

Contents

LIST OF ABBREVIATIONS

AI : Artificial Intelligence

CJEU : Court of Justice of the European Union

CMP : Consent Management Platform

DCSD : Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services

DPA : Data Protection Authority

ECHR : European Court of Human Rights

EDPB: European Data Protection Board

EDPS : European Data Protection Supervisor

EU : European Union

FAANG : Facebook, Amazon, Apple, Netflix, Alphabet/Google

GCC : Greek Civil Code

GDPR : 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

IoT : Internet of Things

OECD : Organization for Economic Cooperation and Development

Proposal : Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content issued by the European Commission in 2015

Rome I : Regulation 593/2008

SMEs : Small and medium-sized enterprises

TFEU : Treaty on the Functioning of the European Union

UCPD : Unfair Commercial Practices Directive 2005/29/EC

UCTD : Unfair Contract Terms Directive 93/13/EEC

V. : Versus

1. Introduction

In September 2017, a cybersecurity company, Kaspersky Lab, did a social experiment. They opened the "Data Dollar Store", in which customers could use only their personal data as a currency to buy artwork. They called this new currency the "data dollar". In this store, someone could buy, for instance, a T-shirt in exchange for five WhatsApp conversations. Through this experiment Kaspersky Lab wanted to raise awareness about the value of personal data and to highlight the need to be cautious when it comes to protecting our privacy on-line.[1] Although the concept of the "data dollar" was used allegorically in this social experiment, a closer look to today's digitised world can prove that the perception of personal data as currency may not be as fictional as it may seem at first glance.

Nowadays, new ways of personal data processing have arisen due to new technological tools, making it possible to generate economic value from them. Due to this, new business models have also arisen. It is a common practice among digital companies to provide digital content or services for free to the consumers, while these companies gain revenue from the exploitation of the data consumers provide in exchange for the content or services. This new situation is challenging for regulators worldwide, who are called to ensure that the legal framework corresponds to the new needs and the arising legal issues. The European Union, which has diachronically been on the forefront of both data protection law and consumer protection law, could not stay inactive. Indeed, Directive 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services (DCSD) is the European response to this new practice. According to article 3 par. 1 of the Directive, "[…]This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose."

Having this article as an example, the purpose of this thesis is to examine the concept of personal data as the currency of the digital age and the arising legal issues. The analysis is focused on the European legal framework and practice, with references to Greek law as well.

[1] "Data Dollar: The new currency based on the value of personal data puts the spotlight on a newly created retail payment method", available at: https://www.kaspersky.com/about/press-releases/2017_data-dollar-the-new-currency-based-on-the-value-of-personal-data and "The Data Dollar Store - A Data Shopping Social Experiment by Kaspersky Lab " accessed by https://www.youtube.com/watch?v=dqcHcnpNHIM

2. Aspects of personal data

2.1. Definition of personal data

First of all, it is necessary to define the term of personal data. Although each legal system may use a different definition of the term, in the context of this thesis the definition adopted by the Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) is to be followed, since it is also the definition adopted by Directive 2019/770[2]. According to article 4 of the GDPR, " 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Therefore, personal data refer to any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Additionally, personal data which have been de-identified, encrypted or pseudonymised but can be used to re-identify a person remain personal data falling within the scope of the GDPR. However, anonymous data through which the individual is not, or no longer, identifiable and the anonymisation is irreversible, are not considered personal data. Personal data fall within the scope of GDPR and are therefore protected regardless of the technology used for processing that data. It applies to both automated and manual processing, as long as the data are organised in accordance with pre-defined criteria, such as alphabetical order. Moreover, personal data are protected regardless of the way they are stored, either in an IT system or on paper. Personal data may consist of information such as names, dates of birth, photographs, video footage, email addresses and telephone numbers, as well as IP addresses and communications content related to or provided by end-users of communications services.[3]

Another interesting definition and categorisation of personal data which is worth mentioning is related mainly to their economic value and can be found in the report of the World Economic Forum of June 2010. According to this definition, personal data are defined as "data (and metadata) created by and about people" and they can be categorised into three groups. Firstly the "volunteered data", referring to data created and explicitly shared by individuals, such as social network profiles. Secondly the "observed data" which are captured by recording the actions of individuals, for instance location data shared when using cell phones. Thirdly, there are also the "inferred data", which are data about individuals based on an analysis of volunteered or observed information, such as credit scores.[4]

[2] According to Article 2 point 8 of Directive 2019/770, "'personal data' means personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679"

[3] European Commission, "What is personal data?" Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data

[4] World Economic Forum, "Personal Data: The Emergence of a New Asset Class", 2011, p.7 and Philippe Jougleux, «European Law of the Internet – Legal Aspects of the Internet in Europe», Sakkoulas Publications S.A., p. 40-43

2.2. Part of the right to privacy (fundamental human right)

Personal data are protected as a human right in national, European as well as international level. In Greece, article 9A of the Constitution establishes the fundamental right of all persons to be protected from the collection, processing and use, especially by electronic means, of their personal data. Articles 57 and 59 of the Greek Civil Code (GCC) are also related to the protection of personal data, as they protect the right to personality. Moreover, the European Union has diachronically held high standards of data protection law. The EU Charter of Fundamental Rights contains an explicit right to the protection of personal data, in its 8th article. According to it, "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority." The entry into force of the Lisbon Treaty in 2009, gave the Charter of Fundamental Rights the same legal value as the constitutional treaties of the EU. Thus, EU institutions and bodies and the Member States are bound by it. In addition, article 16 of the Treaty on the Functioning of the European Union (TFEU) obliges the EU to lay down data protection rules for the processing of personal data.[5] The most important piece of legislation related to data protection in the EU is the General Data Protection Regulation (GDPR), which establishes an important set of strict rules concerning the personal data of EU citizens, creating new rights for individuals in the digital environment as well as several new and detailed obligations for companies and organisations. The GDPR applies not only to European organisations and companies but also to those which, although they are not established in the EU, they do offer goods and services to individuals in the EU or monitor their behaviour.[6] Globally, there is an increasing growth in data laws, many of which have been strongly influenced by the EU rules.[7]

Moreover, data protection is considered part of the right to privacy, and both are related to the absolute fundamental right of human dignity. Privacy is a fundamental human right protected in an international level under article 12 of the United Nations Universal Declaration of Human Rights, under article 17 of the International Covenant on the Civil and Political Rights and article 8 of the European Convention of Human Rights of 1950. The right to privacy is considered to be the "heart of our liberty" and "the beginning of all freedoms", as it is an essential component of individual freedom.[8] According to the case law of the European Court of Human Rights (ECHR), the protection of personal data is a fundamental component of the right to privacy[9]. Moreover, the

[5] Spiros Vlahopoulos, «Fundamental Rights», Nomiki Vivliothiki, 2017, p. 240-242
[6] Article 3 of the GDPR
[7] Ryngaert Cedric & Taylor Mistale, "The GDPR as global data protection regulation?", Symposium on the GDPR and international law, Cambridge University Press, 2020, p. 5-9
[8] Ebrahim Dorraji Seyed, Barcys Mantas, "Privacy in Digital Age: Dead or Alive?! Regarding the New Eu Data Protection Regulations", Social technologies. 2014, 4(2), p. 307-308
[9] See §103 of the Judgment of the ECHR in Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04), in the context of criminal justice, according to which "the protection of personal data is of fundamental

ECHR has held that the right to privacy has not only a vertical character, namely to protect the individual against arbitrary interference by the public authorities, but also a horizontal character, meaning that the state has a positive obligation to ensure respect for privacy in relations between individuals.[10] The both vertical and horizontal character of the right to privacy applies also to the internet.[11] The protection of personal data and the right to privacy are essential for the autonomy of individuals and for the protection of the right to be in control of information about yourself as well as the right to be let alone. Moreover, data protection and privacy are both considered vital components for a sustainable democracy.[12] Privacy is not only an individual right, but also a highly respected social value.[13] Last but not least, digitized data protection has been characterized as a new fundamental human right.[14]

The digitalization of our era is a significant challenge for privacy and data protection. New technologies create new ways of processing and using personal data, and with them also a potential threat to fundamental rights. However, other fundamental rights such as the right to exercise an economic or commercial activity[15] are worth protection as well. The right to privacy and data protection are not absolute rights but can be limited under certain conditions, when in conflict with other fundamental rights. In such a case, a "balancing" among the conflicting rights has to be found. Therefore, data protection has to be weighed up against other public interests, human rights, or public and private interests such as the fundamental rights to economic freedom, respecting in any case the principle of proportionality and the core elements of each right.[16]

importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.", p. 29 of the Judgement.

[10] See §32 of the Judgement of the ECHR in Case of Airey V. Ireland (Application no. 6289/73), in the context of family law, according to which "The Court does not consider that Ireland can be said to have "interfered" with Mrs. Airey's private or family life: the substance of her complaint is not that the State has acted but that it has failed to act. However, although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life", p. 14 of the Judgement.

[11] See §42 of the Judgement of the ECHR in Case of KU v Finland (Application no. 2872/02), according to which "The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life", p.12 of the Judgement. Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p.3

[12] Ebrahim Dorraji Seyed, Barcys Mantas, "Privacy in Digital Age: Dead or Alive?! Regarding the New Eu Data Protection Regulations", Social technologies. 2014, 4(2), p. 307-308

[13] Kirsty Hughes, "The social value of privacy, the value of privacy to society and human rights discourse" in B. Roessler & D. Mokrosinska (Eds.), "Social Dimensions of Privacy: Interdisciplinary Perspectives", Cambridge University Press, 2015, p. 225-243

[14] Rebekah Dowd, The Birth of Digital Human Rights, p. 27-30

[15] Established as the freedom to conduct a business in Article 16 of the EU Charter of Fundamental Rights

[16] European Data Protection Supervisor, "Data Protection", Available at: https://edps.europa.eu/data-protection/data-protection_en and Spiros Vlahopoulos, «Fundamental Rights», Nomiki Vivliothiki, 2017, p. 25-26

2.3. Financial aspects of personal data

Personal data are related to the right to exercise an economic activity due to their financial aspects. These aspects are mainly linked to the phenomenon of interconnectivity, which is one of the core elements of the digital era. According to the "2030 Digital Compass" communication of the European Commission, during the last years and especially during the Covid-19 pandemic, the world has experienced a dramatic shift in dynamic and demand for connectivity, as people rely on technology to stay connected with the world more than ever before.[17] Society is moving towards a "web of the world" in which mobile communications, social technologies and sensors are connecting people, the Internet and the physical world into one interconnected network. Data records are continuously collected on, among others, who we are, what we do, who we know, where we have been and what our interests are. Through their analysis, data give us the ability to understand and even predict where humans focus their attention and activity as individuals, groups and even at a global level. Personal data, especially digital data, fuel economic and societal value creation. There are various types of personal data being collected which can generate commercial value, from the profiles and demographic data to medical records and employment data. There is a continuously growing list of personal data with economic value, such as web searches, visited sites, purchase histories and activity in social media.[18] Moreover, a general feature of personal data is that they can be financially exploited multiple times without loss of their value. The copy is just as good as the original, enabling multiple offers without loss of price or value.[19]

However, a single item of personal data, for example a name or an email address, usually has insignificant commercial value. It is the combination of different types of personal data that makes a commercial difference. For example, one way to realise commercial value is by combining specific classes of personal data to profiles. Profiles can be created bottom up, using the available data to create meaningful subsets of data, or top down, using pre-configured profiles to check in what group specific people would belong. Both forms of profiles add to the monetary value of personal data, since the grouping of data add to the original value of the data. Personal data are valuable especially in certain fields such as marketing and advertising. By analysing data about consumers' characteristics, needs and preferences, digital companies can promote their products more efficiently, by reaching their target group more easily and faster. The personal data are in fact the 'raw material' for personalized and targeted advertisement. The monetary value of personal data is even more significant if we take into consideration the rise of data-sharing practices among individuals. People tend to share details about their preferences, moods and activities through multiple platforms, such as Facebook and Twitter. At the same time when people go on-line they leave traces, such as their geo-location or their "click behaviour". The value of this information is well understood by marketers who try to collect as much data about personal

[17] European Commission, "2030 Digital Compass: The European way for the Digital Decade", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of The Regions, 2021

[18] World Economic Forum, "Personal Data: The Emergence of a New Asset Class", 2011, p. 5

[19] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p. 5

conducts and preferences as possible, allowing them to learn about purchasing habits and strategies, and to make the best suited offers to their customers. [20]

A reasonable question that may be risen is whether and how this economic value can be measured. Since personal data are part of a fundamental right and part of the personality rights of the person, it seems difficult and even problematic to try to define a specific price for them. However, at least an approximate estimation of their financial value seems possible. There are two main methods which can be used in order to estimate the commercial value of personal data. The first one focuses on the provider of the content or service and tries to assess the value of personal data through the measurement of the monetary value of the firm that deals with the personal data. The second perspective has as a starting point for the evaluation the monetary value data subjects attach to their data.[21]

On the one hand, multiple approaches are possible for the assessment from the perspective of the companies. According to a relevant study of the OECD, in order to measure the financial value of personal data one can look either at the stock value of a firm, at the revenues of a firm or at the price of data records on the market. Apart from these three main perspectives, one may also look at the costs of a data breach and at the price of personal data on an illegal market. All these different approaches show some features of the monetary value of personal data, yet each one is accompanied by specific drawbacks. First, the stock value of a firm is a measure of trust in the firm's capacity to produce valuable revenues, expressing the expectation of shareholders in the growth potential of the firm. For firms trading in personal data as their primary source of revenues, the stock value can be used as a proxy for the value shareholders attach to the data collected and the processes that turn the data into profitable products. However, stock values may fluctuate because of contextual factors that do not bear a direct relationship with the primary process of the firm. Fluctuations of stock prices can induce further fluctuations, as was shown by the introduction of Facebook to the stock market. Only in relatively stable markets one might expect a relatively stable relation between the value of a firm's shares and the revenues it realizes on the basis of its business activities. Secondly, the revenues of a firm indicate real cash flows on the market. This method enables cross-comparisons between firms acting on a similar market, since one would expect these firms to encounter similar problems in selling their products. Revenues should be compared to the total number of data records a firm owns during a specific period of time in order to yield a comparative indicator. A drawback of this method is that the prices third parties are willing to pay for specific data on the market could be influenced by external factors.[22]

