UNIVERSITY OF TURKU

PROPORTIZATION OF PERSONAL DATA IN THE EUROPEAN LEGAL ORDER

Arzu Hasanova

Master's Thesis in Law and Information Society
Turku, 2020

University of Turku

Law and Information Society
Department of Law
Master Program

Supervised by

Doctor of Laws, Jusi Jaakkola

UNIVERSITY OF TURKU
Law and Information Society
Department of Law
Arzu Hasanova : Proportization of personal data in the European Legal Order
Master Programme
Master's Thesis 92
November 2020

ABSTRACT

The GDPR, applied since 2018, has largely filled the gaps and shortcomings in personal data protection that existed under the 1995 Directive. However, additional measures are still needed to further harmonize the protection of personal data, as well as to correct the imbalance of power between data subjects and controllers.

One of the options for providing real control of data subjects over personal data is a property regime, which by its nature implies the most complete right that has a binding effect on any third parties. The proportization approach was developed in American doctrine as an alternative to the tort system with limited application, and as a way to avoid a biased legislative process that reflected primarily the interests of lobbying companies.

This study provides an in-depth analysis of the control tools that are already applied in the EU legal system. These tools are compared with the objectives of the Regulation and the prospects for their achievement by the already available mechanisms. It is done to assess how if property regime on personal data can provide something valuable for personal data protection purposes and if the property regime is (in)capable of resolving the set objectives in the context of the European legal order.

Keywords: *personal data protection, data ownership, control over personal data, consent of data subject, fundamental right to personal data protection, empowernment of data subject, fair data processing*

Table of Contents

Table of Contents **4**

Abbreviations **6**

1 Chapter 1. Introduction **7**
- 1.1 The aim of the study 10
- 1.2 Research questions 10
- 1.3 Limitations 10
- 1.4 Methodology 11
- 1.5 Literature Review 11
- 1.6 Outline 12

2 Chapter 2: Threat of personal data protection **14**
- 2.1 Lack of transparency 14
- 2.2 The inefficiency of accountability rules 16

3 Chapter 3: Property right **17**
- 3.1 European property law: main principles 17
- 3.2 Flexible application of property right regime 19
- 3.3 Personal data as an object of property right 21
- 3.4 Conclusion 23

4 Chapter 4: Motherhood of data propertisation theory **24**
- 4.1 Shortcomings of the US information privacy regulation 25
- 4.2 Privacy Concept in the US legal order 26
- 4.3 US tort system and right to data protection 29
- 4.4 US Constitution 33
- 4.5 Code of Fair Information Practices 35
- 4.6 Propertisation as a tool to fill the gaps 36
- 4.7 Criticism of the propertisation arguments 37
- 4.8 Conclusion 39

5 Chapter 5: The EU Data Protection Regulation **41**
- 5.1 Data protection as a dimension of privacy 41
- 5.2 Right to data protection as a fundamental right. Article 8 of the European Union Charter of Fundamental Rights 43
- 5.3 General data protection policy within the EU: the goals 45
- 5.4 Principles of the General Data Protection Regulation 48
  - 5.4.1 Lawfulness, fairness, and transparency 49
  - 5.4.2 Purpose limitations 49
  - 5.4.3 Data minimization 50
  - 5.4.4 Accuracy 51
  - 5.4.5 Storage limitation 51
  - 5.4.6 Data integrity and confidentiality 52
  - 5.4.7 Accountability 52
- 5.5 Shortcomings of available implementation mechanisms 53
- 5.6 Conclusion 56

6 Chapter 6: The possibility of vesting property right in personal data in the EU legal order **58**
- 6.1 Is there compliance between property approach and human-centered approach to personal data protection? 58
- 6.2 The propertisation of personal data within the boundaries of General Data Protection Regulation 60
- 6.3 What property regime has to offer? 62
- 6.4 Conclusion 65

7 Chapter 7: Is there a real match with European data protection system? **67**
- 7.1 Right to self-determination & right to data protection 67
- 7.2 Consent as a mechanism of control 70

7.3 Challenging efficiency of consent mechanism....72
7.4 Does property regime fit in General Data Protection Regulation? 76
7.5 Is property regime solving intricacies of data protection in the EU? 78
7.6 Conclusion....81

8 Conclusion 84

Bibliography 86

Abbreviations

GDPR	General Data Protection Regulation
EU	European Union
CFR	Charter of Fundamental Rights
ECHR	European Court of Human Rights
CJEU	Court of Justice of European Union

1 Chapter 1. Introduction

In the digital era, the problem of personal data protection reaches enormous scale. With the development of information technology, personal data became an asset that is worth money.[1] Nevertheless, the mechanism of effective protection has not yet been developed while the value of personal data is dramatically growing. One of the most controversial and ambiguous approaches to solving this problem is the extension of the property rights on personal data.

This idea of data propertization originates from the US since 1970s. There is a different justification for the theory of the ownership of personal data. Some believe that with the help of propertisation, data owners will be able to regain lost control over their personal information. According to natural rights theory ownership on personal data would recover the essential connection between a person and the data that pertaining to him and create his personality. Others reckon that this is the only option to somehow overcome the limitations of political and legal system of the US. Commenting on US legislation, Purtova notes that the data protection law is too confusing, contains rules that are different in sources, subject matter and applicability. In the US, they are trying to apply traditional rules of privacy protection to new relationships related to personal data.

Proposals for regulatory reform suggested not to prohibit the collection and use of information, but to introduce the practice of fair use of data. For a long time in the United States there were no rules governing the use of data in the private sector, all rules covered only relations with authorities. And still the issue of establishing uniform data protection standards for private sector remains unsolved. The idea of data propertisation in the US is based on economic arguments and flaws of data protection legislation.[2]

The situation with extensive data collection was exacerbated for various reasons, such as providing national security, social welfare, a new marketing system in which profiles were created to meet the needs of consumers. Moreover, the development of technology, the dramatic increase in the integration of the Internet into everyday life has enabled storage of bulks of data, data mining and processing, profiling without obstacles. Using various services on the Internet,

[1]Corien Prins 2006, pg. 224
[2]Purtova 2009

we consciously or unconsciously provide service providers with our personal data, most of users are not aware that all their digital behavior is tracked by data collectors.[3]

Nevertheless, with implementation of property approach, new uncertainties, such as who is the owner of the data, arise? This problem is discussed in the work of Murphy, where he distinguishes two kinds of rules: non-disclosure and disclosure. Non-disclosure implies that a person (data owner) can control the dissemination of private information, while the second is that the control over personal data is initially concentrated in the hands of controllers. He thinks that an individual property right in personal information is the only alternative to no information privacy at all, and the law should intervene and allocate the initial entitlement.[4]

These difficulties associated with the Information and Technology Revolution are also relevant for the EU. Discussions about the loss of control over personal data are also being conducted in Europe, this can also be demonstrated by the new General Data Protection Regulation which specially notes the importance of ensuring users control over their data. Therefore, it is also vital for Europe to develop its perspective on personal data propertisation because this is one of the possible tools at the disposal of law that can ensure users' control on how their information is used.5 One of the scholars, Lessig back to the 1999 asserted that such a mechanism of protection will get accustomed to the European legal system, and the same tools that protect copyright in this sense could also be used to protect privacy. He assumed that the recognition of the fact that we have the ownership over the right will enforce stronger privacy protection.

The main argument against the introduction of property right in personal data in the European context is that, unlike the US, the EU implemented a human-based approach to privacy right. Article 8 of the EU Charter of Fundamental rights explicitly consider data protection as a human right and shapes a framework of the right to personal data protection. The right to personal data protection as it is enshrined in law imposes other obligations on other parties. The controller or the processor of personal data has active obligations to process personal data.

Technically, the Regulation does not contain provisions that preclude the possibility of vesting property right but neither it enshrined the property mechanism in its provisions. Some proponents of data propertisation assert that the ruling principle of the Regulation, and data

[3]Purtova 2010, pg. 193-196
[4]Murphy 1996, pg. 2383-2384
[5]Purtova 2009, pg. 2

protection system in general, of empowering data subject by giving them control over personal information is more reminiscent of property regime. And due to the vague concept of property right that can be applied to describe a relation of a control over some object, the property right on personal information is not necessarily contrary to the European perspective of data protection.

Nevertheless, it is worth noting that the introduction of this system will require significant changes. Moreover, it is not clear whether the EU has a competence to force Member States into propertisation of personal information and to regulate property law.[6] Unlike the US, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and the General Data Protection Regulation that is formulated in compliance with a human right approach provide uniformed framework on protection of personal data for private sector while property law is left to the competence of Member States.[7]

Moreover, presence of owner's title is not the only possible mechanism for protecting data, especially since such an approach is questionably in line with the legal system. The model of property right proposed by Schwartz, according to which the owner cannot alienate his right,[8] can hardly be called a property right. Legislation must empower and give people real control over their data, such attempts are taken by the General Data Protection Regulation. People should perceive their data not as an object of property benefit, but as a value that must be protected from intrusion. Personal data should not be protected as an object of property, but as an integral part of the right to privacy, the right to self-determination.

Current Regulation creates such a data protection system where individuals are given with the tools to manage information about themselves shaping their digital life, in all relations regarding personal data, individuals remain their position of the subject of control.[9]

[6]Purtova 2010, pg. 199
[7]EUROPEAN UNION CONSOLIDATED VERSIONS OF THE TREATY ON EUROPEAN UNION AND OF THE TREATY ESTABLISHING THE EUROPEAN COMMUNITY (2002) (2002/C 325/01), Article 295
[8]Schwartz 2003, pg. 2092
[9]Lazaro - Le Metayer 2015, pg. 19

1.1 The aim of the study

The main goal is to resolve the issue of whether the property approach to the protection of personal data is the most effective in regard to the interest of the individuals to whom this personal data belongs. How the EU legal system will benefit from this approach, and what, if any, risks are associated with the property law approach.

Also, with the entry into force of the General Data Protection Regulation, which is intended to strengthen the position of the data subject, giving him the tools to exercise control over his data. Therefore, it is necessary to assess the existing regulation, its principles and innovations, which can solve the current problems of personal data protection without the necessity to implement new revolutionary approach.

1.2 Research questions

The main questions of the research are the following: **1.** Can personal data propertisation provide effective data protection in the EU? **2.** Is proposed personal data proportization compatible with the EU legal system considering the fundamental right and human-centered approach of EU to personal data protection? **3.** Can the regulation of property rights be extended to personal data? I

In order to answer the main questions, a short introduction to personal data propertization concept will be given by looking at the US data protection regulation and reasons why the introduction of property right in personal data can be justified. Therefore, within this study, two sub-questions must be addressed: **4.** What are the common features and differences in the protection of the personal data of the two legal systems? Such an insight has a significant impact in applying the personal data ownership approach. **5.** Is property in personal data the only way of providing effective protection or it can be achieved by enhancing the users control over the use of their data?

1.3 Limitations

When familiarizing with the theory of personal data proportization, this research will not cover the theory of data commodification. The main attention will also not be focused on economic argumentation of data propertisation. The institute of property rights and the US approach to

the protection of personal data will be considered to the extent that they appropriately assess how the concept of proprietary regime on personal data corresponds to the EU fundamental right approach to data protection and if such a concept can effectively fill the gaps of EU data protection regulation (as it is expected within the US legal order).

Considering the possibility of personal data to be an object of property right and accordingly to be protected under a property regime, the main problems and obstacles in the application of the property regime in the civil law system will be highlighted. Common law practice and traditions will be touched upon only for purposes of comparative analysis. Also, this study is not aimed at profound study of the history and development of property law in Europe.

1.4 Methodology

To answer the main question of the research if property in personal data is compatible with EU legal system, the dogmatic method will be utilized, the possibility of data ownership will be viewed in conjunction with the legislation and case law related to the protection of personal data and the property rights model. The study implies also legal pragmatism[10], since the main focus is on challenging the merits and disadvantages of proportization of personal data as a more powerful tool for protecting personal data, as well as the effectiveness of this approach in the European context. It is also essential to employ comparative law method to carry out the analysis between the two different approaches in case of data protection that can impede the adoption of the theory emerged in the US legal doctrine.

1.5 Literature Review

Discussions about a proprietary approach to personal data protection have emerged in the United States. Most of the works used in this study are also by American legal scholars. To understand the reasons for the emergence of discussions, the shortcomings of the American legal system were highlighted, which were pointed out in the works of Bergelson, Solove, Gavison. Also, to get acquainted with the forms of property protection of personal data, Cohen and Newman's articles were used, who believed that the property right to personal data contributes to the perception of the significance of personal data. Murphy, Schwartz, and Samuelson noted the importance of limited property rights and some default rules.

[10]Butler 2002

The main source for describing the European system and approach to personal data protection was the GDPR itself. The research tried to disclose the content of the principles and main innovations of the Regulation. Analysis of the relationship between the right to privacy and the right to personal data protection was mostly based on the books of Andrej Savin, Serge Gutwirth and Mireille Hildebrandt. The Commission's report on the experience with the implementation of the GDDR over the past two years has provided a good insight into the challenges that have not yet been overcome by the GDPR.

The most comprehensive research on the possibility of using the property approach to personal data protection in the European legal system was conducted by Purtova. However, her work clarified the advantages of the property regime in comparison with the 1995 Directive, and there are very few relevant works discussing the need to apply property approach after the application of the GDPR. Jacob M. Victor mapped the new approach in the light of the drafted Regulation. Schwartz's concerns about the effectiveness of the property regime were also used in this study because his doubts have not lost their relevance nowadays. The work of Rouvroy Antoinette, Poullet Yves has become the centerpiece of the link between fundamental rights and the right to personal data protection, thus providing a comprehensive understanding of the European approach to data protection regulation. And the work of Ritter Jeffrey, Mayer Anna provided a good basis for advocating the GDPR as an effective instrument for achieving the goals set by the Union in personal data practices.

1.6 Outline

The Second Chapter of this study fluently touches on the main challenges posed by the development of information and communication technologies, which are especially relevant in the context of the GDPR, namely the lack of transparency in the processing of personal data and the accountability of controllers and processors. The Third Chapter outlines the concept of property law in the civil legal system and its fundamental principles. The chapter also addresses the main intricacies of applying the property regime to personal data. The Forth Chapter of the study is devoted to the history and reasons for the emergence of the theory of proportization of personal data in the American legal system. Chapter Five is devoted to the protection of personal data in the European legal system, and in particular to the analysis and familiarization with the main act of the Union governing the fair processing of personal data. The Sixth Chapter discusses the potential for introducing a property-based personal data protection regime into the

European legal system, as well as the possible positive effect of a property approach to personal data. And the final Chapter Seven is devoted to the main research question, namely the necessity and effectiveness of the property approach in the context of the European legal system and order.

2 Chapter 2: Threat of personal data protection

The threat of a massive collection of personal information, about every action, preferences, lifestyle has been around since the nineteenth century. Commercial companies, in search of more effective marketing, began indiscriminate collection and processing of personal data on citizens that were collected by the state during the census. Today there are not only private enterprises that buy personal data for marketing purposes, but also entities whose business model consists of a collection of personal data and further sale to enterprises that need this data to implement an effective marketing strategy.[11] And at the moment, the turnover in the secondary information market exceeds several billion dollars.[12]

To some extent, it is possible to justify the wide business practice in gathering and processing personal data for solicited marketing in order to improve the quality of goods and services, bringing these goods and services in line with the requirements and expectations of users, which undoubtedly gives significant positive results in the development of a successful business. However, this is not the only practice of using users' personal information. Today, personal data is used not only for marketing purposes, but personal data is also considered to be a very precious asset, and enterprises are actively exploiting the value of personal data of their customers by transferring it to third parties in the information market.

2.1 Lack of transparency

The majority of the data subjects (the person to whom the personal data pertain) do not even suspect how much of their personal information is collected and processed for different purposes on a daily basis. Besides the information that data subjects themselves provide to various platforms, for example on social networks, or when making online purchases, an enormous amount of information about users' preferences and lifestyle is collected by controllers (actors who are collecting and processing personal information) without due notice.

New technologies make it possible to store an unthinkably huge amount of information without particularly high investments. With the help of cloud computing technology, it is not necessary for businesses to have their own servers for data storage, modern technologies allow to do it

[11]Solove 2001, pg. 1408
[12]Solove 2001, pg. 1407

using programs located on someone else hardware.[13] And it is obvious that very few of the users know where their personal information is stored, for what purposes, when it was collected, and by whom exactly.

New technologies that has emerged for the past decades allow data controllers to make the data collection process invisible. Each person using a mobile device provides information about their geolocation to a number of different controllers completely unaware of it.[14] Various mobile applications have access to the user's contact data or to the gallery. Not only behavioral information is readily available without the data subject's knowledge, but also sensitive information concerning health, political or religious beliefs, minority affiliation.

The lack of transparency in operations performed with personal data deprives the data subject of control over data pertaining to him. That means that if the data subject is not aware of what personal information is available to third parties, the data subject will think twice about the actions that he takes since there is always a possibility that his every decision, every action is tracked.

