

„BABEȘ-BOLYAI” UNIVERSITY CLUJ-NAPOCA
FACULTY OF EUROPEAN STUDIES
"EUROPEAN PARADIGM" DOCTORAL SCHOOL

DOCTORAL THESIS
Towards a digital single market:
Regulating data in the European Union
- SUMMARY -

Scientific coordinator:

Prof. Dr. Vasile Pușcaș

Doctoral student:

Iulia-Daniela Mureșan

Cluj-Napoca

2022

The research embodied in the doctoral thesis entitled "Towards a digital single market: Regulating data in the European Union" presents and evaluates the electronic data regulatory regime at EU level. The examination of the legislative framework on personal and non-personal data focuses on the economic implications and the EU internal market.

The opportunity of conducting the research stems from the current societal metamorphosis that represents not an incremental evolution but a systemic disruption characterized by the spread of digital technology in all sectors of the economy coupled with the emergence of new disruptive technologies such as artificial intelligence, Big Data, Blockchain, 5G, Augmented Reality and Virtual Reality. Starting from 2020, the SARS-Cov-2 pandemic has represented an additional impetus for the accelerated adoption of digital technology by the general population as well as by small and medium-sized enterprises. Even the Romanian public administration, known for its bureaucratic inertia illustrated by the famous "folder with fastener", has implemented digital technologies in relation to the public¹. Digital technologies no longer constitute a specific field, but the foundation of all the economic systems of modern innovative societies². Therefore, in order to participate in modern society, a digital presence is inevitable, which automatically leads to the generation of electronic data. Thus, data has the potential to generate significant economic value if analyzed together with services and products, becoming a major driver of economic development. "Data value chains are based on various data-related activities such as data creation and collection; data aggregation and organization; data processing; data analysis, marketing and distribution; use and re-use of data"³. As a result, electronic data, as a key factor in the development of the digital economy, has the status of a valuable resource, surpassing oil in importance⁴ and known as the "new gold"⁵.

¹ GEO no. 38/2020 on the use of electronic documents at the level of public authorities and institutions published in the *Official Gazette of Romania*, no. 289, of 07.04.2019, which stipulates the general obligation for documents issued in electronic format by public authorities and institutions to be signed with a qualified electronic signature, not sent by a simple e-mail. Public authorities and institutions are also required to receive electronically signed documents.

² Recital 1 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free movement of non-personal data within the European Union, <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018R1807&from=RO>, accessed on 25.01.2022.

³ *Ibidem*, recital 2.

⁴ *** „The world’s most valuable resource is no longer oil, but data”, *The Economist*, 06 May 2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>, accessed on 17.01.2022.

⁵ *Data is the New Gold: Marketing and Innovation in the New Economy*, Washington D.C.: US Chamber of Commerce Foundation, 2014, www.uschamberfoundation.org/data-new-gold-marketing-and-innovation-new-economy, accessed on 04.02.2022.

However, it is not clear which legal regime will govern the data, respectively to whom the data belongs, who has control over data, what other rights exist regarding data, the conditions under which it can be sold or what data protection measures exist. The approach of the competent authorities, faced with the task of regulating an innovative, complex and dynamic field, was either to issue rules in the absence of the necessary knowledge, in a state of anxiety and external pressure, or enter a state of paralysis and ignore the subject⁶. The "inertia of the law" works on the principles of the law of inertia, Newton's first law, which states that "if a body is at rest or moving at a constant speed in a straight line, it will remain at rest or keep moving in a straight line at constant speed unless it is acted upon by a force"⁷. In the absence of a significant disruption, the regulatory framework will retain its original state.

In this context, the research analyzed the electronic data regulatory regime, by identifying the applicable tools, both hard law and soft law instruments, and by subsequently evaluating them. The analysis of the existing legislative framework, as well as of the draft legislative proposals, is based on Brownsword's⁸ tripartite classification regarding the adaptation of the legislative system to technological changes, organized on levels of complexity, called Law 1.0, Law 2.0 and Law 3.0. Thus, if the Law 1.0 approach refers to a traditional application of the existing rules, standards and principles of law to the concrete facts of a singular case, legislating through the jurisprudence that aims to maintain the coherence of the system, the Law 3.0 approach proposes the use of technology itself as a regulatory tool. On the other hand, the Law 2.0 approach, as an intermediate stage, abandons the recycling of traditional concepts of law and involves the articulation of new rules and a specific regulatory framework to serve directly a given purpose⁹.