Furthermore, the prices of personal data as these are sold at the marketplace[23] offer another indicator. This price reflects the value purchasers attach to these data, which in turn will depend on the profitability purchasers expect to realize. The Financial Times have presented an interactive sheet that enables calculating market prices for specific sorts of data. It distinguishes between demographic data, family and health data, property, sport and leisure activities and consumer data. Demographic data such as age, gender, ethnicity, zip-code and education level are worth USD 0.005 per piece. Job information is worth USD 0.1 if being an entrepreneur and up to USD 0.72 if

[20] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p.5-8
[21] Ibid.
[22] Ibid., p.5-7
[23] In jurisdictions and markets where this is possible, for example in the USA.

being a health professional, pilot or non-profit worker. For information on credit history, criminal records, bankruptcies or convictions of persons one has to pay USD 30-40 per record. Firms specialize in inquiries for this kind of background information. Apparently, one is willing to pay higher prices for specific records of particular persons.[24] However, such a "price catalogue" of personal data seems like an excessive "commodification" of personal data which could not be accepted in European jurisdictions, since it is not compatible with the aspect of personal data as a fundamental right. Another alternative method is by relating the value of personal data to the cost of data breaches. A data breach, which lead to the leak of personal data of numerous consumers, can significantly disturb the operation of a company and create significant directly and indirectly attributable losses, including the costs of recovering from the hack, the fines to be paid and the loss of the reliability of the consumers.[25]

On the other hand, the monetary value of personal data can be also measured by focusing on the value individuals attribute to their own personal data. However, since each person has different principles, needs and values, it seems difficult to define the value people attribute to personal data in a generic way. Indeed, what one individual may consider to be highly private information, such as income or health data, another individual might not bother to share or sell. In dealing with how people value personal data, there seem to be two main perspectives. Firstly, people could attribute a specific monetary value to these data, which is the commercial value of personal data. Secondly, one can investigate what people are willing to pay to keep personal data private. The reasons for keeping these data private could vary. Data could be seen as delicate or sensitive data which people want to keep for themselves. Besides that, people might not want to have data made public because they think the economic benefits do not outweigh the disadvantages, for instance getting loads of advertisements. In order to understand what people value in privacy, the traditional economic models should be supplemented with models that look at behavioural features.[26] Additionally, studies have shown that while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behaviour, this rarely translates into actual protective behaviour. This is known as the "privacy paradox". Indeed, although an intention to limit data disclosure exists, actual disclosure often significantly exceeds intention. Despite the fact that users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services. In the context of users' social network activities, a similar pattern is observed. [27]

After taking all the examined alternatives into consideration, it seems that calculating prices per data record helps in understanding the value of personal data. A calculation from general revenues or the stock value of a firm to a price per record offers some insight in the value that is represented by the personal records a company owns. However, stock value is a measure that is very dependent on external influences that bear no relationship with the value of the personal data. Revenues and profit per data record seem to offer a better perspective on the value of these data records. Data breaches represent a specific measure of the price of personal data as well. The examination of the

[24] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p.7-8
[25] Ibid.
[26] Ibid., p. 8-11
[27] Susanne Barth, Menno D.T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", Telematics and Informatics, 34, 2017, p. 1039-1040

different ways to estimate the value of personal data from a firm's perspective, yields some comparative indicators. They highlight different aspects of the valuation of personal data. Revenues and profits per data record are more reliable indicators than stock market value. The impact of data breaches is high. In addition to that, the individuals' views about the monetary value of their data, although it offers some indications, it cannot be used as a trustworthy method. Although the measurement of the monetary value of personal data is a complicated issue, the factual reality shows that the financial aspects of personal data are expected to become even more significant in the upcoming years, since the market for personal data is growing explosively. In the coming years, new services are expected to be developed on the basis of the collection, aggregation and dissemination of personal data. The characterisation of personal data as the new "currency" or the new 'oil', is therefore not unreasonable.[28]

3. Influence of technological developments to the perception of personal data in the digital age

3.1. Big Data

As already mentioned, interconnectivity has played a crucial role in the increase of value of personal data. According to the "Connected Consumer 2030" report by "Vodafone Smart Tech", by 2030 the number of connected devices globally is estimated to reach 125 billion, representing around 15 devices per individual consumer. Enabling more people to tap into global flows of communication and services could add billions to national GDP by 2030 and unlock greater human potential at the same time. Connectivity means a greater quantity and "quality" of personal data. Although personal data have been considered valuable for a relatively long time, either as ancillary to the core operations of running a business or limited to specific categories of data, in the digital era almost all data are seen as valuable, due to the new methods of using them.[29]

In terms of quantity, consumers generate huge amounts of data in the digital era, which brands are using to understand their desires, at times arguably even better than consumers do themselves. By 2025, an average connected person anywhere in the world is estimated to interact with connected devices nearly 4,800 times per day up from 601 in 2020, according to the International Data Corporation. This is translated into one interaction every 18 seconds.[30]

The enormous amount of personal data that are available to businesses nowadays is also of a significant quality, and it is often described as "big data". The core elements of big data are often referred to as the "3 V's"; high volume, high velocity and high variety.[31] The term includes both

[28] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p. 11-13

[29] Viktor Mayer-Schönberger and Cukier Kenneth, "Big Data: A Revolution that will transform how we Live, Work, and Think, Houghton Mifflin Harcourt Publishing Company, 2013, p.62

[30] Vodafone, "The Connected Consumer 2030", Vodafone Smart Tech, 2022

[31] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p. 71

structured data, such as transactions that can reside in databases, and unstructured data, such as videos, photos, social media content, and Internet of Things (IoT) sensor data that can exist in many format types.[32] Big data consists of cyber data generated by mass volume of internet use on mobile phones and other devices connected to the internet. Big data contains front end-data as well as meta-data. The first term refers to personal details that are divulged as text is typed, whereas the latter includes likes, content visited, internet use patterns and internet profiling of users.[33] Therefore, the process of extracting and analysing these big data for business insight, referred to as "Big Data Analytics", has radically increased the quality of data and consequently their monetary value. Indeed, big data is perceived as critical resource for the businesses of the digital era, in the same way the traditional physical assets, namely money, labour, machines and raw material, have been for previous generations of companies. Big data have a significant impact on business operations such as customer service and marketing, and on a wide range of decisions including what products and services are valued by consumers.[34] Personal data are in fact so valuable for the marketing sector, that according to Dan Zarella, "marketing without data is like driving with eyes closed".[35]

Concerning the sources of information that constitute big data, these are both online and offline. First of all, businesses gain benefit from the monitoring and processing of the online actions of consumers. These sets of data typically contain information about individuals' transactions, email, video, images, clickstream, logs, search queries, health records, and social networking interactions. Secondly, companies gather individuals' personal information from a variety of offline sources, such as retailer's sales records. Finally, businesses collect big amounts of information from devices used to record and transmit data. This last source is the broadest and encompasses information generated by mobile phones, surveillance cameras, global positioning satellites, utility-related sensors, communication networks, and phonebooths, among others. Nearly every business collects information that can potentially be used in big data analytics, with the most obvious examples being in the technology sector. Additionally, telecom companies, financial services businesses, health care providers, and governmental entities process an inconceivably large amount of data every day. While only a few big companies such as Google have both the technical expertise and the quantity and quality of data needed to perform big data-style analyses on their own, the majority of companies do not. These smaller companies, in order to benefit from big data, have to obtain access to data and data analysis services from third parties. Access to data can be obtained either by entering into agreements with companies that specialize in "second-order data aggregation"[36] or by paying for access to relevant data sets that other "first-order aggregators" possess. Big data methodologies are used by businesses in order to improve the core services they provide and to perform several secondary functions, such as pattern analysis, predictive analysis and modelling as well as incident prediction. While the potential for analytics to help private

[32] Salvatore Parise, "Big data: A revolution that will transform how we live, work and think, by Viktor Mayer-Schonberger and Kenneth Cukier", Journal of Information Technology Case and Application Research, 18:3, Routledge, 2016, p.186

[33] Rebekah Dowd, "The Birth of Digital Human Rights - Digitized Data Governance as a Human Rights Issue in the EU", Information Technology and Global Governance Series, Springer, 2022, p. 6-8

[34] Salvatore Parise, "Big data: A revolution that will transform how we live, work and think, by Viktor Mayer-Schonberger and Kenneth Cukier", Journal of Information Technology Case and Application Research, 18:3, Routledge, 2016, p. 186-190, and Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p. 3

[35] Evangelos Margaritis, «Personal Data & Consumer Protection», Nomiki Vivliothiki, 2020, p. 13

[36] This term refers to the collection and centralization of information from public and private primary sources.

entities achieve their goals is not uncommon, the breakthroughs underlying the Big Data movement, that is the increased availability of information and the ability to analyse unstructured data, have drastically expanded the number of economically feasible applications.[37]

It is apparent that Big Data are vital for companies, especially the big ones. It is argued that the successful business model of firms like Facebook, Amazon, Apple, Netflix, Alphabet/Google (the so-called "FAANG") relies upon the generation of big data as an economic commodity similar to labor or capital.[38] Data-based service providers do not usually explicitly admit that their profits depend on the collection of consumers' personal data and that they may also sell this data to other corporations. Instead, they promote the idea that internet interaction represents users having critical access to an information space, similar to that of press freedom, although the reality is that these companies offer users the right to access the internet marketplace. The services provided by big digital companies have generated enormous caches of data that have fueled the largest amount of growth in the information and communication technology sector to date. It is predicted that data-rich markets will continue to evolve and impact the financial sector worldwide, and that they will more probably disproportionately benefit big digital companies.[39] If smaller companies do not manage to adapt to the commodification of meta-data and adjust their business practices accordingly, their ability to profit from data-rich markets is expected to be significantly minimized.[40]

The market for personal data is rapidly growing, and expectations are of double-digit growths in the coming years.[41] The existence of Big Data is highly attributed to the technological developments which have created new methods to extract commercial value from personal data. In particular, new technologies such as Artificial Intelligence and blockchain have created new ways of processing and exploiting personal data, through which the latter obtain significant commercial value.

3.2. Artificial Intelligence

Artificial Intelligence (AI) has radically changed the way personal data are collected and processed. AI is an "umbrella" term, referring to computer systems able to collect information from their environment, process it and then make autonomous decisions and proceed to actions in response to what their sensors have collected. Artificial Intelligence is capable of exploiting digital personal data to automate and assist existing human activities, as well as find new ways of doing things that people had not imagined before. AI is expected to add up to $15.7 trillion to the global

[37] Helveston Max N., "Consumer Protection in the Age of Big Data.", Washington University Law Review, vol. 93, no. 4, 2016, p. 868-871
[38] Viktor Mayer-Schönberger and Cukier Kenneth, "Big Data: A Revolution that will transform how we Live, Work, and Think, Houghton Mifflin Harcourt Publishing Company, 2013, p.14,15
[39] Viktor Mayer-Schönberger and Thomas Ramge, "Reinventing Capitalism in the Age of Big Data", John Murray, 2018
[40] Rebekah Dowd, "The Birth of Digital Human Rights - Digitized Data Governance as a Human Rights Issue in the EU", Information Technology and Global Governance Series, Springer, 2022, p. 6-8
[41] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p. 11-13

economy by the end of this decade.[42] Artificial Intelligence applications can process big data and through complicated mathematical and computer-based models extract correlations and conclusions about consumers' characteristics, desires and needs. Frank Pasquale has proposed an interesting metaphor for AI applications. He used the term "black box". AI systems are data-monitoring systems, like the black boxes used in aircrafts. At the same time, AI just like a black box, is mysterious for the average individual, since he or she has no clear view about the exact uses and consequences of it.[43] This metaphor highlights a challenging aspect of AI, that is the threat to the "sovereignty" of individuals over the processing and use of their data. Indeed, the biggest difference AI brings in data processing is the intense, complex processing of huge amounts of data without human interference, which generates important knowledge for businesses.[44] AI is already extensively used by most of the biggest companies, transforming many core aspects of their business model and operation. Businesses use the information extracted from AI applications to improve their products and services, as well as to attract more costumers. The attraction of more costumers is translated into more users of their services or products, and therefore more data and better AI results. That allows a company to attract more customers, more users, and better outcomes. According to a metaphor used by Andrei-Dragos Popescu, "if AI is our rocket ship, data is the fuel for this rocket". Artificial Intelligence creates a cycle, in which more personal data bring more accurate AI and better results. AI generates significant "Data Capital", which is a valuable asset of the big businesses of the digital era.[45]

3.3. Blockchain

Moreover, another important innovation regarding the economic value of personal data is blockchain technology. In the era of digital economy, data, just like labour and capital, play a fundamental role in economic activities, becoming a crucial factor of production in the supply of goods and services. The blockchain technology facilitates the realization of personal data's economic value by increasing the amount of data being processed, linking "isolated data islands", as well as by contributing to the security of data use.[46] Blockchain is crucial for securing and processing information in the digital era. The aim of this new technology is the development of an autonomous, sustainable and efficient digital financial system, by processing complex operations according to a pre-determined algorithm and without human intervention. Blockchain is structured in automated and irreversible sequences of actions from block to block. Although its original function was to structure a public transaction ledger of bitcoin, blockchain rapidly proved that it is useful in several fields of economic activity. The design of blockchain is considered highly reliable because it makes possible to have the relevant data verified and confirmed by the consent

[42] Anand Rao S., Gerard Verweij, "PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution – Sizing the prize", Pwc, 2017, p. 1-5
[43] Frank Pasquale, "The black box society – the secret algorithms that control money and information", Harvard University Press, 2015, p.3
[44] Alessandro Mantelero, "Beyond Data - Human Rights, Ethical and Social Impact Assessment in AI", Information Technology and Law Series, Volume 36, Asser Press, 2022, p. 2-3
[45] Andrei-Dragos Popescu, "The value of Data from an Artificial Intelligence Perspective", Annals of the University of Craiova for Journalism, Communication and Management, Volume 5, 2019, p. 176-177
[46] Zheng Xuejing, Xiong Hang, "How the Blockchain Technology Facilitate Data to Realize Value: The Case of Food Supply Chain", Journal of Agricultural Big Data, Vol.2, No.3, 2020, p.13-14

of the numerous users of the blockchain. Additionally, blockchain safeguards the integrity of personal data during their processing because it prevents the potential retroactive alteration of data once they passed to the subsequent block. Moreover, the mass-distributed control of the data contributes to the high level of quality and accuracy of the data. However, the absence of any control by any authorities and the irrevocable character of the procedure once it has started have raised severe concerns about data security and data treatment.[47]