Observing every aspect of data subjects' lives would fundamentally destroy the existence of individual autonomy. If the data subject is deprived of the right to not disclose personal information, to keep it secret, then he will adjust his life, his behavior, and his personality to "normal" standards for fear of negative consequences.[15]

For instance, with the help of profiling, the process of categorizing individuals or groups of people based on certain criteria, not only compiles personal information into a single profile but also is able to predict behavior or preferences that are typical for a certain category of individuals or groups of people. Such a prediction can be made on the basis of already available information about an individual, or it can be made indirectly by judging the preferences or behaviors of people from a similar group.[16]

[13]COM(2010) Brussels, 4.11.2010 609 final, pg. 2
[14]COM(2010) Brussels, 4.11.2010 609 final, pg. 2
[15]Antoinette - Poullet 2009, pg. 47
[16]Hildebrandt 2008, pg. 40

In Orwell's world, there is no place for the right to self-determination and self-development, to individualism. A totalitarian regime that monitors its citizens is frequently used as an anticipated future by advocates[17] for privacy and high standards of personal data protection.

Lack of transparency and information about who, when, where, to what extent has access to personal information, and for what purposes it is used creates a huge imbalance of power between controllers and data subjects. Lack of transparency weakens the position of the data subject, while controllers gathering more information respectively gain more power.[18]

2.2 The inefficiency of accountability rules

The lack of transparency is caused by insufficient rules of accountability and responsibility of controllers. It is the controllers who decide what personal data they need and for what purposes in order to provide the data subject with certain services. That is, they should be held responsible for providing relevant information, which would make the process of collecting and processing personal data transparent and fair. In this case, the data subjects would have the freedom of choice, and, accordingly, would have some degree of control over the personal data.

The problem of accountability is also caused by the complex and tangled chain of personal data flow from one controller to other actors (other controllers or processors[19]). In such a complex multilateral relationship, it is difficult to understand how responsibility and accountability for the lawful processing of personal data, as well as for taking appropriate measures to ensure the security of personal data are distributed. This problem is further exacerbated by the opacity of this chain.[20] Thus, when a violation of the data processing rules is revealed, it is difficult to find out at what point of that chain the violation occurred and to figure out who was included in this flow of personal information, and who is responsible for the violation.

As noted above with cloud computing, controllers carry out various operations with personal data not only by their own means but also by utilizing outsource services. That is, the modern practice of data processing is immensely complicated, and for and an incompetent data subject defending his rights and interests in the event of a violation becomes merely impracticable

[17]Solove 2001, pg. 1414
[18]Regan 1995, pg. 2
[19]GDPR Article 4(8) '*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'*
[20]Purtova 2011, pg. 49

3 Chapter 3: Property right

In the legal doctrine, discussions are gaining momentum about a new generation of personal data protection regulation through the implementation of a well-known property regime. It is assumed that property rights are best able to provide real control over personal data by allowing the owner himself to enter into negotiations with the actors of the information industry. This would allow the data subject, that is, the owner, to control and decide on the conditions on which he would like to give his consent to the disclosure and use of personal information pertaining to him. Property rights will be able to best reflect the interests of the data subject in relations with the controllers.

Nevertheless, even though the property regime assumes indisputable control over property, the first concerns appear with the possibility of applying the institution of property rights to new relations and objects. The question arises if it is possible to extend the property regime to new relations that are not enshrined as property relations in the statutes. Furthermore, the nature of personal data also raises questions as to if data can be regarded as a new object of property right, especially given their intangible nature. How flexible is the institution of property rights to cover the relationship on the use of personal data of data subjects by other actors in the information market?

3.1 European property law: main principles

The institution of property law is left to regulation by the competent authorities at the national level by the Member States. There is no supranational legal act that would harmonize the general concepts of the property regime, as well as its basic principles. However, all the legal systems of the Member States share common features that are inherent to any property relationship.

The right to property grants its owner the exclusive right to exercise power over the fate of the property belonging to him.[21] Mainly, the property law divides the property into the category of movable and immovable property,[22] from which it follows that the objects of property rights are tangible things.[23]

[21]van Erp 2012, pg. 13
[22]Akkermans 2008, pg. 91
[23]Ramaekers 2013, pg. 250

Property rights are considered the most comprehensive and full rights because according to the inalienable principle of *erga omnes*, the property rights of the owner are opposed to and can be forced against any third parties. Therefore, the right is also called the fullest right, its action has a binding effect for absolutely everyone. The owner has the right to exclude all third parties from interfering with the free exercise of his property right. Also, the owner is entitled to use and dispose of his property as he wishes. This right, however, is not absolute, its exercise is limited by the interests and rights of third parties, which may be harmed as a result of abuse of one's property right.

The opposite of property law is a personal right, or in other words, the law of obligations, which imposes obligations only on the parties to the corresponding agreement,[24] and contracts are of short-term effect. Whilst property right is not limited in time, it lasts as long as the object of property rights exists.[25] Property law is aimed at creating wealth, regulating the acquisition and distribution of wealth, so it is of great importance for owners that these property relations are stable and constant.[26]

Since property right is the most burdensome right for third parties, it must also comply with the *principle of transparency* (which is further divided into the *principle of specificity and the principle of publicity)*. This means that it must be clear and explicit which specific object is subjected to a property right, the object must be clearly defined. Thus, the fact of the existence of property rights to the object must be publicly available. For the overarching effect of a property right to have a real meaning, third parties must know in relation to which specific object there is a property right in order to refrain from any actions that prevent the right holder from exercising his right.[27]

Each aforementioned principle is an integral characteristic of property law. However, there is a principle that resolves the question of applicability of the property regime to certain legal relations. This principle is a *principle of numerus clausus*, which initially determines the (in)applicability of other principles.[28]

[24]Akkermans 2008, pg. 65
[25]Purtova 2011 , pg. 67-68
[26]van Erp 2009, pg. 2
[27]van Erp - Akkermans 2012, pg. 75-76
[28]Akkermans 2008, pg. 5

The numerus clausus principle refers to legal restrictions on parties in the creation of property rights. This usually means that the national legislator has established an exhaustive list of property rights in a legal act (like Civil Codes of France, Germany, Netherlands). Such a closed system of property regime enshrines what property rights are permissible and determines their content. Therefore, the parties cannot create property relations that are not known by laws.[29]

Principle numerus clausus has a more flexible application in the common law system. This principle in the common law system is not enshrined in the statute but is implemented in court decisions. Also, in the civil law system, the right of ownership is defined as the most complete form of the right. While common law recognizes the existence of different property rights to the same object, also known as the concept of fragmented ownership in the legal doctrine.[30] Moreover, each such holder of a lesser right has its own claims to the same property object, and each of them is provided with the same level of protection.[31]

Another important rule for fragmented ownership is the nemo dat rule. It lies in the fact that the holder of the lesser (meaning not full) property right cannot transfer more rights to the property than he has himself. The holder of the fragmented property right on an object cannot transfer full property right to this object to another person.[32]

The system of common law is recognized as a more flexible environment for accepting new property relations, but since the system of civil law reigns in the Member States of the Union, the fundamental point for the EU discussion is how open the civil law order is in order to apply a stricter property regime to new relations that have arisen as a result of social-technological development.

3.2 Flexible application of property right regime

The property regime is a long-standing institution, and the principles described earlier also remain invariably relevant. With the incessant, rapid development of society, economy, culture, it is predictable to face a problem when new relationships appear, for example, due to the era of technological breakthroughs, and old legal mechanisms and tools are too rigid to embed them into new realities.

[29]Akkermans 2008, pg. 6-7
[30]Purtova 2011, pg. 72
[31]Purtova 2011, pg. 78
[32]Akkermans 2008, pg. 377, 412

Quite a few legal scholars[33] have been concerned about the need to give the parties the freedom to create new property rights and determine their content. They also proposed to revise the principle of numerus clausus, which is the most limiting principle among other conditions.

Sjef van Erp anticipated that with the emergence of new relationships, immensely stringent application of the principle of numerus clausus can lead to undesirable implications.[34] The development of technology poses serious challenges for the policy and the lawmakers, the legal order does not keep pace with the dynamics of the development of society. If one takes an overly meticulous approach to the application of familiar mechanisms, it will be difficult to achieve effective regulation and protection of new relations. So, if one strictly adheres to the letter of the law, new objects created as a result of a technological boost, and which is of high value, may generally remain without legal protection.

The classical model of property regime has proven effective in overcoming the feudal system by allowing the fair distribution of the wealth among the working class of citizens too. To counterbalance the situation, the idea of fragmented ownership had to be abandoned.[35]

Nevertheless, taking into account the current development of different aspects of the society, there is a new need to reshape property law again in order to ensure the interests of new owners, to effectively regulate the relations of owners in regard to new property objects.

Such steps towards a new ownership model have already been taken, as evidenced by the less meticulous application of the principles of property law. Thus, the legislation provides a special regime to protect the interests of the legal owner (the creditor) and the economic owner (the debtor). The property can be transferred to another person for the purposes of property management (a trust). New property objects have emerged, such as information that has high economic value for businesses known as trade secrets, or the results of creative and intellectual work known as intellectual property.[36]

These relations were not previously known at the time of the formation of the classical property

[33] van Erp 2009, See also Akkermans 2008
[34] van Erp 2003, pg. 5
[35] van Erp 2009, pg. 14
[36] van Erp 2009, pg. 17-19

regime. However, progress and development contributed to the need to move away from the approach of a rigid application of the property regime. Therefore, today, the civil law system acquires more and more similarities with more flexible common law.

3.3 Personal data as an object of property right

Personal data is undeniably acknowledged as a modern asset of tremendous economic value in the information industry. The value of personal data, which gives controllers enormous power, is often misused and abused. The controllers do not give much regards to the subjects to whom this personal data pertains, the interests of the data subjects are not taken into account when processing and otherwise using valuable personal information.

Due to such an imbalance in power, unfair consideration of the interests of the parties, it is assumed that the vesting the property right in personal data with data subjects will contribute to the equilibration of positions of controller and data subject. The erga omnes principle in this context is the most essential since it will allow data subjects to use their dominion over their personal data against everyone.

Nevertheless, personal data is not a conventional object of property right. That is why the discussion of the possibility of introducing property rights to personal data is associated with the concern about the possibility of personal data to be regarded as an object of property right takes the central place.

Even if, as was suggested, it is possible to overcome the rigidity of applying the principle of numerus clausus, then there is another obstacle in the employment of the property regime, namely the principle of transparency. The principle of transparency as described earlier, stipulates that the property object must be clearly identifiable, must be specific, in order to provide legal certainty for other parties.

There is a harmonized concept of personal data, enshrined in Article 4 (1) of the GDPR, according to which personal data is:

> *any information relating to an identified or identifiable natural person ('data subject') ...*

As can be judged by the definition, the concept of personal data captures a huge range of different types of information that can be attributed to a natural person. And at first glance, satisfaction with the principle of transparency seems very doubtful which is fundamental for the attribution of property right. The concept of personal data is overly broad and may introduce ambiguity in the specification of the object of protection. The situation is further aggravated by the constant development of technologies that enhance the ability to identify previously anonymous information.[37]

The Working Party also noted the possibility of this shift from non-identifiable to identifiable data, also explaining this by technological advancement in the processing of data.[38]

Also, the information has to relate to a natural person, data must be about a person. Personal information includes characteristics, the identity of a person, behavioral information, any other data that has an impact on the perception, assessment of this person by others. Moreover, personal information includes information that has an impact on the interests and freedoms of a person.[39] In order to ensure high protection for data subjects' interests, the legislator deliberately made the scope of the concerned concept broad.

And lastly, conventionally the objects of property rights are tangible objects. In the digital age, this approach is too restrictive since online goods are not attached to a physical carrier in the online space. It is for this reason that the CJEU, taking into account the widespread use of online "goods", ruled that the sale or licensing of objects of intellectual property on the Internet also depletes the right of the copyright holder to exclusive distribution.[40] Despite the fact that the Court did not explicitly recognize intangible objects as objects of property rights, certain steps have been taken in this direction which has a groundbreaking impact on the perception of property objects.

[37] Purtova 2017, pg. 14
[38] Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, Adopted on 20th June, pg. 15
[39] Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, Adopted on 20th June, pg. 10-12
[40] Case C-128/11 UsedSoft GmbH v Oracle International Corp (2012), para. 72

3.4 Conclusion

Despite the rigidity of the application of the property regime in the civil law system, the rapid technological, social, economic, and cultural progress indicates the need to reshape property law to meet the needs of the new reality. The opposite can be detrimental to the interests of the parties to the new relationship. New objects emerging from technological development have an extremely high economic value for both natural people and businesses, and property law is the most powerful tool for ensuring control over a valuable object and protecting economic interests of the rightholder.

Personal data has proven its economic value to the information market. For the sake of seizing this value, controllers often abuse the position of data subjects, collecting and processing personal data unlawfully.

Undoubtedly, the attribution of personal data to objects of property law seems to be quite problematic. The blurred boundaries of the concept of personal data and its intangibility impede compliance with the transparency principle, which is fundamental to the property regime. Nevertheless, CJEU has already taken certain steps to proportization of intangible objects, which, due to the era of digitalization, is of great practical importance.

4 Chapter 4: Motherhood of data propertisation theory

In the digital era, the problem of personal data protection reaches an enormous scale. With the development of information technology, personal data became an asset that is worth money.[41] Nevertheless, the mechanism of effective protection has not yet been developed while the value of personal data is dramatically growing.

Collectors are most interested in collecting personal, and in particular sensitive data for the further sale of a database of these data in the information market.[42]American scholars believe that citizens have lost control of their privacy and their personal data,[43] and also excluded from the list of the stakeholders who benefit from the disposal of their personal data.[44]

The main reason for the lack of consistent regulation of information privacy in the American legal system is the lack of a clear and concise understanding of the essence of an individual's interest in owning and protecting private information. While in the EU legal system, comprehensive regulation, and high standards of protection of information privacy is ensured by following the fundamental right approach to personal data protection.[45]

In order to reaffirm the right to privacy and, in particular, the right to personal data protection, it is necessary to return control over personal data to the subjects of personal data. And there are several approaches presented in the legal literature on how the control over personal data can again be concentrated in the hands of the data subjects.

One of the most controversial and ambiguous approaches to solving the problem caused by global technological breakthrough is the extension of the property right regime on personal data. Vesting property right to personal data can be a solution to the problem of determining interest in the protection of personal data.46

This idea of data propertization originates from the US since 1970s. There is a different justification for the theory of introducing property right on personal data. Some reckon that

[41]Corien Prins 2006, pg. 224
[42]Waldrop 1994, pg. 46, 49
[43]Laudon 1996 pg. 92, 94
[44]Bergelson 2003, pg. 383
[45]Samuelson 2000, pg. 1170-1171
[46]Samuelson 2000, pg. 1171

this is the only option to somehow overcome the limitations of the political and legal system of the US. The theory of personal data propertization was put forward due to a lack of the rules governing the use of data in the private sector in the American legal system, all legal norms covered only relations with authorities or were addressed to specific sectors. And still the issue of establishing uniform data protection standards for the private sector remains unsolved.

Others believe that with the help of propertisation, data owners will be able to regain lost control over their personal information. According to natural rights, property right approach on personal data would recover the essential connection between a person and the data pertaining to him.

Within the framework of this chapter, those imperfections of the personal data protection system that have led to the compulsion of new measures to protect the right concerned will be discussed and analyzed.

4.1 Shortcomings of the US information privacy regulation

The need to respect an individual's privacy was first announced in 1890 when American scholars Samuel Warren and Louis Brandeis published The Right to Privacy in Harvard Law Review,[47] which substantiated the need for judicial protection of privacy from intrusion, similar to how it is protected good name from slander and libel. Shortly after publication, individual states gradually began to adopt civil law standards to protect privacy as an intangible good.

The shortcomings of the US data protection system are associated with the highly fragmented US legislation.[48] It does not have a single and coherent data protection framework but rather includes a bundle of constitutional, federal, and state statutory and tort law.[49]

The relations of citizens with private organizations collecting and processing personal data of users are regulated by federal laws relating to individual industries, for example, education,[50] telecommunications,[51] banking,[52] financial, medical[53] and so on.[54]These laws are very harshly

[47]Warren - Brandeis 1890, pg. 193-220
[48]Bergelson 2003, pg. 392-393
[49]Fred H. Cate 1997
[50]The Family Educational Rights and Privacy Act of 1974 ("FERPA")
[51]The Cable Communications Policy Act of 1984 ("CCPA") of 1984
[52]The Fair Credit Reporting Act of 1970 ("FCRA")
[53]Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
[54]Solove 2001, pg. 1441-14443

criticized by privacy advocates, arguing the laws concerned were adopted under the great influence of lobbying companies operating in the respective industries whose interests are taken into account in the first place when developing regulation.[55]

Moreover, disadvantages of legal regulation of the protection of personal data begin with the conceptualization of privacy. Even though that in the US legal system there are several acts regulating the processing of personal data in certain sectors, there is no single systemic and comprehensive act.

4.2 Privacy Concept in the US legal order

One of the main reasons for data propertisation theory emergence relates to how the data protection problem was conceptualized in the US. Solove emphasizes in his work the relevance of the problem of the definition of the concept of private life. Some scholars give a narrow definition, while others include in private life a very diverse range of rights, such as the freedom speech and thoughts, the right to personal information, the inviolability of the home, and so on. Solove also cites very reasonable concerns about the progressive development of relationships that affect the privacy of each individual. And in such conditions, it is hard to define a concept so that it can provide an effective basis for the development of relevant legislation and law enforcement practice. In the absence of a clearly defined concept, it is difficult to establish the goals and principles of further regulation.[56]

Solove believes that privacy should not be conceptualized using the general elements and principles of different theories of privacy, but rather a definition of privacy should be given in the context of those practices that affect privacy. Many theorists are trying to give a comprehensive definition of privacy, which would contain the basic elements of any relationship relating to the privacy of individuals, and Solove sees that approach as the main drawback of existing concepts of private life.[57]

Historically, the US law adhered to a very narrow understanding of the right to privacy, where privacy was mainly identified with the issue of secrecy and the right to be left alone.