The thesis is structured in 5 main chapters, each divided into several sections. The research thus begins with a presentation of the historical evolution of the EU's internal market, from the Treaty of Rome and to the Single Market Act of 2012 and identifies the regulatory strategies used in the process of economic integration. The expansion of the internal market to include the digital space and the EU's

⁶ Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, „Regulation tomorrow: What happens when technology is faster than the law?“, in *American University Business Law Review*, Vol. 6, No. 3, 2017, 561-594, <https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1028&context=aubl>, accessed on 08.04.2022.

⁷ *Britannica*, <https://www.britannica.com/science/law-of-inertia>, accessed on 08.04.2022.

⁸ Roger Brownsword, *Law 3.0. Rules, Regulation, and Technology*, Abingdon: Routledge, 2021, 1-6.

⁹ *Idibem*.

strategy to establish the European digital decade is the subject of the next section. If at the time of its establishment, the EU internal market was designed for an economy based on the transfer of physical goods and the provision of services face-to-face, technological development has demonstrated the need to adapt it. Thus, the EU's single market has gradually developed to include both the digital space in general and electronic data in particular as constitutive elements of the information society.

The second chapter presents the introductory aspects required to outline the social, economic and political context in which the normative instruments on electronic data are inserted. The paper defines and presents several relevant concepts, namely the notion of "data" used in EU legislative instruments, the notion of "information" used especially in US law and the notion of "knowledge". This research effort made it possible to formulate a working definition that represents the basis of the thesis and allows for the establishment of limits to the research. The term "electronic data" is thus used interchangeably with the notion of "information", defined as semantic units, factual, in digital format, so that they can be transmitted or processed using a computer device.

To put the study in context and illustrate the relevance of data, Section 2 describes the historical evolution and functioning of the data economy as a result of the evolution of digital technologies. The massive collection of electronic data, both personal and non-personal, is now a *fait accompli* worldwide. It is estimated that by 2025, the volume of newly produced data will reach 175 zettabytes, and the introduction of new technologies in mass production, such as IoT, signifies additional interactions with devices that collect data every 18 seconds¹⁰. The analysis of the activity carried out on social media platforms shows that in 2018, in one minute, users posted 473,400 messages on Twitter, shared 2 million photos via Snapchat, posted 49,380 photos on Instagram and the LinkedIn platform gained 120 new users¹¹. All this data is an essential resource for growth, innovation, job creation and the progress of society as a whole¹². From the perspective of an individual, data is personal information, which requires strict protection against the risks involved in non-compliant use. From a company's perspective, data, both personal and non-personal, has a major commercial value. For state bodies, data is both a way of optimizing their activity and a resource for which they need to establish a regulatory framework that ensures a balance between competing interests. Therefore, both

¹⁰ Bernard Marr, „How much data is there in the World?“, *Bernard Marr & Co.*, <https://bernardmarr.com/how-much-data-is-there-in-the-world/>, accessed on 02.02.2022.

¹¹ *Ibidem*.

¹² *A Digital Agenda for Europe*, Brussels: European Commission, 2010, <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52010DC0245&from=en>, accessed on 02.03.2022.

public and private actors collect databases of impressive size, in order to integrate data into all possible activities¹³.

The next section identifies the main features of data that make it possible to extract economic value, as well as the basic operations of the data life cycle. The specific business models indicate an excessive commercialization of the digital space, characterized by opacity. For example, the paper presented the large volume of data and the data flows involved in a simple digital retail transaction. The last two sections analyze electronic data from a legal point of view, initially by trying to qualify them as a good in the legal sense and its inclusion in the existing categories for the classification of goods and later by introducing and applying the concept of Law 1.0.

The third chapter analyzes the concrete efforts to regulate electronic data, both legislative and jurisprudential, the formation at EU level of 2 parallel regimes, respectively for personal data and non-personal data, and proceeds to introduce them in the tripartite classification of Brownsword. The first section presents the main EU data regulation instrument, namely the General Data Protection Regulation no. 2016/679¹⁴ known as GDPR. Next, the second section analyses the regulatory history of personal data in the European space, both at national level and through international organizations, such as the Council of Europe. The third section investigates the existence of legislative instruments with alternative or cumulative application to the GDPR for the regulation of personal data, as well as the cases in which regulatory competence rests with the Member States. The framework for regulating non-personal data as well as how to distinguish between the two parallel regimes and identify the points of interaction between them, especially given that the demarcation line is not always clear, is the subject of the next section. The sixth section presents the future evolution of regulation for advancing the field and adapting it to economic and social realities, through initiatives such as the Digital Services Act, the Digital Markets Act or the Data Governance Act. Furthermore, given the importance of the free movement of data both within the EU and in relation to third countries, to ensure the functioning of the internal market and to extract the economic value of data, the thesis