All in all, new technologies and big data analytics have a revolutionary impact on the uses of personal data in the digital era. They are no longer just part of a fundamental right and part of the personality of the individual, but they have remarkable monetary value, comparable to currency. Therefore, the existing legal framework shall be re-evaluated in order to examine whether law effectively addresses the new social needs. Regulation however needs to strike a balance between different rights and values, and this is far from a simple task.[48]

4. Economic value of personal data, especially for big companies

4.1. The notion of data as "value"

Due to the increasing financial value of personal data in the digital era, data can generate profit, especially for big companies. "Commodified" personal data is a term used by some scholars to describe a discrete package of personal information that can be exchanged for something else. The process of commodifying data into a profit generating asset involves four main stages, that is the collection, processing, mining, and usage of data. In the digital field there are several methods for collecting information, from example through "clickstream data" and "cookies". Such techniques are used by websites to identify and correlate personal data through the online activity of individuals. Several methods such as algorithms and analytics software enable big companies to collect personal data. These data are then utilized to increase sales and generate revenue in many ways, for example through targeted advertising or by trading information through data brokerage companies. By merely using a smartphone or credit card in the digital era, individuals unknowingly expose their personal data to companies, the types of which vary from information about their personal life and choices to medical information and travel history.[49]

Due to their monetary value, it has been supported that personal data have become a subject of "trade". Bart Custers and Gianclaudio Malgieri categorize this "trading" of data into two different types. The first one, called "primary personal data trade", occurs when personal data are offered in exchange for money or a service. The second type is called "secondary personal data trade". In this type the data controller exchanges personal data with a third recipient, for example a business,

[47] Giuliano Zanchi, "Blockchain and Privacy" in Senigaglia Roberto, Irti Claudia, Bernes Alessandro (Eds), "Privacy and Data Protection in Software Services", Springer, 2022, p. 187-188
[48] Max N. Helveston, "Consumer Protection in the Age of Big Data.", Washington University Law Review, vol. 93, no. 4, 2016, p. 915-917
[49] Rose Blaire, "The Commodification Of Personal Data And The Road To Consumer Autonomy Through The Ccpa", 15 Brook. J. Corp. Fin. & Com. L., 2021, p. 526-529

that can thus become a second data controller, in exchange for money.[50] In everyday life, although most individuals are not aware of such a trading, they often participate in it. Many free online services, such as search engines and social media, use business models based on the collection and processing of the data of its users. Users do not pay for these services any type of fee or subscription, but they consent to provide access to their data in exchange for these services. In such contracts, though, data are not explicitly characterised as "consideration" or "payment". Businesses claim that they provide their services for free. It is important to clarify at this point and to keep in mind for the analysis below that the supply of pure personal data to a business in most cases is neither profit-generating nor sufficient for the performance of the contract. The core of the counter-performance of the individual is his or her consent as the data subject to the processing of his or her data, which is the legal ground for the processing of the data.[51]

All in all, it is clear that personal data have transformed into a new kind of currency for the digital world. Financial exploitation of personal data can take several forms and serve several purposes. However, although this phenomenon is a "status-quo" in the digital market, in the legal field the particular idea of "payment" with one's own personal data is a new and rather controversial issue. The concept of personal data as a currency in the digital age is therefore a new challenge for regulators, which cannot be dealt with only by referring to the existing data protection law.[52]

4.2. Personal data as a commodity ? - Art. 3 par. 1 (and Preamble No. 24) of Directive 2019/770

As examined above, the exploitation of the commercial value of personal data, which has been a reality for several years especially by big companies, poses a regulatory challenge that needs to be addressed by the legislator. It was not until recently that EU legislation dealt directly with this issue, with Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (referred to as DCSD). The implementation of the Directive has already been completed in most of the Member-states. In Greece, the DCSD was implemented recently, on the 9th of September 2022, by Law 4967/2022 and the amendment of the Greek Civil Code. DCSD is part of the Digital Single Market Strategy for Europe, which aims to tackle in a holistic manner the major obstacles to the development of cross-border online commerce in the Union in order to unleash its full potential.[53] The legal basis of the Directive is article 114 of the Treaty on the Functioning of the European Union and its main objective is the improvement of the establishment and the functioning of the internal market while providing for a high level of consumer protection. The provision of article 3 par.1 in combination with Preamble No. 24 of this Directive is a great example of a regulatory response to the complicated issue of treating personal data as a "currency".

[50] Bart Custers, Gianclaudio Malgieri, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law and Security Law Review, Volume 45, 2022, p. 1-5
[51] Carmen Langhanke and Martin Schmidt-Kessel, "Consumer Data as Consideration", Journal of European Consumer and Market Law, 4, 2015, p. 218
[52] Ibid., p. 221
[53] Preamble 1 of the DCSD

According to article 3§1 of the DCSD, "this Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose." Moreover, according to Preamble No. 24 of the Directive, "Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled."

4.2.1. Rationale of the article

Before Directive 2019/770, in "free" digital services the transaction of supplying a digital service or digital content by the provider was considered independent from the act of giving consent to the processing of his or her personal data by the consumer. The "terms of use" and the "privacy statements" were and still are usually drafted as separate documents by businesses, and in both of them the services are described as offered for free. However, as examined above, in practice businesses earn significant revenue by commercially exploiting consumers' personal data. The processing of the data, either based on consent or on the other legal grounds of article 6 para. 1 of the GDPR, was interpreted as an ancillary unilateral legal act besides the service contract.

However, the new Directive brings a shift of paradigm in the law of personal data with its new approach.[54]

First of all, it is important to mention that this provision in the Directive is a product of thorough discussion and convergence of different views on the issue. According to the "Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content" issued by the European Commission in 2015 (from now on "the Proposal"), the aim of the new Directive is to create a set of simple, clear rules, in order to tackle modern legal issues and remove the existing contract law barriers, and eventually contribute to the faster growth of the Digital Single Market in the EU. Through the choice of full harmonisation, the Directive aims to form a favourable legal framework for businesses, especially small and medium-sized enterprises (SMEs), while at the same time ensuring that consumers benefit from the same high level of consumer protection throughout the EU.[55]

In particular, one of the main aims of the Directive it to extend its scope to certain digital content or services which are provided against another counter-performance than money, namely personal data. The European Commission recognises that in the digital era personal data have a commercial value, "comparable to money". It acknowledges that it is a common practice among businesses to provide digital content and services not in exchange for money, but by giving access to personal data. If the European legislator applied different rules for similar contracts, he would introduce a differentiation depending on the nature of the counter-performance, and thus this would constitute an unwanted discrimination. Such a discrimination could even potentially provide an unjustified incentive for businesses to change their business model and prefer to offer digital content against personal data. Furthermore, defects of the performance features of the digital content provided in exchange for personal data have a negative effect on the economic interests of consumers. Consequently, it was decided that the best solution would be that the applicability of the rules of Directive 2019/770 does not depend on whether a price is paid for the specific digital content in question or not.[56] Nevertheless, it is highlighted that the application and implementation of the new rules must be in full compliance with the legal framework concerning data protection, namely the GDPR. Thus, the European Commission explicitly prioritises the protection of personal data and privacy as a fundamental right over as a "commodity".[57]

4.2.2. Analysis of the article

Article 3 sets, based on the subject matter, the personal and material scope of the Directive. DCSD covers only business-to-consumer transactions, therefore business-to-business transactions are excluded. First of all, it is worth highlighting that the wording of article 3 para.1 subpara. 2 in the

[54] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 1-2

[55] European Commission, "Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content", 2015, p.2

[56] Preamble 13 of the "Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content", European Commission, 2015, p.16

[57] Ibid., Preamble 22, p.18

DCSD Proposal was not the same as the final text of the article. According to article 3 of the Proposal, "This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data." The wording of the DCSD-Proposal was criticised as explicit and narrow at the same time.[58] Firstly, it was explicit that personal data could be interpreted as counter-performance of the consumer. Such a characterisation provoked severe criticism, especially on behalf of the European Data Protection Supervisor. According to him, "there might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation."[59] Finally, the term "counter-performance"[60] was not used in the final text of the Directive, and the European Parliament and the Council avoided to expressly recognize personal data as counter-performance.[61] Moreover, the scope of application was rather narrow with regard to personal data that could qualify as counter-performance. Article 3 para. 1 subpara. 2 only mentioned "actively provided" data, and Recital 14 of the Proposal excluded data automatically generated and collected by cookies as well as data "necessary for the digital content to function in conformity with the contract, for example geographical location where necessary for a mobile application to function properly", and data collected "for the sole purpose of meeting legal requirements". These restrictions were criticized and eventually the European Parliament requested a broader inclusion of personal data into the framework of the Directive.[62]

The revised text of article 3 para. 1 subpara. 2 DCSD addresses these two concerns. The revised text avoids the explicit characterisation of personal data as "counter-performance" and uses a more neutral phrasing, while the reference to personal data is mentioned in a separate subparagraph.[63] On the contrary, it is emphasized especially in article 3 para. 8, Recital 24 as well as Recital 38 of the DCSD that the safeguards of the GDPR remain respected and untouched. Directive 2019/770 avoids clarifying whether personal data should be understood as a synallagmatic counter-performance or not, a question important for the relationship between the duties of the contracting parties. However, the DCSD does not harmonise the duties of the consumer, so such an answer is not necessary to be given by this piece of legislation.[64]

In addition, the wording "actively provided" in article 3 para. 1 subpara. 2 of the Proposal was removed by the final text. Therefore, the DSCD is applicable irrespective of whether the consumer

[58] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 2

[59] European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, p.7-8

[60] For the purposes of this thesis, personal data may be referred to as counter-performance for brevity reasons, without disregarding the different views regarding the use of such a term.

[61] Laura Drechsler, "Data as Counter-Performance: A New Way Forward Or A Step Back For The Fundamental Right Of Data Protection?", Datenschutz & LegalTech/ Data Protection & LegalTech, 2018, p.40

[62] European Parliament, "Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content", A8-0375/2017, 2017, Amendments 21 and 80.

[63] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p.71

[64] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 3-4

provides the data in an active or passive way. Yet, this lack of distinction between actively and passively provided data in the Directive does not provide a clear-cut solution for data collected from a passive consumer. According to Recital 24, it suffices that personal data is "created" with the use of the digital content or service. Even a mere collection of "metadata, such as information concerning the consumer's device or browsing history" may suffice according to Recital 25. This should also cover situations in which the service provider uses cookies to collect personal data of the consumer. But this applies only if the relationship between trader and consumer "is considered to be a contract under national law". It is therefore up to the national legislator to decide about the scope of application of the new rules.

Moreover, according to article 3 para. 1, the Directive "shall apply to any contract (...)". Therefore, a contract is required, as clarified by Recital 24, in order for consumers to benefit from the consumer protection measures taken by the DCSD.[65] However, the new Directive does not harmonise the rules on the formation of contracts[66]. This leaves some important practical legal issues regarding contracts with data as counter-performance to national law, as determined by articles 3, 4 and 6 of Regulation 593/2008 (Rome I) on the law applicable to contractual obligations. The parties may choose the applicable law according to art. 3 of the Regulation based on the service terms and conditions. However, such a choice may not deprive the consumer from the protection afforded to him by the law of his habitual residence under the conditions of art. 6 para. 1, 2 Rome I.[67] Article 3 para. 10 of the Directive determines that the freedom of Member States to regulate aspects of general contract law, such as rules on the formation, validity, nullity or effects of contracts shall not be affected. As a consequence, the law of the Member States is applicable on the requirements and the preconditions of a valid contract. In Greece and other European civil law jurisdictions, such as Germany, the basic preconditions of a valid contract are the offer to conclude a contract and the acceptance of the offer by the consumer.[68] Concerning the offer to conclude a contract, in digital content or digital service contracts the initiative to conclude a contract typically originates from the trader. In any case, it is a matter of interpretation of the communication and conduct of the content or service provider and, more particularly, its general terms and conditions whether the requirements of an offer to conclude a contract are met. According to Greek Contract law, an objective (art. GCC 200) as well as a subjective (art. GCC 173) standard of interpretation must be applied. Therefore, on the one hand the question is how a reasonable consumer shall understand the communication and conduct of the service provider. Most of the big content and service providers such as Facebook, WhatsApp, Spotify and Google give a number of indications for a contract offer. Their "terms of services" are usually detailed and lengthy standardized documents, in which the term "contract" is regularly used.[69] Many of the issues dealt with in the terms and conditions are typical for contractual relationships. Therefore, for an average consumer, this kind of communication shall appear as an offer to conclude a

[65] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 3-5

[66] The DCSD does not harmonize the formation and validity of contracts, see Article 3 para. 10, according to which "this Directive shall not affect the freedom of Member States to regulate aspects of general contract law, such as rules on the formation, validity, nullity or effects of contracts, including the consequences of the termination of a contract in so far as they are not regulated in this Directive, or the right to damages".

[67] Axel Metzger, "Data as Counter-Performance What Rights and Duties do Parties Have?", Jipitec, 2017, p. 3

[68] Mihael Stathopoulos, «Epitome of General Law of Obligations», Sakkoulas Publications S.A., 2016, p. 26-30

[69] See for example the "Terms of Service" of Facebook, Available at: https://www.facebook.com/terms.php

contract. On the other hand, the subjective criterion is also necessary to be examined, so the personal view of the consumer concerning a specific case must be taken into consideration. In relation to the acceptance of the offer by the consumer, it may be explicit, by clicking boxes or similar features on the service's website, or implicit, if the use of the service or reception of the content requires a request by the user. According to article 189 GCC, in order for a contract to come into existence the provider must become aware of the acceptance of the offer. It could be argued that the customary practice for digital services is to expect no kind of an explicit notification of the user of those services. [70]

Regarding the validity of the contract, although the DCSD does not harmonize the formation and validity of contracts, in principle a valid contract shall be required. Yet in some cases, for instance when the data-subject's consent is invalid according to the GDPR, some of the provisions of the DCSD should be applied "mutatis mutandis" to invalid contracts as well, so that consumers enjoy an equivalent level of protection. The legal foundation for such an analogy could be the "abstraction principle", which is a fundamental principle in Greek civil law and other jurisdictions. According to the abstraction principle, the agreement on the rights and obligations of the parties and the transactions in rem have to be separated. One of them may be valid, while the other may be void. Although consent in the processing of personal data is not a transaction in rem stricto sensu, it seems reasonable to distinguish between the contractual promise to provide data and consent on the one hand and the performance of this promise on the other. Such an interpretation is preferable since it results in higher level of protection for the consumers, which is a central aim of the DCSD.[71] If the validity of the contract depended on the validity of consent, then businesses could profit from their non-compliance with the GDPR since consumers would be deprived from the protection of the DCSD. Therefore, even invalid consent shall be considered sufficient to apply the DCSD, if of course the other requirements are met.[72] All in all, it is to the best interests of the consumer to apply a wider interpretation of the term "contract" in article 3 par. 1 so that the invalidity of the contract does not automatically equals the inapplicability of the Directive.