[55]Fenrich 1996, pg. 966-967
[56]Solove 2002, pg. 1089-1090
[57]Solove 2002, pg.1093

The first to determine the right to privacy were Warren and Brandeis, whose work became the foundation for further discussions of the concept of privacy in legal doctrine. The authors defined the right to privacy as the right of each individual to be left alone. They substantiated their theory by the fact that some actions that are possible due to technological progress cause a certain emotional pain to the person in relation to whom these actions were taken. That is, such actions violate not so much the individual's right to receive material benefits from such publication, but violate his personal integrity, and cause mental torment for this individual.[58]

The concept of privacy as secrecy was developed by Judge Posner, who reduced the right to privacy as the right of everyone to keep their affairs secret from the public, that is, to restrict third-party access to the self.[59] This concept is fundamental to the right to information privacy. Thus, the right to information privacy is seen as the right to non-disclosure of personal information which was repeatedly supported in court decisions.[60] Once the information has been disclosed to the public, there can be no more expectations that this information is private.[61]

However, the total secrecy is extremely limiting the effectiveness of the application of this concept, since it does not allow the individual to choose whom he wants or does not want to disclose his information what considerably limits his freedom. To exercise the right to privacy, an individual must conceal his personal information from everyone.[62]

Solove also noted that the right to informational privacy lies not only in the fact that the individual can decide who will be aware of the facts concerning his private life, but also the ability of this individual to decide how and for what purposes the information about him will be used.[63]

Such a narrow concept of privacy protects the information that is kept secret, only in this case, the subject has the right to non-interference from third parties.[64] Thus, as such, the data subject does not have control over his personal information, either he chooses to disclose his data,

[58]Warren – Brandeis 1890, pg. 200, 205
[59]Posner 1978, pg. 397
[60]*See* Supreme Court Whalen v. Roe 429 US 589 (1977): application of Substantive Due Process Clause to personal data protection matters
[61]Hilderbrandt 2015, pg. 189
[62]Solove 2002, pg. 1108
[63]Solove 2002, pg. 1109
[64]Bergelson 2003, pg. 401

transferring it to the public domain, or the subject must observe and protect the complete secrecy and confidentiality of his information from all parties without exception.

According to Solove, one should not stuck with the idea to give a comprehensive definition of a certain concept. Such a complex approach has a risk of the rigid application. Relations change over time with the development of a society. There are a lot of factors that will appear and disappear, but which cannot be foreseen and taken into account beforehand. Therefore, Solove takes a pragmatic approach to conceptualize privacy, strives not to focus exclusively on the theory, since a theory without context, without practical application, does not have a high value.[65]

He means that private life has its value in the context of a certain relationship. Some relationships require stronger protection of confidentiality, and sometimes excessive confidentiality can be detrimental in other cases,[66] for instance, with domestic violence.

According to some authors, the right to privacy is a tool to achieve a higher-end goal. Therefore, speaking of the extent to which the right to privacy is to be protected, it is first of all necessary to determine the goal that we want to achieve through the implementation and protection of this right.[67]

The most appropriate way to defend users' interests is to return the control over personal data to the data subjects, to decide for themselves who and on what basis can process personal information pertaining to him. And as some authors have noted, the problem with protecting personal data is that no one exercises control over it.[68]

American legal scholars decades ago already predicted a rapid development of technology and the problems that would follow the era of information and communication technology. They noted that publishing personal information in the media is not the only threat to privacy. They already warned at that time that the right to non-disclosure of information is not enough, in the new technological generation, personal data subjects should be vested with the right to control the dissemination and use of the information pertaining to them.[69]

[65]Solove 2002, pg. 1143-1144
[66]Solove 2002, pg. 1145-1146
[67]Gavison 1980, pg. 442, See also Westin 1967, pg. 49; Solove 2002, pg. 1145
[68]Solove 2001, pg. 1428
[69]Bezan 1992, pg. 1135-1136

Theorist Alan Westin believes that this form of control should be carried out using the property right of personal information.[70] In further consideration of the American tort system, it will be demonstrated that appropriation tort partially recognizes this data propertization approach in disputes of unlawful use of personal information for commercial purposes.

Since each individual is a social being, every individual has an irresistible desire to be part of this society. But each individual must have freedom of choice, to whom, and to what extent to give them knowledge about self.[71]

And speaking of the control of data subjects over personal information, this is not about absolute control without any interference from other actors. Absolute and unconditional control of data subjects can lead to adverse consequences, which can significantly infringe the essence of privacy.

4.3 US tort system and right to data protection

The US tort law, which plays a key role in privacy protection, also adheres to the narrow notion of privacy. It emphasizes the nature of the information which can get protection under the Fourth Amendment, only if such information is expected to be private, moreover, the court also takes into account whether society considers such expectations reasonable.[72] Furthermore, the court in its decisions asserts that the person who voluntarily disclosed information to third parties cannot refer to privacy expectations in such information because the information concerned is no more private.[73] It is obvious that the identification of the right to privacy, which encompasses informational privacy,[74] with secrecy does not fit well in the days of constant information communication.

For those who seek the protection of their information, there are four kinds of privacy torts defined by Prosser: intrusion upon seclusion, public disclosure of embarrassing facts, the appropriation of name or likeness, publicity in a false light.[75] Decisions of the court within the

[70]Westin 1967, pg. 324
[71]Westin 1967, pg. 324
[72]Katz v. United States, 389 U.S. 347, 351 (1967)
[73]Smith v. Maryland, 442 U.S. 735 (1979).
[74]Bergelson 2003, pg. 401
[75]Bergelson. pg. 405

specified torts unequivocally demonstrate that none of them is capable to effectively solve the personal data related issues set by the scale of data processing and flow.

To understand why none of the available options can be commonly applied to adequately protect information privacy, it is necessary to point out the significant shortcomings of each of them.

In the case of the **intrusion upon seclusion**, the plaintiff must prove the fact of the highly offensive invasion in his solitude or private affairs. Even though it does not require the intrusion in physical space, the plaintiff cannot rely on information protection within the concerned tort if the data subject voluntarily communicated his personal information. Thus, the fact of the intrusion takes place only in case of unauthorized personal data collection. Although it might be also difficult to qualify unauthorized data collection as offensive to a person concerned if it was an innoxious collection of some neutral personal information because the court can find that the significant danger arises only with the consolidation of a large mass of information.[76]

This tort can ensure the protection of the data subjects' right from the collection of their personal data without the proper procedure, namely, without obtaining the consent of the data subject to collect his personal data. Nonetheless, this mechanism is unable to address the issues of further data use and processing if that data has been once disclosed by the data subject.[77]

In order to sufficiently regulate the modern relations of individuals with public and private controllers of personal information, the voluntary disclosure of their information should not be regarded as a deprivation of the right to privacy. If it is recognized that information privacy consists of possession of individual control over his personal data, then the fact of disclosing information will not entail the deprivation of control over information by the subject. Control will allow data subjects to restrict access to himself[78] and to decide how his data can be used, to whom it can be transferred, decide on further dissemination of his personal data,[79] regardless of whether his personal information was disclosed to a third party for any purpose before.[80]

[76]Solove 2001, pg.1432
[77]Bergelson 2003, pg. 406-408
[78]Westin 1967, pg. 7
[79]Gavison 1980, pg.427
[80]Solove 2002, pg. 1152

Within the **disclosure tort**, in order to benefit from such a protective mechanism, the plaintiff has to prove that the information disclosed is of highly personal or offensive character what is hard to do considering that data collectors usually gather fairly neutral information.

This form of tort will be effective in protecting particularly sensitive information regarding health, family secrets, personal life, the disclosure of which can bring their owner mental anguish.[81] But since in most cases we provide neutral information about ourselves,[82] and exactly the information about our lifestyle[83] is particularly valuable for direct marketing purposes, disclosure tort cannot impose a universal tool of protecting any personal data but only a specific category of highly sensitive information.[84]

The vague criteria that the court is guided by when considering cases of unlawful disclosure of personal information, namely, reasonable expectations of privacy, make this tort outdated. To date, a huge amount of personal information of users is transmitted to the controllers located outside the country. Reasonable expectations of privacy may not be the same for everyone; this concept has a great dependence on the social, economic, and political levels.[85] A clear example is Safe Harbor[86], an agreement between the United States and the EU governing matters with high personal data protection. The provisions of this agreement provide better protection of personal data to EU citizens than the American legal system for its citizens. This is clear proof that the expectations considered reasonable vary from country to country.[87]

Moreover, it is not an easy task for the subject of personal data to discover the fact of transferring his personal information from one data controller to another.[88] Usually such a transfer is carried out without the knowledge of the data subject.[89]

The tort of the **appropriation of name or likeness,** in essence, protects the plaintiff's right to benefit from the use of his name, which has some value due to the reputation, the image of the

[81]Bergelson 2003, pg. 410
[82]Solove 2002, pg. 1153
[83]Solove 2002, pg. 1404
[84]Solove 20002, pg. 1433
[85]Bergelson 2003, pg. 415
[86]2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)
[87]Bergelson 2003, pg. 415
[88]Solove, 2001, pg. 1433
[89]Solove 2002, pg. 1154

person to whom the name belongs. Such protection is very similar to the protection of the owner's interests in the use of his property.[90] And according to some legal scholars[91], appropriation tort and the right to publicity have a solid basis to talk about the possibility of introducing property rights to personal data.

Nonetheless, appropriation tort also has limited application for data protection issues because it demands the exploitation of certain information for the defendant's benefit since the tort concerned protects only the commercial value of used information.[92] The court concluded that the tort does not protect the information itself but rather it protects the value of that information that might be used for advertising and business purposes.[93] Moreover, within this tort, the court inferred in its decision that the name of the data subject has the value only after it is been collected and categorized by the defendant.[94]

The appropriation tort does not protect the name of citizens as such, but rather the value, reputation that is associated with this name is subject to protection.95 Thus, an ordinary citizen is unlikely to enjoy these legal remedies, because, unlike media personas, their image and reputation may not be of equal value. Nevertheless, the use of personal data of individual citizens in the direct marketing industry is commercially profitable.96 And in cases when, for example, the data collector sells a list with customer names that will be used for direct marketing purposes, the customer's name is not used to promote any product, the reputation and image of this customer in no way brings any benefit to the data collector.

And lastly, the tort of **false light** has no applicability for personal data related issues. The information concerned in this tort must be erroneous. Such a remedy is not suitable as a measure of granting greater control to the data subject over his data. In this case, the action is illegal if information puts the complainant in an unfavorable, bad light. Such a remedy cannot be used in cases where the plaintiff himself has provided his data to the controller. Illegal data processing, excessive data collection does not necessarily affect subject's right to protect his reputation. The false light tort is not applicable also in cases of further unauthorized transfer of personal data.

[90]Bergelson 2003, pg. 416
[91]Fenrich 1996, pg. 994
[92]Solove, 2001, pg. 1434
[93]Bergelson 2003, pg. 413
[94]Dwyer v. American Express Co. 652 N.E.2d 1351 (1995)
[95]Bergelson 2003, pg. 414
[96]Litman 2000, pg. 1291

Thus, after considering the American system of a tort, it becomes apparent that the system of existing tort in the United States is not able to provide effective protection of the rights of individuals to privacy and to protect personal data in particular against unfair information practices. The courts do not provide coherent decisions on privacy matters.[97] American system of torts provides protection only against the disclosure of personal data that is highly offensive for the data subject or when the action of data collection is intrusive itself.[98]

Even if the courts start interpreting some of the concepts more widely, tort alone as a remedy against private information misuse will not be enough. A tort system cannot provide comprehensive protection because it is aimed at establishing justice after someone's right has been violated, torts eliminate the consequences of the offense, but do not prevent illegal actions. It is the substantive law norms that are intended to establish the rights and positive obligations of the parties of the legal relationship.

And, of course, it is worth mentioning once again that the court, while assessing the alleged violation of the right to informational privacy is guided by very vague (reasonable expectation of confidentiality) and outdated (privacy as secrecy) criteria. The court must evaluate all the circumstances of the case to decide on the fact of a violation. If data subjects can protect their rights to information privacy only through litigation. This can lead to very negative consequences when, due to the significant cost of time and money, individuals will not be encouraged to seek the protection of their rights.[99]

4.4 US Constitution

Considering the limitations of the US legal system, Constitutional law also must be mentioned. First of all, even though the Constitution has a special role in information privacy development, the limited scope of constitutional protection has to be noted. The Constitution is purposed to establish limitations on the state's power constraining government from certain actions.[100] Moreover, constitutional provisions do not create positive obligations, but rather imposes

[97]Gavison 1980, pg. 461-462
[98]Litman 2000, pg. 1291
[99]Bergelson 2003, pg. 418
[100]Schwartz 1996, pg. 6

negative duties not to invade the privacy of citizens without absolute necessity.[101] Also, the Constitution does not regulate relations between private parties.[102]

However, it is reasonable to affirm that with existing global private entities such as Google, Facebook, and entities which provide essential services, the data subject is fairly in the same position as with the government.[103] Nevertheless, the relations between private parties regardless of the actual non-equal footing are of utilitarian nature[104] and almost entirely left to self-regulation. And in most cases, data subjects are bound by terms and conditions imposed by a powerful party.[105]

The Fifth Amendment, which states that no one can be forced to disclose incriminating information in the framework of criminal proceedings. Thus, the Amendment restricts the state's power in collecting information about its citizens. The Amendment has a very limited application exclusively in the framework of criminal prosecution, and the provisions are also addressed specifically to the state but not to private parties.[106]

The Fourth Amendment is designed to protect citizens against "*unreasonable searches and seizures"*. Some authors believe that the Fourth Amendment is the American approach to defining the concept of privacy.[107] But the courts interpreting the Fourth Amendment severely limit its application. The courts are guided by an approach to privacy as an area of life that is expected to be confidential. Such an approach is vague, the expectation of privacy will inevitably differ from person to person depending on person's social-economic background.[108]

To sum up, the above-mentioned shortcomings have forced the US scholars to reconsider the privacy concept supporting the model of control which means that individuals should be granted the right to decide on who, when, and for what purposes can get access to and make use of their personal information. In that sense, privacy, specifically informational privacy, in fact, can be defined as the property right on personal data. That would mean that the data subject is entitled

[101]Solove 2001, pg.1435
[102]Solove 2001, pg.1435
[103]Schwartz 2004, pg. 2081, 2086
[104]Newman 2008, pg. 338
[105]Daniel E. Newman. pg. 339
[106]Solove – Rotenberg - Schwartz 2006, pg. 208
[107]Whitman 2004, pg. 1211
[108]Solove 2001, pg. 1435

to exclude others from accessing his personal information and to determine conditions and terms under which such information can be communicated to others.[109]

4.5 Code of Fair Information Practices

An overview of the American legal system on data protection matters would be incomplete without the Code of Fair Information Practices. The US Department of Health, Education, and Welfare proposed to create a new regulation that could meet the requirements of the era of new technologies and the problems created by their global application. It outlined the problem caused by the rapid development of information technology and set the task of developing a new regulation that could protect the information privacy of citizens.[110]

As a general guideline for the creation of appropriate regulation, the basic principles were drafted, which were to form the framework for the new law. Five principles were highlighted: 1. the prohibition of secret collection and storage of personal data; 2. the right of the data subject to know what information and for what purposes it is processed; 3. the right of the personal data subject to prevent the processing of data for purposes other than established for the initial collection of data; 4. the right of the data subject to rectify inaccurate information about self; 5. the data controller should be held responsible for the misuse of the collected personal data.

Further in this work, it will be shown that this had a great influence on the construction of the European approach to the protection of personal data, and these principles were also included in the supranational EU acts that consolidate the criteria for the lawful processing of personal data.

The Code of Fair Information Practices was intended to solve the problem of the imbalance of power between data subjects and data controllers[111] by concentrating control over personal data in the hands of the subjects and making the controllers accountable for personal data misuse.

Although this act had a big potential in the shaping of effective protection of personal data, its provisions did not have a direct effect, but rather were of a recommendatory nature and had to be implemented. However, private organizations were not interested in securing high standards

[109]Bergelson 2003, pg. 402
[110]Regan 1995, pg. 77
[111]Solove - Rotenberg - Schwartz 2006, pg. 278

of personal data protection, which could be burdensome and impede the normal operation of these organizations.[112] As a result, relations concerning personal data protection is left to self-regulation by private organizations, except for those organizations that handle special category of sensitive information.[113]

4.6 Propertisation as a tool to fill the gaps

The shortcomings of the tort system and existing laws, which were influenced by the impact of lobbying corporations, became the prerequisites for the emergence of discussions on expanding property rights to personal data. Such an approach was supposed to solve several concerns at once, to strengthen the position of the data subject by concentrating control over personal data in their hands, and also to create the incentives for controllers to take organizational, technological measures aimed at ensuring the security of personal data and their fair use.

This section will focus on the arguments of privacy proponents who advocate for vesting property right in personal data with the data subject. Aware of the indispensable role of personal data for personal freedom,[114] advocates of the proportization approach emphasize the need for default provisions that would outline reasonable limits for the freedom to exercise property right on personal data. These provisions would be designed to protect the interests of the data subjects as a weaker and less competent party.