¹³ David Reinsel, John Gantz and John Rydningm, „Data age 2025. The Digitization of the World from Edge to Core”, *International Data Corporation*, November 2018, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>, accessed on 01.03.2022

¹⁴ 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), <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL>, accessed on 10.01.2022.

contains a case study of the legal instruments that allow for the transfer of personal data from an EU Member State in a third country. Thus, the last two sections analyze how the legal data transfer mechanisms work. These have been severely affected by the recent decision of the CJEU in the famous Schrems II case¹⁵, which invalidated the Privacy-Shield Decision¹⁶ and which, moreover, called into question the legality of transfers made under the Standard Contract Clauses. Following the CJEU decision, the transatlantic companies and the European Commission reacted differently, adopting divergent adaptive strategies such as ignoring the decision, or integrating it into its own activity.

The fourth chapter examines alternative approaches to EU's regulatory framework concerning electronic data. The first 4 sections consist of the presentation of the legislative framework adopted in jurisdictions that present distinct and relevant circumstances regarding the way data is regulated. Thus, the paper describes US policy and legislation regarding data regulation, initially at the federal level and then at the state level. This state has a data policy that is diametrically opposed to that of the EU, despite the interdependence between the two countries, between which cross-border data flows are the largest in the world¹⁷. Of the existing statewide initiatives, the paper focuses on the most developed ones, namely those of California, Virginia and Colorado. China the second largest economy in the world¹⁸ is in the process of establishing its own data regulation legislation. The proposed legislation seeks to accommodate conflicting interests such as the need to have access to data in order to maintain public order and security and the need to align to the standards of its trading partners in order to transfer data to and from China. To present a complex picture of the existing legislative regimes, the paper also assesses how data will be regulated in the United Kingdom after leaving the EU and its detachment from the EU *acquis*. The next 2 sections examine different approaches to data regulation based on Brownsword's classification, from regulating data through the use of technology and code to regulating data by reverting to traditional notions of law, such as applying ownership rights to both

¹⁵ Decision of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, case C-311/18, CJEU.

¹⁶ *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, known as the Privacy Shield Decision, Brussels: European Commission, 2016, <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016D1250&qid=1648468520136&from=EN>, accessed on 10.07.2021.

¹⁷ Joshua P. Meltzer, „The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment”, *Brookings*, Global economy and development Working Paper no. 79, October 2014, 4-7, <https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf>, accessed on 28.02.2022.

¹⁸ ***, „GDP Ranked by Country 2022”, *World Population Review*, <https://worldpopulationreview.com/countries/countries-by-gdp>, accessed on 14.02.2022.

electronic data itself and to digital assets that allow data collection. The last section examines the possibility of regulating data at international level, as part of a concerted effort, with a proposal to include data in the existing WTO regulatory regime. The interaction between the current EU legal regime on data and the existing WTO standards runs the risk of identifying disguised trade restrictions.

The last chapter investigates Romania's national approach to data regulation. In terms of its membership to the EU, Romania is part of a complex legal system, based on supranational rules and the interaction between them and the national legal regime. Thus, the first section analyzes the national policy on the digital economy, both in the public and in the private area. The next section presents the national legal regime for electronic data, its compliance with European standards as well as national initiatives in cases where regulatory competence falls to national authorities. The last chapter analyzes the implementation of regulations by the competent administrative bodies, respectively the Authority for the Supervision of Personal Data Processing and by the national judicial bodies.

Due to the vastness of the topic and the multiple areas in which electronic data is used, the research was limited to analyzing the legislative framework applicable to electronic data processed exclusively by the private sector. References to the public sector have only a purely informative role, in order to allow a clear delimitation of the research. The study of data regulation in the public sector, in particular as regards to data used by criminal investigation bodies and intelligence services, is to be further investigated. In addition, the object of a separate study will be the provisions of criminal law, which penalizes acts regarding electronic data, such as illegal access to a computer system¹⁹ or alteration of the integrity of computer data²⁰. It is also necessary not to confuse the legal regulation of electronic data with the legal regulations concerning the infrastructure required for the transmission of data and to facilitate the EU's objective of free movement of data within its territory. The thesis analyzes mainly the first category of regulations, adopting a neutral approach to the technology used for electronic data processing.

The research is structured around 3 main research questions on how to regulate electronic data. Firstly, it was necessary to identify the regulatory framework applicable to electronic data at EU level and

¹⁹ Article 360 Law no. 286/2009 regarding the Criminal Code, published in the *Official Gazette of Romania*, no. 510, from 24.07.2009.