Furthermore, the Directive does not apply to cases "where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose". This exception is reasonable, because in these occasions personal data are not commercially exploited, so there is no need for the consumers to enjoy the same consumer rights as if they were paying with money. In other words, in these cases personal data do not function as a 'counter-performance'. The Proposal in its 14th Preamble offer some examples that fall within the exception. For instance, data necessary for the digital content to function in conformity with the contract may be the geographical location, in the case for example of the mobile application

[70] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 2-6 and General Principles of Greek Civil Code

[71] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p.3

[72] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 6-8

"Google Maps".[73] Concerning the exception of the sole purpose of meeting legal requirements, Preamble 25 of the DCSD mentions as example cases where the registration of the consumer is required by applicable laws for security and identification purposes.[74] By contrast, data provided, for instance, for registration purposes on the basis of a contract that allows access to user's data, would be subject to the DCSD.[75] Moreover, according to Preamble 25 of the DCSD, "this Directive should also not apply to situations where the trader only collects metadata, such as information concerning the consumer's device or browsing history, except where this situation is considered to be a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of this Directive to such situations, or to otherwise regulate such situations, which are excluded from the scope of this Directive." "Metadata" means data on (other) data, while the "information concerning the consumer's device or browsing history" include data such as the version of software or the serial number of the device. Metadata fall within the scope of the Directive only in case its collection is recognised by national law as part of a contract. It should be mentioned that the reference to "cookies" which was found in the Proposal has been removed from the final text, so it is up to the interpretation of national contract law in which cases there is a contract, including those where data are collected through cookies following the express consent of the consumer.[76]

4.2.3. Interplay with data protection law – the intervention of EDPB

As already made clear, in the digital age personal data are the subject matter not only of data protection law but also of contract law and consumer protection law. On the one hand, contract law focuses on the regulation of the new technological developments that affect the economic activity, aiming to create an effective legal framework which respects the will of the parties and promotes economic growth. Consumer law aims to protect the interests and rights of the consumers, which are affected due to the new technologies. Data protection law, on the other hand, focuses on the controlling of personal data as part of the personality of individuals, by providing them with legal rights and setting rules and restrictions to private and public entities that process them. In other words, "consumer law deals with fair contracting, data protection law with fair processing".[77] The interplay between them is inevitable when it comes to the regulation of the

[73] Preamble 14 of the Proposal for a Directive of the European Parliament And Of The Council on certain aspects concerning contracts for the supply of digital content", European Commission, 2015, p.16-17

[74] Preamble 25 of the DCSD, according to which "Where digital content and digital services are not supplied in exchange for a price, this Directive should not apply to situations where the trader collects personal data exclusively to supply digital content or a digital service, or for the sole purpose of meeting legal requirements. Such situations can include, for instance, cases where the registration of the consumer is required by applicable laws for security and identification purposes."

[75] Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p.6

[76] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p. 72

[77] Natali Helberger, Frederik Zuiderveen Borgesius & Reyna Agustin, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", Common Market Law Review, Volume 54,

monetary value of personal data and their use as a "counter-performance", posing several legal issues.

As already mentioned, the GDPR is the most important and detailed piece of legislation regarding data protection in the EU. It contains general principles and rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.[78] These rules are of mandatory nature, meaning that it can be enforced by data protection authorities regardless of the data subject's will, while sanctions for breach of the GDPR are mainly of an administrative nature.[79] Therefore, the GDPR is an instrument of public law seeking to protect the fundamental rights of individuals and so its rules are mandatory. On the other hand, Directive 770/2019 is an instrument of private law aiming to contribute to the proper functioning of the internal market while providing for a high level of consumer protection.[80] As a result, a contract for the supply of digital content or services in exchange for personal data is subject to at least two distinct legal regimes, the private law regime of the DCSD, as implemented in national law, and the public law regime of the GDPR. The fact that a contract for the supply of digital content will be subject to two distinct legal regimes raises the question of their mutual relationship. Directive 2019/770 states explicitly in article 3(8) that its provisions shall be without prejudice to the data protection legislation. In the event of conflict between them, the latter prevails.[81]

Firstly, it should be examined which is the legal basis, among those indicated by article 6(1) GDPR, for the process of personal data when they function as a "counter-performance" in contracts falling within the scope of DCSD. Under this provision, there are three main legal grounds for data processing that could be relevant in our occasion. The first one is the case where consumer gives his or her consent[82], the second refers to the processing which is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject[83] and the third one is related to the over-riding legitimate interests of the data controller.[84] As mentioned above, cases where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with the DCSD or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose, do not fall within the scope of DCSD. Therefore, consent seems to be the only possible legal ground for the process of personal data falling within article 3(1) of the DCSD.[85]

According to the GDPR, there are some specific prerequisites in order for the consent to be valid. First of all, the consent must be freely given. According to article 7(2) of the GDPR, individuals are able to give consent "in the context of a written declaration which also concerns other matters",

---

Issue 5, 2017, p.5 and Evangelos Margaritis, «Personal Data & Consumer Protection», Nomiki Vivliothiki, 2020, p. 259

[78] Article 1 of the GDPR

[79] Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p. 3

[80] Article 1 of the DCSD

[81] Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p. 5-6

[82] Article 6(1)(a) of the GDPR

[83] Article 6(1)(b) of the GDPR

[84] Article 6(1)(f) of the GDPR

[85] Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p. 5-6

as long as the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language". Moreover, consent may be withdrawn at any time[86]. The withdrawal has an ex nunc effect, therefore the processing prior to the withdrawal remains legal. Furthermore, according to article 7(4) GDPR, "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". The consent to the contract for the provision of a service is conceptually and legally different from consent to data processing, thus it shall be indicated separately[87]. The purpose of article 7(4) GDPR is to prevent any pressure on the consumer's freedom of choice and to make sure that his or her consent is genuine, reflecting their real will. [88] Someone may argue that since in contracts falling within article 3(1) of the DCSD consent is given in exchange for a digital service or digital content and, therefore, under the condition that they receive this service or content, the consent is conditional and thus not freely given. However, bearing in mind that the aim of article 7(4) GDPR is to ensure that the consent is a free genuine choice of the data subject, it seems that as long as the participation of the consumer in the contract is his or her genuine choice, then consent should also be considered freely given. Therefore, contracts with personal data as a "counter - performance" are in principle compatible with the provisions of GDPR, having the consent of the consumer as a legal basis.

Furthermore, the EDPB's Guidelines 2/2019 contain several interesting points on the issue. Regarding the legal basis of processing, the EDPB holds that in order for article 6(1)(b) of the GDPR to be applied, the processing needs to be either "objectively necessary for the performance of a contract with a data subject" or "objectively necessary in order to take pre-contractual steps at the request of a data subject".[89] EDPB explains that the content of the terms of the contract is not enough in order to distinguish what is necessary for the performance of the contract. Moreover, the reference or mention of data processing in a contract is not by itself an adequate indicator to conclude that the processing of personal data in question fall within article 6(1)(b). Furthermore, the existence of terms which explicitly impose additional conditions relating to "advertising, payments or cookies, amongst other things" cannot lead to "artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of article 6(1)(b)".[90] It is also worth mentioning that article 29 Working Party on its Opinion 06/2014 emphasized that in relation to Directive 95/46, which was then repealed by the GDPR, the provision must be interpreted strictly, limited only to occasions in which the processing is genuinely necessary for the performance of a contract. Therefore, the cases in which the contract may be a lawful basis for the processing of personal data for the supply of digital content or services are very limited, taking also into consideration the exceptions of article 3(1) of the DCSD. In case the service or content provider wants to proceed to the "profiling" of his or her customers, even if he or she includes a relevant provision on the

[86] Article 7(3) of the GDPR
[87] for example, in different clauses or boxes to tick
[88] Rafał Mańko and Shara Monteleone, "Briefing - Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service, European Parliament, May 2017, p. 5-6
[89] European Data Protection Board, "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects", Version 2.0, 2019, p. 8
[90] Ibid., p. 9-10

contract, this mere indication does not make this specific processing "necessary for the performance of the contract" in light of data protection law and the provider will need to rely on a different legal basis to conduct the profiling activity. Thus, the mere fact that the purposes of the processing are covered by contractual clauses drafted by the service or content provider dot not automatically mean that the processing is necessary for the performance of the contract. Yet, the EDPB argues that "processing for personalisation of content […] may constitute an essential or expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases". However, "where personalisation of content is not objectively necessary for the purpose of the underlying contract, for example, where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service, data controllers should consider an alternative basis". [91] Moreover, the EDPB highlights the distinction between the concept of entering into a contract and giving consent within the meaning of article 6(1)(a). This distinction is important for service or content providers, because these concepts have several differences especially regarding data subject's rights and expectations. EDPB also emphasizes that the "necessity for the performance of a contract" does not constitute a legal ground for the processing of special categories of personal data and service or content providers need to have the explicit consent of consumers, in accordance with the GDPR conditions when processing such data.[92] Another important issue is whether traders can rely on article 6(1)(b) as the legal basis for processing personal data for its subsequent versions and updates, taking into consideration that service updates are crucial in order to keep the services safe and secure.[93]

On the other hand, the European Data Protection Supervisor (EDPS) has explicitly opposed to the concept of treating personal data as a type of counter-performance. In Opinion 4/2017, the EDPS recognised that the data-driven economy is important for the growth of the EU and supported the aim of the proposed DCSD to ensure the protection of consumers who are required to disclose data as a condition for the supply of digital goods or services. However, it was unsupportive against the idea that people can pay with their data. EDPS warned against any provisions stating that "people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity". [94] It is important to note that the EDPS' Opinion refers to the DCSD in its version as a proposal and not as official text.[95] The EDPS acknowledges that the scope of the proposed DCSD has the objective to cover services generally considered as "free", which tend to be based on "an economic model where personal data are collected by the providers in order to create value from the data processed". However, personal data cannot be compared to a price, as it is related to the fundamental right to the protection of personal data. The EDPS also supported that "there might well be a market for personal data, just

[91] European Data Protection Board, "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects", Version 2.0, 2019, p. 14-16
[92] Ibid.
[93] Maria de Almeida Alves, "Directive on certain aspects concerning contracts for the supply of digital content and digital services & the EU data protection legal framework: are worlds colliding?", Unio - Eu Law Journal, Vol. 5, No. 2, 2019, p. 38-40
[94] European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, p. 3
[95] Maria de Almeida Alves, "Directive on certain aspects concerning contracts for the supply of digital content and digital services & the EU data protection legal framework: are worlds colliding?", Unio - Eu Law Journal, Vol. 5, No. 2, 2019, p. 37-38

like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation". Whilst the comparison seems at first glance quite disproportionate, it is not completely irrational in legal terms to avoid the monetization of a fundamental right, as if it were nothing more than a commercial transaction. Furthermore, there are noticeable differences between paying a price with money and giving data as a counter-performance, as stated by the EDPS: "while the consumer is aware of what he is giving when he pays with money, the same cannot be said about data. Standard contractual terms and privacy policies do not make it easy for the consumer to understand what is precisely made with the data collected about him/her".[96] Moreover, EDPS proposes some alternatives to avoid the characterisation of personal data as counter-performance. The first one refers to a broader definition of "services", in order to include services where a price is not paid but they are normally provided for remuneration, while the second one proposes the use of similar terms to the GDPR, in order to define the scope of the DCSD, avoiding in any case the reference to data used as counter-performance.[97] As already mentioned, the DCSD avoided to explicitly refer to personal data as "counter-performance", without however adopting the alternatives of the EDPS.

4.2.4. Arising legal issues

4.2.4.1 Withdrawal of the consent to process personal data provided as "counter – performance"

Its was analysed above that consent is the main legal basis concerning the process of personal data provided in a contract falling within the scope of Directive 2019/770. One of the main legal issues related to consent is related to the right of withdrawal, and especially the contractual consequences of exercising this right. According to article 7 para. 3 of GDPR, "the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent." Moreover, according to recital 42 of the GDPR, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." As a result, and due to the supremacy of the GDPR over the DCSD, individuals shall always be free to withdraw their consent, even in case their personal data are given in exchange for a service. This is also explicitly mentioned in the DCSD in preamble 39. According to it, "the right to erasure and the consumer's right to withdraw consent for the processing of personal data should apply fully also in connection with the contracts covered by this Directive. The right of the consumer to terminate the contract in accordance with this Directive should be without prejudice to the consumer's right under Regulation (EU) 2016/679 to withdraw any consent given to the processing of the consumer's personal data." If the consumer withdraws his or her consent, the supplier of the

[96] European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, p. 6-10
[97] Ibid., p. 10-11

content or service is obliged to stop processing the data collected by this specific consumer and in principle delete them. However, such a withdrawal will create a severe imbalance in the contractual relationship. Therefore, there may be further consequences for the contract as a whole, which are not clearly regulated by either GDPR or the DCSD.[98]

First of all, the fact that the data subject can withdraw his or her consent freely seems to be in contradiction with the binding nature of the notion of obligation. However, this is an issue present also in other service contracts. In medical treatment contracts, for instance, which interact with public law regulation and fundamental rights, patients are allowed to retract their consent in every stage of the medical treatment. Yet, unlike contracts with personal data as "counter-performance", the data object, that is the patient, is informed about all stages of the treatment and observes the treatment which makes it easier for the patient to retract. One solution for contracts with personal data as "counter-performance" could be to include a term in the contract specifying the consequences of the withdrawal of consent as well as what happens with regard to the future use of data. Such a contractual term shall in any case be in accordance with the provisions of the GDPR, namely preserving the "freely given" character of the consent.[99]

In the absence of such specification, it is not clear according to the existing legal framework whether the withdrawal of consent shall lead to the termination of the contract**.** One possible solution would be that, as a consequence of the withdrawal of consent, the service obtained in exchange for data as a counter-performance, will also be legitimately terminated. This approach considers data provided by the consumer as consideration and treats it as a "license" to use the data for the service or digital content. Contracts where personal data are provided as "counter-performance" for a digital service or digital content can be regarded as long-term contracts, due to the fact that the consent requirement does not form the subject matter of the contract but it is rather a duty of the consumer to tolerate the processing thereof. Accordingly, the result of the withdrawal of consent would be the termination of the contract in question. Indeed, article 7(3) of the GDPR can also be interpreted within the concept of long-term contracts as it produces only effects for the future without affecting the lawfulness of the past processing of data subject's data.[100]

Another solution would be the partial termination of the contract. If partial termination is possible, the arising legal issue is which specific parts of the services or content shall not be provided anymore and on what grounds. For instance, if the consumer exercises his or her right to withdrawal because of the abuse of personal data, breach or non-performance on behalf of the service or content provider, then maybe the contract should continue to operate with regards to the benefits received before the date of the termination. In such a case, the consumer may also be entitled to compensation, although the calculation of it would be another legal issue.[101]

A solution could also be that the withdrawal of consent constitutes a breach of contract. It is claimed that withdrawal of consent should give the right to the digital content or service provider to terminate the contract unilaterally as it may become burdensome to the latter to provide the

[98] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 6-8

[99] Cemre Bedir, "Contract Law in the Age of Big Data", European Review of Contract Law, 16(3), Tilburg Law School Research Paper Forthcoming, 2020, p. 358-362

[100] Ibid.