Cohen[115] has consistently emphasized the importance of discussions about property rights to personal data, since this would, to a certain extent, contribute to educating people to value their personal data and to be more conscious and responsible in matters of its disposal. Some authors believe that control over the dissemination of personal data is possible through partial property rights to personal data.[116]

Vera Bergelson argues that the choice between the protection of personal data through tort or property rights is identical to the choice between the proprietary regime and the liability regime.[117] These regimes are not interchangeable, and each of them pursues different goals, one

[112]Regan 1995, pg. 78
[113]Regan 1995, pg. 7
[114]Solove 2001, pg. 1446
[115]Cohen 2000, pg. 1378-1379
[116]Murphy 1996, pg. 2384
[117]Bergelson 2003, pg. 379

of them is aimed at preventing violations, and the other at restoring justice after a violation has taken place. And liability rules cannot achieve the goal of concentrating control over personal data in the hands of the data subject.

Likewise, Murphy does not rely on proportional accounting of interests when resolving related disputes by the courts. The American legal order has very detailed regulation of the right to freedom of expression (The First Amendment). By opposing the interests of the press and freedom of expression against the vague notion of privacy, of course, the former will always prevail.[118]

Unlike the tort system, property rights allow taking into account the preferences of the data subject, what information he considers private, to whom, and for what purposes he wants to disclose his personal information. The courts try to operate with the objective concept of a reasonable expectation of privacy, which does not play a favorable role in defending the interests of the data subject.[119]

Moreover, self-regulation by companies of their activities and, in particular, activities related to the use of personal data, does not contribute in any way to the creation of an initiative to develop and invest in PETs (privacy enhancing technologies).[120]

And finally, the advantage of the approach of extending property rules to personal data will bypass the need for the adoption of special regulation by the legislative system, which is influenced by the interests of private corporations.

4.7 Criticism of the propertisation arguments

The purpose of the data propertization is empowering those to whom personal information pertains and giving them control over their information but the theory of personal data propertization within the US context is supposed to tackle the problem of power imbalance. Vesting property right in personal data is expected to encourage entities who collect and use data to create privacy- enhancing technologies. Nowadays companies freely make use of personal data, there is no incentive for them to take into account the interests of individuals.

[118]Murphy 1996, pg. 2388
[119]Murphy 1996, pg. 2393
[120]Cohen 2000, pg. 1391

The introduction of data propertiztion would force companies to change their strategy, focus on developing more appealing privacy terms, better technological solutions for consumers' data protection.

Property right over personal data can indeed serve as a tool for data subjects to exercise control over personal information. However, the discussion about the proportization approach in doctrine has always been accompanied by criticism. The main argument calling into question the effectiveness of this mechanism is dispute about the alienation of the right to personal data.

Some authors believe that the default rules restricting the right to alienate personal data are not in line with the concept of control. Therefore, data subjects should have the right to dispose of their personal data at their own discretion, including in cases of intent to monetize their personal information.[121]

While proponents of complete personal data commodification support the wide scope of the property right, privacy advocates emphasize the necessity for certain default rules and restrictions which would serve for non-market, namely, privacy protection purposes.[122]

Schwartz believes that it will be impossible to achieve privacy goals without fixing the default rules. He explains this by the fact that, firstly, information privacy is also a public good, and the market fails in adequately assessing this value, therefore, protection of this value is impossible without additional interference in the regulation.[123] Thus, Paul Schwartz proposed to introduce such a model of property right which would limit alienability of personal data and default rules that would block the further use or transfer of personal data without the consent of the data subject.[124] Such a property right model is aimed to take into account the social value of privacy and privacy interests of data subjects instead of the goal of facilitating the information market.[125]

If the data subject was granted the right to conclude agreements with controllers for the alienation of their personal data, he would not be able to defend his interests against huge powerful corporations due to insufficient expertise in personal data concerns. It will not be

[121]Kang 1998, pg. 1266
[122]Samuelson 2000, pg. 1187
[123]Schwartz 2004, pg. 2086-2088
[124]Schwartz 2004, pg. 2060
[125]Schwartz 2004, pg. 2100-2105

difficult for such companies to coerce the data subject to agree to their terms of transfer of personal data.

However, as it was pointed out by Jessica Litman, property right is intended to encourage the free and unhindered transfer of goods from one person to another. Therefore, the deprivation of the subjects of the property right to alienate their property seriously distorts this goal.[126]

As noted above, the judicial and legislative system in the US transparently recognizes the value of personal data. Notwithstanding, vesting property right in personal data there is a risk that the court takes into account only the economic value of property, while ignoring the fact that property right also encompasses the non-economic relationship between the subject and his property. Regarding personal information, one must recognize that information about an individual is an integral part of his or her personality and integrity. Recognizing the control of the data subject over his personal information, individuals are able to decide on the way the information about them is used, which is essential in any democratic society.[127] That concern is reflected in Pamela's rather straightforward statement that the idea of endowing individuals with a property right in their fundamental rights is morally unacceptable.[128]

4.8 Conclusion

The need for a new approach to protecting information privacy, and in particular the protection of personal data, arose against the background of the inefficiency of existing mechanisms and tools in the American legal system. The problems start with the lack of a unified concept of privacy, which creates uncertainty for both individuals, private enterprises, and law enforcement agencies.

The USA, being a country with a common legal system, does not have a unified and comprehensive legal act that would provide at least a framework for the regulation of information privacy across the country. The system for regulating personal data protection is extremely fragmented. The tort system also does not provide adequate protection of the right to privacy. Each of the available torts has a limited application that cannot serve as a universal instrument.

[126]Litman 2000, pg. 1295
[127]Newman 2008, pg. 343
[128]Samuelson 2000, pg. 1143

The introduction of property right over personal data is supposed to solve the problem of the lack of control of data subjects over personal data pertaining to them, as well as correcting the imbalance of power between controllers and data subjects. Nevertheless, many supporters of the theory of personal data proportization justify the need for default rules that would restrict the freedom of data subject to transfer ownership to the controller. Otherwise, it would be impossible to ensure and achieve the goals that follow the approach of personal data proprtization as an effective tool of protection.

In the context of the American legal system, the introduction of property rights (even with restrictions, some may call it quasi-property) will help to find a more fair balance in power distribution, this will help to avoid the procedure for adopting federal law, since this procedure is very undesirable due to the dependence of the legislating decisions and process on interests of lobbying companies.

Even though the approach of proportization of personal data has the potential to fill significant gaps in the American legal system, this theory is also subject to serious criticism. The problem is not that data subjects cannot exercise control over their personal data. The main problem of information privacy is that misuse of personal data is carried out in ignorance of the data subject. Businesses do not consider the need to comply with their own privacy conditions, which they so eloquently promise to fulfill. Therefore, the central issue that needs immediate resolution is the issue of the accountability of those actors who have access to personal information of users.

5 Chapter 5: The EU Data Protection Regulation

Over the years, with the rapid development of the information economy, a significant imbalance between data subject and controllers has been escalating. Data subjects submit more and more personal information, including a special category of sensitive data. Moreover, new technological tools have also appeared that make the process of classification, profiling, sorting, selection, collection, processing of personal data a easier and relatively cheaper.[129]

The threat of invasion of privacy is now presented not only from the public, state bodies but from private enterprises and the natural persons.[130] Access to personal information of almost any person in current digital era has become commonplace, a matter of a couple of clicks. The ability of some organizations to easily collect a ton of information about users poses a serious threat to the protection of privacy from intrusion by private parties. When searching for some information about someone, the search engine will most likely provide with other information that has not been even sought.

It is for these reasons that the interference of the law in the regulation of the personal data protection of data subjects is increasingly relevant and vital at present.

The European legal system differs from the American legal order in that it highly values the right of everyone to respect for private life, including right to personal data proetction which are enshrined in the Constitution of the Member States, and this right is also enshrined as a fundamental right in supranational legal acts[131].

5.1 Data protection as a dimension of privacy

In the legal literature, two dominant concepts of determining the place and meaning of the right to personal data protection can be distinguished. According to the concept that guides the American legal system and legislators, the right to personal data protection is one of several

[129]Rodota 2009, pg. 77

[130]Savin 2017, pg. 264

[131]The European Convention on Human Rights (ECHR), Article 8:

> *1.Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2.There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

tools that ensure the right of people to privacy. A different concept, which is applied in the EU legal order, gives the right to personal data protection the status of a fundamental right that exists independently along with the right to privacy.[132]

Nevertheless, the right to privacy and the right to personal data protection often overlap. Moreover, both international and national courts tend to interpret the concept of the right to privacy in a much wider manner that might even comprise the right to data protection. In different contexts, under different circumstances and time, the content of the right to privacy can be defined in different ways to meet the new challenges imposed by steady progress in society.[133]

In the broadest sense, the right to privacy is not so much about the right to keep private life secret, but rather about freedom. The right to privacy gives confidence that individuals are entitled to publicly express their beliefs and views without fear of negative consequences. The right to privacy enables individual to determine his own behavior, personality without interference and control by the state or other third parties.[134] Such blurred boundaries of the right to privacy cannot provide clear regulation for relationships related to the collection and processing of personal data.[135] In the European legal context, the right to privacy is alike freedom, it is difficult to determine the scope of such freedom since a strict and rigid definition of this right can lead to negative consequences. It seems impossible to foresee all potential misconduct that could infringe the right to privacy. This flexible approach to the definition of the right to privacy allows it to meet the needs of a continuously developing society. However, vague definition of the concept also creates legal uncertainty.[136]

Another important point is that the right to privacy obliges the state not to interfere with the freedom of private life of citizens. The right to the protection of personal data has a different essence. If the right to privacy implies a passive obligation not to invade a person's private life (in other words, this is a negative right), then the right to personal data protection guarantees a number of rights to the data subject and imposes active obligations of data controllers.[137]Thus,

[132]Hildebrandt 2015, pg. 186
[133]Hildebrandt 2015, pg. 188
[134]Rodota 2009, pg. 79
[135]Hildebrandt 2015, pg. 188
[136]Hildebrandt 2015, pg. 189
[137]Hildebrandt 2015, pg. 189-190

the right to personal data protection is a positive right and brings more certainty for both parties.[138]

5.2 Right to data protection as a fundamental right. Article 8 of the European Union Charter of Fundamental Rights

Despite the fact that the European courts are doing a successful job in interpreting the right to privacy quite broadly, the development of society constantly requires the solution of new problems that were not taken into account at the time of the adoption of a particular statute. However, since modern technology poses a serious threat to the integrity and independence of the individual, the new fundamental right to personal data protection was enshrined in CFR (Charter of Fundamental Rights of the European Union). The Charter for the first time delimited two fundamental rights, having reserved the right to privacy (Article 7) and the right to personal data protection (Article 8) in separate articles. If Article 7 has the same wording as in the Human Rights Convention, then the article on the right to the protection of personal data reads as follow:[139]

> *1.Everyone has the right to the protection of personal data concerning him or her.*
> *2.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 that has been collected concerning him or her, and the right to have it rectified.*
> *3.Compliance with these rules shall be subject to control by an independent authority.*

This provision is a framework provision for the further detailed regulation of the protection of personal data and enshrines the fundamental principles that should permeate all regulation related to personal data processing practices.

And as it was noted earlier, the right to privacy and the right to personal data protection is of a different nature. The right to privacy imposes a negative obligation on everyone not to take any action that may invade a person's privacy. At the same time, the right to the protection of

[138]Hildebrandt 2015, pg. 190
[139]Rodota 2009, pg. 79

personal data empowers data subjects and imposes positive obligations on other actors, in particular on controllers, who must take certain measures to ensure effective protection of personal data and interests of the data subject.[140]

As was fairly noted by Stefano Rodota, while recognizing the right to personal data protection as a fundamental right, legislators and law enforcement authorities should adopt additional safeguards aimed at protecting one's personality. The law should not perceive the data subject as the owner of personal information but should take care of protecting the person himself and his integrity and freedom.[141]

The first tool that was developed to solve the problem of personal data protection, entered into force in 1981. It was Convention on the protection of automatically processed personal data drafted by the Council of Europe. These provisions had to be ratified by the Member States, however, not all countries eventually adopted it in their national laws. Nevertheless, these provisions were the legal source of regulation of personal data processing processes in all EU countries.[142]

The rapid development of digital technology relentlessly set new challenges for the protection of personal data, at some point it was assumed that the existing protection tool had become outdated and ineffective for the task at hand. Given these circumstances, the development of a new protection tool began in 1991. In 1995 the Data Protection Directive entered into force drafted by the European Parliament and the Council.[143]

The Directive did not have a direct effect on the Member States, it had a recommendatory and guiding character. The Directive aimed was to ensure a high level of protection of personal data (it attempted to reunite the best traditions and solutions of regulating the protection of personal data of those countries that are distinguished by high data protection standards), as well as the Directive called on countries to harmonize the regulation[144] across the EU. That is, the Directive had a dual purpose, to ensure the efficient functioning of the market and the flow of data

[140]Rodota 2009, pg. 79-80
[141]Rodota 2009, pg. 81
[142]Savin, 2017, pg. 26
[143]Savin 2017, pg. 269
[144]Savin 2017, pg. 269

between countries, as well as to establish a high level of protection of personal data of data subjects in all Member States.[145]

Even though the former Directive to some point resolved the issue of fragmented regulation of matters related to the protection of personal data in the EU, it still failed to effectively regulate the processing of personal data of EU citizens outside the EU. So, if the personal data of EU citizens was processed in non-EU countries using equipment not located in the EU, then EU laws did not apply to the operations of processing personal data, even if this data concerns its own citizens.[146]

5.3 General data protection policy within the EU: the goals

The central objectives at that time of the already 20-year-old Data Protection Directive were to ensure the smooth functioning of the internal market and the free flow of data between the Member States, as well as the effective protection and establishment of a high level of personal data protection across all EU countries.[147] The subsequent regulation of personal data protection concerning collection and processing came into force in 2016 but started its application in 2018. The new General Data Protection Regulation aimed to strengthen the rights of data subjects and providing better harmonization.[148]

The new Regulation mainly borrowed key concepts, principles, and ideas from the previous document.[149] However, the essential and main distinguishing feature is that the Regulation can be applied by national authorities directly, and all private patties also bounded by its provisions, it does not need to be implemented in national laws.

Such direct application achieves the goal of ensuring the smooth functioning of the market and protecting personal data, making sure that from the moment it is applied, harmonization will be ensured in establishing a high level of protection of the right to personal data.

Another important advantage of the Regulation and another step towards ensuring effective protection of personal data of data subjects is the change in the provision on the territorial scope

[145]Savin 2017, pg. 270
[146]Savin 2017, pg. 272
[147]Savin 2017, pg. 275
[148]Savin 2017, pg. 282
[149]Savin 2017, pg. 283

of the Regulation which was the significant flaw of the Directive 1995. Thus, according to Article 3, the Regulation is applicable when controllers or processors are established in the EU, even if the processing takes place outside the Union, and also in cases when the personal information of EU citizens is subject to processing for marketing purposes or behavioral monitoring.[150]

It can be observed that the objectives of the previous and current regulation are mostly the same. However, the new General Data Protection Regulation takes serious steps in empowering the data subject and retaining the control over their data. This is evidenced by a number of innovations, namely new rights of data subjects and rules of controllers' and processors accountability, that are enshrined in the provisions of the concerned regulation.

The consent mechanism which was already used before the Regulation has undergone fewer changes. The new Regulation solidified the accountability of the controller[151], therefore it is the controller's responsibility to obtain the informed consent from the data subject. The burden of proof of validity of the consent accordingly lies with the controller.

One of the innovations presented in the new regulation is the child's consent[152] to the offered informational social services. Thus, the processing of personal data will be legal if the child has reached the age of 16 (national laws may reduce this age to 13, but not younger). If the child is younger than the specified age, the controller must ensure that consent to the processing of personal data can be obtained from the person holding parental rights for the child.

The category of sensitive information is not a new discovery of the Regulation, however, this category has been expanded, and now includes, along with others, genetic and biometric data, as well as information regarding the sexual orientation of the data subject.[153]

The principle of purpose-binding data processing has been further regulated in more details, namely, the controller's obligation to obtain consent separately for each new purpose of data processing. If, however, the controller processes the personal data of the data subject for a purpose other than the original purpose, then the burden of proving the compatibility of the

[150]Savin, 2017, pg. 283
[151]Article 24 GDPR
[152]Article 8 GDPR
[153]Article 9 GDPR

processing with initial purpose lies with the controller, who must take into account a number of circumstances listed in Article 6 (4).

In pursuance of the Regulation's aim to strengthen the rights of data subjects, the Regulation has created a number of new rights. One of these is the right to be forgotten, enshrined in Article 17 with a succession of the court's position in the Google Spain[154] case regarding the role and responsibility of search engines.[155]To exercise the right to erasure, the data subject must base his decision on one of the following six grounds listed in the Article 17: personal data is no longer necessary for the collection and processing; the exercise of the right to withdraw consent to data processing when such processing has been carried out based on consent; the exercise of the right to object when there is no overriding public interest or interest of the controller, and in any case if the processing was carried out for marketing purposes; the data processing has been unlawfully processed; the controller's obligation to erase personal data established by the Member Country; in case of collection and processing of personal data of children under the age specified in Article 8 (1).