²⁰ Article 362 Law no. 286/2009 regarding the Criminal Code, published in the *Official Gazette of Romania*, no. 510, from 24.07.2009.

establish how to classify it according to Brownsword's theory. Although at first glance the two main instruments, the GDPR and the Non-Personal Data Regulation, govern data, the research has identified a veritable maze of competing regulations, which in order to be technologically neutral and flexible, uses vaguely defined concepts. The online purchase of a good or service thus entails the application of at least 4 or 5 separate legal instruments established at European level, to which is added the existing legislation at national level. Even a simple application of the GDPR, a regulation that does not require transposition, and which at first glance ensures strong harmonization, is a real balancing act. The GDPR allows Member States to introduce derogations through national regulations on more than 50 issues. Therefore, any application of the GDPR requires verification and analysis of national provisions, actions hampered by differences in language and legal culture between Member States. In the case of Romania, several national implementing provisions have been adopted which affect the harmonization of the field of personal data. The completion of the internal market is thus significantly hampered by the baroque architecture of this system.

By creating an extensive and dedicated legislative framework, the approach taken by the EU is an example of applying a Law 2.0 model to data regulation. It does not take into account and does not seek to ensure legislative coherence neither by applying legal principles to the specifics of data nor by framing the new legislation as part of the traditional system. The organization of the internal market and the division of competences between the EU and the Member States do not even allow for a system based on the specific principles of the Law 1.0 model.

The thesis further examined whether the EU-wide electronic data regulatory architecture is appropriate for the purpose of translating internal market-specific freedoms into the digital space. The single market is based on 4 fundamental economic freedoms, on the free movement of all factors of production, respectively: the free movement of goods, the free movement of services, the free movement of persons and the free movement of capital. Data sharing, preferably in real time and continuously, as well as its cross-border transfer, are at the core of business processes and are essential for enabling online business transactions, but also for physical transactions that often involve making online payments. .

Therefore, the research concluded that under the existing legal instruments, the exercise of fundamental freedoms in the internal market is part of a subsidiary right to free movement of data.

Using the model of the customs union, the EU has removed the borders between Member States in terms of data transfers. Ensuring the uniform application of these rules is done on the basis of the updated "new approach" on harmonization, through a combination of voluntary regulations and standards, adopted by ISO in combination with European standardization bodies. If traditionally the "new approach" involved the adoption of directives containing minimum technical requirements, most directives are now being replaced by regulations, as is the case with the regulation of personal data. Common conditions for the export of data have been established at the external borders, according to Chapter V of the GDPR. If in the case of the customs union imports were protected, in particular in order to ensure the quality of goods entering the EU, in the case of data the conditions governing the export of personal data from an EU Member State to a third country are regulated. In both cases, the aim is to protect EU citizens in order to ensure that the way the world economy is organized does not affect the basic level of rights guaranteed by the EU.

At first reading, human rights appear to be a priority in the case of the regulation of personal data, and economic considerations are subsidiary values. The rules on the application of mixed data sets support the view that economic interests are subordinated to the objective of protecting fundamental rights in the European legal order. However, the case study in the last part of Chapter 3 on data transfer to third countries showed that during implementation priority is given to economic factors. The European Data Protection Board initially concluded that, if an adequate legal basis for transfers to a third country cannot be found, personal data should not be transferred outside the EU and all processing activities should take place within the EU. However, following the Schrems II judgment which invalidated the data transfer scheme, the transfers were not suspended and the transfer activity was maintained at a "business as usual" level. The procedure against Facebook for suspending data flows is the only notable initiative, but it has been in limbo for two years, imposing no practical consequences. Thus, the subsidiarity of the free movement of data is called into question, being rather interpreted as a freedom in itself, a fifth fundamental economic freedom. Starting with 2019, the date from which both the GDPR and the Regulation on non-personal data, directly applicable and derived instruments, apply in parallel, we can consider that the freedom of movement regarding most EU data has been completed.

The research also identified a number of obstacles to the free movement of data, which prevent the consolidation and functioning of the internal market. Thus, there are 6 categories of personal data

excluded from the general regulatory system established at European level. They do not fall under the scope of the GDPR and remain either unregulated falling under the provisions of national law, at the Law 1.0 level or are subject to other type Law 2.0 legislative instruments issued at state or union level. Thus, for certain types of data different standards still apply in each Member State. It is also possible for data to belong simultaneously to several categories regulated at European level and thus involve the cumulative application of the protections offered and the legal regimes. For example, the results of a blood test represent both medical and biometric data, and if the blood belongs to a minor under 16, it is also the personal data of a child. The implementation of European legislation on the data rights of children is also complemented by the national law of each Member State regarding legal capacity. In addition, the CJEU, through its activity of interpreting the legislation, creates a new series of "rules" and new categories of data.