[101] Ibid.

service or content. Yet, it is not clear at what moment the service or content provider can consider the performance of his obligation burdensome for him or her in the lack of the collection of personal data. Additionally, it needs to be considered whether the service or content provider still owes any responsibility to the consumer in the first place in cases where the former does not terminate the contract.[102]

However, an approach according to which withdrawal of consent does not constitute a breach of contract seems more dogmatically correct. According to the GDPR, the consumer must be free to withdraw consent at any time. If withdrawal was considered breach of contract, it would mean that the consumer would be obliged by the contract to consent, and therefore this would be equivalent to a waiver of the right to withdrawal. However, such a waiver would infringe mandatory law. Accordingly, withdrawal cannot provide the other party either with a claim for damages. However, such an absolute rule may be unfair for the service or content provider on some occasions. Indeed, if we want to develop a basic concept of consumer data as consideration, Carmen Langhanke and Martin Schmidt-Kessel suggest that we accept at least two possible exceptions to this exclusion of damages in case of withdrawal. First, the strong effects of the mandatory nature of the right to withdraw shall not protect the consumer from liability for fraud, in cases where the consumer deludes the business as to his intention concerning the continuity of the consent to process with the personal data. A second exception could be the situation of a "mistimed" withdrawal. This refers to the general need under a contract with an obligation to provide personal data to provide for a kind of transitional period. Such a transitional period would aim to give the business the opportunity to set an end on its data processing activities and to prevent the business from being liable for processing in the meantime of that transitional period.[103]

All in all, withdrawal of the consent to process the personal data of the consumer cannot leave the contract unaffected. Since personal data are offered in exchange for content or service, the withdrawal of consent will most probably frustrate the purpose of the contract and its future enforcement. The best solution seems to be the case-by-case examination, based on factors such as whether the consumer by withdrawing his or her consent also intends to terminate the contract, whether the service or content provider has contributed to the decision of the consumer to withdraw, the amount of data already obtained and used, as well as the position of the business in the market. If the withdrawal results in the frustration of the whole synallagmatic contractual relationship, then it would be fair for the other party, namely the business, to have a right to terminate the contract unilaterally and only exceptionally ask for compensation. In general, typical general clauses on fundamental breach or fundamental disruption of a contract would usually help to find a sufficient solution in practice.[104]

[102] Cemre Bedir, "Contract Law in the Age of Big Data", European Review of Contract Law, 16(3), Tilburg Law School Research Paper Forthcoming, 2020, p. 358-362 and Carmen Langhanke and Martin Schmidt-Kessel, "Consumer Data as Consideration", Journal of European Consumer and Market Law, 4, 2015, p. 218-222

[103] Carmen Langhanke and Martin Schmidt-Kessel, "Consumer Data as Consideration", Journal of European Consumer and Market Law, 4, 2015, p. 222 and Cemre Bedir, "Contract Law in the Age of Big Data", European Review of Contract Law, 16(3), Tilburg Law School Research Paper Forthcoming, 2020, p. 358-362

[104] Carmen Langhanke and Martin Schmidt-Kessel, "Consumer Data as Consideration", Journal of European Consumer and Market Law, 4, 2015, p. 222

Although a uniform solution in European level to the legal issue of withdrawal of consent would be beneficial[105], according to article 3 (10) of the DCSD it is up to the national legislator to regulate the aspects of general contract law, including the rules on the formation, validity, nullity or effects of contracts, the consequences of the termination of a contract in so far as they are not regulated in the Directive and the right to damages. Therefore, the solution to this legal issue is to be found in national level. In Greece, in the explanatory statement of Law 4967/2022, the Law that incorporates the DCSD in the national law, the Greek legislator emphasizes the supremacy of EU legislation concerning the protection of personal data. Moreover, it is highlighted that it would be impossible, especially in consumer contracts, merely the exercise of a right under data protection law to lead to consequences in relation to the function of a contract, such as in the field of compensation. It is not excluded, however, that the exercise of such rights on behalf of the recipient of the service, such as the right to withdraw his or her consent to the processing of his or her data, may affect the contractual relationship between the individual and the business, especially in contracts with duration. An important criterion in the evaluation and assessment of the extent of the above effect on the function of the contract is the eventual frustration of the balance between performance and counter-performance.[106] Therefore, in the example of Greece, it seems that the aforementioned proposed solution could be in accordance with the views and aims of the national legislator.

4.2.4.2 Relation to the notion of unfairness under Consumer Protection Law

Another important legal issue is raised in cases where the economic exploitation of personal data may constitute an unfair commercial practice falling within the scope of Directive 2005/29 (Unfair Commercial Practices Directive – UCPD) or may be related to an unfair contract term falling within the scope of Directive 93/13/EEC (Unfair Contract Terms Directive – UCTD).

The "commodification" of personal data as such does not constitute an unfair commercial practice. However, additional elements may make it unfair, if the process of personal data in the situation in question materially distorts or is likely to materially distort the economic behaviour of the consumer and in general if the conditions of the UCPD are met.[107] It is a common practice for many digital services to claim that they are provided for free, explicitly or implicitly. For example, in Facebook's terms and conditions it is mentioned that "it does not cost money to use Facebook. Instead, we charge advertisers to show ads on the Facebook family of apps and technologies. This helps us make Facebook available to everyone without charging people for access to it".[108] Although this statement is true, it does not clarify that personal data of the users are used in exchange of the provided services. Consumers are often not aware, or at least not fully aware, that when they use a "free" service, the data they provide, and to be precise their consent to the

[105] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p. 73
[106] Explanatory statement of Law 4967/2022, interpretation of Article 5, p. 48-49
[107] Evangelos Margaritis, «Personal Data & Consumer Protection», Nomiki Vivliothiki, 2020, p. 257-258
[108] Facebook Terms and Conditions, available at : https://www.facebook.com/terms.php

processing, function as a counter-performance. Furthermore, users rarely read the terms and conditions of online platforms such as Facebook, especially when they are provided without paying a subscription fee. The practice of labelling a service-for-data transaction as "free" could possibly fall under the UCPD's blacklist. According to the UCPD, describing a product as 'free' although the consumer has to pay anything other than the "unavoidable cost" of responding to the commercial practice and collecting or paying for delivery of the item, is categorically unfair.[109] Facebook and other businesses with similar practices may be held to have infringed this blacklisted practice by promising that a product is for free when they actually collected data from their users and monetised it. [110]

Another legal issue can be spotted on the relation between the "commodification" of personal data and the unfairness of contractual terms based on the Unfair Contract Terms Directive (UCTD). Under the UCTD, the assessment of the unfairness cannot be conducted on terms relating to the "definition of the main subject matter of the contract nor to the adequacy of the price and remuneration".[111] If we accept that personal data are nowadays understood as "price" or "digital representation of value" according to Directive 2019/770, then the application of the UCPD to instances of monetization of consumers' personal data by traders seems to have been excluded. However, if we share the view that personal data are not a "price" nor a "counter-performance", then the UCTD may apply.[112]

Furthermore, the new uses of personal data by big companies due to the technological development can be problematic in terms of fairness. As already made clear, personal data can generate profits to businesses in many ways. One of them is called "personalized pricing" and it refers to the practice of businesses to use personal data offered by the consumers in order to vary the prices offered to them according to their special characteristics. When personalized pricing comes in the form of lowered individual prices, this trend could be seen as a positive one. Indeed, some consumers can receive lower prices due to algorithmic formulas, through pop-up discounts aimed at consumers who display hesitant qualities. However, other consumers are charged higher prices. Personalized pricing takes into consideration personal data such as the geographical location, the browsing history and purchasing history of consumers and provides businesses with information about the special characteristics of consumers, according to which these businesses determine how much they will charge them. Although personalized pricing is increasingly common among companies, it is increasingly unpopular among consumers. The European Commission has found that a "clear majority of Internet and online platforms users" (ranging from 55%-58%) feel uncomfortable with the use of their personal data to "tailor advertisements or content."[113] As derived from article 6(d) of the UCPD, businesses must disclose the price of their services and the manner in which the price is calculated. In Case C-611/14 (Canal Digital Danmark), the CJEU held that a practice is misleading when it is likely to "give the average consumer the false

[109] Point 20 of the list of commercial practices which are in all circumstances considered unfair in Annex 1 of the Directive 2005/29/EC (Unfair Commercial Practices Directive)
[110] Lucas Forbes, "Modernizing Consumer Law in the Fourth Industrial Revolution", Columbia Journal of European Law, Vol. 27, No. 2, 2021, p. 210-211 and Goanta Catalina and Mulders Stephan, "'Move fast and break things': Unfair commercial practices and consent on Social Media.", Journal of European Consumer and Market Law, 8, 2019, p. 136, 146
[111] Article 4(2) of the UCTD
[112] Mateja Durovic and Franciszek Lech, "A Consumer Law Perspective on the Commercialization of Data", European Review of Private Law 5-2021 Kluwer Law International BV, 2021, p. 725-726
[113] Report to the Commission from TNS opinion & social: Online Platforms, 2016, 52

impression that he has been offered a favourable price." Thus, as long as businesses duly inform consumers about the prices and the way they are calculated, they are free to personalize prices. However, it is not clear if a statement of "personalized pricing" is sufficient or if a more elaborate explanation is needed.[114]

4.2.5. Case law – decisions of DPAs

These issues are only a few of the numerous legal issues that arise because of the perception of personal data as a "currency" in the digital age. In the context of this examination, it would also be interesting to look through the case law of the Court of Justice of the European Union (CJEU), the national Courts of the Member - States as well as decision of Data Protection Authorities (DPAs) relevant to the legal issues arising from the commercialization of personal data. As examined above, article 8 of the EU Charter of Fundamental Rights defines data protection as a fundamental right, without setting any rule about "market-inalienability" of personal data[115]. In other similar cases of fundamental rights, prohibitions on certain activities are explicit, such as the one of article 3.2 of the Charter in which it is explicitly prohibited to make human body and its parts a source of financial gain. Using the argumentum in contrario, it could be said that the European legislator intended to differentiate the legal regimes between corporeal and incorporeal attributes of personality.[116]

In most cases the CJEU has dealt with the issue of balancing the right to data protection against public interests or other fundamental rights[117]. Case C-275/06 (Promusicae v Telefonica de Espana) and Case C-131/12 (Google Spain SL, Google Inc v Agencia Espaiola de Proteccion de Datos) are two cases in which the Court in its Judgements tried to balance the data protection right against economic rights. In the "Promusicae" Case the Court focused mainly on the procedures of transposing and implementing EU Directives that affect different fundamental rights, and in particular in relation to the rights to intellectual property and data protection. The CJEU in §70 of its decision ruled that "when transposing those directives, Member States [must] take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those

[114] Lucas Forbes, "Modernizing Consumer Law in the Fourth Industrial Revolution", Columbia Journal of European Law, Vol. 27, No. 2, 2021, p.208-210

[115] Something that is market inalienable is not to be traded in market

[116] Giuseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection.", European Review of Contract Law, vol. 14, no. 4, 2018, p. 384-386.