Another new right granted to data subjects is the right to restrict processing.[156] This right is valuable because it limits the possibilities for data processing, during the period of checking the grounds for the data subject's claim when he asserts the inaccuracy of personal data, as well as in the event of objecting the processing of personal data. Two other conditions for the exercise of the right to restriction of processing, when, in the event of the unlawfulness of data processing, the data subject requires the restriction of processing instead of erasing the data. The right is also relevant where personal data are no longer needed for the purposes of their collection and processing, but they are necessary for the data subject for legal purposes.

A completely new right of data subjects is the right enshrined in Article 20 under the title 'Right to data portability' which is applicable where the processing of data has been carried out based on the consent of the data subject and by automatic means. According to this provision, the data subject has the right to receive or demand from the controller the unhindered transfer of his personal data to another controller *'in a structured, commonly used and machine-readable*

[154]CJEU C-131/12 Google Spain vs Mario Costeja González, para 94-96 (search engines were qualified as controllers of personal data)
[155]Savin 2017, pg. 286-287
[156]Article 18 GDPR

format'.[157] The right to data portability is also expected to contribute to increasing the interoperability in the Union.[158]

In addition to creating new rights aimed at strengthening the position and control of the data subjects, the Regulation also enshrines additional guarantees for the protection of data subjects against profiling and decisions made exclusively on automatic processing.[159] The Regulation gives the definition of the mentions types of data processing.

And finally, in Article 25 a new concept is enshrined, which should permeate all the activities of controllers. According to the Article, the data controllers and processors must ensure data protection by design and by default. The protection of personal data on design requires the controllers and processors to take appropriate technical and organizational measures to ensure adequate protection of personal data. These measures should be taken in compliance with the substantial principles of the Regulation. And the default protection concept means that the controller collects and processes the minimum amount of data that is fundamentally necessary for the purpose of such processing (principle of data minimization).[160]

5.4 Principles of the General Data Protection Regulation

However, the primary source of principles for the regulation of issues related to the lawful collection and processing of data are enshrined in the CFR, in the article devoted to the fundamental right to the protection of personal data in Article 8. Since the adoption of this article, the European legal order has followed a fundamental approach to the right to the protection of personal data. Denoting the same principles, the new regulation also pays extra attention to the matters of accountability and security breach notification.[161]

These principles are reflected in each provision of the Regulation, and Article contains principles related to the processing of personal data in the form of a list of seven principles that must be applied and followed in any personal data use practice by any controller and processor.

[157]Article 20(1) GDPR
[158]Savin 2017, pg. 287
[159]Article 22 GDPR
[160]Savin 2017, pg. 288
[161]Hildebrandt 2015, pg. 200

5.4.1 Lawfulness, fairness, and transparency

The first in the list of principles for processing personal data is the principle of legal, transparent, and fair data processing. This principle is the most general and is reflected in all other principles.[162]Each of the three components of this principle has a distinct meaning.[163]

For the processing to be lawful, it must be based on one of the grounds enshrined in Article 6 (1) of the Regulation. Also, when processing a special category of personal information, the controller must be guided by Article 9, which establishes a special regulation justified by the vulnerability of sensitive information. Nevertheless, the Regulation empowers the Member States with some degree of flexibility to develop more detailed regulation on the grounds for the processing, in particular when the processing is carried out in compliance with the controller's legal obligations (Article 6 (1c)), and when the processing is necessary for the public interest (Article 6 (1e)). Thus, the lawfulness of the processing is determined by compliance with the requirements and conditions established by Union law and the national law of the Member States.

For the processing of data to be considered fair and transparent, the controller is responsible to properly inform the data subject about what information is necessary for processing, the purpose of processing, the rights of the data subject, information about the controller, about the recipients of personal data, the period of storage, about the source of information, when the data is not provided by the data subject, about the additional safeguards when transferring data to a third country. The data subject must be aware of the profiling and automated decision-making, the logic behind it, and the consequences such processing might entail.[164] The information related to the data processing should be provided by thecontroller in an accessible and easy to understand form.

5.4.2 Purpose limitations

The principle of purpose limitation establishes a requirement that any personal information must be *'collected for specified, explicit and legitimate purposes and not further processed in*

[162]Bygrave 2002, pg.58
[163]Purtova 2011, pg. 151-152
[164]Recital 39 and 60, Article 15

a manner that is incompatible with those purposes'[165]. The principle significantly limits the freedom of controllers, requiring them to clearly define what data and for what purposes the collection and processing of personal data is necessary and obliges them to unambiguously inform the subject of personal data.[166] For any new purpose for data collection and processing, the controller must obtain the new consent of the personal data subject separate from the previously obtained consent or comply with other grounds for processing.[167] The principle prevents abuse by the controller, where the controller defines a highly fluid purpose in an attempt to justify further use of the data by that vague purpose.

If the controller has legitimate grounds for storing personal data after the purpose of their collection and the purpose of processing has been achieved, the controller has no right in the future to process data for purposes incompatible with the original purposes.[168] And as was stated earlier, the burden of proof of compatibility lies with the controller.

Thus, from the principle, three obvious requirements for the controller can be derived. Firstly, the controller is obliged to properly inform the data subject about the category of information and the purposes of their processing. Second, each new processing purpose requires a separate legal basis. And finally, the goal set by the controller must be legitimate.[169]

5.4.3 Data minimization

In addition to the fact that the legislator makes the controllers and processors of personal data responsible for the data collection and processing following a strictly formulated purpose, but also prohibits the collection of that information that is not necessary for the fulfillment of the purpose determined by the controller.[170] Thus, it is possible to trace a logical correlation with the principle of purpose limitation.[171]

Under the data minimization principle, the controller is obliged to collect the minimum necessary information that will be sufficient to fulfill the goal of processing to avoid wasteful

[165]Article 5 (1)(b)
[166]Hoeren – Kolany-Raiser – Yankova - Hecheltjen 2013, pg. 66
[167]Hildebrandt 2015, pg. 204
[168]Hildebrandt 2015, pg. 204, See also Hoeren – Kolany-Raiser – Yankova - Hecheltjen 2013, pg. 66
[169]Kuner 2007, pg. 100
[170]Hoeren – Kolany-Raiser – Yankova - Hecheltjen 2013, pg. 68
[171]Bygrave 2002, pg. 59

data processing.[172] The collection of an excessive amount of personal data that is objectively not needed for the claimed purpose is not in line with the principle of data minimization.

5.4.4 Accuracy

The principle of accuracy sets the requirement that personal data be *'accurate and, where necessary, kept up to date'*[173]. This principle gives rise to the rights of the data subject to request that inaccurate information to be erased[174] or rectified[175]. The principle itself, in its wording, establishes the controller's obligations, correlating with the rights of the data subject, to take active measures to timely remove inaccurate information or correct it.

This principle is intended to ensure the quality of the array of personal information that is collected by numerous controllers for various purposes.

5.4.5 Storage limitation

The storage limitation principle obliges the controller not to store personal data of subjects when this information is no longer needed. That is, the personal data provided by the data subject or other authorized person has a limited storage period, there is no concept of indefinite storage of data in the databases of the controllers. Although the provisions of the Regulation provide for some exceptions when information can be stored for a longer period for public, scientific or historical research purposes, and statistical purposes, and where it is possible, such information should be pseudonymized[176]. If the controller has grounds for longer storage of personal data, then he must ensure that he can provide sufficient technical and organizational measures for safe storage.

For the purposes mentioned, Article 89 (2) allows for some derogations from other provisions of the Regulation. The data subject cannot exercise his rights to access his data (Article 15), demand rectification of personal data (Article 16), the right to restrict processing (Article 18), and the right to object (Article 21), as otherwise would significantly interfere fulfilling the objectives exhaustively listed in Article 89 (1).

[172]Kuner 2007, pg. 74
[173]Article 5 (1)(d) GDPR
[174]Article 17 GDPR
[175]Article 16 GDPR
[176]Article 89 GDPR

5.4.6 Data integrity and confidentiality

The principle of integrity and confidentiality imposes an obligation on the controller[177] to take sufficient and effective measures to ensure the security of personal data. The principle is aimed at preventing cases of unauthorized data processing, its loss, or other damage to personal data. To effectively implement this principle, the Regulation introduces such a concept as protection by default and by design[178], which states that the controller is obliged to take the necessary technical and organizational measures to secure personal data. Appropriate measures should not be applied after the collection of data, but be already incorporated prior to any operations concerning personal data.[179] This position of the Union is consistent, the discussion of the so-called PETs (Privacy Enhancing Technologies)[180] that has been going on for a long time.

In cases where the processing of personal data is carried out based on a contract by another party - a processor - the controller must take precautions and make sure that the processor can ensure the proper level of security of personal data, and that the processor takes the necessary technical and organizational measures to comply with the principle of integrity and confidentiality personal data.[181] If the processor is unreliable, the controller is also responsible for the processor's actions.

5.4.7 Accountability

Generally speaking, the principle of accountability boils down to the fact that the responsibility for complying with the provisions of the protection of personal data almost always rests with the controller.[182] Moreover, every right of the data subject, enshrined in the Regulation, is supported by a correlating obligation of the controller. The right to erasure, rectification, or processing restriction is backed-up by the controller's notification obligation.[183]

Competent regulation of the protection of personal data imposes the obligation to determine the purpose and means of collecting and processing personal data on the data collectors. That is

[177]For example, Article 24 GDPR
[178]Article 25 GDPR
[179]Robinson – Graux - Botterman - Lorenzo 2009, pg. 9
[180]Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), 2007
[181]Article 28 GDPR
[182]Purtova 2011, pg. 158
[183]Article 19 GDPR

why the legislator makes the controller accountable for compliance with the necessary measures to ensure a high level of protection of personal data and compliance with data protection principles.[184] In such circumstances, when the personal data collector himself has determined the scope of the purposes of data processing, he is best aware of the scope of his freedom of action and responsibility for violation of the established limits of data processing.[185]

For instance, since the controller himself decides on the means of personal data processing, he bears the onus to ensure that the processor applies the necessary technical and organizational measures to ensure the security of personal data.

Another example, the Regulation does not relieve the controller from the responsibility to comply with the principles of personal data protection regulation, even if the data subject has provided his informed, free, and unambiguous consent to the collection and processing of his data.[186] That is, even if the subject of personal data gives his consent to the collection of an excessive amount of his personal data for the purpose determined by the controller, the controller is still accountable for the obligation to collect and process only the amount of personal data that is necessary to achieve the purpose of data collection. The collection of excessive personal information is considered arbitrary and contrary to the principle of data minimization, even if such collection was authorized by the data subject himself.

5.5 Shortcomings of available implementation mechanisms

After getting acquainted with the history of personal data protection in the EU, and describing, and explaining the principles and key provisions of the General Data Protection Regulation, it is possible at that point to draw, among other things, some conclusions about the shortcomings of the Regulation. The central question here is whether the Regulation has achieved the goals it was intended to achieve and how effective its provisions are in ensuring the fundamental right to the protection of personal data.

The GDPR began its implementation only in 2018, that is, relatively very recently.

[184]Hoeren - Kolany-Raiser – Yankova – Hecheltjen 2013, pg. 65
[185]Hildebrandt 2015, pg. 205
[186]Article 29 Working Party Guidelines on consent under Regulation 2016/679, 28 November 2017, pg. 3

Nevertheless, the Commission has already managed to issue a report[187] on the experience of applying the Regulation over the past two years.

The Commission itself notes a number of advantages of the GDPR, in particular, strengthening the position of the data subject and vesting with new right with the data subjects, stronger safeguards especially when transferring data to non-EU countries, greater transparency of operations with personal data, increased accountability of those who handle data, significant steps towards further harmonization and thereby ensuring the successful functioning of the internal market.[188]

The deficiencies noted by the Commission mainly relate to problems of the enforcement, as well as harmonization and cooperation of data protection authorities.[189]

Achieving harmonized regulation across 28 countries is an extremely difficult task. Usually, the legal framework enshrines broad concepts and principles and provides national legislators with a certain degree of discretion in the implementation of the supranational framework regulation.[190] The Data Protection Directive was advisory in nature, but the GDPR has a direct effect in the Member States. However, the task of full harmonization has not been achieved at the moment, and significant discrepancies in national laws can be observed.

The problem with the lack of cooperation between the authorities of the Member States is essential in achieving the objectives of the smooth functioning of the single market. The Commission denotes that additional initiatives are needed to improve the procedure for resolving cross-border complaints.[191]

However, the problem of harmonization does not end with a lack of cooperation between authorities, but also with the fragmentation of national regulation of the Member States. Almost all Member States have developed a national law regulating the protection of personal data. Although the Regulation itself has given some margin of appreciation to the Member States, such fragmentation hinders the smooth operation of the single market. As an example, the Commission cites the situation with the age of the child, when the child has the right to consent

[187]COM(2020) 264 final Brussels, 2020
[188]COM(2020) 264 final Brussels, 2020, pg. 1- 2
[189]COM(2020) 264 final Brussels, 2020, pg. 5
[190]Bygrave 2002, pg. 35
[191]COM(2020) 264 final Brussels, 2020, pg. 5

to the processing of his personal data. Some countries have opted for a minimum age of 13, creating legal uncertainty that makes it difficult for data subjects and controllers to understand and comply with the rules. Also, although the logic of the GDPR is to establish a single standard for the protection of personal data, with the empowerment of the Member States, at their own discretion, to enshrine in their legislation higher protection of personal data, the Commission recognizes that additional requirements can put unduly burden on the companies.[192]

Different approaches were taken by the Member States also regarding the regulation of derogations from a special regime of sensitive data processing for health and research purposes.[193]

Another disadvantage of the Regulation is the silence about the achievement of a balance between two values, namely the right to freedom of expression and the right to personal data protection. Thus, national legislators have taken different approaches to resolving this matter. In some national legal systems, the right to personal data protection prevails, while in others the prerogative is given to the right to freedom of expression.[194]

Further, although the Commission notes a positive trend in the awareness of data subjects about existing data protection laws and their rights regarding personal data pertaining to them, data subjects do not fully use all available mechanisms of strengthening control that are provided to them by the Regulation, for instance, right to data portability is barely exercised by the data subjects.[195]

Positive for data subjects on the one hand, and unduly burdensome on the other, is the principle of accountability and related provisions. As mentioned earlier in this chapter, the subject of almost all obligations implemented in the Regulation is the controller of personal data. It should be noted that this approach of the legislator has become burdensome for small and medium-sized enterprises. Although the Commission believes that healthy competition is maintained in this way, various guides on less risky activities have been issued specifically to help SMEs, such as different templates, consultation lines, and the like.[196]

[192]COM(2020) 264 final Brussels, 2020, pg. 7
[193]COM(2020) 264 final Brussels, 2020, pg. 7- 8
[194]COM(2020) 264 final Brussels, 2020, pg. 7
[195]COM(2020) 264 final Brussels, 2020, pg. 9
[196]COM(2020) 264 final Brussels, 2020, pg. 9

The mechanism of free and informed consent is still a controversial tool for strengthening the control of data subjects over personal data. The doubts expressed by jurists ten years ago are still relevant today. The concerns mainly boil down to the use by controllers of complex and incomprehensible wording in a request for consent, which contains fundamentally important information regarding the processing of personal data. As a result, data subjects do not even make an effort to get to know what data, for what purposes, how and by which means it will be processed.[197]

Also, there are ubiquitous cases of data subjects' dependence on controllers, for example in labor relations. However, employers actively use this basis for data processing, leaving no choice for data subjects. Such consent is obtained with coercion; therefore, it is contrary to the provisions of the Regulation. And it is in such situations that it is very unlikely that the data subject will exercise his rights to request the erasure of data or seek legal assistance from the relevant authorities due to possible adverse consequences in the workplace.

5.6 Conclusion

The main document regulating the processing of personal data in the EU is General Data Protection Regulation, which started its application in 2018. The new Regulation inherited the objectives of its predecessor, the Directive 1995, namely, to empower the position of data subjects and achieve harmonized the regulation of lawful data processing.

The 1995 Directive had many shortcomings, chief among them was the recommendatory nature of the document, which was subject to ratification by the Member States. Also, the previous regulation enshrined very weak rules of accountability of controllers considering complexity of data processing operations, the principle of purpose limitation was not detailed enough. The shortcomings of the previous regulation could not ensure adequate protection of the interests of data subjects. Data subjects were prevented from exercising meaningful control over personal data.

The new Regulation also has its drawbacks. There is still a need to take additional measures to achieve harmonization, which is of particular importance for the enforcement of the data processing rules and cooperation of the data protection authorities.

[197]Robinson 2009, pg. 29-30

Moreover, despite the valuable tools for exercising control by data subjects, these tools are not yet used to their full extent, therefore it is of great importance to inform and educate data subjects about their rights concerning personal data pertaining to them.

The new Regulation transparently follows a fundamental approach to the protection of personal data, ensuring that the position of data subjects is strengthened with innovative rights that were not enshrined in previous Union acts. The principles contained in the Regulation are of great practical importance, since they limit the freedom of controllers in the processing of personal data and their storage, restricting their freedom by the principle of data minimization and the purpose limitation. Also, a lot of attention in the Regulation is paid to the responsibility and accountability rules of controllers and processors.

The GDPR is a promising tool in ensuring a high level of protection of personal data, as well as a fair balance of interests of data subjects and controllers by balancing power between them.

6 Chapter 6: The possibility of vesting property right in personal data in the EU legal order

The provisions of the GDPR do not directly impede the implementation of proprietary rights in personal data, but also it does not contain any provisions that would explicitly indicate that this approach is followed or accepted. Moreover, the GDPR does not dispose of proprietary terminology, the data subject is not denoted as the owner, and the personal data is not identified as property.[198]

Some authors claim that the European legislator has enshrined control mechanisms in its law that are akin to the nature of property rights.[199] However, the fact that the Regulation sets as one of its goals the empowerment of the position of the data subject, and in particular, the strengthening of control over personal data, creates the basis for the assumption that the regulation creates a property-like protection regime for personal data.