Analyzed in depth, the European data protection regime appears to be inflated and complex. The established obligations and rights, both for the natural persons and for the controllers, represent a disproportionate burden in relation to the existing resources, so that the legal provisions remain without practical efficiency, a form without substance. This is one of the reasons why the USA, influenced by the industry lobby, refuses to adopt at federal level, data regulation legislation. The premise on which the personal data regulation regime is based, information self-determination, is also an unusable concept, considering the technological evolution and organization of the digital economy. Moreover, the use of consent as a basis for data processing, and more recently even the legitimate interest represents numerous vices regarding their effectiveness. Another disadvantage of data legislation is the high degree of complexity and abstraction, which makes implementation difficult. On the other hand, the main advantage of the legislation is that it is technology-neutral, and any future invention on data storage or transmission does not lead to the inapplicability of the law, but allows the maintenance of existing rights. We can thus conclude that the absence of an effective legal framework is an obstacle to the digital single market and leads to the splitting of the internal market according to national borders or industries.

As regards non-personal data, they are governed by legislative documents only in the EU and India, as opposed to the general approach to use voluntarily applicable technical standards. The framework created at EU level is flexible and focuses exclusively on the completion of the internal market through the 3 main categories of provisions.

Finally, as a consequence of the answers to the previous questions, the paper identified and interpreted alternative ways of regulating data, which belong to distinct theoretical models, such as Law 1.0, Law 2.0 and Law 3.0. The complexity of the data economy and the rapid development of technological capabilities have highlighted the inadequacy of the approach adopted by both the EU and the USA or UK. The deficiencies inherent in the adoption of a Law 1.0 approach were presented in several sections. It is therefore appropriate to shift to the next level, namely Law 3.0, which involves the use of technology as a normative tool for regulating technology. The possibility of using technology as a regulatory tool is suggested by the GDPR itself, by introducing the concepts of "privacy by design" and "pseudo-anonymization". An effective example of the use of technology as a regulatory tool, albeit reprehensible, is the Golden Shield, dubbed the "Great Chinese Firewall", which manages to monitor and censor information available online in China. The application of technology as a regulatory tool is still in its infancy in the North Atlantic, but is in the process of developing.

Law 3.0 specific tools can also be used to limit the characteristics of data, in the sense of transforming data from a non-rival good into a rival good and bringing it closer to the characteristics of tangible goods. Subsequently, a classic Law 1.0 approach can be applied through traditional legal institutions, such as applying ownership rights to electronic data. The interaction and comparison of the European system with the US and Chinese systems outlines the contemporary global market based on data. The international system is also organizing and adapting to new realities, by regulating data and the ICT sector within multilateral international trade organizations such as the WTO or the OECD.

This interdisciplinary research has interpreted and evaluated the legal framework and case law on electronic data, not limited to concepts of law or notions of European integration, but by analyzing the interactions between them and the current level of technological development. Thus, the thesis found that certain legal concepts, which aim to ensure the free movement of data and the integration of the internal market, such as anonymization of data, have lost their effectiveness due to the current conditions of technological development.

The aim of the thesis is not to end the debate on data regulation and the completion of the European digital single market, but to open up new avenues for further research and analysis. The data does not disappear, but multiplies and continues to occupy a central place in social, economic and political life.

In addition, the fast pace of technological development gives the research subject flexibility and a need for continuous updating. Due to the impact of the digital revolution and the insertion of data in all sectors of the economy, and the resulting interdependencies and interconnections, an inadequate regulation of data has the effect of disrupting the functioning of the 4 economic freedoms and of the the single market.

Thus, this paper is the starting point for several future research directions. One of them concerns the application and implementation at national level of the 4 EU legislative proposals on data and the digital environment, namely: the Digital Services Act, the Digital Markets Act, the Data Governance Act and the Data Act, and the analysis of their effect on the digital single market and European integration. In-depth studies are also needed on the qualification of free movement of data either as a fifth fundamental economic freedom of the single market or as only a subsidiary tool to translate the 4 classical freedoms into the digital environment and to adapt the EU economy to the new technologies. Another aspect worthy of detailed research is the application of the concept of Law 3.0 to blockchain technology, used in the case of cryptocurrencies and "smart" contracts, contracts that are executed automatically when the conditions mentioned in the software are met. Their promise to be a way to record, verify and track ownership of a digital or physical asset has the potential to reduce internal market frictions resulting from a lack of homogeneity. This control over assets will increase the confidence of the entities involved in the economy and will encourage companies to expand their business from national to European level.