[117] e.g. C-93/09, Volker und Markus Schecke GBR and Hartmut Eifert v Land Hessen, in which the Court dealt with the issue of the European Union's interest to guarantee the transparency of its acts and ensuring the best use of public funds, Case C-291/12, Michael Schwarz v Stadt Bochum, where the Court struck a balance between the right to data protection and the public interest of preventing illegal entry into the European Union, and Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Ireland and Kdrntner Landesregierung, Michael Seictlinger, Christof Tschohl and others, in which the data protection was in conflict with the public interest of fighting serious crimes. Giuseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection.", European Review of Contract Law, vol. 14, no. 4, 2018, p. 382-384.

fundamental rights or with the other general principles of Community law, such as the principle of proportionality". In the "Google Spain" case, the Court gave a clear preference to the data protection right at the expense of the freedom to conduct a business. It stated that the processing of personal data carried out by the operator of a search engine, with side effects on the fundamental rights to privacy and to the protection of personal data, "cannot be justified by merely the economic interest which the operator of such an engine has in that processing"[118]. Therefore, in the specific case, the freedom to conduct a business could not be a barrier to the recognition of the so-called right to be forgotten, which entails, under the request of a data subject, the obligation of the economic operator to remove personal information relating to that subject from the list of results displayed on the search engine. From these two Judgements it may be concluded that according to the European Court of Justice data protection rights can impose limits on economic rights, but they cannot exclude them altogether. In any case, a balancing is needed.[119]

Moreover, it is worth mentioning the Opinion of Advocate General Campos Sánchez-Bordona delivered on 6 October 2022 in Case C-300/21 (UI v Österreichische Post AG), which is about non-material damage resulting from unlawful processing of data, and constitutes an interesting approach on the issue. In footnote 53, the Advocate General argues that "I am not ruling out that the body of legal rules is evolving in the direction of granting property rights to the data subject. However, I doubt that this would lead to the maximisation of individual control: a position where data subjects had powers of ownership over personal data may not fit well with the development of the economy and innovation; its compatibility with the fundamental right aspect is questionable. See recital 24 of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ 2019 L 136, p. 1): 'While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity …'." Moreover, in §78-82 he argues that "it is helpful to point out that the protection of personal data is expressed as an objective of the GDPR, in addition to the aim of promoting the free movement of data. Strengthening individuals' control over their personal information in the digital environment is one of the recognised aims of the modernisation of the rules on the protection of personal data, albeit not an independent or isolated aim. The Commission, in the Communication accompanying its proposal for the GDPR, associated a high level of protection of data with trust in online services, which enables the potential of the digital economy to be fulfilled and encourages 'economic growth and the competitiveness of EU industries'. The modernisation (and increased harmonisation) of the EU legislation enhances 'the Single Market dimension of data protection'. In light of the clear value of (personal and non-personal) data to economic and social progress in Europe, the GDPR does not seek to increase the control of individuals over information concerning them, by merely giving way to their preferences, but rather to reconcile each person's right to protection of personal data with the interests of third parties and society. The aim of the GDPR is not, I stress, to limit systematically the processing of personal data but rather to legitimise it under strict conditions. That aim is served especially by promoting confidence on the part of data subjects that processing will be carried out in a safe environment, to which the data subjects themselves

[118] § 81 of the Judgment

[119] Giuseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection.", European Review of Contract Law, vol. 14, no. 4, 2018, p. 384-386.

contribute. This encourages the willingness of data subjects to permit access to and use of their data in, among other spheres, the sphere of online commercial transactions."[120]

Furthermore, the Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020 on the Joined Cases C-682/18 and C-683/18 [Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C-682/18) and Elsevier Inc. v Cyando AG (C-683/18)], is important because, although it does not deal with a balancing between data protection and economic rights, it explicitly recognizes that personal data represent a price. More specifically, the Advocate General argues that services provided by operators such as Youtube and Cyando are provided "for remuneration" and "the fact that an operator such as YouTube is remunerated in particular from advertising and that it does not require payment directly from users of its platform does not call this interpretation into question."[121] "The service cannot […] be described as being 'free' for users. […] YouTube gathers a large amount of personal data concerning its users, that data representing, in themselves, a price."[122] From these Opinions it could be argued that the economic value of personal data is acknowledged and, although under strict conditions, the Advocate Generals proceed to a balancing between the fundamental right to data protection and economic rights.

Furthermore, in relation to the aforementioned legal issue of the interpretation of the Unfair Commercial Practices Directive in the light of personal data as a commodity, it is interesting to see an example of how a national Court has dealt with it. On 6 October 2021, Hungary's Supreme Judiciary body (Kúria) ruled in its Judgment on Case BH2022.24 (Facebook Ireland Ltd. v Hungarian Competition Authority) that the previous slogans on Facebook's opening page "free and anyone can join", later "free and will remain free" did not constitute a misleading commercial practice in terms of § 6(1) lit. c) of Act XLVII of 2008, which transposed the Unfair Commercial Practices Directive into Hungarian law. The provision corresponds to Article 6(1)(d) UCPD. The legal issue was whether the prohibition of misleading information with regard to the 'price' as the consumer's counter-performance for a product or a service also covers the provision of personal data as the counter-performance in exchange for a product or a service. In contrast to the Hungarian Competition Authority, Hungary's Supreme Court refrained from an expansive interpretation of the concept of 'price' in its Judgment. The Kúria pointed out that the information in the Help Centre of Facebook clearly implied that the terms "free" and "payment" meant free of any payment of money, since the introductory question of the information was put in this context: "Does it cost money to use Facebook?" In addition, the phrase "free and will remain free" on the opening page means that if the consumer perceives the service as free while visiting the opening page, this will not change. The Kúria shared the view of the Budapest Regional Court that the data provided by the consumers 'in exchange' for the use of the social network service and the 'tolerance' of targeted advertising do not fall within the scope of § 6(1) lit. c) UCP Transposing Act. This case highlights the possible discrepancy which, after the entry into force of the DCSD, might exist between the 'status' of personal data in consumer contracts (article 3(1) 2nd subpara DCSD) and the valuation of business models involving the provision of personal data by consumers under

[120] Opinion of Advocate General Campos Sánchez-Bordona delivered on 6 October 2022 in Case C-300/21 (UI v Österreichische Post AG)
[121] Footnote 11, par. 142 and footnote 132 of the opinion
[122] Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020 on the Joined Cases C 682/18 and C 683/18 [Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C 682/18) and Elsevier Inc. v Cyando AG (C 683/18)]

unfair commercial practices law.[123] However, it is an interesting coincidence that since August 2019, the welcome tagline of Facebook was changed from "it's free and always will be" to "it's quick and easy". This happened three months after the adoption of the DCSD (20 May 2019). Mark Bartholomew, professor at the University at Buffalo, has commented on this change that it may have come "because of public sentiment. […] The public, no longer sees Facebook as 'free' — that rings hollow now. […] It's almost a cliché to say that you are the product, but everyone now realizes that Facebook tracks you and beams ads to you. It's not a public service."[124]

Furthermore, in case CdS – 202102630, the Italian Council of State found that Facebook failed to provide its users with transparent information concerning the commercial exploitation of their personal data. At the same time, it found that the opt-out approach used for registering users to the platform did not constitute an aggressive conduct. The Italian Court made some interesting points claiming that the information provided in Facebook's privacy and cookie policy are "general and unspecific" and the stress is on the free nature of the services, rather than the actual use of personal data. On the other hand, the user is presented with "intimidating" information about the consequences of opting out to the use of personal data for commercial purposes. Hence, the "user remains convinced that the achievement of the advantages associated with access to the platform is free, not being able […] to recognise and realise that in return for the advantage there is automatic profiling for commercial use, not clearly and immediately indicated at the time of first access, as an inevitable consequence of the provision of the data."[125]

Moreover, Decisions of national Data Protection Authorities have expressed some interesting views on the issue as well. The Greek DPA, by Decision No 35/2022, found that in the case of "Clearview AI Inc", an American company which markets facial recognition services, violated the principles of lawfulness and transparency (art. 5 paragraphs 1(a), 6, 9 GDPR) and its obligations under articles 12, 14, 15 and 27 of the GDPR, imposing a fine of twenty million euros. This company collects photos that are publicly available on the Internet and extracts information from these including geolocation metadata as the photo may contain and information derived from the facial appearance of individuals in the photos. According to the DPA, "the automated processing of personal data […] for the purpose of assessing the personal aspects of a natural person constitutes profiling and the making available to users of the defendant's services, who search the defendant's facial recognition platform, constitutes surveillance on the internet. Moreover, the purpose of the tool marketed by the defendant is to enable the identification and collection of information in relation to a particular person. Biometric processing techniques used by the defendant to enable a person to be targeted ultimately lead to profiling as a result of a search by a user of the defendant's tool. This search is renewed over time, as the database is constantly updated, which makes it possible to establish the possible evolution of information relating to a particular person, in particular if the results of successive searches are compared with each other." Although in the context of this decision the Greek DPA did not discuss the issue of the financial value of personal data, it is important because it refers to the "added-value" of personal data created

[123] Ferenc Szilágyi, "Personal Data as Consideration for the Facebook Service -Case Note on Facebook Ireland Ltd. v Gazdasági Versenyhivatal (Hungarian Competition Authority) (Case BH2022.24)", EuCML, 2022, p.154-157
[124] Bote Joshua, "Facebook tweaks homepage, no longer says it is 'free and always will be", USA Today, Available at:https://eu.usatoday.com/story/tech/2019/08/27/facebook-no-longer-says-free-and-always-be-homepage/2133300001/
[125] CdS – 202102630 - Facebook Inc. V. Autorità Garante della Concorrenza e del Mercato, Giustizia Amministrativa and https://gdprhub.eu/CdS_-_202102630

through the practices of new technologies, and clarifies that the fact that data objects make personal data of theirs public on the Internet does not mean that they consent to any commercial processing of them by third parties.[126]

The Norwegian Data Protection Authority in case 20/02136-18 fined an online dating application about €6,4 million (NOK 65 million) for not collecting users' valid consent for sharing through software development kits sensitive personal data of its users with several third parties for profiling and advertising purposes. The personal data in question included advertising ID, IP address, GPS, location, gender, age, device information and app name. The Norwegian DPA adopted the view of the EDPS that personal data cannot be considered as a tradeable commodity, stating that the Norwegian DPA "has never endorsed the view that personal data may be used to pay for digital services"[127]. On the other hand, a decision of the Spanish DPA, Decision E/03624/2021, concerning the same issue, namely the processing of personal data for advertisement purposes by the same online dating application, found no violations of GDPR as to consent regarding processing of personal data for advertisement purposes or the processing of special categories of personal data. Firstly, it has to be mentioned that in the Norwegian decision a fine was imposed based on the processing that occurred using the previous "Consent Management Platform (CMP)", which had many problematic issues regarding the validity of consent, while the Spanish DPA dealt with the updated CMP, which corrected these issues, probably in response to the complaint in Norway. The Spanish DPA explicitly acknowledges that the Norwegian DPA is conducting a similar investigation and disagrees with the opinion that this service provider deals with sensitive data, regarding a person's sexual orientation.[128] The fact that there are two different decisions in almost identical cases shows on the one hand the complexity and the dynamic character of the arising legal issues, and on the other hand the need for coordination and communication between the national DPAs in order to have a homogenous interpretation of the European legal framework, without that meaning that the discussion and the potential "conflicts" between national authorities cannot be fruitful.

In case PS/00500/2020 the Spanish DPA imposed a fine of €3,000,000 to a bank for carrying out profiling for marketing purposes without obtaining valid consent. Consent was not valid because it was neither specific nor informed. After examining the way the bank was obtaining consent for the processing of personal data, the DPA concluded that the bank, as the data controller, was not providing the consumers, acting like data subjects, enough information about profiling. All the relevant information could be found in the conditions of the credit contract; however it was not specified that the client could receive, this way, marketing from third companies and from unrelated products. Consumers did not receive either information about what specific personal data would be used for such processing, nor how detailed the created profile was. The DPA concluded that the data subjects could not effectively know what kind of personal data were being processed for the profiling, since there was a difference in what was stated in the privacy policy and what the controller communicated to the DPA. The Spanish DPA came to the conclusion that the controller had not obtained valid consent as defined in article 4(7) GDPR, as it was, firstly, not

[126] Hellenic Data protection Authority, Decision 35/2022

[127] Norwegian Data Protection Authority, Decision in case 20/02136 and https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/02136-18

[128] Spanish Data Protection Authority, Decision E/03624/2021 and https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_E/03624/2021

specific, since purposes were not individually defined, nor could they be gradually consented, and secondly, not informed, since the provided information was not enough. Therefore, consent was not valid as a legitimate basis from article 6(1) GDPR, in relation to article 7 GDPR, and thus processing was unlawful. This decision highlights the importance of the freely given consent, clarifying in detail its special characteristics in order to be valid when it comes to the processing of personal data for profiling purposes.[129]

5. Effects of the perception of personal data as the currency of the digital age

5.1. Positive effects

The monetary value of personal data and their recognition as an alternative "currency" has several positive effects for the relevant market, individuals and society as a whole. Many of them have already been mentioned during the analysis above. New technologies have created new methods of collecting and processing personal data, which create significant revenue for big companies. Indeed, some of the biggest companies worldwide today such as Meta, Alphabet and Amazon have gained remarkable profits by receiving personal data as counter-performance for their services. Personal data are actually at the centre of global trade, and cross-border data flows have grown up to 112 times over from 2008 to 2020.[130] The legal recognition and regulation of personal data as a currency, under specific conditions and prerequisites and under fully harmonized cross-border rules can provide a stable ground for the further development of these companies and the elimination of the aforementioned legal issues. Moreover, the recognition of the financial value of personal data is beneficial for the individuals as well. One can hardly ignore that consumers benefit in many ways from the valuable services they receive over the Internet and other digital service providers, starting from contents and technology of every kind that makes their life easier, to search engines and social media platforms, which help them to keep up their social contacts. Consumers would have to pay a considerable share of their income if all of these services were only available on a paid with money basis. [131] At the same time, the recognition of personal data as a currency by consumer protection law can provide consumers with strong consumer rights when offering their personal data in exchange for content or services and enhance their bargaining power. Although the DCSD does not explicitly recognize personal data as a currency, the recognition of them as a valuable, "sui generis" type of "counter-performance" is important and a positive development. Furthermore, society as a whole benefits from the monetary value of personal data. Taking into account that famous companies with data-driven business models, such as Google, Apple, Facebook and Amazon have a market value exceeding the whole German car industry, it is obvious that business models which are based on personal data produce significant welfare and contribute

[129] Spanish Data Protection Authority, Decision PS/00500/2020 and https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00500/2020

[130] Matthew J Slaughter., and David H.McCormick., "Data Is Power: Washington Needs to Craft New Rules for the Digital Age.", Foreign Affairs, vol. 100, no. 3, 2021, p. 54

[131] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p.12

to the development of the economic sector and to societal progress. These businesses contribute to modern society not only through the taxation of their activities but also because due to their size they are able to support innovation and technological advancement, leading to the further broadening of digital era's horizons. [132]

5.2. Negative effects

On the other hand, this new understanding of personal data does not come without negative effects as well. First of all, there is the view that the commercialization of personal data is incompatible with their "fundamental right" nature, and therefore the recognition of them as a currency poses serious threats against human rights. Furthermore, it is argued that the creation of a "market model" is problematic, as there are several indications for market failure. The first one is relevant to the lack of competition. It is true that on many occasions consumers do not really have the opportunity to choose between paid services and services which are based on the processing of personal data, neither have the choice between more or less "data-intensive" services. In the market for personal data there are some "dominant" internet services, especially in the field of social media, which the majority of people use. These dominant businesses in fact impose their business model to consumers, without the latter having a choice to alter the terms and conditions. A second problem is related to information asymmetry. Despite overly detailed and lengthy terms and conditions or privacy statements of big companies, consumers are rarely aware of what they consent to. Consumers hardly ever read terms, but instead they just tick boxes and continue with the use of the service. The blame for the length and complexity of privacy statements does not solely lie with the service providers but also with the European and national legislatures which have created a "regulatory jungle" for all the parties involved.[133] Consequently, consumers tend to actually have limited bargaining power when concluding digital service or digital content contracts, which reduces their autonomy.[134] This data subject's limit in freedom of choice as to what contracts to conclude and on what terms in combination with the fact that digital platforms such as Facebook and WhatsApp have become integral part of modern communication and connectivity, may also raise questions about whether their consent is in fact freely given, according to the GDPR. Moreover, when personal data are used as a means of exchange in contracts, other fundamental rights and values may also be endangered. Personal data offered as counter-performance by individuals may be used for profiling purposes, which may consequently lead to discrimination. Indeed, the personal data of consumers may be used against them. For instance, businesses may exclude people from specific services or offer them specific services at a higher or lower price according to their special characteristics.[135] Profiling and personalisation of services or content through the processing of personal data also raises concerns about the balance of power,

[132] Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p.12
[133] Ibid., p.12-14
[134] Cemre Bedir, "Contract Law in the Age of Big Data" European Review of Contract Law, vol. 16, no. 3, 2020, p.4
[135] Marc Van Lieshout, "The value of personal data", Conference Paper in IFIP Advances in Information and Communication Technology, 2015, p. 11-13

transparency and the autonomy of consumers.[136] All in all, all these effects, both positive and negative, shall be taken into consideration when it comes to the regulation of personal data as a currency.