Nevertheless, when discussing the possibility of the existence of property rights to personal data in the European legal order, special attention should be paid to the Union's approach to defining the right to protection of personal data as a special category of fundamental rights that need special protection and enforcement.

6.1 Is there compliance between property approach and human-centered approach to personal data protection?

From a first glance, the answer to the question posed is quite obvious, the fundamental approach and the property approach to solving the problem of personal data protection are opposite to each other. And the proprietary approach is pursuing economic goals of the right holder, which is true for American legal order, and the fundamental approach, which in deployed in Europe, puts respect and ensuring fundamental rights and freedoms of individual at the head of discussion.

However, it is not so evident. The right to the protection of personal data is recognized by the Union as a fundamental right. And the property right presupposes the freedom of the

[198] Jacob M. Victor 2013-2014, pg. 522
[199] See Purtova 2011

right holder in the disposal and use of his property. Therefore, a logical question immediately arises. If a property right over personal data to be recognized, then does this mean that a person will be able to waive his fundamental right, exercising his right to freedom to dispose of his property.

Such a possibility exists, and the law enforcement authorities represented by the European Court of Human Rights repeatedly supported this in its decisions[200]. An individual has the right to waive his fundamental right on the condition that his will has been expressed in an explicit and unambiguous manner.

Moreover, as some authors assert, both fundamental rights and property rights are aimed at strengthening the position of and empowering the right holder.[201] And both approaches indicate the special bond between the subject and object of the right. And since the status of a fundamental right does not exclude the possibility of waiver of concerned right, and the goal of both approaches is similar, the European legal order does not exclude or prevent the possibility of vesting property right in personal data as a more powerful mechanism to ensure control of the data subject over personal information pertaining to him.

Granting property right in personal data to data subject will allow him to bargain in his own interests, ensuring the autonomy of the individual.[202] The autonomy of the individual also implies the freedom to conclude the contract and negotiate the terms and conditions of an agreement. The freedom to conclude a contract also provides an opportunity for the parties to achieve the desired balance of interests, thus securing mutual rights and obligations in the agreement. Property right also ensures an undeniable and most complete control over the object of the right.

Moreover, recognizing that objectively the data subject in a given relationship will always be a weak party, freedom of contract does not mean the possibility of concluding a contract that would harm the interests and rights of the weaker party. General principles of private law always defend the interests of the weaker side.[203]

[200]De Wilde, Ooms, Verspy/Belgium ECHR 18 June 1971; Deweer/Belgium ECHR 27 February 1980
[201]Corien Prins 2006, pg. 241-242
[202]Corien Prins 2006, pg. 241
[203]Corien Prins 2006, pg. 243-244

6.2 The propertisation of personal data within the boundaries of General Data Protection Regulation

The main argument of the followers of the proportization approach is the already existing proprietary control of data subjects over personal data, which manifests itself through the mechanism of informed and specific consent to the collection and processing of personal data. As proponents of property regime assert it is the requirement of consent that establishes the unambiguous and strong control of the data subject over his personal data, which serves as a prerequisite for the discussions of the possibility of the property right over personal data in the EU legal system.[204]

Also, according to the GDPR, one of the requirements for lawful data processing based on consent is the explicitly of the given consent. That is, consent has to be expressed not by silence, but through affirmative action of data subject. Moreover, the controller is also obliged to inform the data subject's right to withdraw his consent to data processing at any time without giving reasons and without negative consequences after such revocation. That said, revoking consent should be as easy as giving it.[205]

Even when there are other legal grounds for the processing of personal data, the controller has the obligation to provide data subject with all relevant information concerning operations with his personal data,[206] and, most importantly, about the rights of the data subject to demand rectification, erasure of personal data, restrictions of its processing.[207] These provisions are aimed at maintaining data subjects' control over information pertaining to him.

Thus, even if the processing of data is carried out on grounds other than the consent of the data subject, the degree of control of the data subject over his personal data still remains. If the data processing is based on other grounds, the data subject is still not deprived of his right to question lawfulness of such processing,[208] through his right to object.[209]

Another argument in favor of the possible proportization of personal data within the framework of the GDPR is the fact that any restrictions on personal data, for example, the purpose

[204]Purtova 2011, pg. 193
[205]Article 7(3) GDPR
[206]Bygrave 2002, pg. 64-65
[207]Article 14 GDPR
[208]Bygrave 2002, pg. 65
[209]Article 21 GDPR

limitation, the requirement of the data subject to rectify or erase personal information, follow the asset,[210] namely personal data.[211] In other words, if the data subject has requested the erasure of personal information, then not only the initial controller to whom the request was addressed is obliged to comply with this requirement, but also all other data controllers and processors who has access to that data,[212] even if the data subject himself was not in any legal relationship with these third parties.[213] The restrictions put by the data subject has a binding effect on any third parties since the interest of the data subject is embedded in the data itself.[214]

Such restrictions also accompany personal data in time, that is, personal data submitted for processing for one purpose cannot be freely processed for other purposes in the future. That binding effect of restrictions is similar to the erga omnes principle of property right that puts the obligations on everyone but not only on the parties of the relevant contract.

The property right to personal data does not necessarily have to be employed in the classical sense. Schwartz states that certain limits are necessary in order to ensure the interests of the data subject. However, he also believes that personal data protection can benefit from proportization. One of these benefits is an affirmative action on information processing. In this case, the data subject will retain the right to exit at any time (employing the right to withdraw the consent), which will prevent the duration of agreements concluded on terms that are unfavorable for the data subject.[215]

Secondly, such a framework will ensure that control remains in the hands of the data subject, who will be able to decide the fate of his data in the future. That is, the data subject can prohibit the further transfer or use of his personal information by third parties or for different purposes.[216]

Another argument testifying to the property regime is the goal pursued by the legislator in the protection of personal data. Namely, the lawmaker seeks to prevent unwanted deprivation of personal data by the other party, which is also the purpose of establishing property rights. Just as the GDPR provides for the possibility of data processing with the consent of the data subject,

[210]Hansmann - Kraakman 2002, pg. S378-S379
[211]Schwartz 2004, pg. 2097
[212]Article 17(2) GDPR
[213]Jacob M. Victor 2013-2014, pg. 519
[214]Schwartz 2004, pg. 2098
[215]Schwartz 2004, pg. 2100-2107
[216]Schwartz 2004, pg. 2095-2100

the property regime implies the use of the personal data is possible only with the consent of the owner.[217]

And finally, the GDPR protects the data subject as the weak party creating additional safeguards to ensure the interests of data subjects. Moreover, it provides the data subject with the similar legal remedies in case of violation of his right to personal data protection from unlawful processing as the property regime for owners whose property rights have been violated.[218]

Thus, the data subject, through the request for the erasure[219] of personal data, can restore the position that was before the alleged violation. Also, the data subject can apply directly to the court or the supervisory authority for a court order requiring the controller to take certain actions, for example, changing, deleting personal data. And, of course, substantially high administrative fines,[220] penalties[221] or compensations [222]can be imposed on the violator.

6.3 What property regime has to offer?

The proponents of the property approach are confident that in order to achieve stronger protection of informational privacy, it is necessary to replace the used protection mechanisms with a more powerful instrument of the property regime.[223] Since the lawmakers deployed the approach of privacy as control, property right seem to be the most reliable way to concentrate control in the hands of the data subject, that is, in the hands of the property owner.[224]

The logic is similar to that of the protection of interests of a copyright holder in controlling and limiting the distribution and use of their work. This control is exercised by copyright holders through the property rights to their creation. The same scheme should be applied to data subjects wishing to control disclosure and use of their personal information without transferring the property right itself.[225]

[217]Janger, Privacy Property 2003, pg. 914
[218]Jacob M. Victor 2013-2014, pg. 526-527
[219]Article 79 GDPR
[220]Article 83 GDPR
[221]Article 84 GDPR
[222]Article 82 GDPR
[223]Corien Prins 2006, pg. 231 (citing Sholtz, The Economics of Personal Information Exhange, 2000)
[224]Bergelson 2003, pg. 383
[225]Corien Prins 2006, pg. 233 (citing Zittrain footnote 45)

Since the privacy advocates of the propertization approach talk about limited alienability, it is proposed to provide the possibility of concluding licensing agreements between the data subject and the controller, which would contain all the necessary information, allowing the data subject to make an informed decision. If the data subject does not agree to the terms of processing or other use of the data pertaining to him, then the processing of such data must be anonymous or pseudonymous.[226]

Moreover, the vesting property rights with personal data will not mean the possibility of complete alienation of rights to personal data. In order to tackle the problem of asymmetry of power, as well as to ensure the interests of the data subject, such rights as the right to erasure, to rectification of erroneous information, the right to access information, the right to restrict processing, the right to withdraw the consent must be inalienable by default.[227] That is, supporters of this approach are suggesting to introduce a new limited property right over personal data.[228]

In cases where there is an obvious imbalance of power, the rules of private law restrict the freedom of the powerful party and assigns additional obligations to the more competent party, (for instance, the obligation to provide full information).[229] So the property regime also has the appropriate instruments to protect the weaker party to the agreement.

Thus, the data subject will have undeniable control over personal data, and also the data subject will be given the freedom to conclude a contract. Through licensing agreements, the data subject will not transfer the property right in his data, but only a limited right to use it. The parties will be able to agree on the (im)possibility of the subsequent transfer of data to a third party, having discussed the benefits accorded to the data subject as well. And in the case where the controller does not comply with his contractual obligations, then the data subject has the right to revoke his license (just as according to the GDPR, the data subject has the inalienable right to withdraw the consent). In this way, it will be possible to achieve a greater awareness of the data subject about the terms and conditions to which he gives his consent since it would require his active participation in drawing the provisions of the agreement.[230]

---

[226] Ritter - Mayer 2017-2018, pg. 229
[227]Bergelson 2003, pg. 444
[228]Lund,2011, pg. 10
[229]Corien Prins 2006, pg. 244
[230]Basho 2000, pg. 1525

According to proponents of proportization, the property regime will establish a default rule, consent will become the priority ground for personal data processing, which will further strengthen the control of data subjects over personal information. The interests of the data subject in such circumstances will always prevail over the interests of the controller.[231] Also, the vesting property right in personal data will encourage controllers and processors to apply measures and technologies that secure stronger protection of personal data. That will also contribute to creating greater incentives for businesses to respect and regard data subjects' interests.[232]

One of the main benefits of a proportization approach is the erga omnes effect, which will address the issue of responsibility and accountability of all parties in personal data processing in a uniform and universal way. Given the intricate data transmission chain, the widespread use of outsource services by controllers, the principle of erga omnes will ease the process of protecting data subjects' right in case of violation. The property regime will also create a negative obligation for all third parties to refrain from committing actions that violate the right of the data subject.[233]

Hence, the categorization of the parties involved in the processing of personal data will not make any difference. The data subject will not have to figure out who got access to his data, who provided his personal data, he will be able to lodge a complaint against any actor who is involved in wrongful operations using his personal data.[234]

Some authors also pay great attention to the advantages of using proprietary legal remedies.[235] The proprietary data protection regime also has advantages when it comes to available legal remedies for the subject whose rights have been violated. Contractual rights or tort rights are protected by compensation for the damage caused. While property rights are enforced by court injunctions.[236]

Under the property regime, the controller who has violated the data subject's right will not be able to get off with the payment of a fine. An unfair controller can fall under criminal penalties,

[231]Purtova 2011, pg. 239
[232]Basho 2000, pg. 1526
[233]Akkermans 2008, pg. 65
[234]Purtova 2011, pg. 242
[235]Bergelson 2003, pg. 417
[236]Ritter 2017-2018, pg. 249

a judicial order, and incomparably high fines. And in general, the property regime will not allow the controller to process personal data without authorization of the data subject, without any exceptions.[237]

It is also assumed that with the assignment of property right over personal data to data subjects, entities will bear the cost of collecting and processing data, since at the moment the conditions are such that the collection and implementation of data is carried out by them freely, and only companies benefit from the use of personal data.[238]

Moreover, the recognition of property right of data subjects will dot the issue of who owns the data, unambiguously asserting the rights to the data subjects, and not to the company that collects and processes personal information.[239]

6.4 Conclusion

The European legal system following the human-centered approach does not necessarily deny the possibility of using the property regime to ensure stronger protection of personal data. Both approaches pursue the same goal, strengthening the position of the data subject by exercising control over personal data pertaining to him. Both approaches aim at resolving power imbalances between the controller and the data subject, as well as providing stricter rules of accountability and responsibility for those handling personal data.

As well as the European approach, the property right approach uses the tool of unambiguous and informed consent to the data processing as a control mechanism for data subjects. And the right to information, the right to request rectification or erasure ensure control over the data in cases when the data processing was carried out on other grounds.

According to the GDPR, all restrictions in relation to the purpose of processing personal data, or the requirement of the data subject to limit the processing, change or erase personal data follow the personal data when they are transferred to other controllers or processors. That is, the restrictions and requirements of the data subject have a binding effect not only for the original controller who was the party of the contract but also for everyone else who was not

[237]Janger 2003, pg. 914
[238]Corien Prins1996, pg. 104
[239]Litman 2000, pg. 1290

directly involved into the original collection and processing of data. The principle of erga omnes of property rights resolves the issue of accountability and responsibility of all third parties in a very clear manner.

Also, the data subject, having the property right to personal data, will be able to actively negotiate on the terms and conditions of use of his data that would be more favorable for data subject, which is supposedly the best way to provide an informed decision on the processing of personal data. And the rules of private law can provide protection for the weaker party, imposing additional obligations on the more competent party.

The proponents of the property regime approach are convinced that in order to ensure the strong position of the data subject, it is necessary to use the mechanism that presupposes the most complete control over the object, that is, property right.

7 Chapter 7: Is there a real match with European data protection system?

Undoubtedly, the property regime for the protection of personal data has several advantages. Among the main ones, the most complete control of the data subject over personal data can be emphasized. The property regime allows the owner to exercise his right against everyone, which already implies a strong position of data subject.

Nevertheless, before deciding on the need for a new regime and approach for personal data protection, it is necessary to weigh the risks and threats that property regime on personal data may entail. It is also necessary to assess the existing and applied protection mechanism to understand if the system needs to apply a new regulation approach to the concerned relations. Even though the previous regulation did not provide an adequate level of personal data protection given the constantly emerging challenges caused by the technological breakthrough of society, the GDPR took into account the mistakes of the past and made certain steps to achieve the goals of empowering data subjects and retaining their control over personal data.

7.1 Right to self-determination & right to data protection

For the first time, the concept of the right to self-determination was given by the German Constitutional Court in 1983 in its decision rendered based on Article 1 (the right to dignity) and Article 2 (personality right) of the Constitution, which stated that the right to self-determination is the right of everyone to determine himself to whom, when, and to what extent he wants to disclose information about himself,[240] right of exercising control over personal information.

If an individual is deprived of the right to exercise control over personal information pertaining to him, then such a circumstance will have a detrimental effect on self-development, preventing the individual from building his behavior, his views, and beliefs without fear of constant observation and judgment. In its turn, that will make the functioning of a democratic society

[240]German Federal Constitutional Court First Senate Judgment of 15 December 1983 1 BvR 209, 269, 362, 420,440, 484/83 (Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html Accessed 19.09.2020)

impossible.[241] That is, the right to self-determination has a value not only for an individual but is also a core principle of any democratic society.[242]

The reality now is that policymakers and lawmakers are overwhelmingly encouraging transparency and disclosure of personal data, backing it up with the significance of the free flow of information and access to information. Such a tendency can most likely have a pernicious effect on the position of the right to personal data protection, and hence the right to self-determination, in the system of generic values.[243]

By collecting, processing, profiling, storing personal data, public and private parties make decisions about the data subject on the basis of the available information about the individual. It makes the individual's right to determine his personhood and behavior meaningless since his digital personality has already been built by various actors who have access to personal information pertaining to a concerned individual without the participation of the data subject himself.[244]

Some authors, even before securing the right to protect personal data as a fundamental right, were highly concerned about it and anticipated the threats that such recognition could entail. In the era of "possessive individualism", if the right to the protection of personal data is recognized as an independent value, then data subjects will not hesitate to commodify personal information and immediately receive remuneration for its disclosure and use.[245]

When the right to the protection of personal data acts as a tool for ensuring and achieving personal autonomy from outside influence and interference, the person is not endowed with the right to dispose or alienate his right. Such exploitation of the right to the protection of personal data as an intermediate tool intended to guarantee the right to self-determination that has a higher value both for an individual and for society as a whole.[246]

However, it must be noted that the right to informational self-determination is not limited to personal data as such, but it consists of exercising control of the data subject over personal

[241] Antoinette - Poullet 2009, pg. 47
[242] Schwartz 2004, pg. 2086-2088
[243] Antoinette – Poullet 2009, pg. 49
[244] Antoinette - Poullet 2009, pg. 68-69
[245] Antoinette - Poullet 2009, pg. 50
[246] Antoinette - Poullet 2009, pg. 50

information when it accordingly shapes his life.[247] The GDPR as its main goal set the empowering the position of the data subject through exercising control over personal data. That is, the Regulation provides the data subject with the real possibility for self-determination and self-management of his data.

The right to self-determination and the right to personal data protection have the vital goal of limiting the actions of public and private parties to collect, process, use personal data. In the era of an exponential development of information technology, otherwise would create a threat to exert strong pressure on individuals to refrain from actions, decisions that, being known to everyone, could harm their personal interests. It is particularly relevant for instances when the collection or processing of discreditable or shaming information is carried out, which the data subject would prefer to keep secret.[248] It is for these reasons the Regulation also enshrines provisions on a special category of information[249], for example, about race, religious or political beliefs, sexual orientation, which may become the basis for subsequent discrimination.

The main threat for an individual is not simply about data disclosure, but that the collection and combination of various information about one data subject may jeopardize the exercise of other rights of the data subject (right to privacy, non-discrimination, equal treatment) .[250]

It is apparent that given the imbalance of power between the individuals and public and private entities, and the possibility of abuse of that power, the simple acknowledgment of the right to self-determination and to personal data protection is insufficient. Therefore, despite the fact that the right to privacy (which was broadly interpreted encompassing the right to make free choices[251]) in the classical doctrinal sense imposes a negative obligation on the state to refrain from exercising any control over aspects of the life of individuals, the European Court of Human Rights expanded the state's obligation by imposing positive obligations on the state to take the necessary measures and decisions that will facilitate the right to privacy.[252]

But still the autonomy and self-determination of an individual cannot be regulated by laws. With the help of laws and regulations, it is possible to create only favorable conditions and

[247]Antoinette - Poullet 2009, pg.51
[248]Reiman 1976, pg. 40
[249]Article 9 GDPR
[250]Hildebrandt 2015, pg. 191-192
[251]X and Y v. Netherlands, 8978/80 (1985) ECHR, Beldjoudi v. France, 12084/86 (1992) ECHR
[252]Antoinette - Poullet 2009, pg. 66

opportunities for the individual, so that he can freely decide for himself what life he wants to live, what personhood he wants to develop.[253] And the Regulation creates such an environment in which these rights remain meaningful and enforceable.

The development of new technologies, new ways, and methods of collecting, processing, storing data sets new challenges for the autonomy and self-determination of the individual.[254] Therefore, the regulation of personal data protection, namely the General Data Protection Regulation, is designed to ensure the fundamental values of human dignity and his right to self-determination and self-development. Hence, interpretation, application, and enforcement of relevant legal provisions should be carried out in the light of these values.

As mentioned earlier, the right to self-determination, the right to exercise control over personal data, is of tremendous importance for a democratic society.[255] Ensuring the right to self-determination and control over personal data contributes to the free exercise and enjoyment by an individual of his rights and freedoms, for example, freedom of expression, freedom of organization. That is why it is impossible to transfer these rights and values to self-regulation for the individuals themselves, and especially for private enterprises, since these rights have value not only exclusively for the interests of an individual but are of great importance for the functioning and mere existence of democratic society and liberty.[256]

7.2 Consent as a mechanism of control

The GDPR pays great attention to the regulation of the consent of the data subject as the basis for the legitimacy of the personal data processing and as the mechanism of exercising control over personal data. The definition of consent is enshrined in Article 4 (11), which defines consent as:

> *... freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

[253] Reiman 1976, pg. 39
[254] Antoinette - Poullet 2009, pg. 68
[255] Solove 2004, pg. 57
[256] Antoinette - Poullet 2009, pg. 57

By definition, the processing of personal information will only be lawful if certain conditions are met. First, the consent must express the true and free will of the data subject, consent given under any coercion, deception, delusion is invalid. Secondly, the consent must be specific and informed, that is, the data subject must know for which specific one purpose of data processing he consents to. At the same time, the legislator emphasizes that each new purpose for processing requires a separate consent[257] accompanying every request for the consent with relevant information.[258] And the requirement of specific consent is one of the innovations of the GDPR in comparison with the previous Directive.[259] Finally, consent must be given through an endorsement act. The controller cannot use the default consent mechanism, or silence as consent, or the so-called opt-out.[260]

In addition to the requirements for valid consent, the legislator also obliges the controller to inform the data subject of his right to revoke a previously given consent.[261]

Though the actual control of the data subject is ensured not simply by the consent mechanism for the processing of personal data, but by the fact that the controller must obtain separate consent for each new purpose of data processing.[262] By agreeing once to the collection and processing of data, the data subject does not alienate the right to use his personal data, but only sanctions the processing of data for a specific and clear purpose, which has been determined by the controller. Any processing of data for a vague, ambiguous, amorphous purpose would automatically deprive the data subject of control since such manipulation would grant the controller substantial discretion in arbitrary processing of the data.

Also, a greater degree of control to the data subject grants the subject's right to information[263] about the controller's personality, purposes, and means of processing, information about other rights of the data subject, which must be provided by the controller himself. Such an obligation of the controller to provide the information is intended to make sure that the given consent is based on the informed decision of the data subject.

[257]Article 6(1a) GDPR
[258]Recital 3, Article 13 GDPR
[259]Article 2(h) Directive 95/46/EC
[260]Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, November 2017, pg. 15
[261]Article 14 (2d) GDPR
[262]Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017, pg. 11-12
[263]Brownswor 2009, pg. 85

7.3 Challenging efficiency of consent mechanism

As some proponents[264] of the proprietary regime claim recognition of property right over personal data will contribute to more responsible treatment of personal data by both data subjects and controllers, which will already achieve adequate protection of personal data. If the data subjects are convinced that they are the owners of their data, then the mechanism of simple consent to the collection and processing of data will be sufficient, since the data subject himself will take measures to better protect his data, giving his personal information a higher value as his property. So, the mechanism of already applied consent to the collection and processing of data is asserted to be sufficient.[265]

Proponents of the property regime to personal data protection see the proprietary control of data subjects over their personal data in the consent mechanism for data processing. However, the Regulation does not talk about the alienation of personal data after giving consent, there is not even a subtle hint of this in the Regulation. Firstly, even if the data subject has given his consent to the processing of his personal information, and it subsequently turns out that the controller has obviously collected excessive data that are not necessary for the purposes of the processing, such consent will be invalid, even if it was freely given by the subject data without pressure and coercion. Secondly, the legislator speaks of the right to revoke the consent previously given to data processing. Moreover, a special reservation has been made that there are no exceptions to this rule[266], the data subject reserves the right to withdraw consent to data processing at any time without any subsequent adverse consequences due to such a decision.

Also, the concept of incompatibility of the purpose of processing, which is utilized by the legislator, does not bring more certainty, but, on the contrary, gives a certain margin of appreciation for the controller of personal data. Many businesses collect personal user data for their networking, such information can be stored in the database for a long time, and this data can be used in the future by this business, which seems to be a compatible purpose, but nevertheless, data subjects may not be able to foresee or expect such a long term storage of his or her personal data.267

[264]Hildebrandt 2015, pg. 202
[265]Hildebrandt 2015, pg. 202
[266]Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017, pg. 29-30
[267]Hoeren, - Kolany-Raiser – Yankova - Hecheltjts 2013, pg. 67

Even though consent plays a meaningful role in the European data protection system, the legislator does not link the legitimacy of data collection and processing solely with the consent of the data subject. According to Article 6 of the Regulation, in order for the action of data processing to be lawful, the controller must comply with at least one of the conditions listed in this Article. That is, the controller is not always obliged to obtain the consent of the data subject to the processing of his data if he can justify the need for processing by other grounds, enshrined in Article 6.[268] And no legal act makes the obtaining of the consent of the data subject more preferable over all other grounds for the legal processing of personal data.[269]

In many cases, the controller will be able to justify the legitimacy of the processing of personal data on other grounds[270] enshrined in Article6(1) of the GDPR. The proponents of the property regime do not bring more clarity to how the owner of personal data can exercise his right where processing was carried out on legal grounds for processing personal data other than consent.

The general position of the policy and lawmakers is that data processing based solely on the consent of the data subject may have a detrimental effect on the data subject's own interests,[271] since the prevailing factor is the incompetence of the data subject in an adequate assessment of the risks of processing personal data pertaining to him, or the special position of the data subject, which prevents him from making a free and informed decision.

The main purpose of the consent tool is to exercise control over personal information by data subjects. However, this mechanism has many pitfalls and can hardly be considered an effective mechanism for retaining control over personal data in the hands of the data subjects themselves.

The current reality is that every person spends hours every single day surfing the Internet. It is very doubtful that each user will mindfully read the information regarding who processes personal data, what data, and for what purposes. Due to the endless notifications of the same type and requests for consent to processing operations, we have already managed to develop the habit of automatically ticking the box where it is required in order to further freely use wanted services and web pages.[272]

[268]Savin 2017, pg. 274
[269]Bygrave 2009, pg. 165-166
[270]Bygrave 2002, pg. 66
[271]Article 29 Working Party Guidelines on consent under Regulation 2016/679, 28 November 2017
[272]Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017, pg. 17

The introduction of the property right to personal data will make consent a preferable ground for personal data processing, and maybe even as a default rule. This will shift a great deal of responsibility onto the shoulders of the data subjects, which can be too burdensome, since the data subjects will have to keep the track of where, what data, for what purpose, to whom they give their consent for processing. And with dozens of different controllers handling our data on a daily basis, this would be cumbersome and too risky. One should seriously consider whether this universal mechanism is desirable for the data subjects themselves.

Some authors are convinced that obtaining consent from a data subject for the controller is a kind of routine work, satisfying the requirements for valid consent is not a big deal for those entities, therefore it is considered that there is no serious perception of the consent mechanism as a real control tool.[273]

Understanding this, many controllers may abuse users' negligence with their personal data, and request the collection of excessive and unnecessary data that can be used for purposes that were not mentioned in an initial request for the data collection and processing.[274] Under such circumstances, it is extremely difficult to talk about exercising any real control over the data.

Moreover, consent cannot solve the main problem in the relationship between data subjects and controllers, namely the asymmetry of power. In any case, it will be difficult for the data subject to control the compliance of the third actors (for example, another controller, processor) with the agreement that was concluded with the original controller.[275]

That is why the legislator ensures that control over personal data is retained[276] even after giving consent for data processing through the data subject's right to withdraw consent to the processing of personal information.[277] The control is retained also by a number of rights enshrined in the Regulation, namely the right to require the controller to restrict processing or to delete the stored data, right to rectification or completion of data, and also principles of the GDPR plays the core role in correcting the imbalance of power. And none of these rights can be waived by the agreement.[278]

[273]Brownswor 2009, pg. 87
[274]Savin 2017, pg. 274
[275]Antoinette - Poullet 2009, pg. 73-74
[276]Jacob M. Victor 2013-2014, pg. 524
[277]Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017, pg. 5
[278]Jacob M. Victor 2013-2014, pg. 524

Another problem with the effectiveness and vulnerability of consent as a legal basis for personal data processing is mentioned in the text of the Regulation itself, in Recital 43, the legislator foresaw frequent cases when the data subject is in a dependent position when obtaining consent cannot be considered valid due to the actual lack of freedom of choice. For such legal entities, when there is an obvious inconsistency of power, the consent of the data subject to the processing of personal information is not a lawful basis for processing. In these cases, the controller must be guided by other legal grounds for processing personal data.[279] The legislator has prevented in advance the adverse consequences of the absolute validity of consent and absolute control of data subjects over personal information.

For instance, in labor relations, when an employee must give his consent to the collection and processing of his personal data, then the mechanism of consent as control is quite meaningless and it fails its task of free and independent expression of the will of the data subject. It is apparent that when the employer confronts the fact of the need to process the data of his subordinates, de facto employees are excluded from any freedom of decision, they simply have no choice[280], since disagreement can cause unfavorable consequences for the employee.[281]

In many cases, even if the controller has received the consent of the data subject to process the data, this is not a guarantee that the processing was carried out on a legitimate basis, because the moment of deception, coercion is omnipresent. And in some cases, consent as the basis for the processing of personal data is not recommended at all due to the contextual specifics, such as the transfer of personal data outside the EU or dependent position of the data subject.[282]

Thus, the legislator deliberately limits the universality of consent as a basis for the processing of personal information, as otherwise could have pernicious consequences for the interests of data subjects, and as was stated in the previous paragraph, for the interests of the society as well.

Interestingly, Mireille singles out the European approach to balancing the disparity of powers, as she calls it the *"EU-style data protection"* approach, as distinct from the approach of vesting

[279]Article 29 Working Party Guidelines on consent under Regulation 2016/679, 28 November 2017, pg. 6
[280]Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017, pg. 5
[281]Hoeren – Kolany-Raiser – Yankova - Hecheltjen 2013, pg. 83
[282]Kuner 2007, pg. 211

property rights with data subjects. And here, as the root of the European approach, she notes the principles enshrined in personal data protection regulations. And as the main advantage of the European approach, Mireille notes the ability of the European approach to deal with the problems and challenges imposed by modern technologies and the threats that they entail.[283]

7.4 Does property regime fit in General Data Protection Regulation?

The imperfection of the consent mechanism is not the only argument testing the claimed effectiveness of the property regime. First of all, the property regime imposes negative obligations on all third parties not to interfere with the owner's right to dispose of and use his property. While the right to the protection of personal data in accordance with both the Charter of Fundamental Rights and the GDPR establishes positive rights and obligations.

The relationship between the controller and the data subject is clearly and in detail regulated by law, leaving almost no freedom to negotiate on the terms and conditions of the contract. The Regulation does not allow the parties to negotiate deviations from its provisions.

In contrast to the Directive, the GDPR explicitly stands up for the weaker side, that is, given the imbalance of power and information in controlling dissemination and use of personal data. That is why the provisions of the Regulation and its general principles are imperative and have direct application and binding effect, and the level of protection of personal data, established by the Regulation, is mandatory for all controllers, processors dealing with the processing and other use of data. Therefore, the GDPR does not leave the freedom either to the data subject or the controller to bargain and conclude contracts for the collection, use, transfer of personal data.

Given the fact that the GDPR establishes a minimum framework regulation, minimum standards for the protection of personal data across the EU, the parties cannot agree, for example, on "softening" the controller's obligations and responsibility. The regulation also addresses the issue of what data can be processed by enforcing the principle of minimization which will not allow the controller to collect and process excessive information even if the data subject is willing to give his consent to the excessive collection.[284]

[283]Hildebrandt 2015, pg. 201
[284]JRC Digital Economy Working Paper 2017-01, The economics of ownership, access and trade in digital data, 2017, pg. 16

Data processing with the consent of the data subject is indisputably the cornerstone of the Regulation and the European approach to the protection of personal data. Nevertheless, despite the fact that policymakers and lawmakers pin great hopes on this control mechanism, believing that this is the main tool for exercising real control over personal data, in reality, the situation is quite opposite.

Unfortunately, the consent tool has many shortcomings, and this mechanism is easily manipulated by controllers, who actually establish and impose their own conditions for the collection, processing, and storage of personal data, leaving no real freedom of choice for the data subject.

The GDPR does not prohibit the processing of personal data without the assent of the data subject, it is not assumed that the processing of data depends exclusively on the decision and will of the subject himself. But the Regulation enshrines provisions that ensure fair data processing and other use that respects the rights and freedoms of the individual as promised by the Union. Not only the data subject cares about his interests and freedoms, but the provisions of the Regulation are aimed at using the most effective mechanisms for the implementation of these interests.

The great complexity of the relationship for the processing of personal data is the imbalance of power, which cannot be resolved by the consent mechanism alone. That is why the legislator did not limit himself to the consent mechanism, realizing that this tool is not enough, equipping the data subject with other rights, enhancing the accountability of the controllers, encouraging the incentives to develop and employ privacy-enhancing technologies, ensuring effective judicial and administrative rules that can in conjunction balance the position of the data subject and the controller.

And none of the data subject's rights enshrined in the provisions of the GDPR for his empowerment can be considered as a property right.[285] But still under the terms of the Regulation, there is no doubt that the interests of the data subject prevail over the interests of the controller. The introduction of ownership of personal data will not bring anything new in this aspect. The burden of proof of the overriding interest of the controller itself lies with the

[285]Jacob M. Victor 2013-2014, pg. 522

controller itself[286]. Thus, Regulation as a default rule already puts the dominance of the subject's interests over the interests of the controller.

The implementation of the property regime is also not able to solve the problem of already collected, stored personal data before the introduction property right to personal data. Whereas the general principles of the GDPR solve these issues through the principle of data minimization and storage limitations that is applicable to any personal data inclusive data collected before the GDPR came to force and application.

The Regulation has become a useful reform in the protection of personal data, which universally applies to any actor that processes personal data, namely controllers and processorss. The GDPR appears to be a promising tool for solving new challenges posed by the development of communication and information technologies, and new business models.[287] Unlike its predecessor, the 1995 Directive, the Regulation enshrines strong accountability and responsibility rules of controllers for the processing of personal data that does not comply with general principles for data processing.

The GDPR also perfectly reflects the European approach to the protection of personal data as a fundamental right, securing additional guarantees to protect the interests of data subjects from the bad faith of controllers. Expansion of the rights of data subjects, which cannot be circumvented by the provisions of the agreement, significantly strengthens the position of the data subject, giving him greater control over the operations carried out with information pertaining to him. This human-centered approach does not completely, but to some extent corrects the imbalance of power in the concerned relationship, where the data subject is obviously the weaker and incompetent party.