6. Challenges to regulate personal data as currency

6.1. By means of legislation

It is clear that the regulation of personal data as a "currency" is not an easy task for legislators. The main challenge is the "dual character" of personal data, both as part of a fundamental right and as a "commodity". The fact that personal data are protected as a fundamental right in the European Union in combination with the strict rules set by the GDPR make the regulation of personal data in contract law and consumer law a challenge. In principle, personal data are inalienable, meaning that individuals cannot waive or transfer their rights on them.[137] Moreover, in the EU there is no legal concept of ownership of personal data.[138] Data ownership can be found in the area of intellectual property rights and there are also sui generis property rights for databases. Some authors argue that personal data ownership should be introduced in the EU, whereas others are hesitant or argue against this.[139] Personal data ownership is complicated, as it raises complex issues similar to those well-known in the field of intellectual property rights. Typically, it is complicated to describe what exactly is covered by such property rights, to assign ownership, and to enforce such rights, as information is easily copied and distributed.[140] Although ownership of personal data could be beneficial to some extent, such a concept seems incompatible with their character as part of the right to privacy and of the personality of the individual. In other words, the "personal" element shall weight more than the "data" one, and therefore they shall not be assimilated to property.

However, the legislator cannot ignore the actual practices in the data-driven sector of the market, in which personal data is treated and traded by both companies and people as a counter-performance similar to payment. The contrast between the legal framework stating that personal data is not and cannot be a commodity and actual business practices that treat personal data as such is problematic, because it creates legal uncertainty in transactions. Furthermore, the persistence in disregarding the use of personal data as a counter-performance is contradictory to the EU's goals regarding the creation of a Digital Single Market. The EU strategy to expand the European Single

[136] Stefan Grundmann, Hugh Collins, Fernando Gomez, Jacobien Rutgers, Pietro Sirena (eds), "European Contract Law in the Digital Age", European Contract Law and Theory Series, Volume 3, Intersentia Ltd, 2018, p. 181-182
[137] Bart Custers, Gianclaudio Malgieri, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law and Security Law Review, Volume 45, 2022, p. 10-11
[138] Gianclaudio Malgieri, "'User-provided personal content' in the EU: digital currency between data protection and intellectual property", International Review of Law, Computers & Technology, 32:1, 2018, p. 136-137
[139] See in Erp Sjef Van, "Ownership Of Data: The Numerus Clausus Of Legal Objects", Property Rights Conference Journal, Vol. 6:235, 2017, p. 235-257
[140] Custers Bart, Malgieri Gianclaudio, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law and Security Law Review, Volume 45, 2022, p. 1-5

Market highlights the importance of the free flow of data for a strong European data economy.[141] It seems that the EU's legal framework for personal data protection is torn between the idea of restricting data flows to protect people versus encouraging data flows to enhance the data economy. Disqualifying personal data as a commodity is not a problem in itself, but building an economy on something that does not qualify as a commodity is. The EU already has an economy based on personal data, but one may wonder whether that is despite rather than due to the current legal framework. The main challenge here is to strike a balance between the different intentions of the EU, which on the one hand wants to protect people's personal data without considering them as a mere commodity, and on the other wants to promote a data-driven economy. Both goals are legitimate, but since it is impossible to have it all, the EU has to make some important choices here.[142]

Directive 2019/770 seems to be to the right direction, although it does not offer a complete solution, since important issues remain unclear. Its purpose is to secure a high level of consumer protection on the different markets for digital contents and services as well as to increase legal certainty and reduce transaction costs, in particular for small and medium-sized enterprises.[143] The DCSD aims to achieve these goals by a one-sided harmonisation of the contractual rights and remedies of the consumer. It does not address the contractual rights of the provider of the content or service, or seen from another perspective the consumer duties, with the exception of some consumer duties in case of the termination of the contract in article 17 DCSD.[144] As analysed above, there are several legal issues that are not clearly dealt with in the DCSD. Besides article 17, both the contractual rights of the trader and the obligations of the consumers are left to the national contract law of the member states as aspects of "general contract law",[145]

Another challenge for the legislator is whether he or she should introduce a provision about the right of the consumers to know the value of their personal data. Such a provision would make sense because although the commodification of personal data is a reality in the digital era, the average individual is not fully aware of the monetary value of his or her personal data and tend to underestimate his or her economic power within the data-driven economy. Introducing a right for consumers to know the value of their personal data would have several positive effects. It could increase consumers' awareness and controllership on their own personal information, make them aware of their power in the digital market and effectively empower them for the protection of their privacy on-line. As long as legislators are willing to take into account the new digital reality, a

[141] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe", 2015, p. 14-15

[142] Bart Custers, Gianclaudio Malgieri, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law and Security Law Review, Volume 45, 2022, p. 10-11

[143] Preamble 3 of the DCSD

[144] According to Article 17 of the DCSD in relation to the obligations of the consumer in the event of termination, "1. After the termination of the contract, the consumer shall refrain from using the digital content or digital service and from making it available to third parties. 2. Where the digital content was supplied on a tangible medium, the consumer shall, at the request and at the expense of the trader, return the tangible medium to the trader without undue delay. If the trader decides to request the return of the tangible medium, that request shall be made within 14 days of the day on which the trader is informed of the consumer's decision to terminate the contract. 3. The consumer shall not be liable to pay for any use made of the digital content or digital service in the period, prior to the termination of the contract, during which the digital content or the digital service was not in conformity."

[145] see Article 3 para. 10 of the DCSD. Axel Metzger, "A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services", Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019, p. 8-10

right for data subjects to know the value of their personal data would be a practical and realistic approach to empower data subjects towards this commodification of digital identities. According to Gianclaudio Malgieri and Bart Custers, a provision about such a right could be something like: "in each data processing where the value of customers' personal data is relevant for the economic transaction, the price of these data should be communicated to the consumer". [146] The introduction of such a right would probably meet the criticism of those already opposing to the idea of the perception of personal data as a commodity. Moreover, the calculation of the monetary value of personal data is not an easy task, and there are moral concerns as well. All in all, it seems that the benefits of introducing such a right outweigh the drawbacks. In any case, it is up to the legislator to do the balancing and decide whether the introduction of such a right is needed.

6.2. By means of self-regulation / codes of conduct

When it comes to the regulation of personal data as a currency though, legislation alone is not enough. The traditional regulatory framework based on the law-making process seems insufficient in the digital era, so there is a need for new concepts. Supplementary to the existing legal framework, self-regulation and codes of conduct are useful instruments for companies to hold themselves accountable, show their compliance with privacy regulations, keep their consumers informed by clearly stating their priorities and keep up with technological changes. They also enable companies to become clearer about their privacy policies and this way be trusted by consumers. Self-regulation is "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt common guidelines amongst themselves".[147]

There are several different models of self-regulation, ranging from pure self-regulation to co-regulation. In its purest form, self-regulation has no element of direct or indirect public intervention. However, such a model is rare. In most cases there is at least some level of participation of the authorities in the way a business is regulated. Self-regulation has numerous benefits for the parties concerned. First, it costs less and is more effective than state regulation. Businesses can individually adapt to their own special needs and purposes and be more efficient in the implementation of their own regulations. Moreover, self-regulation is more "elastic" and can keep up quickly with new technological developments, in contrast with government regulation which needs to follow complex and time-consuming procedures to adapt. Additionally, it can promote deliberate and efficient ways to deal with consumer privacy, since self-regulation can foster competition between companies in achieving the best privacy laws. However, it should be noted that when self-regulating, companies have as a priority primarily the promotion of their own goals and interests and not the protection of consumer rights and personal data. Moreover, sometimes they are vague, incomplete and open to interpretation, undermining consumer trust. Therefore, self-regulation alone does not seem as a satisfactory regulatory mechanism. Co-regulation is presented as a hybrid solution between self-regulation and government regulation. It

[146] Custers Bart, Gianclaudio Malgieri, "Pricing privacy – the right to know the value of your personal data", Computer Law & Security Review, Volume 34, Issue 2, 2018, p. 289-303
[147] European Commission, European Parliament & Council of Ministers, 'Inter-Institutional Agreement on Better Lawmaking', 2003, p. 1.

can be defined as "a mechanism whereby attaining the objectives laid down in a legislative act is entrusted to parties which are recognised in the field. The basic legislative act defines the framework and the extent of the co-regulation. The parties concerned are then able to conclude voluntary agreements between themselves in order to achieve the objectives of the legislative act."[148] In relation to personal data issues, co-regulation mechanisms consist of an effective regulatory solution.[149]

The alternative solution of co-regulation seems to be the approach adopted by the GDPR, as understood by its article about data protection by design and by default. According to article 25, "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this article." According to the EDPS, the obligation of data protection by design has four dimensions. The first one acknowledges the fact that the processing of personal data supported by IT systems should always be the outcome of a design project. The GDPR requires consideration of safeguards both at the design and operational phase, aiming at the whole project lifecycle and clearly identifying the protection of individuals and their personal data within the project requirements. The second dimension consists of the risk management approach, with a view to selecting and implementing measures for effective protection. Although there is no indication of obligatory measures, the legislator gives directions on the factors that the organisation must take into account in the selection of the appropriate measures. According to the third dimension, the chosen measures must be appropriate and effective. The fourth dimension is the obligation of the data controller to integrate the identified safeguards into the processing. All four dimensions are equally important and become an integral part of the accountability od data controllers.[150] This way, the EU legislator tries to boost the respect to ethics in technology and emphasizes the importance of self-regulation in the protection of personal data, which is also relevant concerning the regulation of them as a currency.[151]

[148] European Union, "Interinstitutional Agreement on better law-making", 2011, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al10116
[149] Ana Isabel Segovia Domingo, Villar Nathalie Desmet, "Self-regulation in data protection", BBVA Research, 2018, p. 1-3
[150] European Data Protection Supervisor, Opinion 5/2018 - Preliminary Opinion on privacy by design, 2018, p.5-7
[151] Ibid., p.19-22

All in all, in relation to the regulation of personal data in general and of personal data as a currency in particular, co-regulation can provide a complete and balanced regulatory framework that combines the benefits of both state regulation and self-regulation; the safeguards for consumer protection and the credibility of the former, and the flexibility and adaptability of the latter.[152]

6.3. Towards "Law 3.0"?

Nevertheless, the most important challenge in the field of regulation is deeper and has to do with the way the legislator chooses to deal with law and technology in general. It is supported that the regulation of new technologies, in order to be successful, requires a whole new way of legal thinking. According to Roger Brownsword, existing legal rules need to be updated and revised in order to fulfil their purposes in the digital era. Rules that are fit for their purpose, in our case rules regulating the financial aspects of personal data, are not enough; they need to be supplemented by the appropriate technical solutions. This view in fact highlights the need to reimagine and reinvent law as a whole, in a way that "Law 3.0" is born. "Law 1.0" refers to the way of legal thinking which focuses on the application of rules and general principles to specific facts. "Law 2.0" goes one step further and focuses not only on the courts and historic codes but on the political field as well. Here, the form of reasoning is policy-directing and instrumental. In "Law 3.0", though, the regulatory mindset focuses on the potential use of a range of technological instruments[153].