7.5 Is property regime solving intricacies of data protection in the EU?

The exponential advancement of technology only exacerbates the asymmetry of power between controllers and data subjects.[288] Modern information technology allows the storage and collection of an unlimited amount of data. And the growing importance and attractiveness of

[286]Article 21(1) GDPR
[287]Ritter 2017-2018, pg. 249
[288]Antoinette - Poullet 2009, pg. 68

the information market are pushing controllers to endlessly invent new goals for collecting and processing data.[289]

In a utilitarian society, it is worth doubly weighing the pros and cons of creating a new property, and assessing how the owners will wish to dispose of their property. And would not such right and its enjoyment jeopardize other values?

In the case of databases, the legislation explicitly recognizes the property right of enterprises in the created databases in order to justify their large investment in data compilation.[290] The compilation of personal data of thousands users has a high economic value, and it is considered to be a valuable business asset. Here the economic interest of creators in their creations – databases – is completely justified.

In the case of protecting the personal data of the user/data subject himself, this fundamental right does not serve any economic purpose, it is aimed at the implementation of other interests.

The proposal to regulate the property right over personal data, similar to the intellectual property regime, lacks sufficient argumentation. When some authors[291] suggest using the logic of an intellectual property law regime, where property rights are also somewhat limited, it should be understood that the holders of the intellectual property rights have an economic interest in exploiting their rights, as a result of which the whole society will benefit.

That is, the legislator deliberately vested property right in the results of intellectual activity with the inventor in order, firstly, to reimburse those intellectual, creative investments of the creator, and, secondly, to encourage the creator to disclose the results of his work, which have a huge contribution to the creative, scientific development of society in general.

The mentioned examples of a special property regime for certain categories of property, such pursue the goal of protecting the economic interests of the owner.

[289]Nissenbaum 1998, pg. 576
[290]The Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
[291]Samuelson 2000

Talking about personal data, there is no such goal as encouraging the disclosure or dissemination of information, on the contrary, the protection of personal data is aimed at preventing excessive and unnecessary collection and processing of personal information. It is particularly crucial when it comes to the role of data control in the exercise of the right to privacy, the right to self-determination, right not to be the subject of discrimination. In that context, it is difficult to argue about the protection of personal data for the sake of the property interests of the data subject.[292]

It is a controversial argument that the recognition of property rights in personal data will affect data subjects' perception of the importance of personal information, and will contribute to encouraging data subjects to exercise effective and meaningful control over personal data. As an example, each user of various digital services indicates that data subjects do not accord much value to their personal data, providing it freely to dozens of social networks, viewed by thousands of other users.[293]

The right to personal data protection means the protection of personal data from unauthorized disclosure and use of personal data. In no way does any of the legal acts speak of the protection of personal data as protecting the proprietary or economic interests of the subjects of personal data in the use or disclosure of personal information pertaining to them.

Moreover, if the protection of personal data were carried out under a property regime, then the data subject would be deprived of the help of the competent authorities in defending their interests. The burden of discovering the misuse of personal data concerning him would lay on the data subject, that in the context of the imbalance of power and information would have been virtually impossible.

Moreover, the application of the property regime for the protection of personal data will nullify all the efforts of the legislator to achieve harmonized regulation. The GDPR is a framework act, which, nevertheless, establishes a fairly detailed and defined standard and level of protection. While the property right is left to the discretion of the national laws of the Member States, and each government can adapt property law to the peculiarities of its economic and social policies. This means that with the transition to a property regime for regulating the rights to personal

[292]Corien Prins 2006, pg. 226
[293]Lazaro - Le Métayer 2015, pg. 5

data, the EU will have an extremely fragmented regulation, which will inevitably lead to the disruption of the single market. At the moment, thousands of services are provided in digital format, online, so the GDPR is of invaluable practical importance for the new online market. While in America the goal of harmonization of regulation of certain relations is not set before the legislation, the EU has long adhered to the goal of harmonization in various aspects, and the property approach can in no way become an instrument for achieving the goals of harmonization.

And lastly, if the data subject has property right to personal data, then he has the right to give them his own assessment of the value. Thus, the right to protection of personal data under the property regime will have different values depending on the socio-economic status of the data subject as was warned by Schwartz.

The main problem with personal data protection boils down to the failure of the market to cope with the task of disciplining businesses to refrain from unauthorized use of personal data and ensure transparent and fair use of personal data.[294] And the property right regime does not offer any solutions to intricacies of efficient personal data protection that the actors and the market itself cannot cope with. So, the question of how the property regime in personal data will contribute to a better regulatory solution remains open.

The right to protection of personal data is not so much about the right of the data subject not to disclose information about himself or bargain on the terms of such disclosure. The right to the protection of personal data ensures the transparency of any operations performed with the use of personal data so that the data subject knows that his information is being processed for purposes known to him. And the GDPR has done a good work to ensure that transparency.

7.6 Conclusion

Before deciding on the need to apply a new approach to regulation and protection of the right, it is necessary to assess the existing mechanisms, their effectiveness in achieving the set goals.

The European legal system takes a fundamental approach to the protection of personal data. Information privacy and the right to the protection of personal data are vital for the realization

[294]Corien Prins 2006, pg. 231

of self-determination and self-development of individuals, for the right of an individual to build and shape his own life and personality without pressure and fear. This right is essential not only for the individual but also for society as a whole. The right to personal data protection not only boils down to data control but also has an important role in protecting and exercising other fundamental rights.

For these reasons, transferring the protection of personal data primarily to self-regulation and own discretion is risky for the freedom of the individual himself.

While proponents of the property regime believe that property regime itself guarantees greater respect for the protection of personal data by both the data subject and the controller, the consent tool has many flaws to rely on as the primary control mechanism. Therefore, the legislator does not link the legitimacy of data processing solely to the compliance with the consent requirement and does not give this ground priority over others.

The property regime is difficult to apply in the context of the GDPR, which does not leave the freedom to negotiate derogations from its rules. The GDPR also does not grant the data subject's rights to bargain with his data or the right to use it. The regulation sets out minimum standards for the protection of personal data, and no departure from this level is permissible on any grounds. The aim of the legislator was not to provide freedom to use their data at their discretion but to ensure fair data processing by tackling the imbalance of power between the controller and the data subject, who was previously deprived of meaningful control over personal information.

The goal of EU in reaching the harmonized regulation across Member States and ensure smooth functioning of the single market cannot be achieved by property right regime because property law left to the discretion of national legislators.

The protection of personal data can in no sense pursue the economic or property interests of the data subject. Otherwise, it would inevitably lead to the commodification of the personal data, as is the case with intellectual property rights or databases. And that is an undesirable implication for the interests of the data subject.

Therefore, the Regulation is a good attempt to ensure the effective protection of personal data, guided by the value of human integrity and autonomy. While it is not without its shortcomings,

some effort must be made to address the unresolved issues with harmonization and implementation of all available empowerment mechanisms by the data subjects. The Regulation takes the right track in achieving the autonomy and independence of data subjects from powerful controllers.

8 Conclusion

The theory of proportization of personal data emerged against the backdrop of the shortcomings of the American legal system, which was unable to provide adequate protection of the interests of data subjects against the interests of private companies that abuse their influence and power in the unauthorized and unfair use of users' personal data. The tort system has partial application and has no preventive action, and the law on personal data protection is highly fragmented and has limited application. Therefore, American legal scholars, understanding the corruption of the legislative system, trying to avoid the biased legislating process have found an alternative in using the existing regimes for the protection of rights to new relationships. Although, it should be noted that the drafted Code of Fair Information Practice, and most importantly, the principles of fair processing of personal data enshrined in this code, had great potential in solving problems posed by modern technologies.

In the European context, this proportization tool does not make as much sense as in the American system. The new Regulation that has a direct binding effect on all controllers and processors of personal data, replacing the 1995 Directive, enshrines the fundamental principles that were also emphasized by the Code of Fair Information Practice.

Moreover, the American legal system does not aim to harmonize regulation between states, that is why the property regime for personal data can be considered as an appropriate tool for the American system. Meanwhile, Regulation has taken significant steps to achieve harmonization in the EU, and property law being in the competence of the national legislators does not match the goals of the EU.

Moreover, the property right protects conventionally protects the economic interests of the owner. The right to personal data protection is not intended to satisfy the economic interests of the parties. The protection of personal data is a mandatory factor in the implementation of other fundamental human rights that ensure the autonomy and integrity of the individual. Guided by this value, the legislator enshrines the principles of highly restrictive controllers' actions and provides strong protection for the weak and incompetent position of the data subject.

New rights of data subjects enshrined in the Regulation, rules of accountability and responsibility of controllers and processors, especially established by the authorities for the

protection of personal data, all of these tools are aimed at strengthening data subjects and keeping them in control of personal information.

The property regime has nothing to offer the European legal order since the gaps existing in the previous acts were mostly filled with the provisions of the new Regulation. The goals of harmonization and greater respect for the individual's autonomy and self-integrity are hard to achieve by the property right approach. In the context of European law, the property regime poses more threats to the effective protection of personal data than it has a positive impact. Steps taken towards the commodification of personal data can jeopardize the right to autonomy of individuals, and, accordingly, the existence of a democratic society.

Bibliography

Books

– Akkermans Bram, The principle of numerus clausus in European property law, Maastricht University, 2008

– Andrej Savin, EU Internet Law, Elgar European Law Series, 2017

– Bygrave Lee Data Protection Law: Approaching Its Rationale, Logic and Limits, Information Law Series: Kluwer Law International, 2002

– Cate, Fred H. , Privacy In The Information Age , Brookings Institution Press, 1997

– Hildebrandt Mireille, Smart Technologies and the End(s) of Law, Edward Elgar Publishing, 2015

– Hoeren Thomas, Barbara Kolany-Raiser, Silviya Yankova, Martin Hecheltjen, Legal Aspects of Digital Preservation, Edward Elgar Publishing, 2013

– Kuner, European Data Protection Law: Corporate Compliance and Regulation., Oxford University Press; 2nd edition, 2007

– Purtova Nadezda, Property rights in personal data: Learning from the American discourse, Tilburg Institute for Law, Technology, and Society, The Netherlands, 2009

– Purtova Nadezda, Property rights in personal data: A European perspective, Oisterwijk: BOXPress BV., 2011

– Ramaekers E., European Union Property Law from Fragments to a System (Intersentia 2013)

– Regan, Legislating Privacy: Technology, Social Values, and Public Policy, The University of North Carolina Press, 1995

– Schwartz Paul, Reidenberg Joel, Data Privacy Law: A study of United States Data Protection, Charlottesville, Virginia: MICHIE Law Publishers, 1996

– Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt, Reinventing Data Protection?

– van Erp S, From 'Classical' to Modern European Property Law? Maastricht University, 2009

– van Erp S and B Akkermans, Cases, Materials and Text on Property Law: Ius Commune Casebooks for the Common Law of Europe, 1st ed., Hart Publishing, 2012

– van Erp S, Salomons Arthus, Akkermans Bram, The Future of European Property Law, Sellier European Law, 2012

– Westin Alan, Privacy and Freedom, Athenum, 1967

Articles

– Basho Kalinda, 'The Licensing of the personal information. Is that a solution to Internet Privacy?', 88 California Law Rev., 2000, pp. 1507-1546

– Bergelson Vera, It's Personal but Is It Mine - Toward Property Rights in Personal Information, 37 U.C. Davis L. Rev. 379, 2003, pp. 379-451

– Bezan Randall, The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990, California Law Review Vol 80, 1992, pp. 1133-1176

– Brian E. Butler, "Legal Pragmatism: Banal or Beneficial as a Jurisprudential Position? Essays in Philosophy Vol 3 Issue 2, Pragmatism and Neopragmatism, 2002

– Brownswor Rogerd, Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality (in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt, Reinventing Data Protection?), Springer, 2009, pp. 83-110

– Cohen Julie, Examined Lives: Informational Privacy and the Subject as Object, Stanford Law Review, Vol 52, No 5, 2000, pp. 1373-1437

– Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, Kluwer Law International, 2006, pp. 223-257

– Fenrich William, Common Law Protection of Individuals' Rights in Personal Information, Fordham Law Review 951, Vol 65, Issue 3, 1996, pp. 951-1003

– Gavison Ruth, Privacy and the Limits of Law, The Yale Law JournalVolume 89, Number 3, January 1980, pp. 421-471

– Hansmann Henry & Reinier Kraakman, Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights, *The Journal of Legal Studies,* Vol 31, No S2, 2002, S373-S421

– Jacob M. Victor, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy 123 Yale L. J. 513 2013-2014., pp. 513-528

– Janger Edward J, Privacy Property, Information Costs, and the Anticommons, 54 H ASTINGS Law Journal, 2003, pp. 899-929

– Kang Jerry, Information Privacy in Cyberspace Transactions, Stanford Law Review, Vol 50, 1998, pp. 1193-1294

– Laudon, Kenneth, Markets and Privacy; Privacy Regulation in National Networks, Association for Computing Machinery. Communications of the ACM, Sept. 1996, pp. 92-104

– Lazaro Christophe & Daniel Le Metayer, Control over personal data: Trues Remedy or Fairy Tale? Volume 12, Issue 1, June 2015

– Litman Jessica, Information Privacy/Information Property, Stanford Law Review 52, 2000, pp. 1283-1313

– Lund, Jamie, Property Rights to Information, Northwestern Journal of Technology and Intellectual Property, Vol 10, 2011

– Mireille Hildebrandt, Defining Profiling: A New Type of Knowledge? Springer, 2008, pp.17-45

– Murphy Richard, Property rights in personal information: An economic defense of privacy, Georgetown Law Journal, Vol 84, No 7, 1996, pp. 2381-2417

– Newman Daniel, European Union and United States Personal Information Privacy, and Human Rights Philosopthy – Is There a Match? 22 Temp. Int'l & Comp. L.J. 307 2008, pp. 307-343

– Nissenbaum H., Protecting Privacy in a Information Age: the Problem of Privacy in Public,17 Law and Phil., 1998, pp. 559-596

– Posner Richard, The Right of Privacy, Georgia Law Review Vol. 12, No. 3, 1978, pp. 393-422

– Purtova Nadezda, Prpoperty in personal data: a European perspective on the instrumentalist theory of propertisation, European Journal of Legal Studies Vol.2 No.3, 2010

– Purtova Nadezda, Do property rights in personal data make sense after the Big Data turn? Individual control and transparency, Tilburg Law School Research Paper No. 2017/21, 2017

– Reidenberg Joel, Privacy Wrongs in Search of Remedies, 54 H ASTINGS L.J. 877 (2003), pp. 877-898

– Reiman Jeffrey, Privacy, Intimacy, and Personhood, Philosophy and Public Affairs, Vol. 6, No. 1, 1976, pp. 26-44

– Ritter Jeffrey, Mayer Anna, regulating data as property: A new construct for moving forward, Duke Law & Technology Review 16, 2017-2018, pp. 220-277

– Robinson Neil, Graux Hans, Botterman Maarten, Valeri,Lorenzo Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office, RAND, 2009

– Rouvroy Antoinette and Yves Poullet, The Right to Informational Self-Determination and the Value of Self-Development, Springer, 2009 (in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt, Reinventing Data Protection?), pp. 45- 76

– Samuelson Pamela, Privacy as Intellectual Property, 52 Stanford Law Review 1125 (2000)

– Schwartz Paul, Property, Privacy, and Personal Data, Harward Law Review, Vol 117, No 7, 2004, pp. 2055-2128

– Solove Daniel, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393, 2001, pp. 1393-1462

– Solove Daniel, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002), pp. 1087-1156

– Stefano Rodota, Data Protection as a Fundamental Right, Springer, 2009 (in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt, Reinventing Data Protection?), pp. 77-82

– van Erp, A Numerus Quasi-Clausus of Property Rights as a Constitutive Element of a Future European Property Law?, 2003, (Available at **https://www.ejcl.org/72/art72-2.PDF**)

– Warren Samuel; Louis D. Brandeis “The Right to Privacy” Harvard Law Review, Vol. 4, No. 5., 1890, pp. 193- 220

– Whitman James, The Two Western Cultures of Privacy: Dignity Versus Liberty, Yale Law Journal 113, 2004, pp. 1151-1221

Official materials

– Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data, Adopted on 20th June

– Article 29 Working PartyGuidelines on consent under Regulation 2016/679, 28 November 2017

– EUROPEAN UNION CONSOLIDATED VERSIONS OF THE TREATY ON EUROPEAN UNION AND OF THE TREATY ESTABLISHING THE EUROPEAN COMMUNITY (2002) (2002/C 325/01)

– Communication from the Commission to the European Parliament, the Council, the Economic an Social Committee and the Committee of the regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010 COM(2010) 609 final

– Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), 2007

– Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition -two years of application of the General Data Protection Regulation, Brussels, 2020 COM(2020) 264 final

– JRC Digital Economy Working Paper 2017-01, The economics of ownership, access and trade in digital data, 2017

Case Law

– CJEU Case C-128/11 UsedSoft GmbH v Oracle International Corp (2012)

– Dwyer v. American Express Co. 652 N.E.2d 1351 (1995)

– Katz v. United States, 389 U.S. 347, 351 (1967)

– Smith v. Maryland, 442 U.S. 735 (1979)

– De Wilde, Ooms, Verspy/Belgium ECHR 18 June 1971

– Deweer/Belgium ECHR 27 February 1980

– German Federal Constitutional Court First Senate Judgment of 15 December 1983 1 BvR 209, 269, 362, 420, 440, 484/83

– X and Y v. Netherlands, 8978/80 (1985) ECHR,

– Beldjoudi v. France, 12084/86 (1992) ECHR