The ineffectiveness of "Law 1.0" and "Law 2.0" and therefore the need for "Law 3.0" derives from the fact that nowadays the legal framework for data protection is constantly outpaced by the technological developments, which as examined above have led to new uses of personal data.[154] The use of technological tools by the regulator that shall accompany the legal rules can be taxonomized on a spectrum from soft to hard. At the soft end of the spectrum, the technologies are employed in support of the legal rules. At the hard end of the spectrum, measures of 'technological management' focus on limiting the practical options of individuals. Whereas legal rules back their prescriptions with ex post penal, compensatory, or restorative measures, the focus of technological management is entirely ex ante, aiming to anticipate and prevent wrongdoing rather than punish or compensate after the event. Concerning the regulation of personal data, it seems that there are already some technocratic measures in force. As mentioned above, the General Data Protection Regulation introduced "privacy enhancing technologies" and "privacy by design", and data controllers are required to take appropriate technical and organisational measures to ensure that the requirements of the Regulation are met. With initiatives of this kind, it could be supported that the European legislator is already moving towards a "Law 3.0" approach, or at least towards a view that technology might be part of the solution to our regulatory problems.[155]

As a first step of reimagining law towards a "Law 3.0", we should broaden the field for juristic inquiry by operating with a notion of the regulatory environment that accommodates both

[152] Domingo Ana Isabel Segovia, Villar Nathalie Desmet, "Self-regulation in data protection", BBVA Research, 2018, p. 1-3
[153] Roger Brownsword, "Law 3.0: Rules, Regulation, and Technology" (1st ed.). Routledge, 2020, p.1-6
[154] Ibid., p. 23
[155] Ibid., p. 28-30

normative rule-based and non-normative technocratic approaches. While normative regulation is directed at actions that are and remain possible, technological management redefines what is and is not possible. Technological measures are able to manage certain kinds of risks by completely excluding the possibility of certain actions. In other words, while legal rules define what businesses and individuals must and must not do, technological measures define what they can and cannot do, eliminating the potential source of danger at its source. Moreover, technological management might be employed by both public regulators and private self-regulating agents. What "Law 3.0" reflects is the use of technological tools for regulatory purposes and the coexistence of rule and non-rule instruments not only in the regulatory toolbox but also in the everyday experience of regulatees. Accordingly, the regulatory environment shall consist of both formal and informal normative codes as well as non-normative technological tools and codes.[156]

As mentioned above, a "co-regulation" approach seems suitable for the regulation of personal data as a currency. This approach can be part of "Law 3.0", in which government regulators set the general targets and objectives and business determine which measures they will use in order to meet these goals. Technological measures can be of two types; those that are merely supportive of existing rules or assistive or advisory in relation to decision-making, and those that aim to eliminate or redefine the practical options.[157] The technological measures shall always respect the fundamental values of the society, especially the fundamental rights of the individuals, and their use must be conditioned by principles that give them legitimacy.[158] Furthermore, the establishment of a national or even an international body would be beneficial. The purpose of such an institution would be to inform the public, set standards for the ethical use of new technologies related to personal data, underline the responsibilities of businesses as well as facilitate the development of the regulatory framework for these technologies.[159]

All in all, "Law 3.0" distinctively includes a technocratic element. This proposed new way of legal thinking acknowledges the available technological options as an effective means of serving regulatory purposes. To facilitate the reimagining of law, it is suggested that we adopt a broad understanding of the regulatory environment, so that it includes both formal and informal rules and the supplementary technological measures.[160] However, no one can guarantee that rules and technological measures can peacefully coexist, or that "Law 3.0" would solve all the arising legal issues.[161]

[156] Roger Brownsword, "Law 3.0: Rules, Regulation, and Technology" (1st ed.). Routledge, 2020, p. 51-53
[157] Ibid., p. 54-57
[158] Ibid., p. 71, 77, 81-84
[159] Ibid., p. 98, 101
[160] Ibid., p. 115
[161] Ibid., p. 119

7. Concluding remarks

After taking everything into consideration, new technologies have formed personal data as, if not already a form of currency today, a de facto currency of tomorrow.[162] Personal data, just like coins, have two sides. From the one side they are an integral part of the individual's personality and deserve protection as a human right. From the other side they have monetary value and they are a counter-performance in contracts. The example of Directive 2019/770 highlights the complexity of the issue, and probably generates even more questions than answers. The problematic of the concept of personal data as the currency of the digital age includes the interplay between contract law, consumer protection law and data protection law and the emergence of several legal issues, such as the contractual consequences of the withdrawal of consent and the interplay with the notion of unfairness.

There are several different approaches towards the arising legal issues. Solutions can be found either through the interpretation of the existing legal framework or through the creation of new rules. Although the latter would create more legal certainty and stability in the market, this does not mean that the interpretation of the existing rules is not fruitful. In fact, it can lead to effective solutions, especially the interpretation of those rules that are more flexible, such as those of contract law.[163] In any case, the proposed solutions shall respect the mandatory legislation and be in accordance with the core aims of the European Union. In our case, these are the protection of individuals regarding the processing of their personal data, the free movement of personal data, the achievement of a high level of consumer protection and the proper functioning of the internal market. The Judgments of national Courts and the CJEU as well as the decisions of national DPAs regarding the issue has shed light to certain aspects, although many issues remain to be interpreted by future case-law.

Personal data as the currency of the digital age arm consumers with more bargaining power, recognizing their data as a valuable "counter-performance" for the market. However, personal data are not like the other currencies a consumer may have on his or her wallet; they are not simply a "data dollar". Taking into consideration the significant, complex and multidimensional impact of the perception of personal data as currency, an effective regulatory environment is crucial. However, the regulation of personal data as a currency is far from an easy task. The best solution seems to be the combination of government regulation and self-regulation, through the creation of co-regulative mechanisms. Nevertheless, the impact of new technologies in society and economy in the digital era is so revolutionary that law may have to be reimagined and reinvented in order to fulfil its purposes. In this context, technological measures ancillary to the co-regulation regulatory approach are highly recommended.

[162] Reiner Schulze, Dirk Staudenmayer, "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020, p. 70
[163] Ibid., p. 74

BIBLIOGRAPHY

Books

1. Brownsword R., "Law 3.0: Rules, Regulation, and Technology" (1st ed.). Routledge, 2020
2. Dowd R., "The Birth of Digital Human Rights - Digitized Data Governance as a Human Rights Issue in the EU", Information Technology and Global Governance Series, Springer, 2022
3. Forbes L., "Modernizing Consumer Law in the Fourth Industrial Revolution", Columbia Journal of European Law, Vol. 27, No. 2, 2021
4. Grundmann S., Collins H., Gomez F., Rutgers J., Sirena P. (eds), "European Contract Law in the Digital Age", European Contract Law and Theory Series, Volume 3, Intersentia Ltd, 2018
5. Jougleux P., «European Law of the Internet – Legal Aspects of the Internet in Europe», Sakkoulas Publications S.A., 2016
6. Mantelero A., "Beyond Data - Human Rights, Ethical and Social Impact Assessment in AI", Information Technology and Law Series, Volume 36, Asser Press, 2022
7. Margaritis E., «Personal Data & Consumer Protection», Nomiki Vivliothiki, 2020
8. Mayer-Schönberger V. and Kenneth C., "Big Data: A Revolution that will transform how we Live, Work, and Think, Houghton Mifflin Harcourt Publishing Company, 2013
9. Mayer-Schönberger V. and Thomas R., "Reinventing Capitalism in the Age of Big Data", John Murray, 2018
10. Schulze R., Staudenmayer D., "EU Digital Law – Article-by-Article Commentary", Nomos Verlagsgesellschaft, 2020
11. Senigaglia R., Irti C., Bernes A. (Eds), "Privacy and Data Protection in Software Services", Springer, 2022
12. Stathopoulos M., «Epitome of General Law of Obligations», Sakkoulas Publications S.A., 2016
13. Vlahopoulos S., «Fundamental Rights», Nomiki Vivliothiki, 2017

Articles

14. Alves M. d A., "Directive on certain aspects concerning contracts for the supply of digital content and digital services & the EU data protection legal framework: are worlds colliding?", Unio - Eu Law Journal ,Vol. 5, No. 2, 2019
15. Barth S., de Jong M. D.T., "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", Telematics and Informatics, 34, 2017
16. Bedir C., "Contract Law in the Age of Big Data", European Review of Contract Law, 16(3), Tilburg Law School Research Paper Forthcoming, 2020
17. Cedric R. & Mistale T., "The GDPR as global data protection regulation?", Symposium on the GDPR and international law, Cambridge University Press, 2020
18. Custers B., Malgieri G., "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", Computer Law and Security Law Review, Volume 45, 2022
19. Custers B., Malgieri G., "Pricing privacy – the right to know the value of your personal data", Computer Law & Security Review, Volume 34, Issue 2, 2018

20. Domingo A. I. S., Villar N. D., “Self-regulation in data protection”, BBVA Research, 2018
21. Dorraji Seyed E., Mantas B., “Privacy in Digital Age: Dead or Alive?! Regarding the New Eu Data Protection Regulations”, Social technologies, 2014
22. Drechsler L., “Data As Counter-Performance: A New Way Forward Or A Step Back For The Fundamental Right Of Data Protection?”, Datenschutz & LegalTech/ Data Protection & LegalTech, 2018,
23. Durovic M. and Lech F., “A Consumer Law Perspective on the Commercialization of Data”, European Review of Private Law 5-2021 Kluwer Law International BV, 2021
24. Erp S. V., “Ownership of Data: the Numerus Clausus of Legal Objects”, Property Rights Conference Journal, Vol. 6:235, 2017
25. Goanta C. and Mulders S., “‘Move fast and break things’: Unfair commercial practices and consent on Social Media.”, Journal of European Consumer and Market Law, 8, 2019
26. Helberger N., Zuiderveen Borgesius F. & Agustin R., “The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law”, Common Market Law Review, Volume 54, Issue 5, 2017
27. Helveston M. N., "Consumer Protection in the Age of Big Data.", Washington University Law Review, vol. 93, no. 4, 2016
28. Hughes K., “The social value of privacy, the value of privacy to society and human rights discourse” in B. Roessler & D. Mokrosinska (Eds.), “Social Dimensions of Privacy: Interdisciplinary Perspectives”, Cambridge University Press, 2015
29. Langhanke C. and Schmidt-Kessel M., “Consumer Data as Consideration”, Journal of European Consumer and Market Law, 4, 2015
30. Malgieri G., “‘User-provided personal content’ in the EU: digital currency between data protection and intellectual property”, International Review of Law, Computers & Technology, 32:1, 2018
31. Mańko Rafał and Monteleone Shara, “Briefing - Contracts for the supply of digital content and personal data protection”, European Parliamentary Research Service, European Parliament, May 2017
32. Metzger A., “A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services”, Working Paper No. 8 des Forschungsinstituts für Recht und digitale Transformation, 2019
33. Metzger A., “Data as Counter-Performance What Rights and Duties do Parties Have?”, Jipitec, 2017
34. Metzger A., Efroni Z., Mischau L. and Metzger J., “Data-Related Aspects of the Digital Content Directive”, JIPITEC, 2018
35. Parise S., “Big data: A revolution that will transform how we live, work and think, by Viktor Mayer-Schonberger and Kenneth Cukier”, Journal of Information Technology Case and Application Research, 18:3, Routledge, 2016
36. Pasquale F., “The black box society – the secret algorithms that control money and information”, Harvard University Press, 2015
37. Popescu A.-D., “The value of Data from an Artificial Intelligence Perspective”, Annals of the University of Craiova for Journalism, opinion ation and Management, Volume 5, 2019
38. Rao S. A., Verweij G., “PwC’s Global Artificial Intelligence Study: Exploiting the AI Revolution – Sizing the prize”, Pwc, 2017
39. Report to the Commission from TNS opinion & social: Online Platforms, 2016
40. Rose B., “The Commodification Of Personal Data And The Road To Consumer Autonomy Through The Ccpa”, 15 Brook. J. Corp. Fin. & Com. L., 2021

41. Slaughter M. J., and David H. M., "Data Is Power: Washington Needs to Craft New Rules for the Digital Age.", Foreign Affairs, vol. 100, no. 3, 2021
42. Szilágyi F., “Personal Data as Consideration for the Facebook Service -Case Note on Facebook Ireland Ltd. v Gazdasági Versenyhivatal (Hungarian Competition Authority) (Case BH2022.24)”, EuCML, 2022
43. Van L. M., “The value of personal data”, Conference Paper in IFIP Advances in Information and Communication Technology, 2015
44. Versaci G., "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection.", European Review of Contract Law, vol. 14, no. 4, 2018
45. World Economic Forum, “Personal Data: The Emergence of a New Asset Class”, 2011
46. Xuejing Z., Hang X., “How the Blockchain Technology Facilitate Data to Realize Value: the Case of Food Supply Chain”, Journal of Agricultural Big Data, Vol.2, No.3, 2020

Legal Documents

47. Charter of Fundamental Rights of the European Union
48. Constitution of Greece
49. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Contract Terms Directive)
50. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services
51. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive)
52. Explanatory statement of Law 4967/2022
53. Greek civil Code
54. 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 (General Data Protection Regulation)

Case – law

55. Case BH2022.24 -Facebook Ireland Ltd. v Hungarian Competition Authority - Kuria
56. Case C-131/12 (Google Spain SL, Google Inc v Agencia Espaiola de Proteccion de Datos)
57. Case C-275/06 (Promusicae v Telefonica de Espana)
58. Case C-291/12 (Michael Schwarz v Stadt Bochum)
59. Case C-611/14 (Canal Digital Danmark)
60. Case C-93/09 (Volker und Markus Schecke GBR and Hartmut Eifert v Land Hessen)
61. CdS – 202102630 - Facebook Inc. V. Autorità Garante della Concorrenza e del Mercato, Giustizia Amministrativa
62. Hellenic Data protection Authority, Decision 35/2022
63. Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd v Ireland)

64. Judgement of the ECHR in Case of Airey V. Ireland (Application no. 6289/73),
65. Judgement of the ECHR in Case of KU v Finland (Application no. 2872/02),
66. Judgment of the ECHR in Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04),
67. Norwegian Data Protection Authority, Decision in case 20/02136
68. Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020 on the Joined Cases C 682/18 and C 683/18 [Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C 682/18) and Elsevier Inc. v Cyando AG (C 683/18)]
69. Spanish Data Protection Authority, Decision E/03624/2021
70. Spanish Data Protection Authority, Decision PS/00500/2020

Other sources

71. European Parliament, "Report on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content", A8-0375/2017, 2017, Amendments 21 and 80.
72. European Commission, "Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content", 2015
73. Opinion of Advocate General Campos Sánchez-Bordona delivered on 6 October 2022 in Case C-300/21 (UI v Österreichische Post AG)
74. European Commission, "What is personal data?" Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
75. "Data Dollar: The new currency based on the value of personal data puts the spotlight on a newly created retail payment method", 2017 accessed by https://www.kaspersky.com/about/press-releases/2017_data-dollar-the-new-currency-based-on-the-value-of-personal-data
76. "The Data Dollar Store - A Data Shopping Social Experiment by Kaspersky Lab" accessed by https://www.youtube.com/watch?v=dqcHcnpNHIM
77. European Data Protection Supervisor, "Data Protection", Available at: https://edps.europa.eu/data-protection/data-protection_en
78. European Commission, "2030 Digital Compass: the European way for the Digital Decade", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of The Regions, 2021
79. European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe", 2015
80. "Terms of Service" of Facebook, Available at: https://www.facebook.com/terms.php
81. Bote J., "Facebook tweaks homepage, no longer says it is 'free and always will be", USA Today, Available at: https://eu.usatoday.com/story/tech/2019/08/27/facebook-no-longer-says-free-and-always-be-homepage/2133300001/
82. https://gdprhub.eu/CdS_-_202102630
83. https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/02136-18
84. https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_E/03624/2021
85. https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00500/2020
86. European Commission, European Parliament & Council of Ministers, 'Inter-Institutional Agreement on Better Lawmaking', 2003

87. European Union, “Interinstitutional Agreement on better law-making”, 2011, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al10116
88. Vodafone, “The Connected Consumer 2030”, Vodafone Smart Tech, 2022
89. European Data Protection Supervisor, “Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content”, 2017
90. European Data Protection Supervisor, “Opinion 5/2018 - Preliminary Opinion on privacy by design”, 2018
91. European Data Protection Board, “Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects”, Version 2.0, 2019